XVIII.

Theorie der algebraischen Funktionen einer Veränderlichen.

[In Gemeinschaft mit Heinrich Weber veröffentlicht im Journal für reine und angewandte Mathematik, Bd. 92, S. 181—290, 1882 (datiert Oktober 1880).]

Einleitung.

Die im nachstehenden mitgeteilten Untersuchungen verfolgen den Zweck, die Theorie der algebraischen Funktionen einer Veränderlichen, welche eines der Hauptergebnisse der Riemannschen Schöpfung ist, von einem einfachen und zugleich strengen und völlig allgemeinen Gesichtspunkt aus zu begründen. Bei den bisherigen Untersuchungen über diesen Gegenstand werden in der Regel gewisse beschränkende Voraussetzungen über die Singularitäten der betrachteten Funktionen gemacht, und die sogenannten Ausnahmefälle entweder als Grenzfälle beiläufig erwähnt oder auch ganz beiseite gesetzt. Ebenso werden gewisse Grundsätze über die Stetigkeit und Entwickelbarkeit zugelassen, deren Evidenz sich auf geometrische Anschauung verschiedener Art stützt. Eine sichere Basis für die Grundvorstellungen sowie für eine allgemeine und ausnahmslose Behandlung der Theorie läßt sich gewinnen, wenn man von einer Verallgemeinerung der Theorie der rationalen Funktionen einer Veränderlichen, insbesondere des Satzes, daß jede ganze rationale Funktion einer Veränderlichen sich in lineare Faktoren zerlegen läßt, ausgeht. Diese Verallgemeinerung ist einfach und bekannt in dem ersten Falle, in welchem die von Riemann mit p bezeichnete Zahl (das Geschlecht nach Clebsch) den Wert Null hat. Für den allgemeinen Fall, welcher sich zu dem eben genannten ähnlich verhält, wie der Fall der allgemeinsten algebraischen Zahlen zu demjenigen der rationalen Zahlen, wiesen die mit bestem Erfolge in der Zahlentheorie angewandten Methoden, die sich an **Kummers** Schöpfung der idealen Zahlen anschließen, und der Übertragung auf die Theorie der Funktionen fähig sind, auf den richtigen Weg*).

Versteht man, analog der Zahlentheorie, unter einem **Körper algebraischer Funktionen** ein System solcher Funktionen von der Beschaffenheit, daß die Anwendung der vier Spezies auf Funktionen des Systems immer zu Funktionen desselben Systems führt, so deckt sich dieser Begriff vollständig mit dem der **Riemannschen** Klasse algebraischer Funktionen. Unter den Funktionen eines solchen Körpers kann eine beliebige als unabhängige Veränderliche und die übrigen als von ihr abhängig betrachtet werden. Für jede dieser „Darstellungsweisen" ergibt sich ein System von Funktionen des Körpers, die als **ganze Funktionen** zu bezeichnen sind, deren Quotienten den ganzen Körper erschöpfen. Unter diesen ganzen Funktionen lassen sich nun wieder Gruppen von Funktionen aussondern, welchen die charakteristischen Merkmale solcher ganzen rationalen Funktionen zukommen, die einen gemeinschaftlichen Teiler haben. Ein solcher Teiler existiert zwar im allgemeinen Falle nicht, wenn man aber die bezüglichen Sätze über rationale Funktionen nicht an den Teiler selbst, sondern an das System der durch denselben teilbaren Funktionen knüpft, so gestatten sie eine vollkommene Übertragung auf die allgemeinen algebraischen Funktionen. Auf diese Weise gelangt man zu dem Begriff des **Ideals**, ein Name, der aus **Kummers** zahlentheoretischen Arbeiten stammt, wo die nicht existierenden Teiler als „ideale Teiler" in die Rechnung eingeführt werden.

Obwohl es sich in der vorliegenden Arbeit keineswegs um „ideale" Funktionen handelt, sondern alle Operationen nur an Systemen wirklich existierender Funktionen ausgeführt werden, schien es doch zweck-

---

*) Die idealen Zahlen sind von **Kummer** zuerst eingeführt durch die Abhandlung: **Zur Theorie der komplexen Zahlen** (**Crelles** Journal, Bd. 35); eine weitere Fortführung und eine allgemeine Darstellung der Theorie der algebraischen Zahlen findet man in der zweiten und dritten Auflage von **Dirichlets** Vorlesungen über Zahlentheorie, sowie in der Abhandlung von **Dedekind**: **Sur la théorie des nombres entiers algébriques** (Paris 1877. Abdruck aus dem Bulletin des Sciences math. et astron. von **Darboux** und **Hoüel**). Die Kenntnis dieser Schriften wird aber in unserer Arbeit nirgends vorausgesetzt.

Aus mündlichen Mitteilungen ist uns jetzt bekannt geworden, daß bereits vor Jahren **Kronecker** mit Beziehung auf die Arbeiten von **Weierstraß** Untersuchungen angestellt hat, die auf derselben Grundlage, wie die unsrigen, beruhen.

mäßig, den Namen „Ideal", der in der Zahlentheorie bereits gebräuchlich ist, beizubehalten.

Mit diesen Idealen läßt sich nach gehöriger Erklärung der Multiplikation ganz nach denselben Regeln rechnen, wie mit rationalen Funktionen. Insbesondere ergibt sich der Satz, daß jedes Ideal auf eine einzige Weise in Faktoren zerlegbar ist, welche selbst nicht weiter zerlegt werden können und daher Primideale genannt werden. Diese Primideale entsprechen den linearen Faktoren in der Theorie der ganzen rationalen Funktionen. Auf Grund derselben gelangt man zu einer völlig präzisen und allgemeinen Definition des „Punktes der Riemannschen Fläche", d. h. eines vollkommen bestimmten Systems von Zahlwerten, welche man den Funktionen des Körpers widerspruchslos beilegen kann.

Eine darauf gegründete formale Definition des Differentialquotienten führt sodann zu der Geschlechtszahl und zu einer ganz allgemeinen, eleganten Darstellung der Differentiale erster Gattung. Hieran schließt sich der Beweis des Riemann-Rochschen Satzes über die Anzahl der willkürlichen Konstanten in einer durch ihre Unendlichkeitspunkte bestimmten Funktion, und die Theorie der Differentiale zweiter und dritter Gattung. Bis zu diesem Punkte kommt die Stetigkeit und Entwickelbarkeit der untersuchten Funktionen in keiner Weise in Betracht. Es würde z. B. nirgends eine Lücke bleiben, wenn man das Gebiet der benutzten Zahlen auf das System der algebraischen Zahlen beschränken wollte. Dadurch wird ein wohl abgegrenzter und ziemlich umfassender Teil der Theorie der algebraischen Funktionen lediglich durch die seiner eigenen Sphäre angehörigen Mittel behandelt.

Freilich ergeben sich alle diese Resultate durch einen weit geringeren Aufwand von Mitteln und als Spezialfälle einer vielumfassenden Allgemeinheit aus Riemanns Theorie; allein es ist bekannt, daß diese Theorie bezüglich einer strengen Begründung noch gewisse Schwierigkeiten bietet, und bis es gelungen ist, diese Schwierigkeiten vollständig zu überwinden, dürfte der von uns betretene Weg oder wenigstens ein verwandter, wohl der einzige sein, der für die Thorie der algebraischen Funktionen mit befriedigender Strenge und Allgemeinheit zum Ziele führt. So würde sich die Theorie der Ideale selbst außerordentlich vereinfachen, wenn man den Begriff der Riemannschen Fläche und insbesondere den eines

Punktes derselben samt den auf die Stetigkeit der algebraischen Funktionen gegründeten Anschauungen voraussetzen wollte. In unserer Arbeit ist umgekehrt auf einem langen Umwege die Theorie der Ideale algebraisch begründet und aus dieser eine vollkommen präzise und strenge Definition des „Punktes der Riemannschen Fläche" gewonnen, welche auch als Basis für die Untersuchung der Stetigkeit und der damit zusammenhängenden Fragen dienen kann. Diese Fragen, wozu auch die auf die Abelschen Integrale und die Periodizitätsmoduln bezüglichen gehören, bleiben von unserer Untersuchung einstweilen ausgeschlossen. Wir hoffen bei einer anderen Gelegenheit darauf zurückzukommen.

Königsberg, den 22. Oktober 1880.

I. Abteilung.

§ 1.

Körper algebraischer Funktionen.

Eine Variable θ heißt eine algebraische Funktion einer unabhängigen Veränderlichen z, wenn dieselbe einer irreduktibeln algebraischen Gleichung

$$F(\theta, z) = 0 \tag{1}$$

genügt. F bedeutet hierin einen Ausdruck von der Form

$$F(\theta, z) = a_0 \theta^n + a_1 \theta^{n-1} + \cdots + a_{n-1} \theta + a_n,$$

worin die Koeffizienten $a_0, a_1, \cdots a_n$ ganze rationale Funktionen von z ohne gemeinschaftlichen Teiler sind. Die vorausgesetzte Irreduktibilität der Gleichung (1) involviert, daß θ nicht einer Gleichung niedrigeren Grades in bezug auf θ genügt, und, wie sich aus dem Algorithmus des größten gemeinschaflichen Teilers ergibt, wenn

$$G(\theta, z) = b_0 \theta^m + b_1 \theta^{m-1} + \cdots + b_{m-1} \theta + b_m = 0$$

eine zweite Gleichung ist, welcher θ genügt, daß $G(\theta, z)$ durch $F(\theta, z)$ algebraisch teilbar sein muß. Es läßt sich nun nachweisen, daß $G(\theta, z)$ auch in bezug auf z nicht von niedrigerem Grade sein kann als $F(\theta, z)$ und nur dann vom selben Grade, wenn sich aus $G(\theta, z)$ ein von z unabhängiger Faktor absondern läßt. Nehmen wir an, die Koeffizienten $b_0, b_1, \cdots b_m$ seien von gemeinschaftlichen Faktoren befreit, und bezeichnen wir mit

$$H(\theta, z) = c_0 \theta^{m-n} + c_1 \theta^{m-n-1} + \cdots + c_{m-n}$$

den vom Nenner befreiten Quotienten von G durch F, so ist

$$kG(\theta, z) = F(\theta, z) \cdot H(\theta, z),$$

worin k eine ganze rationale Funktion von z ist, und die Vergleichung der Koeffizienten ergibt

$$\begin{aligned} k b_0 &= a_0 c_0, \\ k b_1 &= a_0 c_1 + a_1 c_0, \\ k b_2 &= a_0 c_2 + a_1 c_1 + a_2 c_0, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

worin die $c_0, c_1, \cdots c_{m-n}$ gleichfalls ohne gemeinschaftlichen Teiler vorausgesetzt werden können.

Hieraus folgt zunächst, daß k konstant sein muß, und $= 1$ gesetzt werden kann; denn ist durch irgend einen Linearfaktor von k $a_0, a_1, \cdots a_{r-1}, c_0, c_1, \cdots c_{s-1}$ teilbar, a_r, c_s nicht teilbar, so folgt aus

$$k b_{r+s} = \cdots a_{r-1} c_{s+1} + a_r c_s + a_{r+1} c_{s-1} + \cdots$$

der Widerspruch, daß $a_r c_s$ durch denselben Linearfaktor teilbar sein müßte. Hieraus aber folgt weiter, daß der Grad von $G(\theta, z)$ in bezug auf z gleich ist der Summe der Grade von F und H in bezug auf z; denn sind a_r, c_s die ersten unter den Koeffizienten a, c, deren Grad den Maximalwert erreicht, so folgt wieder aus

$$b_{r+s} = \cdots a_{r-1} c_{s+1} + a_r c_s + a_{r+1} c_{-1} + \cdots,$$

daß der Grad von b_{r+s} gleich der Summe der Grade von a_r und c_s ist.

Dividiert man die Gleichung (1) durch a_0, so kann dieselbe auch in die Form gesetzt werden

$$f(\theta, z) = \theta^n + b_1 \theta^{n-1} + \cdots + b_{n-1} \theta + b_n = 0, \tag{2}$$

worin die Koeffizienten $b_1, b_2, \cdots b_n$ auch gebrochene rationale Funktionen von z sein können.

Das System aller rationalen Funktionen von θ und z, $\Phi(\theta, z)$, hat die Eigenschaft, daß seine Individuen sich durch die elementaren Rechenoperationen, Addition, Subtraktion, Multiplikation und Division reproduzieren, und dies System wird daher als ein Körper algebraischer Funktionen Ω vom Grade n bezeichnet. Ist zunächst $\varphi(\theta)$ eine ganze rationale Funktion von θ, deren Koeffizienten rational von z abhängen, so kann man durch algebraische Division zwei eben solche Funktionen $q(\theta)$, $r(\theta)$ bestimmen, von denen die zweite den Grad $n - 1$ nicht übersteigt, so daß

$$\varphi(\theta) = q(\theta) f(\theta) + r(\theta)$$

oder wegen (2)

$$\varphi(\theta) = r(\theta).$$

Ist $\varphi(\theta)$ durch $f(\theta)$ nicht teilbar, so haben diese beiden Funktionen [wegen der vorausgesetzten Irreduktibilität von $f(\theta)$] keinen Teiler gemein, und daher lassen sich durch die Methode des größten gemeinschaftlichen Teilers zwei Funktionen $f_1(\theta)$, $\varphi_1(\theta)$ so bestimmen, daß

$$f(\theta) f_1(\theta) + \varphi(\theta)\varphi_1(\theta) = 1,$$

also wegen (2)

$$\varphi_1(\theta) = \frac{1}{\varphi(\theta)}.$$

Aus diesen beiden Bemerkungen, zusammengenommen mit der Voraussetzung der Irreduktibilität von $f(\theta)$ ergibt sich der folgende

Lehrsatz. Jede Funktion ζ des Körpers Ω läßt sich auf eine einzige Weise in die Form setzen:

$$\zeta = x_0 + x_1\theta + \cdots + x_{n-1}\theta^{n-1},$$

worin die Koeffizienten $x_0, x_1, \cdots x_{n-1}$ rationale Funktionen von z sind. Umgekehrt gehört jede Funktion dieser Form selbstverständlich dem Körper Ω an.

Wählt man unter den Funktionen des Körpers Ω n beliebige aus:

$$\eta_1 = x_0^{(1)} + x_1^{(1)}\theta + \cdots + x_{n-1}^{(1)}\theta^{n-1},$$
$$\eta_2 = x_0^{(2)} + x_1^{(2)}\theta + \cdots + x_{n-1}^{(2)}\theta^{n-1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\eta_n = a_0^{(n)} + x_1^{(n)}\theta + \cdots + x_{n-1}^{(n)}\theta^{n-1},$$

jedoch so, daß die Determinante

$$\sum \pm x_0^{(1)} x_1^{(2)} \cdots x_{n-1}^{(n)}$$

nicht identisch Null ist, so ergibt sich, daß jede Funktion des Körpers Ω auch in der Form dargestellt werden kann

$$\zeta = y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n,$$

deren Koeffizienten $y_1, y_2, \cdots y_n$ rationale Funktionen von z sind. Ein solches System von Funktionen $\eta_1, \eta_2, \cdots \eta_n$ soll eine Basis des Körpers Ω heißen.

Damit ein Funktionensystem $\eta_1, \eta_2, \cdots \eta_n$ des Körpers Ω eine Basis desselben bilde, ist erforderlich und hinreichend, daß zwischen ihnen keine Gleichung (Identität) von der Form

$$y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n = 0$$

bestehe, in welcher die Koeffizienten $y_1, y_2, \cdots y_n$ nicht sämtlich verschwinden. Beispielsweise bilden die Funktionen $1, \theta, \theta^2, \cdots \theta^{n-1}$ eine Basis von Ω.

16*

§ 2.

Normen, Spuren und Diskriminanten.

Wählt man zur Darstellung der Funktionen von Ω eine beliebige Basis $\eta_1, \eta_2, \cdots \eta_n$, so kann man, wenn ζ irgend eine Funktion in Ω bedeutet, setzen:

$$(1)\qquad \begin{cases} \zeta\eta_1 = y_{1,1}\eta_1 + y_{1,2}\eta_2 + \cdots + y_{1,n}\eta_n, \\ \zeta\eta_2 = y_{2,1}\eta_1 + y_{2,2}\eta_2 + \cdots + y_{2,n}\eta_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \zeta\eta_n = y_{n,1}\eta_1 + y_{n,2}\eta_2 + \cdots + y_{n,n}\eta_n, \end{cases}$$

worin die Koeffizienten $y_{\iota,\iota'}$ rationale Funktionen von z sind. Hieraus ergibt sich die Gleichung

$$(2)\qquad \begin{vmatrix} y_{1,1}-\zeta, & y_{1,2}, & \cdots & y_{1,n} \\ y_{2,1}, & y_{2,2}-\zeta, & \cdots & y_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ y_{n,1}, & y_{n,2}, & \cdots & y_{n,n}-\zeta \end{vmatrix} = 0,$$

welche, nach Potenzen von ζ geordnet, die Gestalt hat

$$(3)\qquad \varphi(\zeta) = \zeta^n + b_1\zeta^{n-1} + \cdots + b_{n-1}\zeta + b_n = 0$$

und, wie sich aus dem Multiplikationssatz der Determinanten ohne Schwierigkeit ergibt, von der Wahl der zugrunde gelegten Basis $\eta_1, \eta_2, \cdots \eta_n$ ganz unabhängig ist. Von den Koeffizienten $b_1, b_2, \cdots b_n$ der Funktion φ, welche sämtlich rationale Funktionen von z und durch die Funktion ζ vollkommen bestimmt sind, sollen zwei, die in der Folge von Wichtigkeit sind, durch besondere Namen ausgezeichnet werden. Die Funktion

$$(4)\qquad (-1)^n b_n = \begin{vmatrix} y_{1,1}, & y_{1,2}, & \cdots & y_{1,n} \\ y_{2,1}, & y_{2,2}, & \cdots & y_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ y_{n,1}, & y_{n,2}, & \cdots & y_{n,n} \end{vmatrix}$$

heißt die Norm der Funktion ζ, und wird mit $N(\zeta)$ bezeichnet Von dieser Funktion gelten folgende Sätze.

1. Die einzige Funktion, deren Norm identisch verschwindet, ist die Funktion „Null"; denn macht man in dem System (1) die Annahme daß $N(\zeta) = 0$ sei, so folgt, daß sich ein System rationaler Funktionen von z, die nicht sämtlich verschwinden, $y_1, y_2, \cdots y_n$ so bestimmen läßt, daß

$$\zeta(y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n) = 0,$$

also, da $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω bilden, $\zeta = 0$.

2. Die Norm einer rationalen Funktion von z ist die n^{te} Potenz dieser Funktion. Denn ist ζ rational, so reduzieren sich die Gleichungen (1) auf die Identitäten $\zeta\eta_h = \zeta\eta_h$, woraus $N(\zeta) = \zeta^n$ folgt.

3. Ist ζ' irgend eine zweite Funktion des Körpers Ω und das dem System (1) entsprechende Gleichungssystem für diese Funktion

$$\zeta'\eta_h = \sum^{\iota} y'_{h,\iota}\,\eta_\iota,$$

so folgt:

$$\zeta\zeta'\eta_h = \sum^{\iota,\iota'} y_{h,\iota}\,y'_{\iota,\iota'}\,\eta_{\iota'}$$

und daraus nach dem Multiplikationssatz der Determinanten

$$N(\zeta\zeta') = N(\zeta)\,N(\zeta').$$

4. Aus 2. und 3. folgt:

$$N(\zeta)\,N\left(\frac{1}{\zeta}\right) = 1,$$

also:

$$N\left(\frac{\zeta}{\zeta'}\right) = \frac{N(\zeta)}{N(\zeta')}.$$

5. Endlich ergibt sich aus der Definition der Funktion φ, (2), (3) der wichtige Satz: Ist t eine beliebige Konstante (oder auch eine rationale Funktion von z), so ist

$$\varphi(t) = N(t - \zeta).$$

Es soll sodann die Funktion

$$-b_1 = y_{1,1} + y_{2,2} + \cdots + y_{n,n} \tag{5}$$

die Spur von ζ genannt und mit $S(\zeta)$ bezeichnet werden. Für diese ergeben sich unmittelbar aus der Definition die Sätze:

$$S(0) = 0, \tag{6}$$

$$S(1) = n. \tag{7}$$

Und wenn x eine rationale Funktion von z, ferner ζ, ζ' zwei Funktionen in Ω bedeuten:

$$S(x\zeta) = xS(\zeta), \tag{8}$$

$$S(\zeta + \zeta') = S(\zeta) + S(\zeta'). \tag{9}$$

Es hat sich aus dieser Betrachtung ergeben, daß jede Funktion ζ in Ω einer Gleichung n^{ten} Grades, $\varphi(\zeta) = 0$, genügt, deren Koeffizienten rational von z abhängen. Wenn diese Gleichung irreduktibel ist, so bilden die Funktionen $1, \zeta, \zeta^2, \cdots \zeta^{n-1}$ eine Basis von Ω. Im andern Falle sei

$$\varphi_1(\zeta) = \zeta^e + b'_0\,\zeta^{e-1} + \cdots + b'_{e-1}\,\zeta + b'_e = 0 \tag{10}$$

die Gleichung niedrigsten Grades, deren Koeffizienten in z rational sind, welcher die Funktion ζ genügt, und mithin $\varphi_1(\zeta) = 0$ irreduktibel, $e < n$. Da gleichwohl $\varphi(\zeta)$ verschwindet, so muß $\varphi(\zeta)$ durch $\varphi_1(\zeta)$ algebraisch teilbar sein, und wie in § 1 ergibt sich, daß jede rationale Funktion η von z und ζ in der Form darstellbar ist

$$\eta = x_0 + x_1 \zeta + \cdots + x_{e-1} \zeta^{e-1},$$

deren Koeffizienten x_0, $x_1, \cdots x_{e-1}$ rational von z abhängen *). Ist nun

$$\theta^f + \eta_1 \theta^{f-1} + \cdots + \eta_{f-1} \theta + \eta_f = 0$$

die Gleichung niedrigsten Grades, welcher θ genügt, deren Koeffizienten rational von z und ζ abhängen, so besteht zwischen den $e.f$ Funktionen

(11) $$\zeta^h \theta^k \qquad (h = 0, 1, \cdots e-1;\; k = 0, 1, \cdots f-1)$$

keine lineare Gleichung mit rational von z abhängigen Koeffizienten, während jede Funktion in Ω linear mit rational von z abhängigen Koeffizienten durch diese Funktionen darstellbar ist. Es ergibt sich daraus, daß dieselben eine Basis von Ω bilden, und daß sonach

$$e.f = n,$$

also e ein Teiler von n ist.

Wendet man die Basis (11) zur Aufstellung der Norm von ζ an, so erkennt man leicht mittels der Gleichung (10), daß

$$N(\zeta) = ((-1)^e b'_e)^f = (-1)^n b'^f_e$$

wird. Da ferner für ein beliebiges konstantes t die Funktion $\zeta - t$ einer Gleichung von demselben Grade genügt wie ζ, so ergibt sich der Satz:

Die Funktion $\varphi(t)$ (3) ist entweder irreduktibel oder eine ganze Potenz einer irreduktibeln Funktion.

Ist $\eta_1, \eta_2, \cdots \eta_n$ ein beliebiges System von n Funktionen in Ω, gleichviel ob dasselbe eine Basis bildet oder nicht, so führen wir eine zu diesem System gehörige rationale Funktion von z ein, die wir als dessen Diskriminante, $\Delta(\eta_1, \eta_2, \cdots \eta_n)$ bezeichnen und folgendermaßen definieren

(12) $$\Delta(\eta_1, \eta_2, \cdots \eta_n) = \begin{vmatrix} S(\eta_1 \eta_1), & S(\eta_1 \eta_2), & \cdots & S(\eta_1 \eta_n) \\ S(\eta_2 \eta_1), & S(\eta_2 \eta_2), & \cdots & S(\eta_2 \eta_n) \\ \cdot & \cdot & \cdot & \cdot \\ S(\eta_n \eta_1), & S(\eta_n \eta_2), & \cdots & S(\eta_n \eta_n) \end{vmatrix}.$$

---

*) Aus der Gleichung $\varphi_1(\zeta) = 0$ entspringt ein Körper algebraischer Funktionen Ω_1 vom Grade e, dessen Funktionen sämtlich zugleich im Körper Ω enthalten sind, und der daher als ein Teiler des Körpers Ω bezeichnet werden kann.

Die Diskriminante ist dann und nur dann nicht identisch Null, wenn die Funktionen $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω bilden.

Um den ersten Teil dieser Behauptung zu beweisen, nehmen wir an, es sei $\Delta\ (\eta_1, \eta_2, \cdots \eta_n) = 0$. Es läßt sich unter dieser Voraussetzung ein System rationaler Funktionen $y_1, y_2, \cdots y_n$ von z, die nicht alle identisch verschwinden, so bestimmen, daß

$$\begin{gathered} y_1 S(\eta_1 \eta_k) + y_2 S(\eta_2 \eta_k) + \cdots + y_n S(\eta_n \eta_k) \\ = S\big(\eta_k (y_1 \eta_1 + y_2 \eta_2 + \cdots + y_n \eta_n)\big) = 0. \\ (k = 1, 2, \cdots n) \end{gathered}$$

Wählt man daher ein System rationaler Funktionen $x_1, x_2, \cdots x_n$ von z, ganz beliebig und setzt:

$$\begin{gathered} y_1 \eta_1 + y_2 \eta_2 + \cdots + y_n \eta_n = \eta, \\ x_1 \eta_1 + x_2 \eta_2 + \cdots + x_n \eta_n = \zeta, \end{gathered}$$

so folgt:

$$S(\zeta \eta) = 0.$$

Wenn aber die Funktionen $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω bilden, so kann ζ jede beliebige Funktion in Ω, also, da η nicht verschwindet, beispielsweise auch $\frac{1}{\eta}$ sein. Dann ist aber die letzte Gleichung sicher nicht erfüllt, und es kann also unter dieser Voraussetzung die Diskriminante von $\eta_1, \eta_2, \cdots \eta_n$ nicht identisch verschwinden.

Halten wir die Annahme fest, daß $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω sei, und setzen:

$$\eta'_k = x_{1,k} \eta_1 + x_{2,k} \eta_2 + \cdots + x_{n,k} \eta_n, \qquad (k = 1, 2, \cdots n)$$

so bilden die Funktionen $\eta'_1, \eta'_2, \cdots \eta'_n$ eine Basis von Ω oder nicht, je nachdem die Determinante der rationalen Funktionen $x_{h,k}$ von z

$$X = \sum \pm x_{1,1} x_{2,2} \cdots x_{n,n}$$

von Null verschieden ist oder nicht. Nun ist aber

$$S(\eta'_h \eta'_k) = \sum_{1,n}^{\iota,\iota'} x_{\iota,h} x_{\iota',k} S(\eta_\iota \eta_{\iota'}),$$

und daraus ergibt sich nach dem Multiplikationssatz der Determinanten der **Hauptsatz über die Diskriminanten**

(13) $$\Delta(\eta'_1, \eta'_2, \cdots \eta'_n) = X^2 \Delta(\eta_1, \eta_2, \cdots \eta_n),$$

woraus auch die Richtigkeit des zweiten Teils der obigen Behauptung erhellt, daß die Diskriminante eines Funktionensystems stets dann identisch verschwindet, wenn dasselbe keine Basis von Ω bildet.

§ 3.

Das System der ganzen Funktionen von z im Körper Ω.

Definition. Eine Funktion ω des Körpers Ω soll eine ganze Funktion von z heißen, wenn in der Gleichung niedrigsten Grades, welcher dieselbe nach § 2 genügt:

$$(1) \qquad \varphi(\omega) = \omega^e + b_1 \omega^{e-1} + \cdots + b_{e-1}\omega + b_e = 0,$$

die Koeffizienten $b_1, b_2, \cdots b_e$ ganze rationale Funktionen von z sind; im entgegengesetzten Fall heiße sie eine gebrochene Funktion. Der Inbegriff aller ganzen Funktionen von z in Ω soll mit $\mathfrak{o}$ bezeichnet werden. Da nach § 2 $N(t-\omega)$ eine ganze Potenz von $\varphi(t)$ ist, so folgt, daß für eine ganze Funktion ω auch die sämtlichen Koeffizienten von $N(t-\omega)$ ganze rationale Funktionen von z sind, also insbesondere:

1. Die Norm und die Spur einer ganzen Funktion sind ganze rationale Funktionen von z.

Aus der Definition der ganzen Funktionen ergibt sich ferner:

2. Eine rationale Funktion von z gehört dann und nur dann zu dem System $\mathfrak{o}$, wenn sie eine ganze rationale Funktion von z ist.

3. Jede Funktion η in Ω kann durch Multiplikation mit einer von Null verschiedenen ganzen rationalen Funktion von z in eine Funktion des Systems $\mathfrak{o}$ verwandelt werden. Denn es genügt η nach § 2 einer Gleichung niedrigsten Grades von der Form

$$b_0 \eta^e + b_1 \eta^{e-1} + \cdots + b_{e-1}\eta + b_e = 0,$$

deren Koeffizienten ganze rationale Funktionen von z sind, und diese geht durch die Substitution $b_0 \eta = \omega$ in eine Gleichung von der Form (1) für ω über.

4. Eine Funktion ω des Körpers Ω, welche irgend einer Gleichung von der Form genügt

$$\psi(\omega) = \omega^m + c_1 \omega^{m-1} + \cdots + c_{m-1}\omega + c_m = 0,$$

in welcher die Koeffizienten $c_1, \cdots c_m$ ganze rationale Funktionen von z sind, ist eine ganze Funktion. Denn ist

$$\varphi(\omega) = \omega^e + b_1 \omega^{e-1} + \cdots + b_{e-1}\omega + b_e = 0$$

die Gleichung niedrigsten Grades, welcher ω genügt, so muß $\psi(\omega)$ durch $\varphi(\omega)$ algebraisch teilbar sein:

$$\psi(\omega) = \varphi(\omega)\chi(\omega),$$

was, wie leicht zu zeigen ist, zur Folge hat, daß auch die Koeffizienten von $\varphi(\omega)$ und $\chi(\omega)$ ganze rationale Funktionen von z sind (Gauß, Disq. Ar. art. 42). Hieraus ergibt sich der Hauptsatz über die ganzen Funktionen:

5. Summe, Differenz, Produkt zweier ganzen Funktionen sind wieder ganze Funktionen.

Sind nämlich ω', ω'' zwei ganze Funktionen in Ω, welche resp. den Gleichungen genügen

$$\omega'^{n'} + b'_1 \omega'^{n'-1} + \cdots + b'_{n'-1} \omega' + b'_{n'} = 0,$$
$$\omega''^{n''} + b''_1 \omega''^{n''-1} + \cdots + b''_{n''-1} \omega'' + b''_{n''} = 0,$$

so kann man, wenn man unter $\omega_1, \omega_2, \cdots \omega_m$ die $m = n' n''$ Produkte

$$\omega'^{h'} \omega''^{h''} \quad (h' = 0, 1, \cdots n'-1;\ h'' = 0, 1, \cdots n''-1)$$

und unter ω eine der drei Funktionen $\omega' \pm \omega''$, $\omega' \omega''$ versteht, setzen

$$\omega \omega_1 = x_{1,1} \omega_1 + \cdots + x_{1,m} \omega_m,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\omega \omega_m = x_{m,1} \omega_1 + \cdots + x_{m,m} \omega_m,$$

worin die $x_{h,h'}$ ganze rationale Funktionen von z sind, und daraus erhält man

$$\begin{vmatrix} x_{1,1} - \omega, & x_{1,2}, & \cdots & x_{1,m} \\ x_{2,1}, & x_{2,2} - \omega, & \cdots & x_{2,m} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m,1}, & x_{m,2}, & \cdots & x_{m,m} - \omega \end{vmatrix} = 0,$$

also eine Gleichung für ω, deren Koeffizienten ganze rationale Funktionen von z sind.

Als Korollar ergibt sich hieraus, daß jede ganze rationale Funktion von Funktionen in $\mathfrak{o}$ selbst eine Funktion des Systems $\mathfrak{o}$ ist.

6. Eine ganze Funktion ω heißt durch eine andere ganze Funktion ω' teilbar, wenn ein dritte ganze Funktion ω'' existiert, welche der Bedingung genügt

$$\omega = \omega' \omega''.$$

Aus dieser Definition ergibt sich sofort:

Ist ω teilbar durch ω', ω' durch ω'', so ist auch ω durch ω'' teilbar.

Ist ω' und ω'' durch ω teilbar, so ist auch $\omega' \pm \omega''$ durch ω teilbar, und allgemein: sind $\omega_1, \omega_2, \omega_3, \cdots$ durch ω teilbar, $\omega'_1, \omega'_2, \omega'_3, \cdots$ beliebige Funktionen in $\mathfrak{o}$, so ist auch $\omega'_1 \omega_1 + \omega'_2 \omega_2 + \omega'_3 \omega_3 + \cdots$ durch ω teilbar.

7. Bilden die Funktionen $\eta_1, \eta_2, \cdots \eta_n$ eine Basis von Ω, so kann man (nach 3.) n von Null verschiedene ganze rationale Funktionen von $z, a_1, a_2, \cdots a_n$ der Art bestimmen, daß

$$\omega_1 = a_1 \eta_1, \ \omega_2 = a_2 \eta_2, \cdots \omega_n = a_n \eta_n$$

ganze Funktionen sind, und diese bilden ebenfalls eine Basis von Ω, da

$$\varDelta(\omega_1, \omega_2, \cdots \omega_n) = a_1^2 a_2^2 \cdots a_n^2 \varDelta(\eta_1, \eta_2, \eta_n)$$

von Null verschieden ist. Es gibt also Basen von Ω, $\omega_1, \omega_2, \cdots \omega_n$, welche aus lauter ganzen Funktionen bestehen, und die Diskriminante einer solchen Basis ist, da $S(\omega_r \omega_s)$ ganze rationale Funktionen von z sind, selbst eine von Null verschiedene ganze rationale Funktion von z. Jede Funktion von der Form

$$\omega = x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n, \tag{2}$$

in welcher die $x_1, x_2, \cdots x_n$ ganze rationale Funktionen von z sind, gehört dann zu dem System $\mathfrak{o}$; aber es ist durchaus nicht notwendig, daß umgekehrt jede Funktion in $\mathfrak{o}$ in dieser Form darstellbar sei.

Nehmen wir also an, es existieren in $\mathfrak{o}$ noch andere Funktionen als die in der Form (2) enthaltenen, so müssen sich eine lineare Funktion $z - c$ und gewisse ganze rationale Funktionen $x_1, x_2, \cdots x_n$, die nicht alle durch $z - c$ teilbar sind, so wählen lassen, daß

$$\frac{x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n}{z - c}$$

eine ganze Funktion ist. Die Funktionen $x_1, x_2, \cdots x_n$ lassen sich nun auf ihre nicht sämtlich verschwindenden konstanten Reste c_1, $c_2, \cdots c_n$ in bezug auf $z - c$ reduzieren, und daraus erhellt, daß auch

$$\omega = \frac{c_1 \omega_1 + c_2 \omega_2 + \cdots + c_n \omega_n}{z - c}$$

eine ganze Funktion ist. Ist c_1 von Null verschieden, so bilden auch die n ganzen Funktionen

$$\omega \text{ und } \omega_2, \omega_3, \cdots \omega_n$$

eine Basis von Ω und zugleich ist nach § 2 (13)

$$\varDelta(\omega, \omega_2, \cdots \omega_n) = \frac{c_1^2}{(z-c)^2} \varDelta(\omega_1, \omega_2, \cdots \omega_n),$$

also von niedrigerem Grade als $\varDelta(\omega_1, \omega_2, \cdots \omega_n)$. Da nun diese beiden Diskriminanten ganze rationale Funktionen von z sind, so gelangt man durch wiederholte Anwendung dieses Verfahrens schließlich zu einer aus ganzen Funktionen bestehenden Basis von Ω, $\omega_1', \omega_2', \cdots \omega_n'$, deren Diskriminante im Grade nicht weiter erniedrigt werden kann, und welche folglich die Eigenschaft hat, daß **jede** Funktion ω in $\mathfrak{o}$ in der Form enthalten ist

$$\omega = x_1 \omega_1' + x_2 \omega_2' + \cdots + x_n \omega_n'$$

mit ganzen rationalen Funktionen von z als Koeffizienten. Ein solches System soll eine Basis von $\mathfrak{o}$ genannt werden.

Ist $\omega_1, \omega_2, \cdots \omega_n$ eine Basis von $\mathfrak{o}$ und

$$\omega_\iota' = x_{\iota,1} \omega_1 + x_{\iota,2} \omega_2 + \cdots + x_{\iota,n} \omega_n, \qquad (\iota = 1, 2, \cdots n)$$

so wird das System $\omega_1', \omega_2', \cdots \omega_n'$ dann und nur dann ebenfalls eine Basis von $\mathfrak{o}$ bilden, wenn die Determinante der ganzen rationalen Funktionen $x_{\iota,\iota'}$

$$X = \sum \pm x_{1,1} x_{2,2} \cdots x_{n,n}$$

eine von Null verschiedene Konstante ist. Denn nehmen wir an, es habe diese Determinante irgend einen Linearfaktor $z - c$, so lassen sich Konstanten $c_1, c_2, \cdots c_n$, nicht sämtlich verschwindend, so bestimmen, daß die n ganzen rationalen Funktionen von z

$$c_1 x_{1,\iota} + c_2 x_{2,\iota} + \cdots + c_n x_{n,\iota}$$

durch $z - c$ teilbar werden (d. h. für $z = c$ verschwinden); dann aber ist

$$\frac{c_1 \omega_1' + c_2 \omega_2' + \cdots + c_n \omega_n'}{z - c}$$

eine ganze Funktion und mithin $\omega_1', \omega_2', \cdots \omega_n'$ keine Basis von $\mathfrak{o}$.

Da nun andererseits

$$\Delta(\omega_1', \omega_2' \cdots \omega_n') = X^2 \Delta(\omega_1, \omega_2, \cdots \omega_n)$$

ist, so folgt, daß die Diskriminante einer Basis von $\mathfrak{o}$ von einem konstanten Faktor abgesehen von der Wahl dieser Basis unabhängig ist. Man erhält also eine vollkommen bestimmte ganze rationale Funktion von z, wenn man in der Diskriminante einer beliebigen Basis von $\mathfrak{o}$ den Koeffizienten der höchsten Potenz von z durch Division $= 1$ macht. Diese Funktion soll die Diskriminante des Körpers Ω oder des Systems $\mathfrak{o}$ genannt und mit $\Delta(\Omega)$ oder $\Delta(\mathfrak{o})$ bezeichnet werden.

§ 4.

Die Funktionenmoduln.

Wir betrachten im folgenden Systeme von Funktionen, welche wir Funktionenmoduln oder auch schlechtweg **Moduln** nennen und folgendermaßen definieren. Ein Funktionensystem (in Ω) heißt ein Modul, wenn sich die Funktionen desselben durch Addition, Subtraktion und durch Multiplikation mit ganzen rationalen Funktionen von z reproduzieren.

Bezeichnet man mit $\alpha_1, \alpha_2, \cdots \alpha_m$ irgend m gegebene Funktionen, mit $x_1, x_2, \cdots x_m$ willkürliche ganze rationale Funktionen von z, so bildet der Inbegriff aller Funktionen von der Form

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_m \alpha_m$$

einen Modul. Ein solcher soll ein endlicher Modul genannt und mit

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_m]$$

bezeichnet werden. Das Funktionensystem $\alpha_1, \alpha_2, \ldots \alpha_m$ heißt die Basis dieses Moduls.

Wir wollen ein Funktionensystem $\alpha_1, \alpha_2, \cdots \alpha_m$ rational irreduktibel oder die Funktionen $\alpha_1, \alpha_2, \cdots \alpha_m$ rational unabhängig nennen, wenn eine Gleichung von der Form

$$x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_m \alpha_m = 0$$

für rationale x nur dann bestehen kann, wenn $x_1 = 0, x_2 = 0, \cdots x_m = 0$ ist. Ein Funktionensystem, welches eine Basis des Körpers Ω bildet, ist daher stets rational irreduktibel, und es gibt kein System von mehr als n rational unabhängigen Funktionen in Ω.

Wir beweisen nun zunächst den Satz:

1. Jeder endliche Modul besitzt eine rational irreduktible Basis.

Der Beweis desselben ergibt sich unmittelbar aus dem folgenden Hilfssatz:

Sind die ganzen rationalen Funktionen $y_{1,1}, y_{2,1}, \cdots y_{m,1}$ ohne gemeinschaftlichen Teiler, so lassen sich andere ganze rationale Funktionen $y_{1,2}, y_{2,2}, \cdots y_{m,m}$ so bestimmen, daß

$$\sum \pm y_{1,1}\, y_{2,2} \cdots y_{m,m} = 1\ *).$$

*) Der Satz ist richtig und bekannt für $m = 2$. Nehmen wir also an, er sei bewiesen für $m - 1$, so können wir, wenn ∂ den größten gemeinschaftlichen Teiler von $y_{1,1}, y_{2,1}, \cdots y_{m-1,1}$ bedeutet, der Gleichung genügen

$$\begin{vmatrix} y_{1,1}, & y_{2,1}, & \cdots & y_{m-1,1} \\ y_{1,3}, & y_{2,3}, & \cdots & y_{m-1,3} \\ \cdot & \cdot & \cdot & \cdot \\ y_{1,m}, & y_{2,m} & \cdots & y_{m-1,m} \end{vmatrix} = \partial$$

und wenn wir also die ganzen rationalen Funktionen x, y so bestimmen, daß

$$x\, y_{m,1} - y\, \partial = (-1)^{m-1}$$

Genügen nun die Funktionen $\alpha_1, \alpha_2, \cdots \alpha_m$ einer Gleichung

$$\sum_{1,m}^{\iota} y_{\iota,1}\, \alpha_\iota = 0,$$

in welcher die ganzen rationalen Funktionen $y_{1,1} \cdots y_{m,1}$ ohne gemeinschaftlichen Teiler angenommen werden können, so setze man

$$\sum_{1,m}^{\iota} y_{\iota,2}\, \alpha_\iota = \beta_2,$$

$$\cdots\cdots\cdots$$

$$\sum_{1,m}^{\iota} y_{\iota,m}\, \alpha_\iota = \beta_m;$$

dann ist der Modul $[\alpha_1, \alpha_2, \alpha_m]$ völlig identisch mit dem Modul $[\beta_2, \beta_3, \beta_m]$, dessen Basis eine Funktion weniger enthält. Sind die Funktionen β_ι noch nicht rational unabhängig, so kann man sie in derselben Weise weiter reduzieren, und gelangt schließlich, falls die Funktionen α_ι nicht sämtlich verschwinden (ein Fall, welchen wir von dem Modulbegriff ganz ausschließen wollen) zu einer irreduktibeln Basis. Wir werden in der Folge unter einer Basis schlechtweg stets eine irreduktible Basis verstehen.

2. Obwohl man nach dem vorhergehenden für einen und denselben Modul sehr verschiedene irreduktible Basen auffinden kann, so ist doch die Zahl der Funktionen, die in einer solchen enthalten sind, stets dieselbe, da im entgegengesetzten Fall dasjenige Funktionensystem, welches mehr Funktionen enthält, nicht rational irreduktibel sein könnte. Sind also $\alpha_1, \alpha_2, \cdots \alpha_m$; $\beta_1, \beta_2, \cdots \beta_m$ zwei irreduktible Basen desselben Moduls $\mathfrak{a}$, so ist, da sowohl die α_k als die β_k in $\mathfrak{a}$ enthalten sind:

$$\alpha_k = \sum_{1,m}^{\iota} p_k^{(\iota)} \beta_\iota; \quad \beta_k = \sum_{1,m}^{\iota} q_\iota^{(k)} \alpha_\iota,$$

worin die Koeffizienten p, q ganze rationale Funktionen von z sind. Hieraus aber folgt:

$$\sum_{1,m}^{\iota} q_\iota^{(k)}\, p_\iota^{(h)} = 0 \text{ oder } 1,$$

---

ist, so folgt:

$$\begin{vmatrix} y_{1,1}, & y_{2,1}, & \cdots & y_{m-1,1}, & y_{m,1} \\ \frac{x\, y_{1,1}}{\partial}, & \frac{x\, y_{2,1}}{\partial}, & \cdots & \frac{x\, y_{m-1,1}}{\partial} & y \\ y_{1,3}, & y_{2,3}, & \cdots & y_{m-1,3}, & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ y_{1,m} & y_{2,m}, & \cdots & y_{m-1\,m}, & 0 \end{vmatrix} = 1.$$

je nachdem h von k verschieden ist oder nicht, und daraus:

$$\sum \pm p_1^{(1)} p_2^{(2)} \cdots p_m^{(m)} \cdot \sum \pm q_1^{(1)} q_2^{(2)} \cdots q_m^{(m)} = 1,$$

und da beide Determinanten ganze rationale Funktionen von z sind, so müssen sie beide konstant sein.

3. Definition. Ein Modul $\mathfrak{a}$ heißt durch einen Modul $\mathfrak{b}$ teilbar, oder $\mathfrak{b}$ ein Teiler (Divisor) von $\mathfrak{a}$, $\mathfrak{a}$ ein Vielfaches (Multiplum) von $\mathfrak{b}$ ($\mathfrak{b}$ geht in $\mathfrak{a}$ auf), wenn jede Funktion in $\mathfrak{a}$ zugleich in $\mathfrak{b}$ enthalten ist. $\mathfrak{b}$ soll ein echter Teiler von $\mathfrak{a}$ heißen, wenn $\mathfrak{a}$ durch $\mathfrak{b}$ teilbar, aber nicht mit $\mathfrak{b}$ identisch ist*).

Aus dieser Definition ergibt sich sofort:

Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, $\mathfrak{b}$ teilbar durch $\mathfrak{c}$, so ist auch $\mathfrak{a}$ teilbar durch $\mathfrak{c}$.

4. Definition. Der Inbegriff $\mathfrak{m}$ aller derjenigen Funktionen, welche zugleich in zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind, bildet, falls er nicht aus der einzigen Funktion „Null" besteht, einen Modul (nach der allgemeinen Definition), welcher das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ heißt, weil jeder Modul, welcher ein Vielfaches zugleich von $\mathfrak{a}$ und von $\mathfrak{b}$ ist, auch ein Vielfaches von $\mathfrak{m}$ ist. Das kleinste gemeinschaftliche Vielfache von einer beliebigen Zahl von Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ ist dementsprechend der Inbegriff aller der Funktionen, die zugleich in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ enthalten sind. Man kann dasselbe bilden, indem man nach Belieben je zwei der Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ durch ihr kleinstes gemeinschaftliches Vielfache ersetzt.

5. Definition. Ist α eine beliebige Funktion in $\mathfrak{a}$, β eine beliebige Funktion in $\mathfrak{b}$, so bildet der Inbegriff aller Funktionen von der Form $\alpha + \beta$ einen Modul $\mathfrak{d}$, welcher der größte gemeinschaftliche Teiler der beiden Moduln $\mathfrak{a}$ und $\mathfrak{b}$ heißt. Derselbe ist, wenn $\mathfrak{a}$ und $\mathfrak{b}$ endliche Moduln sind, selbst ein solcher. Ist nämlich

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_r], \quad \mathfrak{b} = [\beta_1, \beta_2, \cdots \beta_s],$$

so ist

$$\mathfrak{d} = [\alpha_1, \alpha_2, \cdots \alpha_r, \beta_1, \beta_2, \cdots \beta_s].$$

Nach der Definition der Teilbarkeit ist $\mathfrak{d}$ ein Teiler sowohl von $\mathfrak{a}$ als von $\mathfrak{b}$. Ist umgekehrt $\mathfrak{d}'$ ein Teiler von $\mathfrak{a}$ und von $\mathfrak{b}$, so sind die Funktionen α sowohl als die Funktionen β, mithin auch die Funktionen $\alpha + \beta$ in $\mathfrak{d}'$ enthalten; daher ist $\mathfrak{d}$ durch $\mathfrak{d}'$ teilbar.

---

*) Der Begriff der Teilbarkeit der Moduln ist der von den Zahlen her gewohnten Anschauung zuwider gebildet, insofern der Teiler einen größeren Inhalt an Funktionen enthält als das Vielfache.

Die Definition des größten gemeinschaftlichen Teilers einer beliebigen Anzahl von Moduln ergibt sich hiernach von selbst.

6. Definition. Ist $\mathfrak{a}$ ein Modul, α jede Funktion in $\mathfrak{a}$ und μ eine beliebige Funktion in Ω, so verstehen wir unter dem Produkt $\mu\mathfrak{a}$ oder $\mathfrak{a}\mu$ den Inbegriff aller Funktionen $\mu\alpha$, welcher wieder ein Modul ist. Ist

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_r]$$

ein endlicher Modul, so ist

$$\mu\mathfrak{a} = [\mu\alpha_1, \mu\alpha_2, \cdots \mu\alpha_r],$$

also ebenfalls ein endlicher Modul, und aus $\mu\mathfrak{a} = \mu\mathfrak{b}$ folgt $\mathfrak{a} = \mathfrak{b}$, wenn μ von Null verschieden ist.

7. Definition. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei Moduln, α, β sämtliche Funktionen in $\mathfrak{a}$, resp. in $\mathfrak{b}$, so verstehen wir unter dem Produkt

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a} = \mathfrak{c}$$

den Inbegriff aller Produkte einer Funktion α und einer Funktion β und aller Summen solcher Produkte, also sämtlicher Funktionen, welche durch das Zeichen

$$\gamma = \sum \alpha\beta$$

bezeichnet werden können.

Dieses Funktionensystem bildet jederzeit einen Modul, und zwar einen endlichen, wenn $\mathfrak{a}$ und $\mathfrak{b}$ solche sind. Sind nämlich $\mathfrak{a}$ und $\mathfrak{b}$ so definiert, wie in 5., so bilden die $r \cdot s$ Funktionen $\alpha_\iota \beta_\varkappa$ eine, wenn auch reduktible, Basis von $\mathfrak{c}$. Ein Produkt aus beliebig vielen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\cdots$ erklärt sich hiernach von selbst, und es gilt für dasselbe der Fundamentalsatz der Multiplikation von der Vertauschbarkeit der Faktoren. Sind die einzelnen Funktionen eines solchen Produkts, deren Anzahl m sei, einander gleich und $= \mathfrak{a}$, so wird dasselbe mit $\mathfrak{a}^m$ bezeichnet, und es ist

$$\mathfrak{a}^{m+m'} = \mathfrak{a}^m \mathfrak{a}^{m'}.$$

Im allgemeinen ist ein Produkt $\mathfrak{a}\mathfrak{b}$ nicht durch $\mathfrak{a}$ teilbar. Dagegen gilt der Satz, dessen Beweis sich unmittelbar aus der Definition ergibt:

Ist $\mathfrak{a}$ teilbar durch $\mathfrak{a}_1$, $\mathfrak{b}$ durch $\mathfrak{b}_1$, so ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}_1\mathfrak{b}_1$.

8. Definition. Unter dem Quotienten $\frac{\mathfrak{b}}{\mathfrak{a}}$ zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ soll der Inbegriff aller derjenigen Funktionen γ verstanden werden, welche die Eigenschaft haben, daß $\gamma\mathfrak{a}$ durch $\mathfrak{b}$ teilbar ist. Dieser

Quotient ist, falls er nicht aus der einzigen Funktion „Null“ besteht, ein Modul $\mathfrak{c}$, was sofort aus der Definition erhellt. Das Produkt $\frac{\mathfrak{b}}{\mathfrak{a}} \cdot \mathfrak{a}$ ist jederzeit durch $\mathfrak{b}$ teilbar, wenn auch nicht immer gleich $\mathfrak{b}$.

§ 5.

Kongruenzen.

Zwei Funktionen α, β heißen kongruent nach dem Modul $\mathfrak{a}$

$$\alpha \equiv \beta \, (\mathrm{mod.}\, \mathfrak{a}),$$

wenn die Differenz der beiden Funktionen, $\alpha - \beta$, in dem Modul $\mathfrak{a}$ enthalten ist.

Aus dieser Definition ergeben sich unmittelbar die folgenden Sätze:

1. Ist $\alpha \equiv \beta$, $\beta \equiv \gamma$ (mod. $\mathfrak{a}$), so ist $\alpha \equiv \gamma$ (mod. $\mathfrak{a}$).

2. Ist $\mathfrak{b}$ irgendein Teiler von $\mathfrak{a}$, so folgt aus $\alpha \equiv \beta$ (mod. $\mathfrak{a}$), daß auch $\alpha \equiv \beta$ (mod. $\mathfrak{b}$) ist.

3. Ist $\alpha \equiv \beta$ (mod. $\mathfrak{a}$), μ eine beliebige Funktion in Ω, so folgt $\mu\alpha \equiv \mu\beta$ (mod. $\mu\mathfrak{a}$), und umgekehrt folgt aus der letzteren Kongruenz die erstere, wenn μ von Null verschieden.

4. Ist $\alpha \equiv \beta$, $\alpha_1 \equiv \beta_1$ (mod. $\mathfrak{a}$), so ist auch $\alpha \pm \alpha_1 \equiv \beta \pm \beta_1$ (mod. $\mathfrak{a}$).

Sind $\lambda_1, \lambda_2, \cdots \lambda_m$ beliebig gegebene Funktionen in Ω, $c_1, c_2, \cdots c_m$ willkürliche Konstanten, so heißt der Inbegriff aller Funktionen von der Form

$$c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_m \lambda_m$$

eine Schar und wird mit $(\lambda_1, \lambda_2, \cdots \lambda_m)$ bezeichnet. Das Funktionensystem $\lambda_1, \lambda_2, \cdots \lambda_m$ heißt die Basis der Schar. Die Funktionen $\lambda_1, \lambda_2, \cdots \lambda_m$ heißen linear unabhängig oder ihr System linear irreduktibel, wenn eine Gleichung (Identität) von der Form

$$c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_m \lambda_m = 0$$

nicht anders bestehen kann, als wenn die konstanten Koeffizienten $c_1, c_2, \cdots c_m$ alle verschwinden.

Hiernach gilt der Satz, daß jede Schar eine linear irreduktible Basis besitzt. Denn ist $c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_m \lambda_m = 0$ und c_1 von Null verschieden, so ist die Schar $(\lambda_1, \lambda_2, \cdots \lambda_m)$ identisch mit der Schar $(\lambda_2, \lambda_3, \cdots \lambda_m)$, deren Basis eine Funktion weniger enthält. Ist diese noch nicht linear irreduktibel, so kann man auf die gleiche Weise weiterschließen. Auch hier soll in der Folge unter einer Basis schlechtweg eine irreduktible Basis verstanden sein. Die Anzahl der Funktionen, welche in einer irreduktiblen Basis einer

Schar enthalten sind, ist stets dieselbe und heißt die Dimension der Schar. Ist m die Dimension, so heißt die Schar auch eine m-fache. Irgend m Funktionen einer solchen Schar bilden eine irreduktible Basis derselben dann und nur dann, wenn sie linear unabhängig sind.

Die Funktionen $\lambda_1, \lambda_2, \cdots \lambda_m$ heißen linear unabhängig in bezug auf den Modul $\mathfrak{a}$, wenn eine Kongruenz von der Form

$$c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_m \lambda_m \equiv 0 \pmod{\mathfrak{a}}$$

für keine anderen als verschwindende konstante Koeffizienten c_1, $c_2, \cdots c_m$ besteht. Zwei Summen von der Form $\Sigma c_\iota \lambda_\iota$ mit verschiedenen Werten der konstanten Koeffizienten c_ι sind dann auch stets inkongruent nach dem Modul $\mathfrak{a}$.

Es seien nun $\mathfrak{a}$ und $\mathfrak{b}$ zwei Moduln, und es werde zunächst angenommen, es existieren in $\mathfrak{b}$ nur eine endliche Anzahl von Funktionen $\lambda_1, \lambda_2, \cdots \lambda_m$, welche nach dem Modul $\mathfrak{a}$ linear unabhängig sind. Jede Funktion β in $\mathfrak{b}$ genügt dann einer und nur einer Kongruenz von der Form

$$\beta \equiv c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_m \lambda_m \pmod{\mathfrak{a}}$$

mit konstanten Koeffizienten $c_1, c_2, \cdots c_m$. Die Schar $(\lambda_1, \lambda_2, \cdots \lambda_m)$ kann daher ein vollständiges Restsystem des Moduls $\mathfrak{b}$ nach dem Modul $\mathfrak{a}$ und $\lambda_1, \lambda_2, \cdots \lambda_m$ eine Basis desselben genannt werden, und man kann in symbolischer Bezeichnung setzen:

$$\mathfrak{b} \equiv (\lambda_1, \lambda_2, \cdots \lambda_m) \pmod{\mathfrak{a}}.$$

Wählt man in $\mathfrak{b}$ irgendein System von m Funktionen $\lambda'_1, \lambda'_2, \cdots \lambda'_m$ aus, so gelten m Kongruenzen

$$\lambda'_h \equiv \sum^{\iota} k_{h,\iota} \lambda_\iota \pmod{\mathfrak{a}}$$

mit konstanten $k_{h,\iota}$, und dies System bildet dann und nur dann eine Basis eines vollständigen Restsystems von $\mathfrak{b}$ nach $\mathfrak{a}$, wenn die Determinante

$$\sum \pm k_{1,1} k_{2,2} \cdots k_{m,m}$$

von Null verschieden ist.

§ 6.

Norm eines Moduls in bezug auf einen andern.

Ist $(\lambda_1, \lambda_2, \cdots \lambda_m)$ ein beliebiges vollständiges Restsystem eines Moduls $\mathfrak{b}$ in bezug auf einen andern $\mathfrak{a}$, so ergibt sich, weil $z\mathfrak{b}$ durch $\mathfrak{b}$

teilbar ist, ein ganz bestimmtes System von m^2 Konstanten $c_{h,k}$, durch welches die Kongruenzen erfüllt werden:

$$\left.\begin{array}{l} z\lambda_1 \equiv c_{1,1}\,\lambda_1 + c_{2,1}\,\lambda_2 + \cdots + c_{m,1}\,\lambda_m \\ z\lambda_2 \equiv c_{1,2}\,\lambda_1 + c_{2,2}\,\lambda_2 + \cdots + c_{m,2}\,\lambda_m \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z\lambda_m \equiv c_{1,m}\,\lambda_1 + c_{2,m}\,\lambda_2 + \cdots + c_{m,m}\,\lambda_m \end{array}\right\} (\text{mod. } \mathfrak{a})$$

und durch Auflösung dieses Systems erkennt man, daß jede Funktion λ_ι, und mithin jede Funktion β des Moduls $\mathfrak{b}$ durch Multiplikation mit der ganzen rationalen Funktion m^{ten} Grades von z

$$(\mathfrak{b}, \mathfrak{a}) = (-1)^m \begin{vmatrix} c_{1,1} - z, & c_{2,1}, & \cdots & c_{m,1} \\ c_{1,2}, & c_{2,2} - z, & \cdots & c_{m,2} \\ \cdot & \cdot & \cdots & \cdot \\ c_{1,m}, & c_{2,m}, & \cdots & c_{m,m} - z \end{vmatrix}$$

in eine Funktion des Moduls $\mathfrak{a}$ verwandelt wird. Diese Funktion $(\mathfrak{b}, \mathfrak{a})$ ist, wie sich aus dem Multiplikationssatz der Determinanten leicht ergibt, von der Wahl der Basis $\lambda_1, \lambda_2, \cdots \lambda_m$ unabhängig, also nur von den beiden Moduln $\mathfrak{a}$, $\mathfrak{b}$ abhängig und soll die Norm von $\mathfrak{a}$ in bezug auf $\mathfrak{b}$ genannt werden.

Ist jede Funktion in $\mathfrak{b}$ zugleich in $\mathfrak{a}$ enthalten, also $\mathfrak{b}$ durch $\mathfrak{a}$ teilbar, so ist $m = 0$ und $(\mathfrak{b}, \mathfrak{a}) = 1$ zu setzen. Wenn dagegen $\mathfrak{b}$ nicht, wie oben angenommen, eine endliche Anzahl in bezug auf $\mathfrak{a}$ linear unabhängiger Funktionen enthält, dann soll festgesetzt werden, daß $(\mathfrak{b}, \mathfrak{a}) = 0$ sei.

1. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{d}$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, so ist jede Kongruenz zwischen Funktionen des Moduls $\mathfrak{d}$ in bezug auf den Modul $\mathfrak{a}$ vollkommen gleichbedeutend mit der Kongruenz derselben Funktionen nach dem Modul $\mathfrak{m}$; andererseits ist jede Funktion in $\mathfrak{b}$ einer Funktion in $\mathfrak{d}$ und umgekehrt jede Funktion in $\mathfrak{d}$ einer Funktion in $\mathfrak{b}$ kongruent nach dem Modul $\mathfrak{a}$. Aus diesen Bemerkungen ergibt sich sofort der wichtige Satz:

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = (\mathfrak{d}, \mathfrak{a}),$$

welcher auch richtig bleibt, wenn $(\mathfrak{b}, \mathfrak{a}) = 0$ ist.

2. Ist der Modul $\mathfrak{a}$ teilbar durch den Modul $\mathfrak{b}$, dieser durch den dritten Modul $\mathfrak{c}$, so ist

$$(\mathfrak{c}, \mathfrak{a}) = (\mathfrak{c}, \mathfrak{b})(\mathfrak{b}, \mathfrak{a}).$$

Der Satz ist offenbar richtig, wenn von den beiden Normen $(\mathfrak{c}, \mathfrak{b})$, $(\mathfrak{b}, \mathfrak{a})$ eine verschwindet. Ist dies nicht der Fall und ist

$$\mathfrak{c} \equiv (\varrho_1, \varrho_2, \cdots \varrho_r) \; (\text{mod. } \mathfrak{b}),$$
$$\mathfrak{b} \equiv (\lambda_1, \lambda_2, \cdots \lambda_s) \; (\text{mod. } \mathfrak{a}),$$

so sind die Funktionen $\varrho_1, \varrho_2, \cdots \varrho_r, \lambda_1, \lambda_2, \cdots \lambda_s$ zusammengenommen linear unabhängig nach dem Modul $\mathfrak{a}$; denn ist

$$\sum^{\iota} c_\iota \varrho_\iota + \sum^{\iota} c'_\iota \lambda_\iota \equiv 0 \; (\text{mod. } \mathfrak{a}),$$

so folgt, da $\mathfrak{a}$ durch $\mathfrak{b}$ teilbar ist und die Funktionen λ_ι in $\mathfrak{b}$ enthalten sind,

$$\sum^{\iota} c_\iota \varrho_\iota \equiv 0 \; (\text{mod. } \mathfrak{b}), \text{ mithin } c_\iota = 0,$$
$$\sum^{\iota} c'_\iota \lambda_\iota \equiv 0 \; (\text{mod. } \mathfrak{a}), \text{ mithin } c'_\iota = 0.$$

Da ferner jede Funktion γ in $\mathfrak{c}$ einer Kongruenz von der Form genügt:

$$\gamma \equiv \sum c_\iota \varrho_\iota + \sum c'_\iota \lambda_\iota \; (\text{mod. } \mathfrak{a}),$$

so ist die $(r+s)$-fache Schar $(\varrho_1, \varrho_2, \cdots \varrho_r, \lambda_1, \lambda_2, \cdots \lambda_s)$ ein vollständiges Restsystem von $\mathfrak{c}$ nach $\mathfrak{a}$, oder

$$\mathfrak{c} \equiv (\varrho_1, \varrho_2, \cdots \varrho_r, \lambda_1, \lambda_2, \cdots \lambda_s) \; (\text{mod. } \mathfrak{a}).$$

Ist daher

$$\begin{aligned} z\varrho_1 &= e_{1,1}\varrho_1 + \cdots + e_{r,1}\varrho_r + \beta_1 \\ &\cdots\cdots\cdots\cdots \\ z\varrho_r &= e_{1,r}\varrho_1 + \cdots + e_{r,r}\varrho_r + \beta_r, \end{aligned}$$

worin die $e_{\iota,\varkappa}$ Konstanten, die β_ι Funktionen in $\mathfrak{b}$ sind, also:

$$(\mathfrak{c}, \mathfrak{b}) = (-1)^r \begin{vmatrix} e_{1,1} - z, & \cdots & e_{r,1} \\ \cdots & \cdots & \cdots \\ e_{1,r}, & \cdots & e_{r,r} - z \end{vmatrix},$$

ferner:

$$\left.\begin{aligned} \beta_1 &\equiv h_{1,1}\lambda_1 + \cdots + h_{s,1}\lambda_s \\ &\cdots\cdots\cdots\cdots \\ \beta_r &\equiv h_{1,r}\lambda_1 + \cdots + h_{s,r}\lambda_s \\ z\lambda_1 &\equiv c_{1,1}\lambda_1 + \cdots + c_{s,1}\lambda_s \\ &\cdots\cdots\cdots\cdots \\ z\lambda_s &\equiv c_{1,s}\lambda_1 + \cdots + c_{s,s}\lambda_s \end{aligned}\right\} (\text{mod. } \mathfrak{a})$$

mit konstanten Koeffizienten $h_{\iota,\varkappa}$, $c_{\iota,\varkappa}$, also

$$(\mathfrak{b}, \mathfrak{a}) = (-1)^s \begin{vmatrix} c_{1,1} - z, & \cdots & c_{s,1} \\ \cdots & \cdots & \cdots \\ c_{1,s}, & \cdots & c_{s,s} - z \end{vmatrix},$$

so folgt:

$$\left.\begin{array}{l} z\varrho_1 \equiv e_{1,1}\varrho_1 + \cdots + e_{r,1}\varrho_r + h_{1,1}\lambda_1 + \cdots + h_{s,1}\lambda_s \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z\varrho_r \equiv e_{1,r}\varrho_1 + \cdots + e_{r,r}\varrho_r + h_{1,r}\lambda_1 + \cdots + h_{s,r}\lambda_s \\ z\lambda_1 \equiv \qquad\qquad\qquad\qquad c_{1,1}\lambda_1 + \cdots + c_{s,1}\lambda_s \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z\lambda_s \equiv \qquad\qquad\qquad\qquad c_{1,s}\lambda_1 + \cdots + c_{s,s}\lambda_s \end{array}\right\} \pmod{\mathfrak{a}}$$

und hieraus

$$(\mathfrak{c},\mathfrak{a}) = (-1)^{r+s}\begin{vmatrix} e_{1,1}-z, & \cdots e_{r,1}, & h_{1,1}, & \cdots h_{s,1} \\ \cdots & \cdots & \cdots & \cdots \\ e_{1,r}, & \cdots e_{r,r}-z, & h_{1,r}, & \cdots h_{s,r} \\ 0 & \cdots 0 & c_{1,1}-z, & \cdots c_{s,1} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots 0 & c_{1,s}, & \cdots c_{s,s}-z \end{vmatrix} = (\mathfrak{c},\mathfrak{b})\,(\mathfrak{b},\mathfrak{a}).$$

3. Wenn die Basis-Funktionen $\beta_1, \beta_2, \cdots \beta_s$ eines endlichen Moduls $\mathfrak{b} = [\beta_1, \beta_2, \cdots \beta_s]$ durch Multiplikation mit von Null verschiedenen ganzen rationalen Funktionen von z in Funktionen eines Moduls $\mathfrak{a}$ verwandelt werden können, so ist die Norm von $\mathfrak{a}$ in bezug auf $\mathfrak{b}$, $(\mathfrak{b},\mathfrak{a})$ von Null verschieden. Zugleich ist das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ ein endlicher Modul $\mathfrak{m}$, von dem eine irreduktible Basis in der Form angenommen werden kann:

$$\begin{aligned} \mu_1 &= a_{1,1}\beta_1, \\ \mu_2 &= a_{1,2}\beta_1 + a_{2,2}\beta_2, \\ &\cdots\cdots\cdots\cdots\cdots \\ \mu_s &= a_{1,s}\beta_1 + a_{2,s}\beta_2 + \cdots + a_{s,s}\beta_s, \end{aligned}$$

worin die Koeffizienten $a_{\iota,\varkappa}$ ganze rationale Funktionen von z sind, und zwar so, daß

$$(\mathfrak{b},\mathfrak{a}) = a_{1,1}\,a_{2,2}\cdots a_{s,s}.$$

Zum Beweise dieses wichtigen Theorems nehmen wir an, es sei $\mathfrak{a}_1$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $[\beta_1]$, $\mathfrak{a}_2$ der von $\mathfrak{a}_1$ und $[\beta_2]$ u. s. f., so daß $\mathfrak{a}_r$ der Inbegriff aller Funktionen von der Form

$$\alpha_r = \alpha + y_1\beta_1 + \cdots + y_r\beta_r$$

ist, wo α eine Funktion in $\mathfrak{a}$, $y_1, \cdots y_r$ ganze rationale Funktionen von z sind. Es ist dann $\mathfrak{a}_s$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$. Da nun jeder Modul $\mathfrak{a}_r$ durch den folgenden $\mathfrak{a}_{r+1}$ teilbar ist, so folgt aus 1. und 2.

$$(\mathfrak{b},\mathfrak{a}) = (\mathfrak{a}_s,\mathfrak{a}) = (\mathfrak{a}_s,\mathfrak{a}_{s-1})\,(\mathfrak{a}_{s-1},\mathfrak{a}_{s-2})\cdots(\mathfrak{a}_1,\mathfrak{a}),$$

und es handelt sich also noch um die Bestimmung von $(\mathfrak{a}_r, \mathfrak{a}_{r-1})$. Es ist aber

$$\alpha_r = \alpha_{r-1} + y_r \beta_r \equiv y_r \beta_r \pmod{\mathfrak{a}_{r-1}},$$

und nach der Voraussetzung gibt es eine von Null verschiedene ganze rationale Funktion x_r von z, für welche

$$x_r \beta_r \equiv 0 \pmod{\mathfrak{a}},$$

also auch

$$x_r \beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}}.$$

Ist nun $a_{r,r}$ unter allen der letzteren Kongruenz genügenden Funktionen x_r eine von möglichst niedrigem Grade m_r, die zugleich so angenommen sei, daß der Koeffizient der höchsten Potenz von $z = 1$ ist, so sind alle andern dieser Kongruenz genügenden Funktionen x_r durch $a_{r,r}$ teilbar; denn es ist für ein beliebiges ganzes rationales q

$$(x_r - q\, a_{r,r})\, \beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}},$$

und wenn x_r nicht durch $a_{r,r}$ teilbar ist, so läßt sich q so wählen, daß $x_r - q\, a_{r,r}$ von niedrigerem Grade wird als $a_{r,r}$, gegen die Voraussetzung.

Setzt man also

$$y_r = q\, a_{r,r} + b_{r,r}$$

und bestimmt q so, daß der Grad von $b_{r,r}$ kleiner als m_r wird, so folgt:

$$\alpha_r \equiv b_{r,r} \beta_r \pmod{\mathfrak{a}_{r-1}}$$

und hieraus

$$\mathfrak{a}_r \equiv (\beta_r, z\beta_r, \cdots z^{m_r-1} \beta_r) \pmod{\mathfrak{a}_{r-1}}.$$

Wenn man daher für den Augenblick setzt:

$$\begin{aligned} a_{r,r} &= c_0 + c_1 z + \cdots + c_{m_r-1} z^{m_r-1} + z^{m_r}, \\ \lambda_k &= z^{k-1} \beta_r, \end{aligned}$$

so folgt:

$$z\lambda_1 = \lambda_2,\ z\lambda_2 = \lambda_3 \cdots$$

$$z\lambda_{m_r} \equiv -c_0 \lambda_1 - c_1 \lambda_2 - \cdots - c_{m_r-1} \lambda_{m_r} \pmod{\mathfrak{a}_{r-1}}$$

also:

$$(\mathfrak{a}_r, \mathfrak{a}_{r-1}) = (-1)^{m_r} \begin{vmatrix} -z, & 1, & 0, & \cdots & 0 \\ 0, & -z, & 1, & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & 0, & \cdots & 1 \\ -c_0, & -c_1, & -c_2, & \cdots -c_{m_r-1} & -z \end{vmatrix} = a_{r,r}.$$

Hieraus ergibt sich wie in 2., daß das Funktionensystem

$$\begin{array}{l} \beta_1, z\beta_1, \cdots z^{m_1-1}\beta_1, \\ \beta_2, z\beta_2, \cdots z^{m_2-1}\beta_2, \\ \cdots\cdots\cdots\cdots \\ \beta_s, z\beta_s, \cdots z^{m_s-1}\beta_s, \end{array}$$

eine Basis eines vollständigen Restsystems von $\mathfrak{b}$ nach $\mathfrak{a}$ bildet, und daß

$$(\mathfrak{b}, \mathfrak{a}) = a_{1,1}\, a_{2,2} \cdots a_{s,s}$$

vom Grade

$$m = m_1 + m_2 + \cdots + m_s$$

ist.

Da nun $a_{r,r}\,\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}}$, so läßt sich eine Funktion μ_r in $\mathfrak{a}$ und ganze rationale Funktionen $a_{k,r}$ so bestimmen, daß

$$\mu_r = a_{1,r}\,\beta_1 + a_{2,r}\,\beta_2 + \cdots + a_{r,r}\,\beta_r$$

wird; die auf diese Weise bestimmten Funktionen

$$\begin{array}{l} \mu_1 = a_{1,1}\,\beta_1, \\ \mu_2 = a_{1,2}\,\beta_1 + a_{2,2}\,\beta_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \mu_s = a_{1,s}\,\beta_1 + a_{2,s}\,\beta_2 + \cdots + a_{s,s}\,\beta_s \end{array}$$

sind, da keine der Funktionen $a_{1,1}, \cdots a_{s,s}$ verschwindet, rational unabhängig und sind sämtlich zugleich in $\mathfrak{a}$ und in $\mathfrak{b}$, also auch in dem kleinsten gemeinschaftlichen Vielfachen $\mathfrak{m}$ dieser beiden Moduln enthalten. Es ist noch nachzuweisen, daß dieselben eine Basis von $\mathfrak{m}$ bilden.

Es sei $\mathfrak{m}_r$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $[\beta_1, \beta_2, \cdots \beta_r]$, $\mathfrak{m}_s = \mathfrak{m}$, so daß unter den Moduln $\mathfrak{m}_1, \mathfrak{m}_2, \cdots \mathfrak{m}_s$ jeder durch alle folgenden, als auch durch $\mathfrak{m}$ teilbar ist, und

$$\nu_r = z_1\,\beta_1 + z_2\,\beta_2 + \cdots + z_r\,\beta_r$$

eine Funktion in $\mathfrak{m}_r$, also auch in $\mathfrak{a}$.

Es ist hiernach

$$z_r\,\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}},$$

also

$$z_r = x_r\,a_{r,r},$$

worin x_r eine ganze rationale Funktion bedeutet. Daher ist

$$\nu_r - x_r\,\mu_r \equiv 0 \pmod{\mathfrak{m}_{r-1}}, \quad \nu_1 - x_1\,\mu_1 = 0,$$

woraus folgt:

$$\nu_r = x_1\,\mu_1 + x_2\,\mu_2 + \cdots + x_r\,\mu_r,$$

also:

$$\begin{array}{l} \mathfrak{m}_r = [\mu_1, \mu_2, \cdots \mu_r], \\ \mathfrak{m} \;= [\mu_1, \mu_2, \cdots \mu_s], \end{array}$$

w. z. b. w.

Hiernach enthält eine irreduktible Basis des Moduls $\mathfrak{m}$ genau ebenso viele Funktionen wie eine irreduktible Basis von $\mathfrak{b}$. Wählt man statt der Basis $\mu_1, \mu_2, \cdots \mu_s$ eine andere $\mu'_1, \mu'_2 \cdots \mu'_s$, so läßt sich $\mu'_1, \mu'_2, \cdots \mu'_s$ in der Form ausdrücken

$$\mu'_k = a'_{1,k}\beta_1 + a'_{2,k}\beta_2 + \cdots + a'_{s,k}\beta_s$$

mit ganzen rationalen Koeffizienten $a'_{\iota,k}$, und aus § 4, 2. ergibt sich

$$(\mathfrak{b}, \mathfrak{a}) = \text{konst.} \sum \pm a'_{1,1} a'_{2,2} \cdots a'_{s,s}.$$

4. Machen wir insbesondere die Annahme, es sei $\mathfrak{a}$ gleichfalls ein endlicher Modul, der eine irreduktible Basis von ebenso vielen Funktionen besitzt wie $\mathfrak{b}$, und es sei außerdem $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, dann lassen sich, wenn

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots \alpha_s]$$

ist, die ganzen rationalen Funktionen $\mathfrak{b}_{\iota,k}$ von z so bestimmen, daß

$$\alpha_k = b_{1,k}\beta_1 + b_{2,k}\beta_2 + \cdots + b_{s,k}\beta_s,$$

und die Voraussetzung von 3., daß die Funktionen β_ι durch Multiplikation mit ganzen rationalen Funktionen von z in Funktionen des Moduls $\mathfrak{a}$ verwandelt werden können, ist erfüllt, wie man durch Auflösung dieses Gleichungssystems erkennt. Zugleich ist hier $\mathfrak{a}$ selbst das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$, und daraus ergibt sich

$$(\mathfrak{b}, \mathfrak{a}) = \text{konst.} \sum \pm b_{1,1} b_{2,2} \ldots b_{n,n}.$$

5. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ und ν eine beliebige Funktion in Ω, so ist, wie sich aus der Definition ohne Schwierigkeit ergibt, $\nu\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache von $\nu\mathfrak{a}$ und $\nu\mathfrak{b}$. Ist $(\mathfrak{b}, \mathfrak{a}) = 0$, so ist auch $(\nu\mathfrak{b}, \nu\mathfrak{a}) = 0$. Ist aber $(\mathfrak{b}, \mathfrak{a})$ und ν von Null verschieden, so ergibt sich

$$(\nu\mathfrak{b}, \nu\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a}),$$

wenn man in 3. die Basis-Funktionen μ_ι, β_ι von $\mathfrak{m}$ und $\mathfrak{b}$ durch $\nu\mu_\iota$, $\nu\beta_\iota$ ersetzt.

§ 7.

Die Ideale in $\mathfrak{o}$.

Ein System $\mathfrak{a}$ von ganzen Funktionen von z im Körper Ω heißt ein Ideal, wenn es die beiden folgenden Bedingungen erfüllt:

I. Summe und Differenz je zweier Funktionen in $\mathfrak{a}$ ergeben wieder eine Funktion in $\mathfrak{a}$.

II. Das Produkt einer jeden Funktion in $\mathfrak{a}$ mit einer jeden Funktion in $\mathfrak{o}$ (§ 3) ist wieder eine Funktion in $\mathfrak{a}$.

Jedes Ideal ist also zugleich ein Modul und alle für die Moduln erklärten Begriffe und Bezeichnungen können auf die Ideale angewandt werden.

Der Modul $\mathfrak{o}$ (das System aller ganzen Funktionen von z) ist selbst ein Ideal, und jedes Ideal ist durch $\mathfrak{o}$ teilbar. Ebenso ist, wenn μ eine beliebige von Null verschiedene Funktion von $\mathfrak{o}$ bedeutet, der Modul $\mathfrak{o}\mu$ (das System aller durch μ teilbaren ganzen Funktionen) ein Ideal. Ein solches Ideal soll ein Hauptideal genannt werden. Ist $\omega_1, \omega_2, \ldots \omega_n$ eine Basis von $\mathfrak{o}$, so ist

$$\mathfrak{o}\mu = [\omega_1\mu, \omega_2\mu, \ldots \omega_n\mu]$$

und $\mathfrak{o}\mu$ ist das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}$ und $\mathfrak{o}\mu$. Daher ist nach § 6, 4. und nach der Definition (4.) in § 2:

$$(1) \qquad (\mathfrak{o}, \mathfrak{o}\mu) = \text{konst.}\, N(\mu)$$

und mithin von Null verschieden.

Ist $\mathfrak{a}$ irgend ein Ideal und α eine beliebige Funktion in $\mathfrak{a}$, so ist (wegen II.) das Hauptideal $\mathfrak{o}\alpha$ teilbar durch $\mathfrak{a}$, und mithin nach § 6, 2.:

$$(2) \qquad (\mathfrak{o}, \mathfrak{o}\alpha) = (\mathfrak{o}, \mathfrak{a})\,(\mathfrak{a}, \mathfrak{o}\alpha),$$

mithin auch $(\mathfrak{o}, \mathfrak{a})$ von Null verschieden. Da nun wieder $\mathfrak{a}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}$ ist, so besitzt $\mathfrak{a}$ nach § 6, 3. eine irreduktible Basis, welche aus n ganzen Funktionen $\alpha_1, \alpha_2, \ldots \alpha_n$ besteht, die demnach auch eine Basis des Körpers Ω bilden.

Die Norm von $\mathfrak{a}$ in bezug auf $\mathfrak{o}$, d. h. die ganze rationale Funktion $(\mathfrak{o}, \mathfrak{a})$ von z soll die Norm des Ideals $\mathfrak{a}$ genannt und mit $N(\mathfrak{a})$ bezeichnet werden. Der Grad dieser ganzen rationalen Funktion heißt zugleich der Grad des Ideals $\mathfrak{a}$.

Ist

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots \alpha_n], \quad \mathfrak{o} = [\omega_1, \omega_2, \ldots \omega_n]$$

und

$$\begin{aligned}
\alpha_1 &= a_{1,1}\omega_1 + a_{2,1}\omega_2 + \cdots + a_{n,1}\omega_n, \\
\alpha_2 &= a_{1,2}\omega_1 + a_{2,2}\omega_2 + \cdots + a_{n,2}\omega_n, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha_n &= a_{1,n}\omega_1 + a_{2,n}\omega_2 + \cdots + a_{n,n}\omega_n
\end{aligned}$$

mit ganzen rationalen Koeffizienten $a_{\iota,\varkappa}$, so ergibt sich aus § 6, 4.:

$$(3) \qquad N(\mathfrak{a}) = \text{konst.} \sum \pm a_{1,1}\, a_{2,2} \cdots a_{n,n}.$$

Da jede Funktion in $\mathfrak{o}$, also auch die Funktion „1“ durch Multiplikation mit $N(\mathfrak{a})$ in eine Funktion des Ideals $\mathfrak{a}$ verwandelt wird, so ist $N(\mathfrak{a})$ stets eine Funktion in $\mathfrak{a}$.

Die Norm des Ideals $\mathfrak{o}$ ist gleich 1 und umgekehrt ist $\mathfrak{o}$ das einzige Ideal, welches diese Eigenschaft hat. Auch ist $\mathfrak{o}$ das einzige Ideal, welches die Funktion „1“ (oder eine Konstante) enthält.

Ist α eine Funktion in $\mathfrak{a}$, so folgt aus (1), (2), (3):

$$(4) \qquad N(\alpha) = \text{konst.}\, N(\mathfrak{a})\, (\mathfrak{a}, \mathfrak{o}\alpha),$$

d. h. die Norm einer jeden in $\mathfrak{a}$ enthaltenen Funktion ist durch die Norm von $\mathfrak{a}$ teilbar.

Für die Kongruenzen in bezug auf einen Idealmodul gilt der folgende Satz, welcher die Ideale wesentlich von den allgemeinen Moduln unterscheidet.

Sind μ, μ_1, ν, ν_1 Funktionen in $\mathfrak{o}$, welche den Kongruenzen genügen

$$\mu \equiv \mu_1, \quad \nu \equiv \nu_1 \pmod{\mathfrak{a}},$$

so ist auch

$$\mu\nu \equiv \mu_1\nu_1 \pmod{\mathfrak{a}}.$$

§ 8.

Multiplikation und Teilung der Ideale.

Aus den Grundeigenschaften I., II. der Ideale und aus den Begriffsbestimmungen in § 4 ergibt sich zunächst:

1. Das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler, das Produkt von zwei (und also auch von beliebig vielen) Idealen sind selbst Ideale. Ebenso ist, wenn ν eine Funktion in $\mathfrak{o}$, $\mathfrak{a}$ ein Ideal ist, das Produkt $\mathfrak{a}\nu$ ein Ideal.

2. Das Produkt aus mehreren Idealen ist durch jeden seiner Faktoren teilbar, und es ist für jedes Ideal $\mathfrak{a}$.

$$\mathfrak{a}\mathfrak{o} = \mathfrak{a};$$

denn nach I., II. ist jede Funktion in $\mathfrak{a}\mathfrak{o}$ zugleich eine Funktion in $\mathfrak{a}$, und, da $\mathfrak{o}$ die Funktion „1“ enthält, auch umgekehrt jede Funktion in $\mathfrak{a}$ zugleich eine Funktion in $\mathfrak{a}\mathfrak{o}$.

3. Ein Hauptideal $\mathfrak{o}\mu$ ist dann und nur dann teilbar durch ein Hauptideal $\mathfrak{o}\nu$, wenn die ganze Funktion μ teilbar ist durch die ganze Funktion ν.

Wir fügen noch folgende Definitionen hinzu:

4. Definition. Eine Funktion α in $\mathfrak{o}$ soll durch das Ideal $\mathfrak{a}$ teilbar heißen, wenn das Hauptideal $\mathfrak{o}\alpha$ durch $\mathfrak{a}$ teilbar, oder, was dasselbe sagt, wenn α eine Funktion in $\mathfrak{a}$ ist.

5. Definition. Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ heißen relativ prim, wenn ihr größter gemeinschaftlicher Teiler $\mathfrak{o}$ ist. Die notwendige und hinreichende Bedingung dafür ist, daß in $\mathfrak{a}$ eine Funktion α, in $\mathfrak{b}$ eine Funktion β existiert der Art, daß

$$\alpha + \beta = 1,$$

oder, anders ausgedrückt, daß in $\mathfrak{a}$ eine der Kongruenz $\alpha \equiv 1 \pmod{\mathfrak{b}}$ oder in $\mathfrak{b}$ eine der Kongruenz $\beta \equiv 1 \pmod{\mathfrak{a}}$ genügende Funktion existiert.

6. Definition. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$ heißt ein Primideal, wenn kein anderes Ideal außer $\mathfrak{p}$ und $\mathfrak{o}$ in $\mathfrak{p}$ aufgeht.

Auf Grund dieser Definitionen ergeben sich nun die folgenden Sätze über die Teilbarkeit der Ideale.

7. Sind $\mathfrak{a}, \mathfrak{b}$ zwei Ideale mit dem kleinsten gemeinschaftlichen Vielfachen $\mathfrak{m}$ und dem größten gemeinschaftlichen Teiler $\mathfrak{d}$, so folgt aus § 6, 1., 2.

$$N(\mathfrak{m}) = N(\mathfrak{b})\,(\mathfrak{b}, \mathfrak{m}) = N(\mathfrak{b})\,(\mathfrak{b}, \mathfrak{a}),$$
$$N(\mathfrak{a}) = N(\mathfrak{d})\,(\mathfrak{d}, \mathfrak{a}) = N(\mathfrak{d})\,(\mathfrak{b}, \mathfrak{a}),$$

folglich $(\mathfrak{b}, \mathfrak{a})$ von Null verschieden und

$$N(\mathfrak{a})\,N(\mathfrak{b}) = N(\mathfrak{m})\,N(\mathfrak{d}).$$

8. Ist das Ideal $\mathfrak{a}$ teilbar durch das Ideal $\mathfrak{b}$, so ist, nach § 6, 2.

$$N(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})\,N(\mathfrak{b}),$$

also $N(\mathfrak{a})$ teilbar durch $N(\mathfrak{b})$.

Ist insbesondere $(\mathfrak{b}, \mathfrak{a}) = 1$, so ist auch $\mathfrak{b}$ teilbar durch $\mathfrak{a}$, und es folgt:

9. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$ und ist zugleich $N(\mathfrak{a}) = N(\mathfrak{b})$, so ist $\mathfrak{a} = \mathfrak{b}$, d. h. beide Ideale sind identisch.

10. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{a}_1$, $\mathfrak{b}$ durch $\mathfrak{b}_1$, so ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}_1 \mathfrak{b}_1$ (§ 4, 7.).

11. Ist ein Ideal $\mathfrak{a}$ teilbar durch ein Hauptideal $\mathfrak{o}\mu$, so sind alle Funktionen in $\mathfrak{a}$ von der Form $\beta\mu$, und der Inbegriff der Funktionen β ist wieder ein Ideal $\mathfrak{b}$, so daß man setzen kann

$$\mathfrak{a} = \mu\mathfrak{b}.$$

12. Ist μ eine beliebige von Null verschiedene Funktion in $\mathfrak{o}$ und das Ideal $\mathfrak{a}\mu$ teilbar durch das Ideal $\mathfrak{b}\mu$, so ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, und aus $\mathfrak{a}\mu = \mathfrak{b}\mu$ folgt $\mathfrak{a} = \mathfrak{b}$.

13. Das kleinste gemeinschaftliche Vielfache zweier Ideale $\mathfrak{a}$, $\mathfrak{o}\nu$, davon eines ein Hauptideal ist, hat nach 11. die Form $\mathfrak{r}\nu$, worin $\mathfrak{r}$ ein Ideal ist. Da andererseits $\mathfrak{a}\nu$ ein gemeinschaftliches Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\nu$, also durch $\mathfrak{r}\nu$ teilbar ist, so ist nach 12. $\mathfrak{r}$ ein Teiler von $\mathfrak{a}$.

14. Ist $\mathfrak{a}$ ein Ideal, ν eine Funktion in $\mathfrak{o}$, so ist nach § 6, 2., 5.:

$$(\mathfrak{o}, \mathfrak{a}\nu) = (\mathfrak{o}, \mathfrak{o}\nu)\,(\mathfrak{o}\nu, \mathfrak{a}\nu) = (\mathfrak{o}, \mathfrak{o}\nu)\,(\mathfrak{o}, \mathfrak{a}),$$

also

$$N(\mathfrak{a}\nu) = \text{konst.}\, N(\mathfrak{a})\, N(\nu).$$

Ist also $\mathfrak{r}\nu$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{d}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{a}$, $\mathfrak{o}\nu$, so ergibt sich aus 7.

$$N(\mathfrak{a}) = N(\mathfrak{r})\, N(\mathfrak{d}).$$

15. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ ist durch ein Primideal $\mathfrak{p}$ teilbar.

Ist nämlich $\mathfrak{a}$ kein Primideal, so hat es mindestens einen von $\mathfrak{o}$ verschiedenen echten Teiler, und von diesen sei $\mathfrak{p}$ ein solcher, dessen Norm von möglichst niedrigem Grade ist. Dieser kann keinen von $\mathfrak{o}$ verschiedenen echten Teiler $\mathfrak{p}'$ haben, denn es wäre auch $\mathfrak{p}'$ ein Teiler von $\mathfrak{a}$ und zugleich (nach 8.) $N(\mathfrak{p}')$ von niedrigerem Grade als $N(\mathfrak{p})$. Dies widerspricht der Voraussetzung über $\mathfrak{p}$, und folglich ist $\mathfrak{p}$ ein Primideal.

16. Ist $\mathfrak{a}$ relativ prim zu $\mathfrak{b}$, so ist $\mathfrak{a}\mathfrak{b}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$, und folglich ist jedes durch $\mathfrak{a}$ und durch $\mathfrak{b}$ teilbare Ideal auch durch das Produkt $\mathfrak{a}\mathfrak{b}$ teilbar.

Denn nach Voraussetzung gibt es in $\mathfrak{a}$, $\mathfrak{b}$ zwei Funktionen α_1, β_1 der Art, daß

$$\alpha_1 + \beta_1 = 1$$

ist (5.). Ist andererseits $\alpha = \beta$ eine Funktion des kleinsten gemeinschaftlichen Vielfachen $\mathfrak{m}$ von $\mathfrak{a}$ und $\mathfrak{b}$, so ist hiernach

$$\alpha = \beta = \alpha_1 \beta + \alpha \beta_1,$$

also eine Funktion in $\mathfrak{a}\mathfrak{b}$. Es ist demnach $\mathfrak{m}$ teilbar durch $\mathfrak{a}\mathfrak{b}$, und da umgekehrt (zufolge 2.) $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{m}$ teilbar ist, so ist $\mathfrak{m}$ mit $\mathfrak{a}\mathfrak{b}$ identisch, und aus 7. folgt noch für diesen Fall

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\, N(\mathfrak{b}).$$

17. Ist $\mathfrak{a}$ ein beliebiges Ideal, $\mathfrak{p}$ ein Primideal, so ist entweder $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar oder $\mathfrak{a}$ relativ prim zu $\mathfrak{p}$; denn da $\mathfrak{p}$ keinen anderen Teiler hat als $\mathfrak{o}$ und $\mathfrak{p}$, so kann auch der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{p}$ kein anderer sein als $\mathfrak{o}$ oder $\mathfrak{p}$.

18. Ist $\mathfrak{a}$ relativ prim zu $\mathfrak{b}$ und zu $\mathfrak{c}$, so ist $\mathfrak{a}$ auch relativ prim zu $\mathfrak{b}\mathfrak{c}$.

Nach Voraussetzung (5.) gibt es in $\mathfrak{b}$, $\mathfrak{c}$ zwei den Kongruenzen

$$\beta \equiv 1, \quad \gamma \equiv 1 \pmod{\mathfrak{a}}$$

genügende Funktionen, folglich nach § 7

$$\beta\gamma \equiv 1 \pmod{\mathfrak{a}}.$$

Da $\beta\gamma$ in $\mathfrak{b}\mathfrak{c}$ enthalten ist, so ist hiermit die Behauptung erwiesen.

Es folgt hieraus noch, daß, falls das Produkt $\mathfrak{a}\mathfrak{b}$ durch ein Primideal teilbar ist, wenigstens einer der beiden Faktoren $\mathfrak{a}$, $\mathfrak{b}$ durch $\mathfrak{p}$ teilbar sein muß, und, auf Hauptideale angewandt, daß, wenn das Produkt zweier ganzen Funktionen, $\mu\nu$, in $\mathfrak{p}$ enthalten ist, wenigstens der eine der beiden Faktoren μ, ν in $\mathfrak{p}$ enthalten sein muß.

19. Ist $\mathfrak{a}$ relativ prim zu $\mathfrak{c}$ und $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{c}$ teilbar, so ist $\mathfrak{b}$ durch $\mathfrak{c}$ teilbar. Nach Voraussetzung gibt es in $\mathfrak{a}$ eine Funktion α, welche der Kongruenz genügt

$$\alpha \equiv 1 \pmod{\mathfrak{c}}.$$

Ist nun β eine beliebige Funktion in $\mathfrak{b}$, so ist hiernach

$$\beta \equiv \alpha\beta \text{ und nach Vor. } \equiv 0 \pmod{\mathfrak{c}},$$

folglich β in $\mathfrak{c}$ enthalten, also $\mathfrak{b}$ durch $\mathfrak{c}$ teilbar.

§ 9.

Gesetze der Teilbarkeit der Ideale.

Alle diese Sätze, die sich meist unmittelbar aus der Definition der Ideale ergaben, reichen nicht aus, um die vollständige Analogie zu beweisen, die zwischen den Gesetzen der Teilbarkeit der Ideale und denen der ganzen rationalen Funktionen herrscht. Wir stützen uns bei diesem Beweis auf folgenden Satz:

1. Ist $\mathfrak{a}$ ein Ideal und k eine beliebige ganze rationale Funktion von z, so läßt sich in $\mathfrak{a}$ eine Funktion α so auswählen, daß $(\mathfrak{a}, \mathfrak{o}\alpha)$ mit k keinen Teiler gemeinschaftlich hat*).

Ist nämlich

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots \alpha_n],$$
$$\mathfrak{o} = [\omega_1, \omega_2, \ldots \omega_n],$$

*) Die Möglichkeit, diesen Satz schon an dieser Stelle zu beweisen, unterscheidet wesentlich die Theorie der algebraischen Funktionen von der der algebraischen Zahlen und gestattet bei ersterer eine nicht unerhebliche Vereinfachung im Vergleich mit letzterer.

und α eine beliebige Funktion in $\mathfrak{a}$, so lassen sich die ganzen rationalen Funktionen $x_{h,k}$ so bestimmen, daß

$$\begin{aligned}
\alpha\omega_1 &= x_{1,1}\alpha_1 + x_{2,1}\alpha_2 + \cdots + x_{n,1}\alpha_n,\\
\alpha\omega_2 &= x_{1,2}\alpha_1 + x_{2,2}\alpha_2 + \cdots + x_{n,2}\alpha_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\alpha\omega_n &= x_{1,n}\alpha_1 + x_{2,n}\alpha_2 + \cdots + x_{n,n}\alpha_n,
\end{aligned}$$

und es ist (§ 6, 4.)

$$(\mathfrak{a}, \mathfrak{o}\alpha) = \text{konst.} \sum \pm x_{1,1}\, x_{2,2} \cdots x_{n,n}.$$

Ist nun $\sum \pm x_{1,1}\, x_{2,2} \ldots x_{n,n}$ durch einen Linearfaktor $z - c$ von k teilbar, so läßt sich eine nicht durch $z - c$ teilbare Funktion ω in $\mathfrak{o}$ und eine Funktion α' in $\mathfrak{a}$ so bestimmen, daß

$$\alpha\omega = (z - c)\alpha' \text{*)}.$$

Setzt man nun, indem man unter t eine unbestimmte Konstante versteht:

$$t(z - c) - \omega = \omega',$$

so ist

$$N(\omega') = t^n(z-c)^n + a_1 t^{n-1}(z-c)^{n-1} + \cdots + a_{n-1}t(z-c) + a_n,$$

worin die von t unabhängigen Koeffizienten $a_1, a_2, \ldots a_n$ ganze rationale Funktionen von z sind. Es kann nun nicht zugleich a_1 durch $z - c$, a_2 durch $(z-c)^2, \ldots, a_n$ durch $(z-c)^n$ teilbar sein, weil sonst gegen die Voraussetzung $\dfrac{\omega}{z-c}$ eine ganze Funktion wäre (§ 2, 5., § 3, 4.). Daher lassen sich nicht alle Glieder von $N(\omega')$ durch $(z-c)^n$ teilen, und wenn also $(z-c)^{n-r}$ die höchste Potenz von $z - c$ ist, durch welche dieselben teilbar sind, so ist $r > 0$ und

$$\frac{N(\omega')}{(z-c)^{n-r}} = t^n(z-c)^r + b_1 t^{n-1} + \cdots + b_{n-1}t + b_n = f(t),$$

worin die ganzen rationalen Funktionen $b_1, b_2, \ldots b_n$ nicht alle für $z = c$ verschwinden. Es gibt daher nur eine endliche Anzahl von konstanten Werten t, für welche $f(t)$ durch $z - c$ teilbar ist. Ist

---

*) Wenn nämlich die Determinante $\Sigma \pm x_{1,1}\, x_{2,2} \cdots x_{n,n}$ durch $z - c$ teilbar ist, d. h. für $z = c$ verschwindet, so kann man ein System von Konstanten $c_1, c_2, \ldots c_n$, die nicht sämtlich verschwinden, so bestimmen, daß die ganzen rationalen Funktionen

$$c_1 x_{k,1} + c_2 x_{k,2} + \cdots + c_k x_{k,n} \qquad (k = 1, 2 \ldots n)$$

für $z = c$ verschwinden, also durch $z - c$ teilbar sind, und es ist dann

$$\omega = c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n$$

zu setzen.

$z - c'$ ein von $z - c$ verschiedener Linearfaktor von k, so wird $f(t)$ auch nur für eine endliche Anzahl von Werten t durch $z - c'$ teilbar. Daraus folgt, daß man über t so verfügen kann, daß $N(\omega')$ nicht durch $(z-c)^n$ und zugleich durch keinen anderen Linearfaktor von k teilbar wird *). Setzt man, wenn dies geschehen,

$$t\alpha - \alpha' = \alpha'',$$

welches ebenfalls eine Funktion in $\mathfrak{a}$ ist, so folgt

$$\alpha\omega' = (z-c)\alpha'',$$

$$N(\alpha'') = \frac{N(\alpha)\,N(\omega')}{(z-c)^n}$$

und mithin, da nach § 7, (4)

$$(\mathfrak{a}, \mathfrak{o}\alpha) = \text{konst.}\,\frac{N(\alpha)}{N(\mathfrak{a})}$$

ist:

$$(\mathfrak{a}, \mathfrak{o}\alpha'') = \text{konst.}\,\frac{(\mathfrak{a}, \mathfrak{o}\alpha)\,N(\omega')}{(z-c)^n}.$$

Die Funktion $(\mathfrak{a}, \mathfrak{o}\alpha'')$ enthält daher den Faktor $z - c$ mindestens einmal weniger als $(\mathfrak{a}, \mathfrak{o}\alpha)$, während sie zugleich keinen anderen Linearfaktor von k öfter enthält als $(\mathfrak{a}, \mathfrak{o}\alpha)$. Durch wiederholte Anwendung dieses Verfahrens ergibt sich die Richtigkeit des ausgesprochenen Satzes.

2. Jedes Ideal $\mathfrak{a}$ kann als größter gemeinschaftlicher Teiler zweier Hauptideale $\mathfrak{o}\mu$, $\mathfrak{o}\nu$ dargestellt werden, von denen das eine ganz beliebig, nur teilbar durch $\mathfrak{a}$, angenommen werden kann.

Beweis. Man wähle nach Belieben in $\mathfrak{a}$ eine von Null verschiedene Funktion ν, und eine zweite Funktion μ derart, daß die beiden Funktionen $(\mathfrak{a}, \mathfrak{o}\nu)$ und $(\mathfrak{a}, \mathfrak{o}\mu)$ keinen gemeinschaftlichen Teiler haben (nach 1.). Ist nun α eine beliebige Funktion in $\mathfrak{a}$, so ist nach § 6 $(\mathfrak{a}, \mathfrak{o}\mu)\alpha$ in $\mathfrak{o}\mu$, $(\mathfrak{a}, \mathfrak{o}\nu)\alpha$ in $\mathfrak{o}\nu$ enthalten, so daß es zwei Funktionen ω, ω' in $\mathfrak{o}$ gibt, für welche

$$(\mathfrak{a}, \mathfrak{o}\mu)\alpha = \mu\omega, \quad (\mathfrak{a}, \mathfrak{o}\nu)\alpha = \nu\omega'.$$

Wählt man daher, was nach der Voraussetzung über $(\mathfrak{a}, \mathfrak{o}\mu)$, $(\mathfrak{a}, \mathfrak{o}\nu)$ möglich ist, zwei ganze rationale Funktionen g, h von z, welche der Bedingung genügen

$$g(\mathfrak{a}, \mathfrak{o}\mu) + h(\mathfrak{a}, \mathfrak{o}\nu) = 1,$$

so folgt

$$\alpha = g\mu\omega + h\nu\omega',$$

*) Diese Schlüsse gelten in der analogen Frage der Zahlentheorie nicht mehr.

d. h. $\mathfrak{a}$ ist teilbar durch den größten gemeinschaftlichen Teiler von $\mathfrak{o}\,\mu$ und $\mathfrak{o}\,\nu$. Und da letzterer umgekehrt durch $\mathfrak{a}$ teilbar ist (weil $\mathfrak{o}\,\mu$ und $\mathfrak{o}\,\nu$ durch $\mathfrak{a}$ teilbar sind), so ist er gleich $\mathfrak{a}$, w. z. b. w.

3. Jedes Ideal $\mathfrak{a}$ kann durch Multiplikation mit einem Ideal $\mathfrak{m}$ in ein Hauptideal $\mathfrak{o}\,\mu = \mathfrak{a}\,\mathfrak{m}$ verwandelt werden.

Beweis. Man wähle (nach 1.) in $\mathfrak{a}$ eine Funktion μ so, daß $(\mathfrak{a}, \mathfrak{o}\,\mu)$ keinen Teiler mit $N(\mathfrak{a})$ gemein hat, hierauf eine zweite Funktion ν so, daß $(\mathfrak{a}, \mathfrak{o}\,\nu)$ mit $(\mathfrak{a}, \mathfrak{o}\,\mu)$ keinen Teiler gemein hat. Dann ist (nach 2.) $\mathfrak{a}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}\,\mu$ und $\mathfrak{o}\,\nu$. Das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\,\mu$ und $\mathfrak{o}\,\nu$ ist (nach § 8, 13) von der Form $\mathfrak{m}\,\nu$, worin $\mathfrak{m}$ ein Teiler von $\mathfrak{o}\,\mu$ ist. Nach § 8, 14 ist alsdann

$$N(\mathfrak{m}) = \frac{N(\mathfrak{o}\,\mu)}{N(\mathfrak{a})} = (\mathfrak{a}, \mathfrak{o}\,\mu),$$

also, nach Voraussetzung, ohne gemeinschaftlichen Teiler mit $N(\mathfrak{a})$. Bestimmt man also wieder zwei ganze rationale Funktionen g, h von z, so daß

$$g\,N(\mathfrak{m}) + h\,N(\mathfrak{a}) = 1,$$

so folgt aus § 8, 5, da $N(\mathfrak{m})$ in $\mathfrak{m}$, $N(\mathfrak{a})$ in $\mathfrak{a}$ enthalten ist, daß $\mathfrak{m}$ und $\mathfrak{a}$ relative Primideale sind, und daraus, nach § 8, 16.

$$N(\mathfrak{m}\,\mathfrak{a}) = N(\mathfrak{m})\,N(\mathfrak{a}) = N(\mathfrak{o}\,\mu).$$

Da nun $\mathfrak{o}\,\mu$ durch $\mathfrak{m}$ und durch $\mathfrak{a}$, also auch durch $\mathfrak{m}\,\mathfrak{a}$ teilbar ist (§ 8, 16.), so ist nach § 8, 9.

$$\mathfrak{m}\,\mathfrak{a} = \mathfrak{o}\,\mu,$$

w. z. b. w.*).

4. Ist ein Ideal $\mathfrak{c}$ teilbar durch ein Ideal $\mathfrak{a}$, so gibt es ein und nur ein Ideal $\mathfrak{b}$, welches der Bedingung

$$\mathfrak{a}\,\mathfrak{b} = \mathfrak{c}$$

genügt, welches der Quotient von $\mathfrak{c}$ durch $\mathfrak{a}$ heißt.

Ist $\mathfrak{a}\,\mathfrak{b}$ teilbar durch $\mathfrak{a}\,\mathfrak{b}'$, so ist $\mathfrak{b}$ teilbar durch $\mathfrak{b}'$, und aus $\mathfrak{a}\,\mathfrak{b} = \mathfrak{a}\,\mathfrak{b}'$ folgt $\mathfrak{b} = \mathfrak{b}'$.

Beweis. Es sei $\mathfrak{c}$ teilbar durch $\mathfrak{a}$ und (nach 3.) $\mathfrak{a}\,\mathfrak{m} = \mathfrak{o}\,\mu$. Es ist alsdann auch $\mathfrak{c}\,\mathfrak{m}$ teilbar durch $\mathfrak{a}\,\mathfrak{m} = \mathfrak{o}\,\mu$ und folglich $\mathfrak{c}\,\mathfrak{m} = \mathfrak{b}\,\mu$

---

*) Man kann das Ideal $\mathfrak{m}$ zugleich so wählen, daß es relativ prim zu einem beliebigen Ideal $\mathfrak{b}$ wird. Dies wird erreicht, wenn man die Funktion μ so annimmt, daß $(\mathfrak{a}, \mathfrak{o}\,\mu) = N(\mathfrak{m})$ keinen Teiler mit $N(\mathfrak{a})\,N(\mathfrak{b})$ gemein hat (§ 8, 8.).

(§ 8, 10., 11.); also, durch Multiplikation der letzten Gleichung mit $\mathfrak{a}$,

$$\mathfrak{c}\mu = \mathfrak{a}\mathfrak{b}\mu$$

und nach § 8, 12.

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b},$$

womit der erste Teil des Satzes bewiesen ist*).

Ist ferner $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}\mathfrak{b}'$, so ist (§ 8, 10.) $\mu\mathfrak{b}$ teilbar durch $\mu\mathfrak{b}'$, also $\mathfrak{b}$ durch $\mathfrak{b}'$. — Ist $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$, so folgt $\mu\mathfrak{b} = \mu\mathfrak{b}'$ und mithin $\mathfrak{b} = \mathfrak{b}'$ (§ 8, 12.).

5. Jedes von $\mathfrak{o}$ verschiedene Ideal ist entweder ein Primideal, oder es läßt sich, und nur auf eine Weise, als Produkt von lauter Primidealen darstellen.

Beweis. Ist das Ideal $\mathfrak{a}$ von $\mathfrak{o}$ verschieden, so ist es (§ 8, 15.) durch ein Primideal $\mathfrak{p}_1$ teilbar, und folglich (nach 4.) $= \mathfrak{p}_1\mathfrak{a}_1$, worin $\mathfrak{a}_1$ ein echter Teiler von $\mathfrak{a}$ ist (denn aus $\mathfrak{a}_1 = \mathfrak{a}$ würde nach 4. folgen $\mathfrak{p}_1 = \mathfrak{o}$). Es ist also der Grad von $N(\mathfrak{a}_1)$ niedriger als der von $N(\mathfrak{a})$. Ist $\mathfrak{a}_1$ von $\mathfrak{o}$ verschieden, so schließt man ebenso, daß $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$ sein muß, wobei der Grad von $N(\mathfrak{a}_2)$ wieder niedriger ist als der von $N(\mathfrak{a}_1)$. Fährt man auf diese Weise fort, so gelangt man schließlich nach einer endlichen Anzahl von Zerlegungen zu einem Ideal $\mathfrak{a}_{r-1} = \mathfrak{p}_r\mathfrak{a}_r$ derart, daß $N(\mathfrak{a}_r) = 1$, also $\mathfrak{a}_r = \mathfrak{o}$ ist. Es ist daher

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r.$$

Wäre eine solche Zerlegung auf eine zweite Art möglich, etwa

$$\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2\ldots\mathfrak{q}_s,$$

so müßte (§ 8, 18.) von den Primidealen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$ mindestens eines, etwa $\mathfrak{p}_1$ durch $\mathfrak{q}_1$ teilbar und also $= \mathfrak{q}_1$ sein, also nach 4.

$$\mathfrak{p}_2\mathfrak{p}_3\ldots\mathfrak{p}_r = \mathfrak{q}_2\mathfrak{q}_3\ldots\mathfrak{q}_s.$$

Hieraus schließt man ebenso $\mathfrak{p}_2 = \mathfrak{q}_2$ usf.

Faßt man in der so gewonnen Zerlegung die einander gleichen Primideale zu Potenzen zusammen, so kann man setzen

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_r^{e_r}.$$

Irgendein Teiler $\mathfrak{a}_1$ von $\mathfrak{a}$ kann dann durch kein von $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$ verschiedenes Primideal und durch keines öfter als $\mathfrak{a}$ teilbar sein. Man erhält also die sämtlichen Divisoren von $\mathfrak{a}$, deren Anzahl endlich, und $= (e_1 + 1)(e_2 + 1)\ldots(e_r + 1)$ ist, wenn man in

$$\mathfrak{p}_1^{h_1}\mathfrak{p}_2^{h_2}\ldots\mathfrak{p}_r^{h_r}$$

---

*) Diese Definition des Quotienten zweier Ideale stimmt mit der in § 4, 8. gegebenen völlig überein.

die Exponenten h_ι die Reihe der Zahlen 0, 1, 2, ... e_ι durchlaufen läßt (wobei unter $\mathfrak{p}^0$ das Ideal $\mathfrak{o}$ zu verstehen ist). Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei Ideale

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_r^{e_r}; \quad \mathfrak{b} = \mathfrak{p}_1^{f_1}\,\mathfrak{p}_2^{f_2} \ldots \mathfrak{p}_r^{f_r}$$

(worin die Exponenten e, f auch zum Teil Null sein können), so erhält man den größten gemeinschaftlichen Teiler und das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ in der Form

$$\mathfrak{p}_1^{g_1}\,\mathfrak{p}_2^{g_2} \ldots \mathfrak{p}_r^{g_r},$$

wenn man für g_1, g_2, ... g_r für ersteren die kleinsten, für letzteres die größten unter den Zahlen e_1, f_1; e_2, f_2; ... e_r, f_r, nimmt.

6. Sind $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Ideale, so ist allgemein

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\,N(\mathfrak{b}).$$

Beweis. Es sei, wie in 5., $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, so gibt es, weil $\mathfrak{a}_1$ ein echter Teiler von $\mathfrak{a}$ ist, in $\mathfrak{a}_1$ eine durch $\mathfrak{a}$ nicht teilbare Funktion η. Das kleinste gemeinschaftliche Vielfache und der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{o}\eta$ sind bzw. $\mathfrak{p}_1\eta$ und $\mathfrak{a}_1$, wie sich (nach 5.) sofort aus der Zerlegung von $\mathfrak{a}$ und $\mathfrak{o}\eta$ in ihre Primfaktoren ergibt. Hieraus folgt aber nach § 8, 14.

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)\,N(\mathfrak{a}_1).$$

Durch Wiederholung desselben Schlusses für $\mathfrak{a}_1$ usf. ergibt sich, wenn $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$ ist:

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)\,N(\mathfrak{p}_2) \ldots N(\mathfrak{p}_r)$$

und daraus

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\,N(\mathfrak{b}).$$

7. Jedes Primideal ist ein Ideal ersten Grades (§ 7) und umgekehrt, jedes Ideal ersten Grades ist ein Primideal*).

Beweis. Ist $\mathfrak{p}$ ein Primideal, so ist $N(\mathfrak{p})$ durch $\mathfrak{p}$ teilbar, und daher wenigstens einer der Linearfaktoren von $N(\mathfrak{p})$, etwa $z - c$, durch $\mathfrak{p}$ teilbar (§ 8, 18.). Ist ω eine beliebige Funktion in $\mathfrak{o}$, welche der Gleichung genügt:

$$\omega^n + a_1\,\omega^{n-1} + \cdots + a_{n-1}\,\omega + a_n = 0,$$

so erhält man daraus, indem man die ganzen rationalen Funktionen a_1, a_2, ... a_n auf ihre konstanten Reste $a_1^{(0)}$, $a_2^{(0)}$, ... $a_n^{(0)}$ nach $z - c$ reduziert, und die ganze Funktion

$$\omega^n + a_1^{(0)}\,\omega^{n-1} + \cdots + a_{n-1}^{(0)}\,\omega + a_n^{(0)}$$

*) Durch diesen Satz unterscheidet sich die Theorie der algebraischen Funktionen wesentlich von der analogen Theorie der algebraischen Zahlen.

in ihre Linearfaktoren $(\omega - b_1)$, $(\omega - b_2)$, ... $(\omega - b_n)$ zerlegt:

$$(\omega - b_1)(\omega - b_2) \dots (\omega - b_n) = (z - c)\,\omega' \equiv 0 \pmod{\mathfrak{p}}.$$

Es muß also wenigstens einer der Faktoren $\omega - b_1$, $\omega - b_2$, ... durch $\mathfrak{p}$ teilbar sein, d. h. es ist

$$\omega \equiv b \pmod{\mathfrak{p}},$$

worin b eine Konstante bedeutet. Da hiernach jede Funktion in $\mathfrak{o}$ kongruent einer Konstanten ist (mod. $\mathfrak{p}$), so ist nach § 6 $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = z - c$ eine lineare Funktion von z, wodurch der erste Teil der Behauptung erwiesen ist.

Umgekehrt: ist $\mathfrak{q}$ ein Ideal ersten Grades, und

$$N(\mathfrak{q}) = z - c,$$

so ist $\mathfrak{q}$ gewiß durch ein Primideal $\mathfrak{p}$ teilbar, und da $N(\mathfrak{q})$ durch $N(\mathfrak{p})$ teilbar ist, so ist $(N(\mathfrak{p}) = N(\mathfrak{q}) = z - c$, also (§ 8, 9.)

$$\mathfrak{p} = \mathfrak{q}.$$

Es ergibt sich hieraus, daß der Grad eines Ideals gleich ist der Anzahl der Primfaktoren, in welche sich dasselbe zerlegen läßt. Ist daher

$$\mathfrak{o}(z - c) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}\dots,$$

so ist

$$e_1 + e_2 + e_3 + \dots = n.$$

Es folgt ferner noch, daß eine ganze rationale Funktion von z dann und nur dann durch ein Primideal $\mathfrak{p}$ teilbar ist, wenn sie durch die Norm von $\mathfrak{p}$ teilbar ist.

§ 10.

Die komplementären Basen des Körpers Ω.

1. Definition. Bilden die Funktionen $\alpha_1, \alpha_2, \dots \alpha_n$ eine Basis von Ω, und setzt man zur Abkürzung

$$S(\alpha_r \alpha_s) = a_{r,s} = a_{s,r},$$

$$\Delta(\alpha_1, \alpha_2, \dots \alpha_n) = \sum \pm a_{1,1}\, a_{2,2} \dots a_{n,n} = a \quad (\S\ 2),$$

so läßt sich, da a von Null verschieden ist, ein ganz bestimmtes Funktionensystem $\alpha'_1, \alpha'_2, \dots \alpha'_n$ aus den linearen Gleichungen bestimmen

$$(1) \qquad \alpha_r = \sum_{1,n}^{\iota} a_{r,\iota}\, \alpha'_\iota,$$

und da

$$\Delta(\alpha'_1, \alpha'_2, \dots \alpha'_n) = \frac{1}{a}$$

von Null verschieden ist, so bilden die Funktionen $\alpha'_1, \alpha'_2, \ldots \alpha_n$ ebenfalls eine Basis von Ω. Diese soll die zu $\alpha_1, \alpha_2, \ldots \alpha_n$ komplementäre Basis heißen.

2. Bezeichnet man, wenn die Indizes r, s der Zahlenreihe $1, 2 \ldots n$ angehören, mit (r, s) die Zahl 1 oder 0, je nachdem r, s gleich oder verschieden sind, so ist

$$S(\alpha_r \alpha'_s) = (r, s), \tag{2}$$

denn durch Auflösung der Gleichungen (1) folgt

$$\alpha'_s = \sum^{\iota} a'_{\iota, s} \alpha_\iota;$$

$$a'_{r,s} = a'_{s,r}; \sum^{\iota} a_{r,\iota} a'_{s,\iota} = (r, s),$$

hieraus:

$$\alpha_r \alpha'_s = \sum^{\iota} a'_{\iota, s} \alpha_\iota \alpha_r; \quad S(\alpha_r \alpha'_s) = \sum^{\iota} a'_{\iota, s} a_{\iota, r} = (r, s).$$

Genügt umgekehrt ein Funktionensystem β_s den Bedingungen $S(\alpha_r \beta_s) = (r, s)$, so ist $\beta_s = \alpha'_s$; denn setzt man $\beta_s = \sum^{\iota} b_{\iota, s} \alpha'_\iota$, so folgt wegen (2).

$$b_{r,s} = S(\beta_s \alpha_r) = (r, s).$$

Daraus folgt unmittelbar, daß die Beziehung der α_ι zu den α'_ι eine gegenseitige ist, d. h., daß die Basis $\alpha_1, \alpha_2, \ldots \alpha_n$ komplementär ist zu $\alpha'_1, \alpha'_2, \ldots \alpha'_n$.

3. Ist η eine beliebige Funktion in Ω, so kann man stets setzen

$$\eta = \sum x_\iota \alpha_\iota = \sum x'_\iota \alpha'_\iota,$$

und durch Anwendung von (2) folgt:

$$x_\iota = S(\eta \alpha'_\iota), \quad x' = S(\eta \alpha_\iota),$$

also

$$\eta = \sum^{\iota} \alpha_\iota S(\eta \alpha'_\iota) = \sum^{\iota} \alpha'_\iota S(\eta \alpha_\iota). \tag{3}$$

4. Ist η eine beliebige von Null verschiedene Funktion in Ω, so ist

$$\frac{\alpha'_1}{\eta}, \frac{\alpha'_2}{\eta}, \ldots \frac{\alpha'_n}{\eta}$$

die zu $\eta \alpha_1, \eta \alpha_2, \ldots \eta \alpha_n$ komplementäre Basis. Dies folgt aus 2. wegen

$$S\left(\eta \alpha_r \cdot \frac{\alpha'_s}{\eta}\right) = S(\alpha_r \alpha'_s) = (r, s).$$

5. Wenn zwei Basen von Ω, $\alpha_1, \alpha_2, \ldots \alpha_n$ und $\beta_1, \beta_2, \ldots \beta_n$ durch die n Gleichungen zusammenhängen

$$\beta_s = \sum^{\iota} x_{\iota, s}\, \alpha_\iota$$

mit rationalen Koeffizienten $x_{\iota, s}$, so hängen die zu ihnen komplementären Basen zusammen durch die n Gleichungen

$$\alpha'_r = \sum^{\iota} x_{r, \iota}\, \beta'_\iota$$

(transponierte Substitution). Es ist dies eine unmittelbare Folge aus 3. wegen

$$x_{r, s} = S(\alpha'_r\, \beta_s).$$

6. Es ist

$$\sum^{\iota} \alpha_\iota\, \alpha'_\iota = 1,$$

also:

$$\sum^{\iota, \iota'} a_{\iota, \iota'}\, \alpha'_\iota\, \alpha'_{\iota'} = \sum^{\iota, \iota'} a'_{\iota, \iota'}\, \alpha_\iota\, \alpha_{\iota'} = 1.$$

Setzt man nämlich zunächst

$$\sum \alpha_\iota\, \alpha'_\iota = \sigma,$$

so folgt aus 3. (auf die Funktionen $\eta\, \alpha_r$ angewandt),

$$\eta\, \alpha_r = \sum^{\iota} \alpha_\iota\, S(\eta\, \alpha_r\, \alpha'_\iota),$$

mithin, nach der Definition der Spur in § 2, (5)

$$S(\eta) = \sum^{\iota} S(\eta\, \alpha_\iota\, \alpha'_\iota) = S(\sum \eta\, \alpha_\iota\, \alpha'_\iota).$$

also:

$$S(\eta\, \sigma) = S(\eta),$$

und daraus, wenn man in 3. einmal $\eta = \sigma$, dann $\eta = 1$ setzt:

$$\sigma = \sum^{\iota} \alpha_\iota\, S(\sigma\, \alpha'_\iota) = \sum^{\iota} \alpha_\iota\, S(\alpha'_\iota) = 1.$$

Wir gehen etwas genauer ein auf die Bildung der komplementären Basen in zwei besonderen Fällen:

7. Es sei $\omega_1, \omega_2, \ldots \omega_n$ eine Basis von $\mathfrak{o}$ und $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n$ die komplementäre Basis (von Ω). Es sei

$$e_{r, s} = e_{s, r} = S(\omega_r\, \omega_s),$$

welches ganze rationale Funktionen sind, und

$$D = \text{konst.} \sum \pm\, e_{1,1}\, e_{2,2} \cdots e_{n,n}$$

die Diskriminante von Ω; ist dann nach 2.

$$\varepsilon_r = \frac{1}{D} \sum^{\iota} \frac{\partial D}{\partial e_{\iota, r}} \omega_\iota,$$

woraus hervorgeht, daß die Funktionen $D\varepsilon_r$ zu den ganzen Funktionen gehören. Aus 6. folgt aber ferner

$$D = \sum^{\iota, \iota'} \frac{\partial D}{\partial e_{\iota, \iota'}} \omega_\iota \omega_{\iota'}$$

und hieraus

$$\varepsilon_r \varepsilon_s = \frac{1}{D^2} \sum^{\iota, \iota'} \frac{\partial D}{\partial e_{r, \iota}} \frac{\partial D}{\partial e_{s, \iota'}} \omega_\iota \omega_{\iota'}$$

$$= \frac{1}{D} \frac{\partial D}{\partial e_{r, s}} + \frac{1}{D^2} \sum^{\iota, \iota'} \left(\frac{\partial D}{\partial e_{r, \iota}} \frac{\partial D}{\partial e_{s, \iota'}} - \frac{\partial D}{\partial e_{r, s}} \frac{\partial D}{\partial e_{\iota, \iota'}} \right) \omega_\iota \omega_{\iota'}$$

und daraus nach einem bekannten Determinantensatz:

$$\varepsilon_r \varepsilon_s = \frac{1}{D} \frac{\partial D}{\partial e_{r, s}} + \frac{1}{D} \sum^{\iota, \iota'} \frac{\partial^2 D}{\partial e_{r, \iota} \partial e_{s, \iota'}} \omega_\iota \omega_{\iota'},$$

woraus das wichtige Resultat folgt, daß auch die Funktionen $D\varepsilon_r \varepsilon_s$ zu den ganzen Funktionen gehören.

8. Es sei θ eine solche Funktion in Ω, daß $1, \theta, \theta^2, \ldots \theta^{n-1}$ eine Basis von Ω bilden, und es sei also

$$(4) \qquad f(\theta) = \theta^n + a_1 \theta^{n-1} + \cdots + a_{n-1} \theta + a_n = 0$$

mit rationalen Koeffizienten a irreduktibel. Es soll die komplementäre Basis zu $1, \theta, \theta^2, \ldots \theta^{n-1}$ aufgesucht werden. Setzen wir, wenn t eine unbestimmte Konstante bedeutet,

$$\frac{f(t)}{t - \theta} = \eta_0 + \eta_1 t + \eta_2 t^2 + \cdots + \eta_{n-1} t^{n-1},$$

oder

$$(5) \qquad \left\{ \begin{array}{ll} \eta_0 & = a_{n-1} + a_{n-2} \theta + \cdots + a_1 \theta^{n-2} + \theta^{n-1}, \\ \eta_1 & = a_{n-2} + a_{n-3} \theta + \cdots + \theta^{n-2}, \\ \cdots & \cdots\cdots\cdots\cdots \\ \eta_{n-2} & = a_1 + \theta, \\ \eta_{n-1} & = 1, \end{array} \right.$$

so bilden die Funktionen $\eta_0, \eta_1, \ldots \eta_{n-1}$ gleichfalls eine Basis von Ω, da die Determinante der Gleichungen (5) $= (-1)^{1/2\, n(n-1)}$, also von Null verschieden ist. Es läßt sich daher jede Funktion ζ in Ω in der Form darstellen

$$\zeta = y_0 \eta_0 + y_1 \eta_1 + \cdots + y_{n-1} \eta_{n-1}.$$

Die Reihe der rationalen Funktionen $y_0, y_1, \dots y_{n-1}$ setzen wir nun fort, indem wir die Funktionen $y_n, y_{n+1}, \dots$ durch die Rekursion bestimmen

(6) $a_n y_r + a_{n-1} y_{r+1} + \cdots + a_2 y_{r+n-2} + a_1 y_{r+n-1} + y_{r+n} = 0.$

Nun ist nach (5)

$$(7) \quad \begin{cases} \theta \eta_0 = \qquad - a_n \eta_{n-1}, \\ \theta \eta_1 = \eta_0 - a_{n-1} \eta_{n-1}, \\ \theta \eta_2 = \eta_1 - a_{n-2} \eta_{n-1}, \\ \dots\dots\dots\dots\dots \\ \theta \eta_{n-1} = \eta_{n-2} - a_1 \eta_{n-1}, \end{cases}$$

also

$$\zeta \theta = y_1 \eta_0 + y_2 \eta_1 + \cdots + y_{n-1} \eta_{n-2} + y_n \eta_{n-1},$$

und ebenso allgemein für jedes ganze positive r:

$$\zeta \theta^r = y_r \eta_0 + y_{r+1} \eta_1 + \cdots + y_{r+n-2} \eta_{n-2} + y_{r+n-1} \eta_{n-1},$$

oder, wenn man $\eta_0, \eta_1, \dots \eta_{n-1}$ durch $1, \theta, \theta^2, \dots \theta^{n-1}$ ausdrückt:

$$\zeta \theta^r = x_0^{(r)} + x_1^{(r)} \theta + x_2^{(r)} \theta^2 + \cdots + x_{n-1}^{(r)} \theta^{n-1},$$

worin

$$\begin{aligned} x_0^{(r)} &= y_r a_{n-1} + y_{r+1} a_{n-2} + \cdots + y_{r+n-2} a_1 + y_{r+n-1}, \\ x_1^{(r)} &= y_r a_{n-2} + y_{r+1} a_{n-3} + \cdots + y_{r+n-2}, \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ x_{n-2}^{(r)} &= y_r a_1 + y_{r+1}, \\ x_{n-1}^{(r)} &= y_r. \end{aligned}$$

Mithin ist [nach der Definition von S, § 2 (5)]

$$\begin{aligned} S(\zeta) &= x_0^{(0)} + x_1^{(1)} + x_2^{(2)} + \cdots + x_{n-1}^{(n-1)} \\ &= y_0 a_{n-1} + 2 y_1 a_{n-2} + \cdots + (n-1) y_{n-2} a_1 + n y_{n-1}, \end{aligned}$$

also, auf $\zeta = \eta_r$ angewandt:

$$S(\eta_r) = (r+1) a_{n-1-r}; \quad S(\eta_{n-1-r}) = (n-r) a_r,$$

worin $a_0 = 1$ zu setzen ist.

Setzt man daher zur Abkürzung

$$S(\theta^r) = s_r,$$

so folgt, so lange $r \gtreqless n$, mittels (5)

(8) $\qquad (n-r) a_r = a_r s_0 + a_{r-1} s_1 + \cdots + a_1 s_{r-1} + s_r$

und nach (4) allgemein

(9) $\qquad 0 = a_n s_r + a_{n-1} s_{r+1} + \cdots + a_1 s_{r+n-1} + s_{r+n}.$

Aus diesen Formeln folgt aber ferner:

$$(10)\quad \begin{cases} f'(\theta) = n\,\theta^{n-1} + (n-1)\,a_1\,\theta^{n-1} + \cdots + 2\,a_{n-2}\,\theta + a_{n-1} \\ \qquad\;\; = s_0\,\eta_0 + s_1\,\eta_1 + \cdots + s_{n-1}\,\eta_{n-1}, \\ \theta^r f'(\theta) = s_r\,\eta_0 + s_{r+1}\,\eta_1 + \cdots + s_{r+n-2}\,\eta_{n-2} + s_{r+n-1}\,\eta_{n-1}. \end{cases}$$

Beachtet man nun den Wert der Determinante des Gleichungssystems (5), so folgt hieraus mit Rücksicht auf die Definition der Norm und der Diskriminante in § 2 (4) und (12) die wichtige Formel

$$(11)\quad N f'(\theta) = (-1)^{1/2\,n(n-1)} \begin{vmatrix} s_0, & s_1, \ldots & s_{n-1} \\ s_1, & s_2, \ldots & s_n \\ \cdot & \cdot \cdot \cdot & \cdot \\ s_{n-1}, & s_n, \ldots & s_{2n-2} \end{vmatrix} = (-1)^{1/2\,n(n-1)} \Delta(1, \theta, \theta^2, \ldots \theta^{n-1}).$$

Die Gleichungen (10) ergeben aber auch mit Rücksicht auf die Definition 1. die zu $1, \theta, \theta^2, \ldots \theta^{n-1}$ komplementäre Basis:

$$\frac{\eta_0}{f'(\theta)}, \quad \frac{\eta_1}{f'(\theta)}, \ldots \frac{\eta_{n-1}}{f'(\theta)}.$$

9. Bedeutet $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots \alpha_n]$ einen Modul, dessen Basis zugleich eine Basis Ω ist, so erhält man aus der zu $\alpha_1, \alpha_2, \ldots \alpha_n$ komplementären Basis von Ω, $\alpha_1', \alpha_2', \ldots \alpha_n'$ einen anderen Modul $\mathfrak{a}' = [\alpha_1', \alpha_2', \ldots \alpha_n']$, welcher der zu $\mathfrak{a}$ **komplementäre Modul** genannt wird. Derselbe ist, wie sich aus 5. in Verbindung mit § 4, 2. sofort ergibt, von der Wahl der Basis von $\mathfrak{a}$ unabhängig.

10. Wir betrachten insbesondere den zu $\mathfrak{o} = [\omega_1, \omega_2, \ldots \omega_n]$ komplementären Modul $\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n]$. Setzen wir

$$\omega_r\,\omega_s = \sum^{\iota} e_{r,s}^{(\iota)}\,\omega_\iota,$$

so ist nach 3.

$$e_{r,s}^{(\iota)} = e_{s,r}^{(\iota)} = S(\omega_r\,\omega_s\,\varepsilon_\iota)$$

eine ganze rationale Funktion von z, und es folgt:

$$\omega_r\,\varepsilon_s = \sum^{\iota} e_{r,\iota}^{(s)}\,\varepsilon_\iota.$$

Hieraus ergibt sich, daß der Modul $\mathfrak{o}\,\mathfrak{e}$ (§ 4, 7.) teilbar ist durch $\mathfrak{e}$; andererseits ist, weil $\mathfrak{o}$ die Funktion 1 enthält, $\mathfrak{e}$ teilbar durch $\mathfrak{o}\,\mathfrak{e}$, also

$$\mathfrak{o}\,\mathfrak{e} = \mathfrak{e},$$

d. h. der Modul $\mathfrak{e}$, der zwar nicht bloß ganze Funktionen enthält, besitzt die charakteristische Eigenschaft II. § 7 der Ideale. Dasselbe gilt infolgedessen auch von dem Modul $\mathfrak{e}^2$. Da die beiden Moduln

$D\mathfrak{e}$, $D\mathfrak{e}^2$ nach 7. nur ganze Funktionen enthalten, so sind dieselben Ideale, und aus 7. ergibt sich noch

$$N(D\mathfrak{e}) = D^{n-1}.$$

11. Ist θ eine Funktion in $\mathfrak{o}$ von der Art, daß $1, \theta, \theta^2, \ldots \theta^{n-1}$ eine Basis von Ω bildet, so daß in der irreduktibeln Gleichung

$$f(\theta) = \theta^n + a_1 \theta^{n-1} + \ldots + a_{n-1}\theta + a_n = 0$$

die Koeffizienten ganze rationale Funktionen von z sind, so kann man für $r = 0, 1, 2, \ldots n-1$ die ganzen rationalen Funktionen $k_\iota^{(r)}$ so bestimmen, daß

$$\theta^r = \sum_{1,n}^{\iota} k_\iota^{(r)} \omega_\iota$$

wird. Wendet man hierauf den Satz 5. und 8. an, so folgt:

$$f'(\theta)\varepsilon_s = k_s^{(0)}\eta_0 + k_s^{(1)}\eta_1 + \cdots + k_s^{(n-1)}\eta_{n-1},$$

und hieraus ergibt sich, daß der Modul

$$f'(\theta)\mathfrak{e} = \mathfrak{k}$$

nur ganze Funktionen enthält. Aus 10. schließt man, daß derselbe ein Ideal ist.

§ 11.

Das Verzweigungsideal.

1. Hilfssatz. Sind je zwei der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ relativ prim, so existiert immer eine Funktion, welche in bezug auf jedes von ihnen einer gegebenen Funktion in $\mathfrak{o}$ kongruent ist.

Beweis. Man setze

$$\mathfrak{m} = \mathfrak{a}\mathfrak{b}\mathfrak{c}\cdots = \mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1 = \mathfrak{c}\mathfrak{c}_1 = \cdots;$$

der größte gemeinschaftliche Teiler von $\mathfrak{a}_1 = \mathfrak{b}\mathfrak{c}\ldots$, $\mathfrak{b}_1 = \mathfrak{a}\mathfrak{c}\ldots$ $\mathfrak{c}_1 = \mathfrak{a}\mathfrak{b}\ldots$ ist alsdann gleich $\mathfrak{o}$, da kein Primideal zugleich in $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1, \ldots$ aufgehen kann. Folglich kann man (§ 4, 5.) α_1 aus $\mathfrak{a}_1$, β_1 aus $\mathfrak{b}_1$, γ_1 aus $\mathfrak{c}_1, \ldots$ so auswählen, daß

$$\alpha_1 + \beta_1 + \gamma_1 + \cdots = 1,$$

also:

$$\begin{array}{llll}
\alpha_1 \equiv 1, & \beta_1 \equiv 0, & \gamma_1 \equiv 0, & \ldots \pmod{\mathfrak{a}},\\
\alpha_1 \equiv 0, & \beta_1 \equiv 1, & \gamma_1 \equiv 0, & \ldots \pmod{\mathfrak{b}},\\
\alpha_1 \equiv 0, & \beta_1 \equiv 0, & \gamma_1 \equiv 1, & \ldots \pmod{\mathfrak{c}},\\
\ldots & \ldots & \ldots & \ldots
\end{array}$$

Sind daher λ, μ, ν, ... gegebene Funktionen in $\mathfrak{o}$, so genügt

$$\omega \equiv \lambda\alpha_1 + \mu\beta_1 + \nu\gamma_1 + \cdots \pmod{\mathfrak{m}}$$

den Bedingungen

$$\omega \equiv \lambda \pmod{\mathfrak{a}}, \quad \omega \equiv \mu \pmod{\mathfrak{b}}, \quad \omega \equiv \nu \pmod{\mathfrak{c}}, \ldots$$

2. Es seien $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2, \ldots$ die sämtlichen voneinander verschiedenen in einer beliebigen linearen Funktion $z - c$ aufgehenden Primideale und

$$\mathfrak{o}(z-c) = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots, \quad e + e_1 + e_2 + \cdots = n \text{ (§ 9, 7.).}$$

Man wähle die Funktionen λ, λ_1, $\lambda_2, \ldots$ teilbar bzw. durch $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$, aber nicht durch $\mathfrak{p}^2$, $\mathfrak{p}_1^2$, $\mathfrak{p}_2^2$, ... und lasse b, b_1, $b_2, \ldots$ beliebige jedoch voneinander verschiedene Konstanten bedeuten. Nach 1. läßt sich dann eine Funktion ζ bestimmen, welche den Kongruenzen genügt

$$\zeta \equiv b + \lambda \pmod{\mathfrak{p}^2}, \quad \zeta \equiv b_1 + \lambda_1 \pmod{\mathfrak{p}_1^2}, \quad \zeta \equiv b_2 + \lambda_2 \pmod{\mathfrak{p}_2^2}, \ldots,$$

also

$$\zeta \equiv b \pmod{\mathfrak{p}}, \quad \zeta \equiv b_1 \pmod{\mathfrak{p}_1}, \quad \zeta \equiv b_2 \pmod{\mathfrak{p}_2}, \ldots,$$

so daß, wenn a irgendeine Konstante bedeutet, $\zeta - a$ höchstens durch eines der Primideale $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2, \ldots$ und niemals durch eines ihrer Quadrate teilbar ist. Ist daher $\varphi(t) = \Pi(t-a)$ eine ganze Funktion der Variablen t mit konstanten Koeffizienten, so ist $\varphi(\zeta) = \Pi(\zeta - a)$ stets und nur dann durch $\mathfrak{p}^m$ teilbar, wenn $\varphi(t)$ algebraisch durch $(t-b)^m$ teilbar ist, und wenn $\mathfrak{p}^m$ die höchste in $\varphi(\zeta)$ aufgehende Potenz von $\mathfrak{p}$ ist, so ist folglich $\mathfrak{p}^{m-1}$ die höchste in $\varphi'(\zeta)$ aufgehende Potenz von $\mathfrak{p}$. Soll daher $\varphi(\zeta)$ durch $z - c$ teilbar sein, so muß $\varphi(t)$ durch die Funktion n^{ten} Grades

$$\psi(t) = (t-b)^e (t-b_1)^{e_1} (t-b_2)^{e_2} \cdots$$

teilbar sein. Mithin ist die Kongruenz

$$x_0 + x_1\zeta + x_2\zeta^2 + \cdots + x_{n-1}\zeta^{n-1} \equiv 0 \pmod{z-c}$$

nur durch solche ganze rationale x zu befriedigen, die alle durch $z - c$ teilbar sind. Setzt man also, indem man mit $k_1^{(0)}$, $k_1^{(1)}$, ... ganze rationale Funktionen von z und mit ω_1, ω_2, ... ω_n eine Basis von $\mathfrak{o}$ bezeichnet:

$$\begin{aligned}
1 &= k_1^{(0)}\omega_1 + k_2^{(0)}\omega_2 + \cdots + k_n^{(0)}\omega_n, \\
\zeta &= k_1^{(1)}\omega_1 + k_2^{(1)}\omega_2 + \cdots + k_n^{(1)}\omega_n, \\
\zeta^2 &= k_1^{(2)}\omega_1 + k_2^{(2)}\omega_2 + \cdots + k_n^{(2)}\omega_n, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\zeta^{n-1} &= k_1^{(n-1)}\omega_1 + k_2^{(n-1)}\omega_2 + \cdots + k_n^{(n-1)}\omega_n,
\end{aligned}$$

so kann die Determinante

$$k = \sum \pm k_1^{(0)} k_2^{(1)} \cdots k_n^{(n-1)}$$

weder identisch verschwinden, noch durch $z - c$ teilbar sein (vgl. die Note zu § 9, 1.).

Es folgt also, daß

$$N(t - \zeta) = f(t, z)$$

irreduktibel ist. Da nun $f(\zeta, z) = 0$, also $f(\zeta, c)$ durch $z - c$ teilbar ist, so muß $f(t, c)$ durch $\psi(t)$ teilbar, also, da beide Funktionen von gleichem Grade sind,

$$f(t, c) = \psi(t)$$

sein, woraus man noch für eine folgende Anwendung schließt:

$$S(\zeta) \equiv eb + e_1 b_1 + e_2 b_2 + \cdots \quad (\text{mod. } z - c),$$

und, indem man dieselbe Betrachtung auf die Funktionen $\zeta^2, \zeta^3 \ldots$ anwendet, was, falls keine der Konstanten b verschwindet, sicher gestattet ist:

$$S(\zeta^2) \equiv eb^2 + e_1 b_1^2 + e_2 b_2^2 + \cdots \quad (\text{mod. } z - c),$$
$$S(\zeta^3) \equiv eb^3 + e_1 b_1^3 + e_2 b_2^3 + \cdots \quad (\text{mod. } z - c).$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Es ist also $\mathfrak{p}^e$ die höchste in $f(\zeta, c)$, also $\mathfrak{p}^{e-1}$ die höchste in $f'(\zeta, c)$ aufgehende Potenz von $\mathfrak{p}$, und da

$$f'(\zeta, c) \equiv f'(\zeta, z) \quad (\text{mod. } \mathfrak{p}^e),$$

so ist $\mathfrak{p}^{e-1}$ auch die höchste in $f'(\zeta, z)$ aufgehende Potenz von $\mathfrak{p}$. Hieraus ergibt sich

$$\mathfrak{o} f'(\zeta, z) = \mathfrak{m}\, \mathfrak{p}^{e-1}\, \mathfrak{p}_1^{e_1 - 1} \ldots,$$

worin $\mathfrak{m}$ und folglich auch $N(\mathfrak{m})$ relativ prim zu $z - c$ ist.

Ist nun D die Diskriminante von Ω, so ist hiernach und nach § 10, (11) und § 2, (13) (von konstanten Faktoren abgesehen)

$$N f'(\zeta, z) = \Delta(1, \zeta, \zeta^2, \ldots \zeta^{n-1}) = D k^2 = (z - c)^{n-s} N(\mathfrak{m}),$$

wenn s die Anzahl der verschiedenen in $z - c$ aufgehenden Primideale $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ bedeutet; und da k und $N(\mathfrak{m})$ durch $z - c$ nicht teilbar sind, so ist $(z - c)^{n-s}$ die höchste in D aufgehende Potenz von $z - c$. Folglich:

(1) $$D = \Pi (z - c)^{n-s},$$

worin das Produktzeichen Π sich auf alle solche linearen Ausdrücke $z - c$ bezieht, in denen weniger als n verschiedene Primfaktoren aufgehen, die also durch die zweite oder eine höhere Potenz eines Primideals teilbar sind.

Es gibt also nur eine endliche Anzahl linearer Funktionen $z - c$, die durch das Quadrat eines Primideals teilbar sind.

Wir setzen nun

(2) $$\mathfrak{z} = \Pi \mathfrak{p}^{e-1},$$

worin sich das Produktzeichen Π auf alle diejenigen Primideale $\mathfrak{p}$ bezieht, von denen eine höhere als die erste, nämlich die e^{te} Potenz in ihrer Norm aufgeht, und nennen dieses Ideal $\mathfrak{z}$ das Verzweigungsideal. Aus (1) und (2) folgt sofort

(3) $$N(\mathfrak{z}) = D.$$

Da ferner $n - s \geqq e - 1$, also $e(n-s) - 2(e-1) \geqq (e-1)(e-2) \geqq 0$ ist, so ist D teilbar durch $\mathfrak{p}^{2(e-1)}$, also auch durch $\mathfrak{z}^2$, und man kann, wenn man mit $\mathfrak{d}$ gleichfalls ein Ideal bezeichnet, setzen:

(4) $$\mathfrak{o} D = \mathfrak{d}\,\mathfrak{z}^2, \quad N(\mathfrak{d}) = D^{n-2}.$$

3. Ist eine Funktion ϱ in $\mathfrak{o}$ durch jedes in $z - c$ aufgehende Primideal teilbar, so ist $S(\varrho)$ durch $z - c$ teilbar.

Beweis. Es sei ζ dieselbe Funktion wie in 2., so daß man setzen kann:

$$x\varrho = x_0 + x_1 \zeta + x_2 \zeta^2 + \cdots + x_{n-1} \zeta^{n-1},$$

worin die Koeffizienten $x, x_0, x_1, \ldots x_{n-1}$ ganze rationale Funktionen von z ohne gemeinsamen Teiler sind, von denen die erste durch $z - c$ nicht teilbar ist (vgl. 2.). Aus unserer Voraussetzung über die Funktion ϱ folgt, wenn die Konstanten b dieselbe Bedeutung wie in 2. haben,

$$x_0 + x_1 b + x_2 b^2 + \cdots + x_{n-1} b^{n-1} \equiv 0 \pmod{z - c},$$
$$x_0 + x_1 b_1 + x_2 b_1^2 + \cdots + x_{n-1} b_1^{n-1} \equiv 0 \pmod{z - c},$$
$$x_0 + x_1 b_2 + x_2 b_2^2 + \cdots + x_{n-1} b_2^{n-1} \equiv 0 \pmod{z - c},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

und hieraus, indem man die Kongruenzen mit $e, e_1, e_2, \ldots$ multipliziert und addiert:

$$x_0 n + x_1 S(\zeta) + x_2 S(\zeta^2) + \cdots + x_{n-1} S(\zeta^{n-1}) = x S(\varrho) \equiv 0 \pmod{z - c},$$

also, da x durch $z-c$ nicht teilbar ist,

$$S(\varrho) \equiv 0 \quad (\text{mod.}\ (z-c)$$

w. z. b. w.

4. Es sei jetzt

$$r = (z-c)\ (z-c_1)\ (z-c_2) \ldots$$

das Produkt sämtlicher voneinander verschiedenen Linearfaktoren von D und

$$\mathfrak{r} = \mathfrak{p}\,\mathfrak{p}_1\,\mathfrak{p}_2 \ldots$$

das Produkt der sämtlichen voneinander verschiedenen in r aufgehenden Primideale. Ist wie oben $\mathfrak{z}$ das Verzweigungsideal, so ist

(5) $$\mathfrak{r}\,\mathfrak{z} = \Pi \mathfrak{p}^e = \mathfrak{o}\,r$$

und mithin

$$N(\mathfrak{r}) = \frac{r^n}{D}.$$

Jede Funktion ϱ in $\mathfrak{r}$ hat nach 3. die Eigenschaft, daß $S(\varrho)$ durch r teilbar ist. Ist nun, wie in § 10

$$\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n]$$

der zu $\mathfrak{o}$ komplementäre Modul, ϱ eine beliebige Funktion in $\mathfrak{r}$, so kann man setzen

$$\varrho = x_1\,\varepsilon_1 + x_2\,\varepsilon_2 + \cdots + x_n\,\varepsilon_n,$$

worin nach § 10, 3.

$$x_\iota = S(\varrho\,\omega_\iota),$$

also, da $\varrho\,\omega_\iota$ eine Funktion in $\mathfrak{r}$ ist, x_ι eine durch r teilbare ganze rationale Funktion von z. Hieraus folgt, daß das Ideal $\mathfrak{r}$ durch den Modul $r\,\mathfrak{e}$ teilbar ist. Es ist also auch das Ideal $D\,\mathfrak{r}$ teilbar durch das Ideal $r D \mathfrak{e}$. Zugleich ist

$$N(D\mathfrak{r}) = r^n D^{n-1}, \quad N(r D \mathfrak{e}) = r^n D^{n-1} \quad (\S\ 10,\ 10.);$$

mithin nach § 8, 9.

$$D\,\mathfrak{r} = r\,D\,\mathfrak{e}$$

oder

(6) $$\mathfrak{r} = r\,\mathfrak{e}.$$

Woraus mittels der obigen Bemerkung über ϱ folgt, daß, wenn ε eine beliebige Funktion in $\mathfrak{e}$ bedeutet, $S(\varepsilon)$ eine ganze rationale Funktion von z ist. Aus der Formel (6) folgt durch Multiplikation mit $\mathfrak{z}$ nach (5)

$$\mathfrak{r}\,\mathfrak{z} = r\,\mathfrak{e}\,\mathfrak{z} = \mathfrak{o}\,r$$

und folglich

(7) $$\mathfrak{e}\,\mathfrak{z} = \mathfrak{o}.$$

Multipliziert man die letzte Gleichung mit D, so ergibt sich aus (4)

$$\mathfrak{e}\, D\, \mathfrak{z} = \mathfrak{z}^2\, \mathfrak{d},$$

folglich

(8) $$D\, \mathfrak{e} = \mathfrak{z}\, \mathfrak{d}$$

und durch Multiplikation dieser Gleichung mit $\mathfrak{e}$ nach (7)

(9) $$D\, \mathfrak{e}^2 = \mathfrak{d}.$$

5. Ist θ eine ganze Funktion von z in Ω und $N(t-\theta) = f(t)$, so ist $f'(\theta)$ teilbar durch das Verzweigungsideal $\mathfrak{z}$.

Beweis. Ist $f(t)$ reduktibel, so ist $f'(\theta) = 0$, also sicher teilbar durch $\mathfrak{z}$. Im anderen Fall ist nach § 10, 11.

$$\mathfrak{e}\, f'(\theta) = \mathfrak{k}$$

ein Ideal, folglich durch Multiplikation mit $\mathfrak{z}$ nach (7)

(10) $$\mathfrak{o}\, f'(\theta) = \mathfrak{k}\, \mathfrak{z}.$$

Zugleich folgt, wenn wir wie in § 10, 11.

$$\theta^r = \sum_\iota k_\iota^{(r)}\, \omega_\iota,$$

$$k = \sum \pm k_1^{(0)}\, k_2^{(1)} \ldots k_n^{(n-1)}$$

setzen,

$$N f'(\theta) = N(\mathfrak{k})\, N(\mathfrak{z}) = D\, N(\mathfrak{k})$$

$$= \text{konst. } k^2 D \quad [\S\ 10,\ (11) \text{ und } \S\ 2,\ (13)],$$

also:

(11) $$N(\mathfrak{k}) = \text{konst. } k^2$$

ein vollständiges Quadrat.

§ 12.

Die gebrochenen Funktionen von z im Körper Ω.

1. Jede beliebige Funktion η in Ω läßt sich nach § 3, 3. auf unendlich viele Arten als Quotient zweier ganzen Funktionen von z darstellen (der Nenner kann sogar eine ganze rationale Funktion von z sein). Es sei also

$$\eta = \frac{\nu}{\mu}$$

und μ, ν ganze Funktionen von z (Funktionen in $\mathfrak{o}$). Ist nun $\mathfrak{m}$ der größte gemeinschaftliche Teiler der beiden Hauptideale $\mathfrak{o}\mu$, $\mathfrak{o}\nu$, also, wenn $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind,

(1) $$\mathfrak{o}\,\mu = \mathfrak{a}\,\mathfrak{m}, \quad \mathfrak{o}\,\nu = \mathfrak{b}\,\mathfrak{m},$$

so folgt (§ 4, 6.)

(2) $$\mathfrak{a}\,\nu = \mathfrak{b}\,\mu \quad \text{oder} \quad \mathfrak{a}\,\eta = \mathfrak{b}.$$

Ist also α eine beliebige Funktion in $\mathfrak{a}$, so ist $\alpha\eta$ in $\mathfrak{b}$ enthalten, also jedenfalls eine ganze Funktion von z. Ist umgekehrt α eine ganze Funktion von z, welche die Eigenschaft hat, daß $\alpha\eta = \beta$ eine ganze Funktion ist, so folgt

$$\alpha\nu = \beta\mu,$$

also nach (1)

$$\alpha\mathfrak{b} = \beta\mathfrak{a};$$

da nun $\mathfrak{a}$, $\mathfrak{b}$ relativ prim sind, so muß α durch $\mathfrak{a}$, β durch $\mathfrak{b}$ teilbar sein, und daraus folgt:

Es ist $\mathfrak{a}$ der Inbegriff aller derjenigen ganzen Funktionen α, welche die Eigenschaft haben, daß $\alpha\eta$ eine ganze Funktion ist, und der Inbegriff aller dieser ganzen Funktionen $\alpha\eta$ ist das Ideal $\mathfrak{b}$; oder anders ausgedrückt:

Es ist $\mathfrak{b}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\eta$ und $\mathfrak{o}$, ebenso $\mathfrak{a}$ das kleinste gemeinschaftliche Vielfache von $\frac{\mathfrak{o}}{\eta}$ und $\mathfrak{o}$. Hiernach muß, wenn $\mathfrak{a}'$, $\mathfrak{b}'$ zwei der Bedingung

$$\mathfrak{a}'\eta = \mathfrak{b}'$$

genügende Ideale sind, $\mathfrak{a}'$ durch $\mathfrak{a}$ teilbar sein. Sei also

$$\mathfrak{a}' = \mathfrak{n}\mathfrak{a},$$

so folgt:

$$\mathfrak{b}' = \mathfrak{n}\mathfrak{a}\eta = \mathfrak{n}\mathfrak{b}.$$

Umgekehrt ist auch für ein beliebiges Ideal $\mathfrak{n}$

$$\mathfrak{n}\mathfrak{a}\eta = \mathfrak{n}\mathfrak{b}.$$

2. Es seien jetzt $\mathfrak{a}$, $\mathfrak{b}$ zwei der Bedingung

$$\mathfrak{a}\eta = \mathfrak{b}$$

genügende Ideale, gleichviel ob relativ prim oder nicht. Der Quotient $\frac{\mathfrak{b}}{\mathfrak{a}}$ ist nach § 4, 8. der Inbegriff aller derjenigen Funktionen γ, welche die Eigenschaft haben, daß $\mathfrak{a}\gamma$ durch $\mathfrak{b}$ teilbar ist. Zu diesen Funktionen gehören gewiß alle Funktionen von der Form $\omega\eta$, wenn ω eine beliebige Funktion in $\mathfrak{o}$ bedeutet. Aber auch umgekehrt ist jede Funktion γ von dieser Form; denn da $\mathfrak{a}\gamma$ durch $\mathfrak{b}$, also auch durch $\mathfrak{o}$ teilbar ist, so ist es ein Ideal (da es die Eigenschaften I., II., § 7 besitzt), also wenn $\mathfrak{c}$ gleichfalls ein Ideal ist:

$$\mathfrak{a}\gamma = \mathfrak{c}\mathfrak{b}$$

und durch Multiplikation mit η

$$\mathfrak{b}\gamma = \mathfrak{c}\mathfrak{b}\eta.$$

Ist nun wie oben $\eta = \frac{\nu}{\mu}$, und, wenn ϱ, σ ganze Funktionen sind, $\gamma = \frac{\varrho}{\sigma}$, so folgt hieraus

$$\mathfrak{b}\,\varrho\,\mu = \mathfrak{c}\,\mathfrak{b}\,\nu\,\sigma,$$

also:

$$\mathfrak{o}\,\varrho\,\mu = \mathfrak{c}\,\nu\,\sigma, \quad \mathfrak{o}\,\gamma = \mathfrak{c}\,\eta.$$

Beides zusammen liefert den Satz

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}. \tag{3}$$

Sind in dieser Darstellung $\mathfrak{b}$, $\mathfrak{a}$ relativ prim, was nach 1. stets und nur auf eine Weise angenommen werden kann, so soll $\mathfrak{b}$ das **Oberideal**, $\mathfrak{a}$ das **Unterideal** der Funktion η heißen.

3. Ist wieder allgemein

$$\mathfrak{a}\,\eta = \mathfrak{b}, \quad \text{also} \quad \mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}$$

und α eine beliebige Funktion in $\mathfrak{a}$, β eine zugehörige Funktion in $\mathfrak{b}$, so ist

$$\eta = \frac{\beta}{\alpha} \text{ und } \mathfrak{a}\,\beta = \mathfrak{b}\,\alpha.$$

Hieraus folgt durch Bildung der Normen

$$N(\eta) = \text{konst.}\,\frac{N(\mathfrak{b})}{N(\mathfrak{a})}.$$

4. Sind η, η' zwei Funktionen in Ω und ist wie in 1.

$$\mathfrak{a}\,\eta = \mathfrak{b}; \quad \mathfrak{a}'\,\eta' = \mathfrak{b}',$$

gleichviel ob $\mathfrak{a}$, $\mathfrak{b}$; $\mathfrak{a}'$, $\mathfrak{b}'$ relativ prim sind oder nicht, so folgt

$$\mathfrak{a}\,\mathfrak{a}'\,\eta\,\eta' = \mathfrak{b}\,\mathfrak{b}'.$$

Es folgen also aus

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}, \quad \mathfrak{o}\,\eta' = \frac{\mathfrak{b}'}{\mathfrak{a}'}$$

die Gleichungen

$$\mathfrak{o}\,\eta\,\eta' = \frac{\mathfrak{b}\,\mathfrak{b}'}{\mathfrak{a}\,\mathfrak{a}'}, \quad \mathfrak{o}\,\frac{1}{\eta} = \frac{\mathfrak{a}}{\mathfrak{b}}, \quad \mathfrak{o}\,\frac{\eta}{\eta'} = \frac{\mathfrak{b}\,\mathfrak{a}'}{\mathfrak{a}\,\mathfrak{b}'}.$$

5. Ist $\mathfrak{a}\,\eta = \mathfrak{b}$, $\mathfrak{a}\,\eta' = \mathfrak{b}'$, so wird auch

$$\mathfrak{a}\,(\eta \pm \eta') = \mathfrak{b}''$$

ein Ideal sein, weil, wenn $\alpha\,\eta$, $\alpha\,\eta'$ ganze Funktionen sind, stets auch $\alpha\,(\eta \pm \eta')$ eine solche ist. Ist also

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}, \quad \mathfrak{o}\,\eta' = \frac{\mathfrak{b}'}{\mathfrak{a}},$$

so folgt

$$\mathfrak{o}\,(\eta \pm \eta') = \frac{\mathfrak{b}''}{\mathfrak{a}};$$

haben die beiden Ideale $\mathfrak{b}$, $\mathfrak{b}'$ einen gemeinsamen Teiler, so ist derselbe auch Teiler von $\mathfrak{b}''$.

6. Es sei jetzt ϱ eine Funktion in Ω, deren Oberideal durch ein beliebig gegebenes Primideal $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist (solche Funktionen existieren stets; dieselben können sogar ganze Funktionen von z sein), also

$$\mathfrak{o}\,\varrho = \frac{\mathfrak{m}\,\mathfrak{p}}{\mathfrak{n}},$$

worin $\mathfrak{m}$, $\mathfrak{n}$ durch $\mathfrak{p}$ nicht teilbare Ideale sind. Sei ferner η eine beliebige Funktion in Ω, deren Unterideal durch $\mathfrak{p}$ nicht teilbar ist, also

$$\mathfrak{o}\,\eta = \frac{\mathfrak{b}}{\mathfrak{a}}$$

und $\mathfrak{a}$ nicht teilbar durch $\mathfrak{p}$. Man wähle eine beliebige Funktion α in $\mathfrak{a}$, die nicht durch $\mathfrak{p}$ teilbar ist, und eine entsprechende Funktion β in $\mathfrak{b}$, so daß

$$\eta = \frac{\beta}{\alpha}$$

wird. Sei

$$\alpha \equiv \alpha_0, \quad \beta \equiv \beta_0 \pmod{\mathfrak{p}}, \quad c_0 = \frac{\beta_0}{\alpha_0},$$

worin α_0, β_0, c_0 Konstanten sind, deren erste von Null verschieden ist. Nach 5. ist

$$\mathfrak{o}\,(\eta - c_0) = \mathfrak{o}\,\frac{\beta - c_0\,\alpha}{\alpha} = \frac{\mathfrak{b}_1}{\mathfrak{a}},$$

und aus

$$\mathfrak{a}\,(\beta - c_0\,\alpha) = \mathfrak{b}_1\,\alpha, \quad \beta - c_0\,\alpha \equiv 0 \pmod{\mathfrak{p}}$$

folgt, da α durch $\mathfrak{p}$ nicht teilbar ist, daß $\mathfrak{b}_1$ durch $\mathfrak{p}$ teilbar sein muß. Setzt man also

$$\eta - c_0 = \varrho\,\eta_1,$$

so ist auch das Unterideal von η_1 durch $\mathfrak{p}$ nicht teilbar. Auf diese Weise läßt sich eine ganz bestimmte Reihe von Konstanten $c_0, c_1, \ldots c_{r-1}, \ldots$ derart ermitteln, daß

$$\begin{aligned}
\eta &= c_0 + \varrho\,\eta_1,\\
\eta_1 &= c_1 + \varrho\,\eta_2,\\
&\cdots\cdots\cdots\cdots\\
\eta_{r-1} &= c_{r-1} + \varrho\,\eta_r, \;\ldots,
\end{aligned}$$

worin die $\eta_1, \eta_2, \ldots \eta_r, \ldots$ Funktionen bedeuten, deren Unterideale keine anderen Primfaktoren haben können als das Unterideal von η

und das Oberideal von ϱ mit Ausschluß von $\mathfrak{p}$. Demnach ist für jedes ganze positive r

$$\eta = c_0 + c_1 \varrho + \cdots + c_{r-1} \varrho^{r-1} + \eta_r \varrho^r.$$

Ist das Unterideal von ζ durch $\mathfrak{p}^s$, nicht durch $\mathfrak{p}^{s+1}$ teilbar, so kann man dieselbe Betrachtung auf die Funktion $\eta = \zeta \varrho^s$ anwenden und erhält

$$\zeta = c_0 \varrho^{-s} + c_1 \varrho^{-s+1} + \cdots + c_{r-1} \varrho^{-s+r} + \eta_r \varrho^{-s+r}.$$

§ 13.

Die rationalen Transformationen der Funktionen des Körpers Ω.

Ist z_1 eine beliebige, nicht konstante, Funktion der Körpers Ω (eine Variable in Ω), so besteht, wie in § 2 nachgewiesen, zwischen z_1 und z eine irreduktible algebraische Gleichung, welche, von Nennern befreit, in bezug auf z_1 vom Grade e, in bezug auf z vom Grade e_1 sei. Es ist, wie eben dort gezeigt, e ein Divisor von n, $n = ef$. Es sei diese Gleichung

$$G(\overset{e}{z_1}, \overset{e_1}{z}) = 0. \tag{1}$$

Jede rationale Funktion ζ von z und z_1 läßt sich (§ 1) mit Hilfe dieser Gleichung auf die beiden Formen bringen

$$\left\{\begin{aligned} \zeta &= x_0 + x_1 z_1 + \cdots + x_{e-1} z_1^{e-1}, \\ \zeta &= x_0^{(1)} + x_1^{(1)} z + \cdots + x_{e_1-1}^{(1)} z^{e_1-1}, \end{aligned}\right. \tag{2}$$

und zwar nur auf eine Weise so, daß $x_0, x_1, \ldots x_{e-1}$ rationale Funktionen von z, $x_0^{(1)}, x_1^{(1)}, \ldots x_{e_1-1}^{(1)}$ rationale Funktionen von z_1 sind.

Ist nun θ eine solche Funktion, daß $1, \theta, \theta^2, \ldots \theta^{n-1}$ eine Basis*) von Ω (in bezug auf z) bilden, so bilden nach § 2 die n Funktionen

$$\left\{\begin{array}{llll} 1, & z_1, & z_1^2, \ldots & z_1^{e-1}, \\ \theta, & \theta z_1, & \theta z_1^2, \ldots & \theta z_1^{e-1}, \\ \ldots & \ldots & \ldots & \ldots \\ \theta^{f-1}, & \theta^{f-1} z_1, & \theta^{f-1} z_1^2, \ldots & \theta^{f-1} z_1^{e-1} \end{array}\right. \tag{3}$$

*) Man könnte statt der Basis $1, \theta, \ldots \theta^{n-1}$ auch eine beliebige andere Basis von Ω dieser Betrachtung zugrunde legen. Es genügt aber für unseren Zweck, wenn wir gerade diese wählen.

gleichfalls eine solche Basis, und daraus ergibt sich nach (2), daß zwischen den $e_1 f = n_1$ Funktionen

$$(4) \qquad \begin{cases} 1, & z, & z^2, \ldots & z^{e_1-1}, \\ \theta, & \theta z, & \theta z^2, \ldots & \theta z^{e_1-1}, \\ \ldots & \ldots & \ldots & \ldots \\ \theta^{f-1}, & \theta^{f-1} z, & \theta^{f-1} z^2, \ldots & \theta^{f-1} z^{e_1-1}, \end{cases}$$

die zur Abkürzung mit

$$\eta_1^{(1)}, \quad \eta_2^{(1)}, \quad \ldots \quad \eta_{n_1}^{(1)}$$

bezeichnet sein mögen, eine Gleichung von der Form

$$x_1^{(1)} \eta_1^{(1)} + x_2^{(1)} \eta_2^{(1)} + \cdots + x_{n_1}^{(1)} \eta_{n_1}^{(1)} = 0$$

nur dann besteht, wenn die rationalen Funktionen $x_1^{(1)}, x_2^{(1)}, \ldots x_{n_1}^{(1)}$ von z_1 sämtlich verschwinden. Daraus folgt nach (2), daß jede Funktion η in Ω, und zwar nur auf eine einzige Art, darstellbar ist in der Form:

$$\eta = x_1^{(1)} \eta_1^{(1)} + x_2^{(1)} \eta_2^{(1)} + \cdots + x_{n_1}^{(1)} \eta_{n_1}^{(1)},$$

worin die $x^{(1)}$ rationale Funktionen von z_1 sind.

Jede solche Funktion η genügt einer algebraischen Gleichung vom Grade n_1, deren Koeffizienten rational von z_1 abhängen, denn es ist

$$\begin{aligned} \eta\,\eta_1^{(1)} &= x_{1,1}^{(1)} \eta_1^{(1)} + x_{1,2}^{(1)} \eta_2^{(1)} + \cdots + x_{1,n_1}^{(1)} \eta_{n_1}^{(1)}, \\ \eta\,\eta_2^{(1)} &= x_{2,1}^{(1)} \eta_1^{(1)} + x_{2,2}^{(1)} \eta_2^{(1)} + \cdots + x_{2,n_1}^{(1)} \eta_{n_1}^{(1)}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ \eta\,\eta_{n_1}^{(1)} &= x_{n_1,1}^{(1)} \eta_1^{(1)} + x_{n_1,2}^{(1)} \eta_2^{(1)} + \cdots + x_{n_1,n_1}^{(1)} \eta_{n_1}^{(1)}, \end{aligned}$$

und mithin

$$\begin{vmatrix} x_{1,1}^{(1)} - \eta, & x_{1,2}^{(1)}, & \ldots & x_{1,n_1}^{(1)} \\ x_{2,1}^{(1)}, & x_{2,2}^{(1)} - \eta, & \ldots & x_{2,n_1}^{(1)} \\ \ldots & \ldots & \ldots & \ldots \\ x_{n_1,1}^{(1)}, & x_{n_1,2}^{(1)}, & \ldots & x_{n_1,n_1}^{(1)} - \eta \end{vmatrix} = 0.$$

Es läßt sich nun zeigen, daß man eine Funktion $\eta = \theta_1$ so auswählen kann, daß θ_1 nicht zugleich einer Gleichung niedrigeren Grades, deren Koeffizienten rational von z_1 abhängen, genügt.

Wir stützen uns zum Beweis dieser Behauptung auf den folgenden Satz, dessen Beweis sich leicht durch den Schluß von $m - 1$ auf m ergibt. Ist

$$F(x_1, x_2, \ldots x_m)$$

eine ganze rationale Funktion von $x_1, x_2, \ldots x_m$, deren Koeffizienten Funktionen in Ω sind, die nicht alle verschwinden, so kann man für die $x_1, x_2, \ldots x_m$ solche konstanten oder rational von z_1 abhängigen Größen setzen, daß F in eine nicht verschwindende Funktion in Ω übergeht. Ist also $F(x_1, x_2, \ldots x_m)$ für alle solche $x_1, x_2, \ldots x_m$ gleich Null, so folgt auch für beliebige konstante oder rational von z_1 abhängige $dx_1, dx_2, \ldots dx_m$

$$dF = F'(x_1)\,dx_1 + F'(x_2)\,dx_2 + \cdots + F'(x_m)\,dx_m = 0.$$

Ist nun

$$\theta_1 = x_1\,\eta_1^{(1)} + x_2\,\eta_2^{(1)} + \cdots + x_{n_1}\,\eta_{n_1}^{(1)}$$

und

$$(5) \cdot \cdot \quad \left\{\begin{array}{l} 1 \;\;= x_{1,0}\;\eta_1^{(1)} + x_{2,0}\;\eta_2^{(1)} + \cdots + x_{n_1,0}\,\eta_{n_1}^{(1)}, \\ \theta_1 \;= x_{1,1}\;\eta_1^{(1)} + x_{2,1}\;\eta_2^{(1)} + \cdots + x_{n_1,1}\,\eta_{n_1}^{(1)}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \theta_1^m = x_{1,m}\,\eta_1^{(1)} + x_{2,m}\,\eta_2^{(1)} + \cdots + x_{n_1,m}\,\eta_{n_1}^{(1)}, \end{array}\right.$$

so sind die $x_{k,h}$ ganze rationale und homogene Funktionen vom Grade h von $x_1, x_2, \ldots x_{n_1}$ und hängen außerdem rational von z_1 ab.

Ist also

$$\varphi(\theta_1) = a_m\,\theta_1^m + a_{m-1}\,\theta_1^{m-1} + \cdots + a_1\,\theta_1 + a_0 = 0$$

die Gleichung niedrigsten Grades, welcher θ_1 genügt, deren Koeffizienten rational von z_1 abhängen, so genügen die Funktionen $a_0, a_1, \ldots a_m$ der Bedingung

$$a_0\,x_{\iota,0} + a_1\,x_{\iota,1} + \cdots + a_m\,x_{\iota,m} = 0, \qquad (\iota = 1, 2, \ldots n_1)$$

und zugleich ist $m \gtreqless n_1$. Da nun nicht alle aus den Koeffizienten $x_{h,k}$ zu bildenden m-reihigen Determinanten verschwinden können, weil sonst θ_1 einer Gleichung von niedrigerem als dem m^{ten} Grade genügen würde, so folgt aus letzteren Gleichungen, daß man die $a_0, a_1, \ldots a_m$ als ganze homogene Funktionen von $x_1, x_2, \ldots x_{n_1}$ voraussetzen kann.

Wenn nun die Gleichung $\varphi(\theta_1) = 0$ für alle rational von z_1 abhängigen $x_1, x_2, \ldots x_{n_1}$ bestehen soll, so muß nach obigem Satze auch

$$d\varphi = \varphi'(\theta_1)\,d\theta_1 + da_m\,\theta_1^m + \cdots + da_1\,\theta_1 + da_0 = 0$$

sein, und wenn $m < n_1$ ist, so lassen sich die $dx_1, dx_2, \ldots dx_{n_1}$, ohne daß sie alle verschwinden, so bestimmen, daß

$$da_m : da_{m-1} : \cdots : da_1 : da_0 = a_m : a_{m-1} : \cdots : a_1 : a_0$$

und folglich

$$\varphi'(\theta_1)\,d\theta_1 = 0$$

ist. Da aber $\varphi'(\theta_1)$ vom Grade $m-1$ ist, so muß $d\theta_1 = 0$, also $dx_1 = 0$, $dx_2 = 0$, ... $dx_{n_1} = 0$ sein. Daher kann nur $m = n_1$ sein.

Ist also θ_1 so bestimmt, daß die Gleichung niedrigsten Grades

$$\overset{n_1}{F_1}(\theta_1, z_1) = 0$$

den Grad n_1 wirklich erreicht, so lassen sich alle Funktionen in Ω, und zwar nur auf eine Weise in der Form darstellen

$$\eta = x_0^{(1)} + x_1^{(1)}\theta_1 + \cdots + x_{n_1-1}^{(1)}\,\theta_1^{n_1-1},$$

worin die Koeffizienten $x_0^{(1)}, x_1^{(1)}, \ldots x_{n_1-1}^{(1)}$ rational von z_1 abhängen; denn man kann unter dieser Voraussetzung $\eta_1^{(1)}, \eta_2^{(1)}, \ldots \eta_{n_1}^{(1)}$ vermittelst der Gleichungen (5) in der angegebenen Weise darstellen.

Es lassen sich also sowohl z_1, θ_1 rational durch z, θ, als auch umgekehrt z, θ rational durch z_1, θ_1 darstellen.

Die Variable z, die wir bisher als die unabhängige bezeichnet haben, kann daher jede beliebige (nicht konstante) Funktion des Körpers Ω sein. Während aber die Gesamtheit aller Funktionen des Körpers Ω gänzlich ungeändert bleibt, sind die Begriffe: Basis, Norm, Spur, Diskriminante, ganze Funktion, Modul, Ideal wesentlich abhängig von der Wahl der unabhängigen Veränderlichen z.

In dem besonderen Falle nur, wenn zwei Variable z, z_1 linear voneinander abhängen, ist eine Basis von Ω in bezug auf z zugleich eine solche in bezug auf z_1; ebenso sind Normen, Spuren und Diskriminanten in diesem Falle für z und z_1 identisch.

Sind α, β irgend zwei Funktionen in Ω, so bestehen zwischen denselben Gleichungen, deren linker Teil eine ganze rationale Funktion von α und β ist.

Unter diesen ist eine (nach § 1)

$$F(\alpha, \beta) = 0,$$

welche sowohl in bezug auf α als in bezug auf β von möglichst niedrigem Grade ist, und diese soll die zwischen α und β bestehende irreduktible Gleichung heißen. Diese ist, von einem konstanten Faktor abgesehen, völlig bestimmt.

II. Abteilung.

§ 14.

Die Punkte der Riemannschen Fläche.

Die bisherigen Betrachtungen über die Funktionen des Körpers Ω waren rein formaler Natur. Alle Resultate waren rationale, d. h. nach den Regeln der Buchstabenrechnung mittels der vier Spezies abgeleitete Folgerungen aus der zwischen zwei Funktionen in Ω bestehenden irreduktiblen Gleichung. Die numerischen Werte dieser Funktionen kamen nirgends in Betracht. Man würde sogar, ohne andere Prinzipien anzuwenden, die formelle Behandlung noch wesentlich weitertreiben können, indem man zwei Funktionen des Körpers Ω nicht als durch eine Gleichung verbunden, sondern als unabhängige Veränderliche auffaßt, wobei dann alles auf algebraische Teilbarkeit von rationalen Funktionen zweier Veränderlichen hinausläuft. Wir haben auch diesen Weg durchgeführt, der jedoch in Darstellung und Ausdrucksweise sehr schwerfällig ist und bezüglich der Strenge nicht mehr leistet als der im vorhergehenden benutzte Gang. Nachdem nun aber der formale Teil der Untersuchung soweit geführt ist, drängt sich die Frage auf, in welchem Umfange es möglich ist, den Funktionen in Ω solche bestimmten Zahlenwerte beizulegen, daß alle zwischen diesen Funktionen bestehenden rationalen Relationen (Identitäten) in richtige Zahlengleichungen übergehen. Es erweist sich bei dieser Untersuchung als zweckmäßig, auch das Unendlichgroße als eine bestimmte Zahl ∞ (Konstante) zu betrachten, mit welcher nach bestimmten Regeln gerechnet wird*). Die mittels der rationalen Operationen in dem so erweiterten Zahlengebiet ausgeführten Rechnungen führen stets zu einem ganz bestimmten Zahlenresultat, wenn nicht im Verlaufe der Rechnung eines der Zeichen $\infty \pm \infty$, $0 \cdot \infty$, $\frac{0}{0}$, $\frac{\infty}{\infty}$ auftritt, Zeichen, welchen kein bestimmter Wert zukommt. Das Auftreten einer solchen Unbestimmtheit in einer Gleichung ist nicht als ein Widerspruch aufzufassen, da in diesem Falle die Gleichung gar keine bestimmte Be-

*) Das Unendliche als einen bestimmten Wert zu betrachten ist in der Funktionentheorie vielfach üblich und nützlich. Es spricht sich dies bei Riemann z. B. darin aus, daß er seine die algebraischen Funktionen darstellenden Flächen als geschlossen betrachtet.

hauptung mehr enthält, also von der Wahrheit oder Unwahrheit derselben auch keine Rede sein kann. Unter den Funktionen des Körpers Ω finden sich außer unendlich vielen Veränderlichen auch sämtliche Konstanten, d. h. Zahlen. Hiernach gelangt man durch die oben gestellte Forderung zu folgendem Begriff.

1. Definition. Wenn alle Individuen $\alpha, \beta, \gamma, \ldots$ des Körpers Ω durch bestimmte Zahlwerte $\alpha_0, \beta_0, \gamma_0, \ldots$ so ersetzt werden, daß

$$\text{(I.)} \quad \alpha_0 = \alpha, \text{ falls } \alpha \text{ konstant ist, und allgemein}$$

$$\text{(II.)} \quad (\alpha + \beta)_0 = \alpha_0 + \beta_0, \qquad \text{(IV.)} \quad (\alpha\beta)_0 = \alpha_0 \beta_0,$$

$$\text{(III.)} \quad (\alpha - \beta)_0 = \alpha_0 - \beta_0, \qquad \text{(V.)} \quad \left(\frac{\alpha}{\beta}\right)_0 = \frac{\alpha_0}{\beta_0}$$

wird, so soll einem solchen Zusammentreffen bestimmter Werte ein Punkt $\mathfrak{P}$ zugeordnet werden [den man sich zur Versinnlichung irgendwie im Raume gelegen vorstellen mag *)], und wir sagen, in $\mathfrak{P}$ sei $\alpha = \alpha_0$, oder α habe in $\mathfrak{P}$ den Wert α_0. Zwei Punkte heißen stets und nur dann verschieden, wenn eine Funktion α in Ω existiert, die in beiden Punkten verschiedene Werte hat.

Aus dieser Definition des Punktes soll nun die Existenz desselben, sowie der Umfang des Begriffes deduziert werden. Zunächst ist aber hervorzuheben, daß nach dieser Definition der „Punkt" ein zum Körper Ω gehöriger invarianter Begriff ist, der in keiner Weise abhängt von der Wahl der unabhängigen Veränderlichen, durch welche man die Funktionen des Körpers darstellt.

2. Satz. Ist ein Punkt $\mathfrak{P}$ gegeben, und z eine in $\mathfrak{P}$ endliche Variable in Ω (eine solche existiert für jeden Punkt; denn ist $z_0 = \infty$, so ist $\left(\frac{1}{z}\right)_0 = 0$, also endlich), so hat auch jede ganze Funktion ω von z in $\mathfrak{P}$ einen endlichen Wert ω_0 — denn zwischen ω und z besteht eine Relation von der Form

$$1 = a\,\frac{1}{\omega} + b\,\frac{1}{\omega^2} + \cdots + k\,\frac{1}{\omega^m},$$

*) Eine geometrische Versinnlichung des „Punktes" ist übrigens keineswegs notwendig und trägt zu einer leichteren Auffassung nicht einmal viel bei. Es genügt, das Wort „Punkt" als einen kurzen und bequemen Ausdruck für die beschriebene Wert-Koexistenz zu betrachten.

worin $a, b, \ldots k$ als ganze rationale Funktionen von z nach (II.), (III.), (IV.) in $\mathfrak{P}$ endliche Werte haben. Mithin kann $\left(\frac{1}{\omega}\right)_0$ nicht gleich 0, also ω_0 nicht gleich ∞ sein.

3. Satz. Ist z irgendeine in $\mathfrak{P}$ endliche Variable, so ist der Inbegriff $\mathfrak{p}$ aller derjenigen ganzen Funktionen π von z, welche in $\mathfrak{P}$ verschwinden, ein Primideal in z; wir sagen, der Punkt $\mathfrak{P}$ erzeuge dies Primideal $\mathfrak{p}$. Ist ω eine ganze Funktion von z, welche in $\mathfrak{P}$ den Wert ω_0 hat, so ist $\omega \equiv \omega_0$ (mod. $\mathfrak{p}$).

Beweis. Ist $\pi_0' = 0, \pi_0'' = 0$, so ist auch $(\pi' + \pi'')_0 = \pi_0' + \pi_0'' = 0$, und wenn ω eine beliebige ganze Funktion von z, also ω_0 endlich ist, so folgt aus $\pi_0 = 0$ auch $(\omega\pi)_0 = \omega_0\pi_0 = 0$; also ist $\mathfrak{p}$ ein Ideal in z (§ 7, I., II.). Das Ideal $\mathfrak{p}$ ist von $\mathfrak{o}$ verschieden, da es die Funktion „1" nicht enthält.

Hat ω in $\mathfrak{P}$ den Wert ω_0, so ist $(\omega - \omega_0)_0 = 0$, folglich $\omega \equiv \omega_0$ (mod. $\mathfrak{p}$), also jede ganze Funktion von z einer Konstanten kongruent nach dem Modul $\mathfrak{p}$. Daher ist (§ 9, 7.) $\mathfrak{p}$ ein Primideal.

4. Satz. Dasselbe Primideal $\mathfrak{p}$ kann nicht durch zwei verschiedene Punkte erzeugt werden.

Denn zunächst ist der Wert einer jeden ganzen Funktion ω in einem das Ideal $\mathfrak{p}$ erzeugenden Punkt $\mathfrak{P}$ durch die Kongruenz $\omega \equiv \omega_0$ (mod. $\mathfrak{p}$) vollkommen bestimmt. Ist aber η eine beliebige Funktion in Ω, so lassen sich nach § 12, 1. zwei ganze Funktionen α, β, die nicht beide durch $\mathfrak{p}$ teilbar sind, so bestimmen, daß

$$\eta = \frac{\alpha}{\beta}$$

wird. Da nun die endlichen Werte α_0, β_0 nicht beide verschwinden, so folgt aus (V.)

$$\eta_0 = \frac{\alpha_0}{\beta_0},$$

also ebenfalls durch $\mathfrak{p}$ vollkommen bestimmt.

Es ergibt sich hieraus noch, daß zwei Punkte, in denen eine Variable z endliche Werte hat, dann und nur dann voneinander verschieden sind, wenn eine ganze Funktion von z existiert, welche in beiden verschiedene Werte hat.

5. Satz. Ist z irgendeine Variable in Ω und $\mathfrak{p}$ ein Primideal in z, so gibt es einen (und nach 4. auch nur einen) Punkt $\mathfrak{P}$,

welcher dies Primideal erzeugt, und welcher der **Nullpunkt** des Ideals $\mathfrak{p}$ genannt werden soll.

Beweis. Es sei η eine beliebige Funktion in Ω, und ϱ eine solche, deren Oberideal durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist. Es lassen sich dann nach § 12, 6. stets und nur auf eine Weise eine ganze Zahl m, eine von Null verschiedene endliche Konstante c und eine Funktion η_1, deren Unterideal nicht durch $\mathfrak{p}$ teilbar ist, so bestimmen, daß

$$\eta = c\,\varrho^m + \eta_1\,\varrho^{m+1}.$$

Wir setzen

$$\eta_0 = 0, \quad c, \quad \infty,$$

je nachdem m positiv, Null oder negativ ist. Dieser Wertbestimmung der Funktionen des Körpers Ω entspricht ein Punkt $\mathfrak{P}$, da die Bedingungen (I.) bis (V.), wie man sofort übersieht, erfüllt sind*).

Jede Funktion, deren Oberideal durch $\mathfrak{p}$ teilbar ist, also insbesondere jede Funktion in $\mathfrak{p}$ erhält nach dieser Festsetzung in $\mathfrak{P}$ den Wert Null, d. h. der so bestimmte Punkt $\mathfrak{P}$ erzeugt das Primideal $\mathfrak{p}$.

Jede Funktion, deren Unterideal durch $\mathfrak{p}$ teilbar ist, und nur eine solche hat in $\mathfrak{P}$ den Wert ∞, und daraus geht hervor, daß eine ganze Funktion von z in keinem Punkte, in welchem z einen endlichen Wert hat, unendlich ist, und, da eine gebrochene Funktion von z im Unterideal gewiß ein Primideal enthält, also mindestens in einem Punkte, in welchem z endlich ist, unendlich sein muß, so ist auch umgekehrt jede Funktion, die in keinem Punkte, in welchem z einen endlichen Wert hat, unendlich ist, eine ganze Funktion von z.

6. Aus 3., 4., 5. ergibt sich nun das folgende Resultat. Um alle existierenden Punkte $\mathfrak{P}$ und jeden nur ein einziges Mal zu erhalten, ergreife man eine beliebige Variable z des Körpers Ω; man bilde alle Primideale $\mathfrak{p}$ in z und konstruiere für jedes derselben den Nullpunkt, so sind alle diejenigen Punkte $\mathfrak{P}$ gefunden, in denen z

---

*) Ist $\eta' = c'\varrho^{m'} + \eta'_1\varrho^{m'+1}$, so ist z. B.

$$\frac{\eta}{\eta'} = \varrho^{m-m'}\left(\frac{c}{c'} + \varrho\,\eta''_1\right),$$

worin

$$\eta''_1 = \frac{c'\eta_1 - c\,\eta'_1}{c'(c' + \varrho\,\eta'_1)}$$

eine Funktion von derselben Beschaffenheit ist wie η_1 (noch einfacher ist der Beweis in den übrigen Fällen).

endlich bleibt; ist $\mathfrak{P}'$ ein von diesen verschiedener Punkt, so hat in ihm $z' = \frac{1}{z}$ den endlichen Wert Null; umgekehrt ist jeder Punkt $\mathfrak{P}'$, in dem z' den Wert Null hat, von den Punkten $\mathfrak{P}$ verschieden. Das durch einen solchen Punkt $\mathfrak{P}'$ erzeugte Primideal $\mathfrak{p}'$ in z' (welches aus allen in $\mathfrak{P}'$ verschwindenden ganzen Funktionen von z' besteht) geht in z' auf, und umgekehrt ist der Nullpunkt eines jeden in z' aufgehenden Primideals $\mathfrak{p}'$ in z' ein Punkt $\mathfrak{P}'$, in welchem $z' = 0$ also $z = \infty$ ist. Mit diesen in endlicher Anzahl vorhandenen, den verschiedenen $\mathfrak{p}'$ entsprechenden Ergänzungspunkten und den vorher aus den Primidealen $\mathfrak{p}$ in z abgeleiteten ist die Gesamtheit aller Punkte $\mathfrak{P}$ erschöpft, deren Inbegriff die Riemannsche Fläche T bildet.

§ 15.

Die Ordnungszahlen.

1. Definition. Ist $\mathfrak{P}$ ein bestimmter Punkt, so betrachten wir die sämtlichen in $\mathfrak{P}$ verschwindenden Funktionen π in Ω, und erteilen jeder derselben eine bestimmte Ordnungszahl nach folgendem Gesichtspunkt.

Eine solche Funktion ϱ hat die Ordnungszahl 1, oder heißt unendlich klein in der ersten Ordnung oder 0^1 in $\mathfrak{P}$, wenn alle Quotienten $\frac{\pi}{\varrho}$ in $\mathfrak{P}$ endlich bleiben. Ist ϱ' eine ebensolche Funktion wie ϱ, so ist $\frac{\varrho'}{\varrho}$ in $\mathfrak{P}$ weder 0 noch ∞, und umgekehrt, ist $\frac{\varrho'}{\varrho}$ in $\mathfrak{P}$ weder 0 noch ∞, so ist ϱ' gleichfalls unendlich klein von der ersten Ordnung. Gibt es ferner für irgendeine Funktion π einen ganzen positiven Exponenten r, so daß $\frac{\pi}{\varrho^r}$ in $\mathfrak{P}$ weder 0 noch ∞ wird, so gilt dasselbe von $\frac{\pi}{\varrho'^r}$, und π erhält die Ordnungszahl r oder heißt unendlich klein in der Ordnung r im Punkte $\mathfrak{P}$. Wir werden auch sagen, π ist 0^r in $\mathfrak{P}$ oder π ist 0 in $\mathfrak{P}^r$.

Um die Frage nach der Existenz solcher Funktionen ϱ und solcher Ordnungszahlen r zu entscheiden, ergreife man eine beliebige in $\mathfrak{P}$ endliche Variable z, bezeichne mit $\mathfrak{p}$ das durch $\mathfrak{P}$ erzeugte Primideal in z, und stelle jede Funktion π (mit Ausnahme der ordnungslosen Konstanten 0) nach § 12 als Quotienten von zwei relativen Primidealen in z dar. Das Oberideal jeder dieser Funktionen ist dann durch $\mathfrak{p}$ teilbar, und es gibt darunter auch solche, deren Oberideal nicht durch $\mathfrak{p}^2$ teilbar ist; diese haben die Ordnungszahl 1; für die übrigen Funktionen π ist die Ordnungszahl der Exponent der höchsten im Oberideal aufgehenden Potenz von $\mathfrak{p}$, was sich aus den Sätzen des § 12 ohne weiteres ergibt.

2. Hat eine Funktion η den endlichen Wert η_0 in $\mathfrak{P}$, so sagen wir, η habe diesen Wert r-mal in $\mathfrak{P}$ oder in r mit $\mathfrak{P}$ zusammenfallenden Punkten oder in $\mathfrak{P}^r$, wenn die Funktion $\eta - \eta_0$ in $\mathfrak{P}$ unendlich klein in der Ordnung r ist. Ist aber $\eta_0 = \infty$, so sagen wir, η habe den Wert ∞ r-mal in $\mathfrak{P}$ oder in r mit $\mathfrak{P}$ zusammenfallenden Punkten, oder η sei ∞^r in $\mathfrak{P}$ oder ∞ in $\mathfrak{P}^r$, wenn $\dfrac{1}{\eta}$ in $\mathfrak{P}^r$ verschwindet.

3. Wird eine Funktion η in $\mathfrak{P}$ ∞^r, so legen wir derselben auch die Ordnungszahl $-r$ bei, wenn aber η in $\mathfrak{P}$ weder 0 noch ∞ wird, so habe sie die Ordnungszahl 0. Hiernach kommt in einem beliebigen Punkte $\mathfrak{P}$ jeder Funktion des Körpers Ω eine ganz bestimmte Ordnungszahl zu, mit Ausnahme der beiden Konstanten 0 und ∞.

4. Ist ϱ eine Funktion, welche in einem beliebigen Punkte $\mathfrak{P}$ die Ordnungszahl 1 besitzt, und η eine Funktion mit der (positiven, negativen oder verschwindenden) Ordnungszahl m, so läßt sich nach dem Schlußsatz des § 12 für jedes beliebige positive r eine Reihe von Konstanten $c_0, c_1, \ldots c_{r-1}$, deren erste nicht verschwindet, und eine in $\mathfrak{P}$ endliche Funktion σ so bestimmen, daß

$$\eta = c_0 \varrho^m + c_1 \varrho^{m-1} + \cdots + c_{r-1} \varrho^{m+r-1} + \sigma \varrho^{m+r}$$

wird.

5. Hieraus ergibt sich unmittelbar, daß die Ordnungszahl eines Produktes zweier oder mehrerer Funktionen gleich ist der Summe der Ordnungszahlen der einzelnen Faktoren.

Die Ordnungszahl eines Quotienten zweier Funktionen ist gleich der Differenz der Ordnungszahlen des Zählers und Nenners.

Ist $\eta_1, \eta_2, \ldots \eta_s$ eine Reihe von Funktionen und m die algebraisch kleinste unter ihren Ordnungszahlen, so ist

$$\begin{aligned} \eta_1 &= e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\ \eta_2 &= e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\ &\cdots\cdots\cdots\cdots \\ \eta_s &= e_s \varrho^m + \sigma_s \varrho^{m+1}, \end{aligned}$$

worin die Konstanten $e_1, e_2, \ldots e_s$ jedenfalls nicht alle verschwinden. Sind daher $c_1, c_2, \ldots c_s$ Konstanten, so ist die Ordnungszahl von

$$\eta = c_1 \eta_1 + c_2 \eta_2 + \cdots + c_s \eta_s,$$

falls $c_1 e_1 + c_2 e_2 + \cdots + c_s e_s$ von Null verschieden ist, ebenfalls m, sonst größer als m.

6. Komplexe von Punkten, welche denselben Punkt auch mehrmals enthalten können, nennen wir Polygone und bezeichnen dieselben mit $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$

Es bedeute ferner $\mathfrak{A}\mathfrak{B}$ das aus den Punkten von $\mathfrak{A}$ und von $\mathfrak{B}$ zusammengesetzte Polygon in der Weise, daß, wenn ein Punkt $\mathfrak{P}$ r-mal in $\mathfrak{A}$, s-mal in $\mathfrak{B}$ auftritt, er $(r+s)$-mal in $\mathfrak{A}\mathfrak{B}$ vorkommt. Daraus ergibt sich die Bedeutung von $\mathfrak{P}^r$ und von $\mathfrak{A} = \mathfrak{P}^r \mathfrak{P}_1^{r_1} \mathfrak{P}_2^{r_2} \ldots$, und die Gesetze der Teilbarkeit der Polygone in vollkommener Übereinstimmung mit denen der Teilbarkeit der ganzen Zahlen und der Ideale. Die Rolle der Primfaktoren übernehmen dabei die Punkte; um aber auch die Einheit zu erhalten, muß man das gar keinen Punkt enthaltende Polygon $\mathfrak{O}$ (das Nulleck) zulassen.

Die Anzahl der Punkte eines Polygons heißt seine Ordnung. Ein Polygon von der Ordnung n wird auch kurz ein n-Eck genannt.

Der größte gemeinschaftliche Teiler zweier Polygone $\mathfrak{A}, \mathfrak{B}$ ist dasjenige Polygon, welches jeden Punkt $\mathfrak{P}$ so oft enthält, als er in $\mathfrak{A}$ und $\mathfrak{B}$ mindestens vorkommt. Ist dies $\mathfrak{O}$, so heißen $\mathfrak{A}, \mathfrak{B}$ relativ prim.

Das kleinste gemeinschaftliche Vielfache von $\mathfrak{A}$ und $\mathfrak{B}$ ist dasjenige Polygon, welches jeden Punkt so oft enthält, als er in $\mathfrak{A}$ und $\mathfrak{B}$ höchstens vorkommt. Sind $\mathfrak{A}, \mathfrak{B}$ relativ prim, so ist $\mathfrak{A}\mathfrak{B}$ ihr kleinstes gemeinschaftliches Vielfache.

Ist $\mathfrak{A} = \mathfrak{P}^r \mathfrak{P}_1^{r_1} \mathfrak{P}_2^{r_2} \ldots$ ein beliebiges Polygon, so gibt es stets Funktionen z in Ω, welche in keinem der Punkte $\mathfrak{A}$ unendlich sind. Denn wenn z in einigen Punkten von $\mathfrak{A}$ unendlich ist, so kann man eine Konstante c so wählen, daß $z - c$ in keinem der Punkte von $\mathfrak{A}$ den Wert 0 hat, und dann ist $\dfrac{1}{z-c}$ in allen Punkten des Polygons $\mathfrak{A}$ endlich. Legt man eine solche Variable z zugrunde, so ist der Inbegriff aller derjenigen ganzen Funktionen von z, welche in den Punkten des Polygons $\mathfrak{A}$ (jeden nach seiner Vielfachheit gezählt) verschwinden, ein Ideal $\mathfrak{a} = \mathfrak{p}^r \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r} \ldots$, und man kann sagen, das Polygon $\mathfrak{A}$ erzeuge das Ideal $\mathfrak{a}$, oder $\mathfrak{A}$ sei das Nullpolygon des

Ideals $\mathfrak{a}$. Der Idealbegriff fällt hiernach vollständig zusammen mit dem Begriff eines Systems ganzer Funktionen, welche alle in denselben festen Punkten verschwinden. Das Ideal $\mathfrak{o}$ wird erzeugt durch das Nulleck $\mathfrak{O}$.

Das Produkt zweier oder mehrerer Ideale wird erzeugt durch das Produkt der Nullpolygone der Faktoren, größter gemeinschaftlicher Teiler und kleinstes gemeinschaftliches Vielfache zweier Ideale durch den größten gemeinschaftlichen Teiler und das kleinste gemeinschaftliche Vielfache der entsprechenden Nullpolygone.

7. Satz. Ist z irgendeine Variable in Ω und n der Grad des Körpers Ω in bezug auf z, so nimmt z jeden bestimmten Wert c in genau n Punkten an. — Denn wenn $\mathfrak{o}$ das System aller ganzen Funktionen von z und c eine endliche Konstante bedeutet, so ist

$$\mathfrak{o}(z-c) = \mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2}\ldots, \qquad e_1 + e_2 + \cdots = n \quad (\S\ 9,\ 7.),$$

wenn $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ voneinander verschiedene Primideale in z bedeuten. Bezeichnet man mit $\mathfrak{P}_1, \mathfrak{P}_2, \ldots$ die Nullpunkte von $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$, so hat nach 2. z den Wert c in e_1 Punkten $\mathfrak{P}_1$ (oder in $\mathfrak{P}_1^{e_1}$), in e_2 Punkten $\mathfrak{P}_2$ (oder in $\mathfrak{P}_2^{e_2}$) usf., also in den n Punkten des Polygons $\mathfrak{P}_1^{e_1}\,\mathfrak{P}_2^{e_2}\ldots$ Umgekehrt: ist $\mathfrak{P}$ ein Punkt, in welchem z den Wert c hat, und $\mathfrak{p}$ das durch $\mathfrak{P}$ erzeugte Primideal in z, so ist $z \equiv c$ (mod. $\mathfrak{p}$), und folglich ist $\mathfrak{p}$ eines der Ideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$, mithin $\mathfrak{P}$ einer der Punkte $\mathfrak{P}_1\,\mathfrak{P}_2\ldots$ Dasselbe Resultat gilt aber auch für $c = \infty$; denn weil n auch der Grad von Ω in bezug auf $\frac{1}{z}$ ist, so nimmt letztere Variable den Wert 0, folglich z den Wert ∞ in genau n Punkten an. Aus § 11 folgt, daß nur für eine endliche Anzahl von Werten der Konstanten c einer der Exponenten $e_1, e_2, \ldots$ größer als 1 sein kann.

Die Zahl n, d. h. die Anzahl der Punkte, in welchen die Funktion z je einen konstanten Wert hat, soll die Ordnung der Funktion z genannt werden. Die Konstanten und nur diese haben die Ordnung Null. Für alle anderen Funktionen in Ω ist die Ordnung eine positive ganze Zahl. Die Ordnung einer Variablen z ist zugleich der Grad des Körpers Ω in bezug auf z.

§ 16.

Konjugierte Punkte und konjugierte Werte.

1. Definition. Ist c ein bestimmter Zahlwert, so entspricht demselben, wie in § 15 gezeigt, ein Polygon $\mathfrak{A}$ von n (gleichen oder

verschiedenen) Punkten $\mathfrak{P}', \mathfrak{P}'', \ldots \mathfrak{P}^{(n)}$, in welchen die Variable n^{ter} Ordnung z eben diesen Wert hat; diese n Punkte sollen konjugiert nach z heißen; durch einen von ihnen (und durch die Variable z) sind die übrigen bestimmt. Läßt man c nach und nach alle Werte annehmen, so bewegt sich das Polygon $\mathfrak{A} = \mathfrak{P}'\mathfrak{P}'' \ldots \mathfrak{P}^{(n)}$, und zwar so, daß stets alle seine Punkte sich verändern. Man erhält hierbei also alle überhaupt existierenden Punkte und nur diejenigen (in endlicher Anzahl vorhandenen) mehrfach, in welchen $z - z_0$ oder $\frac{1}{z}$ in höherer als der ersten Ordnung verschwindet. Es ist daher das Produkt aller dieser Polygone

$$\Pi\mathfrak{A} = T\,\mathfrak{Z}_z,$$

wo T die einfache Gesamtheit aller Punkte, die Riemannsche Fläche, $\mathfrak{Z}_z$ ein bestimmtes endliches Polygon ist, welches das Verzweigungs- oder Windungspolygon von T in z heißt. Jeder in $\mathfrak{Z}_z$ enthaltene Punkt $\mathfrak{Q}$ heißt ein Verzweigungs- oder Windungspunkt von T in z, und zwar von der Ordnung s, wenn er genau s-mal in $\mathfrak{Z}_z$ vorkommt. Es ist $s = e - 1$, wenn $z - z_0$ oder $\frac{1}{z}$ in $\mathfrak{Q}$ unendlich klein von der e^{ten} Ordnung ist. Die Ordnung des Polygons $\mathfrak{Z}_z$ heißt die Verzweigungs- oder Windungszahl w_z der Fläche T nach z. Diejenigen Punkte des Verzweigungspolygons, in welchen z einen endlichen Wert hat, erzeugen zusammen das Verzweigungsideal in z (§ 11).

Will man von dieser Definition der „absoluten“ Riemannschen Fläche, welche ein zu dem Körper Ω gehöriger invarianter Begriff ist, zu der bekannten Riemannschen Vorstellung übergehen, so hat man sich die Fläche in einer z-Ebene ausgebreitet zu denken, welche sie dann überall mit Ausnahme der Verzweigungspunkte n-fach bedeckt.

2. Satz. Ist

$$z' = \frac{c + dz}{a + bz},$$

worin a, b, c, d Konstanten bedeuten, deren Determinante $ad - bc$ von Null verschieden ist, so ist

$$\mathfrak{Z}_z = \mathfrak{Z}_{z'}; \quad \mathrm{w}_z = \mathrm{w}_{z'}.$$

Denn wenn in einem Punkte $\mathfrak{P}$ $z - z_0$ oder $\frac{1}{z}$ unendlich klein in der e^{ten} Ordnung ist, so ist in demselben Punkte auch

$$z' - z'_0 = \frac{(ad - bc)(z - z_0)}{(a + bz)(a + bz_0)},$$

oder falls z_0 unendlich ist:

$$z' - z'_0 = \frac{-(ad - bc)}{b(a + bz)},$$

oder falls $z'_0 = \infty$, also $a + bz_0 = 0$ ist:

$$\frac{1}{z'} = \frac{a + bz}{c + dz}$$

unendlich klein in der e^{ten} Ordnung.

Ist insbesondere $z' = \frac{1}{z}$, so ist die Verzweigungszahl $\mathrm{w}_z = \mathrm{w}_{z'}$ gleich dem Grade der Diskriminante $\Delta_z(\Omega)$ vermehrt um die Anzahl der verschwindenden Wurzeln von $\Delta_{z'}(\Omega) = 0$ (§ 11).

3. Definition. Die Werte $\eta', \eta'', \ldots \eta^{(n)}$, welche eine beliebige Funktion η in Ω in n nach z konjugierten Punkten $\mathfrak{P}', \mathfrak{P}'', \ldots \mathfrak{P}^{(n)}$ annimmt, heißen konjugierte Werte von η nach z.

4. Satz. Ist $N_z(\eta)$ die Norm einer beliebigen Funktion in bezug auf z, so ist der Wert, welchen diese rationale Funktion von z für $z = z_0$ besitzt, gleich dem Produkt $\eta' \eta'' \ldots \eta^{(n)}$ der zu $z = z_0$ gehörigen konjugierten Werte von η, wobei von dem Falle, daß dies Produkt unbestimmt wird, also einer dieser konjugierten Werte 0, ein anderer ∞ ist, abzusehen ist. Beim Beweis dieses Satzes können wir annehmen, es sei z_0 endlich; denn ist $z_0 = \infty$, so legen wir statt z die Variable $z' = \frac{1}{z}$ zugrunde, wobei die Norm ungeändert bleibt. Ferner können wir annehmen, die Werte $\eta', \eta'', \ldots \eta^{(n)}$ seien alle endlich; denn ist einer von ihnen unendlich, so ist n. V. keiner derselben gleich 0, und wir betrachten statt η die Funktion $\frac{1}{\eta}$.

Es sei nun unter diesen Voraussetzungen

$$\mathfrak{o}(z - z_0) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3} \ldots$$

und $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \ldots$ die Nullpunkte der voneinander verschiedenen Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots$ Wir konstruieren ein System ganzer Funktionen λ, μ von z nach folgender Regel:

Es sei

$$\begin{array}{l} \lambda_1 \text{ teilbar durch } \mathfrak{p}_1, \text{ nicht durch } \mathfrak{p}_1^2; \\ \lambda_2 \quad ,, \quad ,, \quad \mathfrak{p}_2, \quad ,, \quad ,, \quad \mathfrak{p}_2^2; \\ \lambda_3 \quad ,, \quad ,, \quad \mathfrak{p}_3, \quad ,, \quad ,, \quad \mathfrak{p}_3^2; \\ \dots\dots\dots\dots\dots\dots \end{array}$$

$$\begin{array}{l} \mu_1 \text{ teilbar durch } \mathfrak{p}_2^{e_2}, \mathfrak{p}_3^{e_3}, \ldots, \text{ nicht durch } \mathfrak{p}_1, \mathfrak{p}_2^{e_2+1}, \mathfrak{p}_3^{e_3+1}, \ldots; \\ \mu_2 \quad ,, \quad ,, \quad \mathfrak{p}_1^{e_1}, \mathfrak{p}_3^{e_3}, \ldots, \quad ,, \quad ,, \quad \mathfrak{p}_2, \mathfrak{p}_1^{e_1+1}, \mathfrak{p}_3^{e_3+1}, \ldots; \\ \mu_3 \quad ,, \quad ,, \quad \mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2}, \ldots, \quad ,, \quad ,, \quad \mathfrak{p}_3, \mathfrak{p}_1^{e_1+1}, \mathfrak{p}_2^{e_2+1}, \ldots \text{*)}. \\ \dots\dots\dots\dots\dots\dots \end{array}$$

Die n Funktionen

$$\begin{array}{lllll} \mu_1, & \mu_1 \lambda_1, & \mu_1 \lambda_1^2, & \ldots & \mu_1 \lambda_1^{e_1-1}, \\ \mu_2, & \mu_2 \lambda_2, & \mu_2 \lambda_2^2, & \ldots & \mu_2 \lambda_2^{e_2-1}, \\ \mu_3, & \mu_3 \lambda_3, & \mu_3 \lambda_3^2, & \ldots & \mu_3 \lambda_3^{e_3-1}, \\ \dots & \dots & \dots & \dots & \dots \end{array}$$

die wir mit $\eta_1, \eta_2, \ldots \eta_n$ bezeichnen, bilden dann eine Basis von Ω; diese Behauptung ist in der nun zu beweisenden allgemeineren enthalten.

Wenn

$$(z - z_0)\zeta = x_1 \eta_1 + x_2 \eta_2 + \cdots + x_n \eta_n$$

mit ganzen rationalen Koeffizienten $x_1, x_2, \ldots x_n$ ist, und ζ in den Punkten $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \ldots$ endliche Werte $\zeta', \zeta'', \zeta''', \ldots$ hat, so müssen die sämtlichen Koeffizienten $x_1, x_2, \ldots x_n$ durch $z - z_0$ teilbar sein In der Tat ist z. B. im Punkte $\mathfrak{P}_1$ die linke Seite unendlich klein mindestens in der Ordnung e_1. Es muß also nach § 15, 5. auch

$$x_1 \eta_1 + x_2 \eta_2 + \cdots + x_{e_1} \eta_{e_1} = \mu_1 (x_1 + x_2 \lambda_1 + \cdots + x_{e_1} \lambda_1^{e_1-1})$$

in dieser Ordnung unendlich klein sein. Dies ist aber nur möglich, wenn $x_1, x_2, \ldots x_{e_1}$ in $\mathfrak{P}_1$ verschwinden, also durch $z - z_0$ teilbar sind, w. z. b. w.

Hiernach können wir setzen:

$$\begin{aligned} \eta \mu_1 \lambda_1^r = {} & \mu_1 (x_1^{(0)} + x_1^{(1)} \lambda_1 + \cdots + x_1^{(e_1-1)} \lambda_1^{e_1-1}) \\ & + \mu_2 (x_2^{(0)} + x_2^{(1)} \lambda_2 + \cdots + x_2^{(e_2-1)} \lambda_2^{e_2-1}) \\ & + \mu_3 (x_3^{(0)} + x_3^{(1)} \lambda_3 + \cdots + x_3^{(e_3-1)} \lambda_3^{e_3-1}) + \cdots, \end{aligned}$$

worin die $x_1^{(0)}, x_1^{(1)}, \ldots x_2^{(0)}, \ldots$ rationale Funktionen von z sind, die alle für $z - z_0$ endlich bleiben. In den Punkten $\mathfrak{P}_2, \mathfrak{P}_3, \ldots$ ist die linke

*) Die Möglichkeit, solche Funktionen zu bestimmen, ergibt sich aus § 9, 3., Anmerkung, oder auch nach § 11, 2., wonach man z. B. setzen kann

$$\lambda = \varrho - b, \quad \mu \lambda^e = \psi(\varrho).$$

Seite unendlich klein mindestens in der Ordnung $e_2, e_3, \ldots$ Dasselbe gilt für $\mathfrak{P}_2$ von $\mu_1, \mu_3, \ldots$, aber nicht von μ_2, für $\mathfrak{P}_3$ von $\mu_1, \mu_2, \ldots$ aber nicht von $\mu_3, \ldots$; folglich ist für $z = z_0$

$$x_2^{(0)} = 0, \quad x_2^{(1)} = 0, \quad \ldots \quad x_2^{(e_2-1)} = 0,$$
$$x_3^{(0)} = 0, \quad x_3^{(1)} = 0, \quad \ldots \quad x_3^{(e_3-1)} = 0,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

In $\mathfrak{P}_1$ ist die linke Seite unendlich klein mindestens in der Ordnung r; daher wird, wenn $r < e_1$ ist, für $z = z_0$

$$x_1^{(0)} = 0, \quad x_1^{(1)} = 0, \quad \ldots \quad x_1^{(r-1)} = 0, \quad x_1^{(r)} = \eta'.$$

Dieselbe Betrachtung läßt sich auf die Funktionen $\eta\,\mu_2\,\lambda_2^r$, $\eta\,\mu_3\,\lambda_3^r, \ldots$ anwenden. Setzt man also

$$\eta\,\eta_1 = x_{1,1}\,\eta_1 + x_{1,2}\,\eta_2 + \cdots + x_{1,n}\,\eta_n,$$
$$\eta\,\eta_2 = x_{2,1}\,\eta_1 + x_{2,2}\,\eta_2 + \cdots + x_{2,n}\,\eta_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\eta\,\eta_n = x_{n,1}\,\eta_1 + x_{n,2}\,\eta_2 + \cdots + x_{n,n}\,\eta_n,$$

so werden in der Determinante

$$N(\eta) = \Sigma \pm x_{1,1}\,x_{2,2} \ldots x_{n,n}$$

sämtliche links von der Diagonalreihe stehenden Glieder für $z = z_0$ verschwinden, während von den Diagonalgliedern e_1 gleich η', e_2 gleich η'', e_3 gleich η''', ... werden. Es ist also für $z = z_0$

$$N(\eta) = \eta'^{e_1}\,\eta''^{e_2}\,\eta'''^{e_3} \ldots$$

w. z. b. w.

5. Da nach der Definition der Spur (§ 2)

$$S(\eta) = x_{1,1} + x_{2,2} + \cdots + x_{n,n}$$

ist, so führen dieselben Betrachtungen zu dem Satze:

Es ist für $z = z_0$

$$S(\eta) = e_1\,\eta' + e_2\,\eta'' + e_3\,\eta''' + \cdots,$$

welcher jedoch nur unter der Voraussetzung gilt, daß die Werte $\eta', \eta'', \eta''', \ldots$ endlich sind.

Der Satz 4. ergibt für ein beliebiges konstantes (oder rational von z abhängiges) t für $z = z_0$.

$$N(t - \eta) = (t - \eta')^{e_1}\,(t - \eta'')^{e_2}\,(t - \eta''')^{e_3} \ldots,$$

und daraus durch Vergleichung der Koeffizienten gleicher Potenzen von t für jeden dieser Koeffizienten einen Ausdruck durch die konjugierten Werte (symmetrische Funktionen).

6. Ist $\eta_1, \eta_2, \ldots \eta_n$ eine Basis von Ω, so ergibt sich durch Anwendung von 5. sofort der Wert der Diskriminante dieses Systems für $z = z_0$

$$\varDelta_z(\eta_1, \eta_2, \ldots \eta_n) = (\Sigma \pm \eta_1' \eta_2'' \ldots \eta_n^{(n)})^2,$$

wenn $\eta_\iota', \eta_\iota'', \ldots \eta_\iota^{(n)}$ die sämtlichen gleichen oder verschiedenen, aber als endlich vorausgesetzten, zu $z = z_0$ gehörigen konjugierten Werte von η_ι bedeuten.

§ 17.

Darstellung der Funktionen des Körpers Ω durch Polygonquotienten.

Eine Funktion η des Körpers Ω hat nur in einer endlichen Anzahl von Punkten eine von Null verschiedene Ordnungszahl; die Summe sämtlicher Ordnungszahlen ist gleich 0, also die Summe der positiven gleich der Summe der negativen Ordnungszahlen, und zwar gleich der Ordnung der Funktion η (§ 15). Sind die Ordnungszahlen einer Funktion η für jeden Punkt $\mathfrak{P}$ bekannt, so ist damit die Funktion η bis auf einen konstanten Faktor bestimmt; denn hat η' überall dieselbe Ordnungszahl wie η, so hat $\frac{\eta}{\eta'}$ (nach § 15, 5.) überall die Ordnungszahl Null und ist also (nach § 15, 7.) eine Konstante.

Bilden wir also ein Polygon $\mathfrak{A}$, in welches wir jeden Punkt, in dem η eine positive Ordnungszahl hat, so oft aufnehmen, als diese Ordnungszahl angibt, und ein zweites Polygon $\mathfrak{B}$, in welches wir in entsprechender Weise die Punkte aufnehmen, in welchen η eine negative Ordnungszahl hat, so sind die Polygone $\mathfrak{A}$, $\mathfrak{B}$ von gleicher Ordnung, und zwar von der Ordnung der Funktion η. Durch diese Polygone $\mathfrak{A}$, $\mathfrak{B}$ ist also die Funktion η bis auf einen konstanten Faktor bestimmt. Wir setzen in symbolischer Bezeichnung

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

und nennen $\mathfrak{A}$ das O b e r e c k, $\mathfrak{B}$ das U n t e r e c k der Funktion η *).

Nach dieser Festsetzung sind die beiden Polygone $\mathfrak{A}$, $\mathfrak{B}$ relativ prim; es ist aber zweckmäßig, die Bezeichnung dahin auszudehnen,

*) Alle Funktionen der einfachen Schar (η) haben hiernach dieselbe Bezeichnung $\frac{\mathfrak{A}}{\mathfrak{B}}$, und es würde daher korrekter sein, $(\eta) = \frac{\mathfrak{A}}{\mathfrak{B}}$ zu setzen; indessen führt diese Bezeichnung zu unnötigen Weitläufigkeiten.

daß man auch gemeinschaftliche Faktoren in $\mathfrak{A}$, $\mathfrak{B}$ zuläßt, was durch die Bestimmung geschieht, daß

$$\frac{\mathfrak{M}\mathfrak{A}}{\mathfrak{M}\mathfrak{B}} = \frac{\mathfrak{A}}{\mathfrak{B}}$$

sein soll, wenn $\mathfrak{M}$ ein beliebiges Polygon bedeutet. Setzen wir nach dieser verallgemeinerten Bezeichnung

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

so kann ein Punkt $\mathfrak{P}$, in welchem η die Ordnungszahl m besitzt, m_1-mal in $\mathfrak{A}$, m_2-mal in $\mathfrak{B}$ aufgenommen werden, wenn $m_1 - m_2 = m$ ist. Es ist auch jetzt noch die Ordnung von $\mathfrak{A}$ gleich der von $\mathfrak{B}$, aber nicht mehr gleich der Ordnung der Funktion η.

Aus dieser Definition ergibt sich (nach § 15, 5.) unmittelbar der Satz: Ist

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}}, \quad \eta' = \frac{\mathfrak{A}'}{\mathfrak{B}'},$$

so ist

$$\eta\eta' = \frac{\mathfrak{A}\mathfrak{A}'}{\mathfrak{B}\mathfrak{B}'}, \quad \frac{\eta}{\eta'} = \frac{\mathfrak{A}\mathfrak{B}'}{\mathfrak{B}\mathfrak{A}'}.$$

Nach § 14, 5. ist eine Funktion η' dann und nur dann eine ganze Funktion von η, wenn jeder im Untereck von η' aufgehende Punkt auch in dem von η enthalten ist.

§ 18.

Äquivalente Polygone und Polygonklassen.

1. Definition. Zwei Polygone $\mathfrak{A}$, $\mathfrak{A}'$ von gleichviel Punkten heißen äquivalent, wenn eine Funktion η in Ω existiert, welche (nach § 17) die Bezeichnung hat:

$$\eta = \frac{\mathfrak{A}}{\mathfrak{A}'}.$$

2. Satz. Ist $\mathfrak{A}$ äquivalent mit $\mathfrak{A}'$ und mit $\mathfrak{A}''$, so ist auch $\mathfrak{A}'$ mit $\mathfrak{A}''$ äquivalent; denn aus

$$\eta' = \frac{\mathfrak{A}'}{\mathfrak{A}}; \quad \eta'' = \frac{\mathfrak{A}''}{\mathfrak{A}}$$

folgt:

$$\frac{\eta'}{\eta''} = \frac{\mathfrak{A}'}{\mathfrak{A}''}.$$

3. Definition und Satz. Alle mit einem gegebenen Polygon $\mathfrak{A}$ äquivalenten Polygone $\mathfrak{A}'$, $\mathfrak{A}''$, ... bilden eine Polygonklasse A. Nach 2. kommt dann jedes beliebige Polygon in einer und nur in einer Klasse vor; denn sind $\mathfrak{A}$, $\mathfrak{B}$ zwei äquivalente Polygone, welche zu den Klassen A, B führen, so ist nach 2. jedes Polygon der Klasse B zugleich in A enthalten und umgekehrt, und daher sind beide Klassen identisch.

Alle Polygone einer Klasse haben dieselbe Ordnung, welche die Ordnung der Klasse genannt werden soll.

4. Es können aber Polygone existieren, welche mit keinem anderen äquivalent sind, und deren jedes daher für sich eine Klasse bildet. Solche Polygone mögen isolierte genannt sein.

5. Ist $\mathfrak{M}$ ein beliebiges Polygon, und $\mathfrak{A}$ äquivalent mit $\mathfrak{A}'$, so ist auch $\mathfrak{M}\mathfrak{A}$ äquivalent mit $\mathfrak{M}\mathfrak{A}'$; aber auch umgekehrt folgt aus der Äquivalenz von $\mathfrak{M}\mathfrak{A}$ mit $\mathfrak{M}\mathfrak{A}'$ die Äquivalenz von $\mathfrak{A}$ mit $\mathfrak{A}'$.

6. Ist $\mathfrak{A}$ mit $\mathfrak{A}'$, $\mathfrak{B}$ mit $\mathfrak{B}'$ äquivalent, so ist auch $\mathfrak{A}\mathfrak{B}$ mit $\mathfrak{A}'\mathfrak{B}'$ äquivalent. Die Klasse C, welcher das Produkt $\mathfrak{A}\mathfrak{B}$ angehört, umfaßt daher die sämtlichen Produkte je zweier Polygone der Klassen A, B von $\mathfrak{A}$ und $\mathfrak{B}$ (aber außerdem unter Umständen noch unendlich viele andere Polygone) und soll als das Produkt der beiden Klassen A, B bezeichnet sein:

$$C = AB = BA.$$

Die Definition des Produkts von mehreren Klassen und die Gültigkeit des Fundamentalsatzes der Multiplikation ergibt sich hieraus von selbst.

7. Sind A, B, D drei Klassen, welche der Bedingung

$$DA = DB$$

genügen, so folgt $A = B$; denn sind $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{D}$ drei Polygone der Klassen A, B, D, so folgt aus der Voraussetzung, daß $\mathfrak{D}\mathfrak{B}$ mit $\mathfrak{D}\mathfrak{A}$, und folglich $\mathfrak{B}$ mit $\mathfrak{A}$ äquivalent ist.

8. Geht ein Polygon $\mathfrak{A}$ der Klasse A in einem Polygon $\mathfrak{C}$ der Klasse C auf, so gilt dasselbe von jedem Polygon $\mathfrak{A}'$ der Klasse A; denn aus $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$ folgt nach 5., daß $\mathfrak{C}' = \mathfrak{A}'\mathfrak{B}$ in C enthalten ist, und wir können also, obschon nicht umgekehrt jedes Polygon der Klasse C durch ein Polygon der Klasse A teilbar zu sein braucht, sagen, die Klasse C sei durch die Klasse A teilbar. Ist $\mathfrak{B}'$ irgendein Polygon der Klasse B von $\mathfrak{B}$, so ist auch $\mathfrak{C}'' = \mathfrak{A}'\mathfrak{B}'$ in C enthalten und folglich

$$C = AB.$$

Ist also C durch A teilbar, so gibt es eine und (nach 7.) nur eine Klasse B, welche der Bedingung

$$C = AB$$

genügt.

§ 19.

Die Polygonscharen.

1. Sind $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ bestimmte, und zwar äquivalente Polygone, und $\mathfrak{A}$ ein beliebiges Polygon derselben Klasse A, so existieren s Funktionen in Ω

$$\eta_1 = \frac{\mathfrak{A}_1}{\mathfrak{A}}, \quad \eta_2 = \frac{\mathfrak{A}_2}{\mathfrak{A}}, \quad \ldots \quad \eta_s = \frac{\mathfrak{A}_s}{\mathfrak{A}}.$$

Setzt man, wie in § 15, 5. für einen beliebigen Punkt $\mathfrak{P}$

$$\begin{aligned} \eta_1 &= e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\ \eta_2 &= e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\ &\ldots\ldots\ldots\ldots \\ \eta_s &= e_s \varrho^m + \sigma_s \varrho^{m+1}, \end{aligned}$$

worin ϱ in $\mathfrak{P}$ 0^1 ist, $e_1, e_2, \ldots e_s$ Konstanten, die nicht alle verschwinden, und $\sigma_1, \sigma_2, \ldots \sigma_s$ in $\mathfrak{P}$ endliche Funktionen bedeuten, so folgt, daß jede Funktion η der Schar $(\eta_1, \eta_2, \ldots \eta_s)$, d. h. jede Funktion von der Form

$$\eta = c_1 \eta_1 + c_2 \eta_2 + \cdots + c_s \eta_s$$

in $\mathfrak{P}$ eine Ordnungszahl hat, die nicht kleiner als m ist, und daraus nach § 17, daß die Funktion η in die Form

$$\eta = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

gesetzt werden kann, wo $\mathfrak{A}'$ gleichfalls in der Klasse A enthalten ist.

Wählt man für $\mathfrak{A}$ ein beliebiges anderes Polygon $\mathfrak{B}$ der Klasse A, und setzt

$$\zeta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

$$\eta_1 \zeta = \eta_1' = \frac{\mathfrak{A}_1}{\mathfrak{B}}, \quad \eta_2 \zeta = \eta_2' = \frac{\mathfrak{A}_2}{\mathfrak{B}}, \quad \cdots \quad \eta_s \zeta = \eta_s' = \frac{\mathfrak{A}_s}{\mathfrak{B}},$$

so wird auch

$$\eta \zeta = \eta' = c_1 \eta_1' + c_2 \eta_2' + \cdots + c_s \eta_s',$$

und folglich

$$\eta' = \frac{\mathfrak{A}'}{\mathfrak{B}}.$$

Jedes durch den Nenner $\mathfrak{A}$ und ein Konstantensystem $c_1, c_2, \ldots c_s$ erzeugte Polygon wird daher auch durch jeden anderen derselben Klasse angehörigen Nenner $\mathfrak{B}$ erzeugt, und der Inbegriff der sämtlichen Polygone $\mathfrak{A}'$, die den verschiedenen Werten der Konstanten $c_1, c_2, \ldots c_s$ entsprechen, ist nur abhängig von den Polygonen $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$. Dieser Inbegriff soll daher eine Polygonschar mit der Basis $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ genannt und mit

$$(\mathfrak{A}_1, \quad \mathfrak{A}_2, \quad \ldots \quad \mathfrak{A}_s)$$

bezeichnet werden.

2. Haben die Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ einen größten gemeinschaftlichen Teiler $\mathfrak{M}$, so ist derselbe nach 1. auch Teiler eines jeden Polygons $\mathfrak{A}'$ der Schar $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$, und kann der Teiler der Schar genannt werden; aber es läßt sich in dieser Schar ein Polygon $\mathfrak{A}' = \mathfrak{M}\mathfrak{B}$ derart bestimmen, daß $\mathfrak{B}$ relativ prim zu einem beliebig gegebenen Polygon wird. Ist nämlich unter Beibehaltung der Bezeichnung von 1. ein Punkt $\mathfrak{P}$ genau μ-mal in $\mathfrak{M}$ und ν-mal in $\mathfrak{A}$ enthalten, so ist, wenn

$$\eta = e\varrho^m + \sigma\varrho^{m+1}$$

gesetzt wird, m niemals kleiner als $\mu - \nu$, und es ist $m = \mu - \nu$, wenn man die Konstanten $c_1, c_2, \ldots c_s$ so wählt, daß

$$e = c_1 e_1 + c_2 e_2 + \cdots + c_s e_s$$

von Null verschieden ist. Der Punkt $\mathfrak{P}$ ist daher mindestens μ-mal in $\mathfrak{A}'$ enthalten, und unter der letzteren Voraussetzung auch nicht öfter als μ-mal. Da man nun die Konstanten $c_1, c_2, \ldots c_s$ immer so wählen kann, daß eine beliebige Anzahl von Ausdrücken der Form

$$\Sigma c_\iota e_\iota, \quad \Sigma c_\iota e'_\iota, \ldots,$$

in deren keinem die sämtlichen Konstanten $e_\iota, e'_\iota, \ldots$ verschwinden, von Null verschiedene Werte haben, so folgt die Richtigkeit der aufgestellten Behauptung.

3. Sind die Funktionen $\eta_1, \eta_2, \ldots \eta_s$ in 1. linear abhängig oder unabhängig, so gilt das gleiche von den Funktionen $\eta'_1, \eta'_2, \ldots \eta'_s$. Wir werden dementsprechend auch die Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ linear abhängig oder unabhängig und ihr System linear reduktibel oder irreduktibel nennen.

Da nach § 5, 4. jede Funktionenschar eine irreduktible Basis besitzt, so folgt, daß auch jede Polygonschar eine irreduktible Basis hat. Ist s die Anzahl der Polygone einer solchen Basis, so heißt die Schar eine s-fache, oder s die Dimension der Schar. Irgend s Polygone einer solchen Schar bilden eine irreduktible Basis derselben oder nicht, je nachdem sie linear unabhängig oder abhängig sind (vgl. § 5, 4.).

4. Sind die Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ linear abhängig oder unabhängig, so sind, wenn $\mathfrak{M}$ ein beliebiges Polygon bedeutet, auch $\mathfrak{M}\mathfrak{A}_1, \mathfrak{M}\mathfrak{A}_2, \ldots \mathfrak{M}\mathfrak{A}_s$ linear abhängig oder unabhängig und umgekehrt.

§ 20.

Erniedrigung der Dimension der Schar durch Teilbarkeitsbedingungen.

1. Es sei

$$S = (\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$$

eine s-fache Schar vom Teiler $\mathfrak{M}$. Es wird nach der Mannigfaltigkeit derjenigen Polygone $\mathfrak{A}'$ der Schar S gefragt, welche einen beliebig gegebenen Punkt wenigstens einmal öfter enthalten als der Teiler $\mathfrak{M}$ der Schar.

Ist der Punkt $\mathfrak{P}$ μ-mal in $\mathfrak{M}$ und ν-mal in einem beliebigen mit $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ äquivalenten Polygon $\mathfrak{A}$ enthalten, so ist, wenn wir wie in § 19

$$\frac{\mathfrak{A}_1}{\mathfrak{A}} = \eta_1 = e_1 \varrho^m + \sigma_1 \varrho^{m+1},$$

$$\frac{\mathfrak{A}_2}{\mathfrak{A}} = \eta_2 = e_2 \varrho^m + \sigma_2 \varrho^{m+1},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\frac{\mathfrak{A}_s}{\mathfrak{A}} = \eta_s = e_s \varrho^m + \sigma_s \varrho^{m+1}$$

setzen, $m = \mu - \nu$, und von den Konstanten $e_1, e_2, \ldots e_s$ ist wenigstens eine, etwa e_s, von Null verschieden. Die gesuchten Polygone $\mathfrak{A}'$ sind dann durch die Gleichung charakterisiert

$$\frac{\mathfrak{A}'}{\mathfrak{A}} = \eta' = c_1 \eta_1 + c_2 \eta_2 + \cdots + c_s \eta_s,$$

worin die Konstanten $c_1, c_2, \ldots c_s$ an die Bedingung gebunden sind

$$c_1 e_1 + c_2 e_2 + \cdots + c_s e_s = 0.$$

Hiernach können wir setzen

$$\frac{\mathfrak{A}'}{\mathfrak{A}} = e_s \eta' = c_1 (e_s \eta_1 - e_1 \eta_s) + \cdots + c_{s-1} (e_s \eta_{s-1} - e_{s-1} \eta_s).$$

Daraus aber ergibt sich, wenn wir

$$\begin{aligned} \eta'_1 &= e_s \eta_1 - e_1 \eta_s, \\ \eta'_2 &= e_s \eta_2 - e_2 \eta_s, \\ &\cdots\cdots\cdots\cdots \\ \eta'_{s-1} &= e_s \eta_{s-1} - e_{s-1} \eta_s \end{aligned}$$

setzen, daß die Funktionen η' eine $(s-1)$-fache Schar $(\eta'_1, \eta'_2, \ldots \eta'_{s-1})$ bilden; denn die Funktionen $\eta'_1, \eta'_2, \ldots \eta'_{s-1}$ sind linear unabhängig, wenn es, wie vorausgesetzt, die Funktionen $\eta_1, \eta_2, \ldots \eta_s$ sind. Es bilden also auch die Polygone $\mathfrak{A}'$ eine $(s-1)$-fache Schar

$$S' = (\mathfrak{A}'_1, \mathfrak{A}'_2, \ldots \mathfrak{A}'_{s-1}),$$

wenn

$$\frac{\mathfrak{A}'_\iota}{\mathfrak{A}} = e_s \eta_\iota - e_\iota \eta_s$$

gesetzt wird. Der Teiler dieser Schar ist durch $\mathfrak{M}\mathfrak{P}$ teilbar, wenn auch nicht notwendig damit identisch.

2. Hieraus ergibt sich sofort, daß die Polygone einer Schar S, welche durch ein beliebiges r-Eck $\mathfrak{R}$ teilbar sind, eine mindestens $(r-s)$-fache Schar bilden. Denn nehmen wir an, es sei dies bereits für ein r-Eck $\mathfrak{R}$ bewiesen, so folgt die Richtigkeit der Behauptung für ein $(r+1)$-Eck $\mathfrak{P}\mathfrak{R}$ unmittelbar aus 1., indem durch das Hinzutreten des Punktes $\mathfrak{P}$, wenn $\mathfrak{P}$ im Teiler der durch $\mathfrak{R}$ bereits reduzierten Schar enthalten ist, die Dimension nicht weiter geändert, sonst um 1 erniedrigt wird.

Hieraus folgt als Spezialfall, daß es in einer s-fachen Schar immer wenigstens ein Polygon gibt, welches durch ein gegebenes $(s-1)$-Eck teilbar ist.

3. Man kann, wenn $r \leqq s$ ist, das r-Eck $\mathfrak{R}$ so wählen, daß die durch $\mathfrak{R}$ teilbaren Polygone der Schar S eine genau $(s-r)$-fache Schar bilden. Zu diesem Ende wähle man einen Punkt $\mathfrak{P}$, welcher im Teiler von S nicht enthalten ist; die durch $\mathfrak{P}$ teilbaren Polygone in S bilden nach 1. eine $(s-1)$-fache Schar S'; man wähle einen zweiten Punkt $\mathfrak{P}'$, der nicht im Teiler von S' enthalten ist; die Polygone in S', die durch $\mathfrak{P}'$, d. h. die Polygone in S, die durch $\mathfrak{P}\mathfrak{P}'$ teilbar sind, bilden eine $(s-2)$-fache Schar, usf.; zugleich erhellt aus dieser Bildungsweise, daß man $\mathfrak{R}$ zu einem beliebig gegebenen Polygon relativ prim annehmen kann. Ist $r = s$, so wird hiernach in S kein durch $\mathfrak{R}$ teilbares Polygon existieren.

§ 21.

Die Dimensionen der Polygonklassen.

1. Die Polygone einer Klasse bilden eine Schar von endlicher Dimension, welche die Dimension der Klasse heißen soll.

Beweis. Wählt man in einer Klasse A, deren Ordnung m sei, irgend s Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ aus, so gehören alle Polygone der Schar $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$ zugleich in die Klasse A. Die Anzahl der linear unabhängigen Polygone, die in A enthalten sind, kann daher gewiß nicht größer sein als $m + 1$, weil man sonst (nach § 20, 2.) in der Klasse ein durch ein beliebiges $(m + 1)$-Eck teilbares Polygon finden könnte, was widersinnig ist. Wenn daher s die Maximalzahl der linear unabhängigen Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ der Klasse A ist, so muß jedes Polygon dieser Klasse in der Schar $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s)$ enthalten sein, und s ist die Dimension der Klasse. Das System der Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_s$ soll eine Basis der Klasse genannt werden.

Die isolierten Polygone bilden Klassen von der Dimension 1.

2. Gibt es in einer Klasse C s und nicht mehr linear unabhängige, durch ein gegebenes Polygon $\mathfrak{A}$ der Klasse A teilbare Polygone

$$\mathfrak{C}_1 = \mathfrak{A}\mathfrak{B}_1, \quad \mathfrak{C}_2 = \mathfrak{A}\mathfrak{B}_2, \quad \ldots \quad \mathfrak{C}_s = \mathfrak{A}\mathfrak{B}_s,$$

so ist C durch A teilbar, und es existieren in C auch ebenso viele linear unabhängige Polygone

$$\mathfrak{C}_1' = \mathfrak{A}'\mathfrak{B}_1, \quad \mathfrak{C}_2' = \mathfrak{A}'\mathfrak{B}_2, \quad \ldots \quad \mathfrak{C}_s' = \mathfrak{A}'\mathfrak{B}_s,$$

welche durch ein beliebiges mit $\mathfrak{A}$ äquivalentes Polygon $\mathfrak{A}'$ teilbar sind (§ 18, 8.; § 19, 4.). Diese Zahl s hängt daher nur von den beiden Klassen A, C ab und kann füglich mit (A, C) bezeichnet werden. Der Wert des Symbols (A, C) ist gleich 0 zu setzen, wenn C nicht durch A teilbar ist. Die Dimension einer Klasse A wird hiernach mit (O, A) bezeichnet, wo O die aus dem Nulleck $\mathfrak{O}$ bestehende Klasse bedeutet. Ist (nach § 18, 8.)

$$C = AB,$$

so folgt:

$$(1) \qquad (A, C) = (A, AB) = (O, B);$$

denn die Polygone $\mathfrak{B}_1, \mathfrak{B}_2, \ldots \mathfrak{B}_s$, die sämtlich in B enthalten sind, sind linear unabhängig, daher (O, B) gewiß nicht kleiner als s. Ist umgekehrt $\mathfrak{B}$ ein beliebiges Polygon der Klasse B, so ist $\mathfrak{A}\mathfrak{B}$ in C

enthalten, also auch in der Schar $(\mathfrak{A}\mathfrak{B}_1, \mathfrak{A}\mathfrak{B}_2, \ldots \mathfrak{A}\mathfrak{B}_s)$, mithin $\mathfrak{B}$ in der Schar $(\mathfrak{B}_1, \mathfrak{B}_2, \ldots \mathfrak{B}_s)$ enthalten, d. h. $(O, B) = s$.

Ist a die Ordnung der Klasse A, so ist nach § 20, 2.

$$(A, B) \gtreqless (O, C) - a,$$

und daraus folgt mittels (1) der allgemeine Satz

$$(O, B) \gtreqless (O, AB) - a. \tag{2}$$

3. Haben die sämtlichen Basis-Polygone einer Klasse A den größten gemeinschaftlichen Teiler $\mathfrak{M}$, so ist dieser auch Teiler sämtlicher Polygone der Klasse A. Ist $\mathfrak{M}$ gleich dem Nulleck $\mathfrak{O}$, so heißt die Klasse eine eigentliche, im entgegengesetzten Falle eine uneigentliche vom Teiler $\mathfrak{M}$.

Unterdrückt man in sämtlichen Polygonen einer uneigentlichen Klasse A den Teiler $\mathfrak{M}$, so erhält man eine eigentliche Klasse A' von niedrigerer Ordnung, aber von derselben Dimension. Diese Beziehung von A zu A' soll durch das Zeichen ausgedrückt sein

$$A = \mathfrak{M} A'.$$

4. Der Teiler $\mathfrak{M}$ einer uneigentlichen Klasse A ist stets ein isoliertes Polygon. Ist nämlich

$$A = \mathfrak{M} A',$$

so kann man in der eigentlichen Klasse A' nach § 19, 2. ein Polygon $\mathfrak{A}'$ so wählen, daß es relativ prim zu $\mathfrak{M}$ ist. Ist also $\mathfrak{M}'$ äquivalent mit $\mathfrak{M}$, so ist $\mathfrak{M}'\mathfrak{A}'$ äquivalent $\mathfrak{M}\mathfrak{A}'$, also in A enthalten, mithin durch $\mathfrak{M}$ teilbar. Es ist also auch $\mathfrak{M}'$ durch $\mathfrak{M}$ teilbar, und da $\mathfrak{M}$ und $\mathfrak{M}'$ von gleicher Ordnung sind,

$$\mathfrak{M} = \mathfrak{M}'.$$

Hiernach bildet das einzige Polygon $\mathfrak{M}$ eine Klasse M, und die Bezeichnung $\mathfrak{M} A'$ ist gleichbedeutend mit MA' (§ 18, 6.).

§ 22.

Die Normalbasen von $\mathfrak{o}$.

1. Wir betrachten im folgenden das System $\mathfrak{o}$ der ganzen Funktionen ω einer beliebigen Variablen z in Ω und zugleich das System $\mathfrak{o}'$ der ganzen Funktionen ω' von $z' = \frac{1}{z}\cdot$ Aus der Definition der ganzen Funktionen erhellt sofort, daß die beiden Systeme $\mathfrak{o}$, $\mathfrak{o}'$ nur die Konstanten miteinander gemein haben, daß dagegen jede Funktion ω

durch Multiplikation mit einer bestimmten positiven Potenz von z' in eine Funktion ω' verwandelt werden kann. Ist $\omega z'^r$ in $\mathfrak{o}'$ enthalten, so gilt das gleiche auch von $\omega z'^{r+1}$, $\omega z'^{r+2}, \ldots$ In der Reihe der Funktionen

$$\omega, \quad \frac{\omega}{z} = z'\omega, \quad \frac{\omega}{z^2} = z'^2\omega, \ldots$$

werden also von einem bestimmten Gliede $\omega z'^r$ an alle folgenden Funktionen in $\mathfrak{o}'$ enthalten sein, während alle vorangehenden nicht darin enthalten sind. Die kleinste Zahl r, für welche $z'^r\omega$ in $\mathfrak{o}'$ enthalten ist, soll der Exponent der Funktion ω in bezug auf z genannt werden. Die Konstanten, und nur diese, haben den Exponenten Null. Ist ω von Null verschieden, und r sein Exponent, so ist $r+1$ der Exponent von $(z-c)\omega$; denn ist $\omega = z^r\omega'$, so ist

$$\frac{(z-c)\omega}{z^{r+1}} = (1-cz')\omega' \quad \text{in } \mathfrak{o}' \text{ enthalten},$$

$$\frac{(z-c)\omega}{z^r} = z\omega' - c\omega' \quad \text{nicht in } \mathfrak{o}' \text{ enthalten},$$

da zwar $c\omega'$, nicht aber $z\omega' = \frac{\omega}{z^{r-1}}$ in $\mathfrak{o}'$ enthalten ist. Daraus folgt allgemein:

Ist x eine ganze rationale Funktion von z vom Grade s, und r der Exponent von ω, so ist $(r+s)$ der Exponent von $x\omega$.

2. Wir wählen nun ein Funktionensystem $\lambda_1, \lambda_2, \ldots \lambda_n$ in $\mathfrak{o}$ nach folgender Regel aus:

Es sei λ_1 eine von Null verschiedene Konstante, z. B. 1; λ_2 sei unter denjenigen Funktionen in $\mathfrak{o}$, welche nicht einer Konstanten nach dem Modul $\mathfrak{o}z$ kongruent sind, eine von möglichst niedrigem Exponenten r_2 usf.; allgemein sei λ_s unter denjenigen Funktionen in $\mathfrak{o}$, welche nicht kongruent sind einer Funktion der Schar $(\lambda_1, \lambda_2, \ldots \lambda_{s-1})$ (mod. $\mathfrak{o}z$), eine von möglichst niedrigem Exponenten r_s. Da $(\mathfrak{o}, \mathfrak{o}z) = N(z) = z^n$ vom n^{ten} Grade ist, so gibt es in $\mathfrak{o}$ n und nicht mehr nach dem Modul $\mathfrak{o}z$ linear unabhängige Funktionen (§ 6), und daher kann die Reihe der Funktionen $\lambda_1, \lambda_2, \lambda_3, \ldots$ nicht mehr und nicht weniger als n Glieder enthalten. Es ist dann (§ 5)

$$\mathfrak{o} \equiv (\lambda_1, \lambda_2, \ldots \lambda_n) \text{ (mod. } \mathfrak{o}z).$$

Die Exponenten $r_1, r_2, \ldots r_n$ der Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ genügen der Forderung

$$r_1 = 0, \quad 1 \leqq r_2 \leqq r_3 \ldots \leqq r_n.$$

Jede Funktion in $\mathfrak{o}$, deren Exponent $< r_s$, ist nach dem Modul $\mathfrak{o} z$ kongruent einer Funktion aus der $(s-1)$-fachen Schar

$$(\lambda_1, \lambda_2, \ldots \lambda_{s-1}).$$

Diese Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ bilden eine Basis von $\mathfrak{o}$, wie sich aus folgender Betrachtung ergibt.

Wäre es nicht der Fall, so könnte man (§ 3, 7.) eine lineare Funktion $z - c$ und ein System nicht alle verschwindender Konstanten $a_1, a_2, \ldots a_n$ so bestimmen, daß

$$a_1 \lambda_1 + a_2 \lambda_2 + \cdots + a_n \lambda_n = (z - c)\,\omega$$

wäre. Ist unter den Konstanten a die letzte nicht verschwindende a_s, so ist auch

$$a_1 \lambda_1 + a_2 \lambda_2 + \cdots + a_s \lambda_s = (z - c)\,\omega,$$

und der Exponent von ω ist sicher kleiner als r_s (weil $\dfrac{(z-c)\,\omega}{z^{r_s}}$ in $\mathfrak{o}'$ enthalten ist). Es ist also ω, und mithin, da a_s von 0 verschieden ist, auch λ_s kongruent einer Funktion der Schar $(\lambda_1, \lambda_2, \ldots \lambda_{s-1})$ (mod. $\mathfrak{o} z$), was gegen die Voraussetzung ist.

Die Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ bilden daher eine Basis von $\mathfrak{o}$, und diese soll Normalbasis genannt werden. Die charakteristischen Eigenschaften der Normalbasis sind:

I. Die Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ sind linear unabhängig nach dem Modul $\mathfrak{o} z$.

II. Jede Funktion in $\mathfrak{o}$, deren Exponent kleiner ist als der Exponent r_s von λ_s, ist in der Form enthalten

$$c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_{s-1} \lambda_{s-1} + z\,\omega_s,$$

worin $c_1, c_2, \ldots c_{s-1}$ Konstanten, ω_s eine Funktion in $\mathfrak{o}$.

3. Die in $\mathfrak{o}'$ erhaltenen Funktionen

$$\lambda_1' = \frac{\lambda_1}{z^{r_1}}, \quad \lambda_2' = \frac{\lambda_2}{z^{r_2}}, \quad \ldots \quad \lambda_n' = \frac{\lambda_n}{z^{r_n}}$$

bilden eine Normalbasis von $\mathfrak{o}'$.

Ist nämlich ω eine durch z nicht teilbare Funktion in $\mathfrak{o}$ vom Exponenten r, so ist der Exponent von $\omega' = \dfrac{\omega}{z^r}$ in bezug auf z' ebenfalls r; denn es ist zwar $\dfrac{\omega'}{z'^{\,r}} = \omega$, aber nicht $\dfrac{\omega'}{z'^{\,r-1}} = \dfrac{\omega}{z}$ in $\mathfrak{o}$ enthalten. Da die Funktionen $\lambda_1, \lambda_2, \ldots \lambda_n$ alle durch z nicht teilbar sind, so sind hiernach die Exponenten von $\lambda_1', \lambda_2', \ldots \lambda_n'$ in bezug auf z'

resp. $r_1, r_2, \ldots r_n$. Dies vorausgeschickt beweisen wir, daß das Funktionensystem $\lambda'_1, \lambda'_2, \ldots \lambda'_n$ die Eigenschaften I., II. besitzt, wenn dort $\mathfrak{o}$, z durch $\mathfrak{o}'$, z' ersetzt werden.

Wäre die Bedingung I. nicht erfüllt, so ließen sich die Konstanten $a_1, a_2, \ldots a_s$, deren letzte nicht verschwindet, so bestimmen, daß

$$a_1 \lambda'_1 + a_2 \lambda'_2 + \cdots + a_s \lambda'_s = z' \omega',$$

also auch (durch Multiplikation mit z^{r_s})

$$a_1 z^{r_s - r_1} \lambda_1 + a_2 z^{r_s - r_2} \lambda_2 + \cdots + a_s \lambda_s = \omega,$$

worin

$$\omega = z^{r_s - 1} \omega',$$

also eine Funktion in $\mathfrak{o}$, deren Exponent kleiner als r_s wäre. Dies ist aber, da a_s von Null verschieden, wegen der Voraussetzung über die λ unmöglich, und folglich die Bedingung I. erfüllt; daraus folgt:

$$\mathfrak{o}' \equiv (\lambda'_1, \lambda'_2, \ldots \lambda'_n) \text{ (mod. } \mathfrak{o}' z').$$

Wäre die Bedingung II. nicht erfüllt, und λ' eine Funktion in $\mathfrak{o}'$, deren Exponent $r < r_s$, die nicht in der Form enthalten ist

$$a_1 \lambda'_1 + a_2 \lambda'_2 + \cdots + a_{s-1} \lambda'_{s-1} + z' \omega',$$

so könnte man $e \gtreqless s$ so wählen, daß

$$\lambda' = a_1 \lambda'_1 + a_2 \lambda'_2 + \cdots + a_e \lambda'_e + z' \omega'$$

mit konstanten Koeffizienten, deren letzter a_e nicht verschwindet. Es ist hiernach auch $r_e \gtreqless r_s > r$.

Demnach ist $\lambda = z^{r_e - 1} \lambda'$ eine Funktion in $\mathfrak{o}$, und es ergibt sich durch Multiplikation mit z^{r_e}

$$z \lambda = a_1 z^{r_e - r_1} \lambda_1 + a_2 z^{r_e - r_2} \lambda_2 + \cdots + a_e \lambda_e + z^{r_e - 1} \omega'.$$

Es ist daher $\omega = z^{r_e - 1} \omega'$ eine Funktion in $\mathfrak{o}$, deren Exponent (nach 1.) $\lesseqgtr r_e - 1$, und welche der Kongruenz genügt

$$\omega \equiv a'_1 \lambda_1 + a'_2 \lambda_2 + \cdots + a'_e \lambda_e \text{ (mod. } \mathfrak{o} z),$$

worin $a'_e = -a_e$ von Null verschieden ist. Hiernach müßte aber wegen der Eigenschaft II. der Funktionen λ der Exponent von $\omega \gtreqless r_e$ sein, woraus der Widerspruch erhellt.

Hiermit ist nachgewiesen, daß das Funktionensystem $\lambda'_1, \lambda'_2 \ldots \lambda'_n$ eine Normalbasis von $\mathfrak{o}'$ bildet.

4. Wir bilden nun die Diskriminante von Ω in bezug auf die Variable z und z' mit Hilfe der beiden Normalbasen λ, λ'; es ist:

$$\Delta_z(\Omega) = \text{konst. } \Delta(\lambda_1, \lambda_2, \ldots \lambda_n),$$

$$\Delta_{z'}(\Omega) = \text{konst. } \Delta(\lambda'_1, \lambda'_2, \ldots \lambda'_n).$$

Setzt man aber für λ'_ι die Ausdrücke $z'^{r_\iota}\lambda_\iota$, so folgt aus dem Satze § 2, (13)

$$\Delta_{z'}(\Omega) = \text{konst. } z'^{2(r_1+r_2+\cdots+r_n)}\Delta_z(\Omega).$$

Ist $\Delta_z(\Omega)$ vom Grade δ, so besitzt $\Delta_{z'}(\Omega)$ die Wurzel $z'=0$ $[2(r_1+r_2+\cdots+r_n)-\delta]$-mal, und daraus ergibt sich nach § 16, 2. die Verzweigungszahl

$$\mathrm{w}_z = 2(r_1+r_2+\cdots+r_n),$$

welche hiernach stets eine gerade Zahl ist.

§ 23.

Die Differentialquotienten.

1. Da eine jede von Null verschiedene Funktion des Körpers Ω nur in einer endlichen Anzahl von Punkten den Wert Null hat, so folgt, daß eine Funktion in Ω, von der sich unendlich viele Nullpunkte nachweisen lassen, notwendig identisch Null ist, oder daß zwei Funktionen in Ω, welche in unendlich vielen Punkten denselben Wert haben, identisch sein müssen.

2. Sind α, β irgend zwei Variable des Körpers Ω, so existiert in Ω eine mit $\left(\frac{d\alpha}{d\beta}\right)$ zu bezeichnende Funktion, welche in unendlich vielen Punkten $\mathfrak{P}$ der Bedingung genügt:

$$\left(\frac{d\alpha}{d\beta}\right)_0 = \left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0,$$

welche der Differentialquotient von α nach β genannt wird. Ist nämlich $F(\alpha,\beta)=0$ die zwischen α, β bestehende irreduktible Gleichung, so ist, wenn wir zunächst diejenigen (in endlicher Zahl vorhandenen) Punkte ausschließen, in welchen α_0 oder $\beta_0=\infty$ oder $F'(\alpha_0)=0$ oder $F'(\beta_0)=0$ ist,

$$\begin{aligned} 0 = F(\alpha,\beta) = F(\alpha_0,\beta_0) + (\alpha-\alpha_0)F'(\alpha_0) + (\beta-\beta_0)F'(\beta_0) \\ + \tfrac{1}{2}\{(\alpha-\alpha_0)^2F''(\alpha_0,\alpha_0) + 2(\alpha-\alpha_0)(\beta-\beta_0)F''(\alpha_0,\beta_0) \\ + (\beta-\beta_0)^2F''(\beta_0,\beta_0)\} + \cdots \end{aligned}$$

Von den beiden Quotienten $\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0$, $\left(\frac{\beta-\beta_0}{\alpha-\alpha_0}\right)_0$ ist gewiß der eine endlich; ist es der erstere, so ziehen wir aus der letzten Gleichung die folgende:

$$0 = \frac{\alpha - \alpha_0}{\beta - \beta_0} F'(\alpha_0) + F'(\beta_0)$$
$$+ (\beta - \beta_0) \frac{1}{2} \left\{ \left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right)^2 F''(\alpha_0, \alpha_0) + 2 \left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right) F''(\alpha_0, \beta_0) + F''(\beta_0, \beta_0) \right\} + \cdots,$$

woraus für den Punkt $\mathfrak{P}$ folgt:

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 = - \frac{F'(\beta_0)}{F'(\alpha_0)} = - \left(\frac{F'(\beta)}{F'(\alpha)} \right)_0.$$

Wäre $\left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0$ unendlich, so würden wir ebenso in bezug auf $\frac{\beta - \beta_0}{\alpha - \alpha_0}$ schließen.

Es hat also

(1) $$\left(\frac{d\alpha}{d\beta} \right) = - \frac{F'(\beta)}{F'(\alpha)}$$

die verlangte Eigenschaft. Dies bleibt auch noch richtig, wenn von den beiden Funktionen α, β eine konstant ist; denn ist z. B. α konstant, so ist $F(\alpha, \beta) = \alpha - \alpha_0$ von β unabhängig, also $F'(\alpha) = 1$, $F'(\beta) = 0$.

3. Aus vorstehendem folgt, daß, falls β nicht konstant ist, abgesehen von einer endlichen Anzahl von Punkten $\left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0$ ein endlicher Wert ist. Ist daher γ eine dritte Variable in Ω, so ist in unendlich vielen Punkten

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 = \left(\frac{\alpha - \alpha_0}{\gamma - \gamma_0} \right)_0 \left(\frac{\gamma - \gamma_0}{\beta - \beta_0} \right)_0,$$

also auch

$$\left(\frac{d\alpha}{d\beta} \right)_0 = \left(\frac{d\alpha}{d\gamma} \right)_0 \left(\frac{d\gamma}{d\beta} \right)_0.$$

Hiernach und nach 1. ist aber die Identität erfüllt:

(2) $$\left(\frac{d\alpha}{d\beta} \right) = \left(\frac{d\alpha}{d\gamma} \right) \left(\frac{d\gamma}{d\beta} \right)^{*)}.$$

---

*) Man kann auch den Differentialquotienten durch die Gleichung

$$\left(\frac{d\alpha}{d\beta} \right) = - \frac{F'(\beta)}{F'(\alpha)}$$

definieren und durch algebraische Division zum Beweis des Satzes

$$\left(\frac{d\alpha}{d\beta} \right) = \left(\frac{d\alpha}{d\gamma} \right) \left(\frac{d\gamma}{d\beta} \right)$$

gelangen.

4. Infolge dieses letzten Satzes können wir jeder der Funktionen $\alpha, \beta, \gamma, \ldots$ des Körpers Ω eine Funktion $d\alpha, d\beta, d\gamma, \ldots$ (Differential) in der Weise zuordnen, daß allgemein

$$\frac{d\alpha}{d\beta} = \left(\frac{d\alpha}{d\beta}\right)$$

wird. Die Differentiale der Konstanten, und nur diese sind Null zu setzen; die übrigen sind völlig bestimmt, sobald eines derselben willkürlich angenommen ist. Besteht zwischen den Variablen $\alpha, \beta, \gamma, \ldots$ eine rationale Gleichung

$$F(\alpha, \beta. \gamma, \ldots) = 0,$$

so folgt aus derselben

$$F'(\alpha)d\alpha + F'(\beta)d\beta + F'(\gamma)d\gamma + \cdots = 0; \tag{3}$$

denn auf dieselbe Weise wie in 2. schließt man, daß diese Gleichung für unendlich viele Punkte befriedigt ist.

Unmittelbare Folgen des letzten Satzes sind die bekannten Regeln für die Differentiation von Summen, Differenzen, Produkten und Quotienten:

$$d(\alpha \pm \beta) = d\alpha \pm d\beta, \tag{4}$$

$$d(\alpha\beta) = \alpha d\beta + \beta d\alpha, \tag{5}$$

$$d\left(\frac{\alpha}{\beta}\right) = \frac{\beta d\alpha - \alpha d\beta}{\beta^2}. \tag{6}$$

5. Ist ω eine ganze Funktion von z, so wird im allgemeinen $\frac{d\omega}{dz}$ keine ganze Funktion von z sein. Es ist aber aus dem Ausdruck (§ 3, 7.)

$$\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

ersichtlich, da die Differentialquotienten der ganzen rationalen Funktionen $x_1, x_2, \ldots x_n$ wieder ganze rationale Funktionen sind, daß die Unterideale der sämtlichen Funktionen $\frac{d\omega}{dz}$ in einem bestimmten Ideal aufgehen müssen, nämlich in dem kleinsten gemeinschaftlichen Vielfachen der Unterideale von $\frac{d\omega_1}{dz}, \frac{d\omega_2}{dz}, \ldots \frac{d\omega_n}{dz}$. Es soll untersucht werden, welches dies Ideal ist. Zu dem Ende sei $z - c$ eine beliebige lineare Funktion von z und

$$\mathfrak{o}(z-c) = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots,$$

worin die Primideale $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ voneinander verschieden sind. Es sei nun ζ dieselbe Funktion wie in § 11, 2., d. h. eine ganze Funktion von z, welche in den durch die Primideale $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ erzeugten Punkten $\mathfrak{P}, \mathfrak{P}_1, \mathfrak{P}_2, \ldots$ lauter verschiedene Werte hat und jeden derselben nur einfach; dann läßt sich ω in der Form darstellen

$$\omega = y_0 + y_1 \zeta + \cdots + y_{n-1} \zeta^{n-1},$$

worin die rationalen Funktionen $y_0, y_1, \ldots y_{n-1}$ von z zwar gebrochen sein können, aber den Faktor $z - c$ gewiß nicht im Nenner enthalten. Daraus folgt, daß das Unterideal von $\frac{d\omega}{dz}$ durch keine höheren Potenzen der Ideale $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ teilbar sein kann, als das Unterideal von $\frac{d\zeta}{dz}$. Ist aber

$$f(\zeta, z) = 0$$

die zwischen ζ und z bestehende irreduktible Gleichung, so ist nach § 11, 2.

$$\mathfrak{o} f'(\zeta) = \mathfrak{m} \mathfrak{p}^{e-1} \mathfrak{p}_1^{e_1 - 1} \mathfrak{p}_2^{e_2 - 1} \ldots$$

und $\mathfrak{m}$ relativ prim zu $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ Da aber

$$\frac{d\zeta}{dz} = -\frac{f'(z)}{f'(\zeta)}$$

ist, so kann das Unterideal von $\frac{d\zeta}{dz}$, und mithin auch das von $\frac{d\omega}{dz}$ keinen der Faktoren $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ öfter als $(e-1), (e_1-1), (e_2-1), \ldots$-mal enthalten. Da nun $z - c$ jede beliebige lineare Funktion sein kann, so folgt, daß $\frac{d\omega}{dz}$ kein anderes Unterideal haben kann, als ein solches, welches in dem Verzweigungsideal $\mathfrak{z} = \Pi \mathfrak{p}^{e-1}$ (§ 11) aufgeht. Es ist also, wenn $\mathfrak{a}$ ein Ideal bedeutet:

$$\mathfrak{z} \frac{d\omega}{dz} = \mathfrak{a},$$

also nach § 11, (7)

$$\mathfrak{o} \frac{d\omega}{dz} = \mathfrak{e} \mathfrak{a},$$

woraus hervorgeht, daß die Funktionen $\frac{d\omega}{dz}$ sämtlich dem zu $\mathfrak{o}$ komplementären Modul $\mathfrak{e}$ angehören.

6. Ist die irreduktible Gleichung $F(\omega, z) = 0$ zwischen ω und z vom n^{ten} Grade in bezug auf ω, also $1, \omega, \omega^2, \ldots \omega^{n-1}$ eine Basis von Ω, so ist nach § 11, (10)

$$\mathfrak{o} F'(\omega) = \mathfrak{z}\mathfrak{k},$$

und daher muß wegen

$$\frac{d\omega}{dz} = -\frac{F'(z)}{F'(\omega)}$$

$\mathfrak{o} F'(z)$ durch das Ideal $\mathfrak{k}$ teilbar sein,

$$\mathfrak{o} F'(z) = \mathfrak{k}\mathfrak{a},$$

$\mathfrak{k}$ kann man daher das Ideal der Doppelpunkte in bezug auf ω, z nennen.

7. Ist $\mathfrak{P}$ ein Punkt, in welchem $z - c$ unendlich klein in der ersten Ordnung ist (also kein Verzweigungspunkt in z), so sind nach 5. die Funktionen $\dfrac{d\omega}{dz}$ in $\mathfrak{P}$ alle endlich. Ist also η irgendeine Funktion in Ω, welche in $\mathfrak{P}$ endlich ist, so kann man diese als Quotienten zweier ganzen Funktionen $\dfrac{\alpha}{\beta}$ darstellen, von denen β in $\mathfrak{P}$ nicht verschwindet, und daher ist nach (6) auch $\dfrac{d\eta}{dz}$ in $\mathfrak{P}$ endlich

8. Es seien jetzt α, β irgend zwei Variable in Ω; es soll das Verhalten von $\dfrac{d\alpha}{d\beta}$ in irgendeinem Punkte $\mathfrak{P}$ untersucht werden.

Man wähle eine Variable z in Ω, welche in $\mathfrak{P}$ unendlich klein in der ersten Ordnung ist. Hat α in $\mathfrak{P}$ einen endlichen Wert α_0, so kann man nach § 15, 1., 2. eine positive ganze Zahl r und eine in $\mathfrak{P}$ endliche und von Null verschiedene Funktion α' so bestimmen, daß

$$\alpha = \alpha_0 + z^r \alpha'$$

wird. Dies gilt auch noch, wenn α in $\mathfrak{P}$ unendlich ist; nur ist dann r eine negative ganze Zahl, und α_0 ist durch eine beliebige endliche Konstante, z. B. 0 zu ersetzen. Ebenso kann man

$$\beta = \beta_0 + z^s \beta'$$

setzen; r und s sind dann die Ordnungszahlen von $\alpha - \alpha_0$, $\beta - \beta_0$ im Punkte $\mathfrak{P}$, die sowohl positiv als negativ, aber nicht 0 sein können. Aus (2) ergibt sich dann:

$$\frac{d\alpha}{d\beta} = z^{r-s} \frac{r\alpha' + z\dfrac{d\alpha'}{dz}}{s\beta' + z\dfrac{d\beta'}{dz}}$$

oder

$$\frac{\beta-\beta_0}{\alpha-\alpha_0}\frac{d\alpha}{d\beta}=\frac{r+z\dfrac{d\alpha'}{\alpha' dz}}{s+z\dfrac{d\beta'}{\beta' dz}}.$$

Bezeichnet man nun wieder durch den Index 0 den Wert einer Funktion im Punkte $\mathfrak{P}$, so ist, da

$$\left(\frac{d\alpha'}{\alpha' dz}\right)_0,\quad \left(\frac{d\beta'}{\beta' dz}\right)_0$$

nach 7. endlich sind,

$$\left(\frac{\beta-\beta_0}{\alpha-\alpha_0}\frac{d\alpha}{d\beta}\right)_0=\frac{r}{s}, \tag{7}$$

also endlich und von Null verschieden. Hieraus ergibt sich, daß die Ordnungszahl des Differentialquotienten $\frac{d\alpha}{d\beta}$ gleich ist der Differenz der Ordnungszahlen von $\alpha-\alpha_0$ und $\beta-\beta_0$. Ist $r \gtrless s$, so ist $\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0$ und mithin $\left(\frac{d\alpha}{d\beta}\right)_0$ Null oder unendlich. Ist dagegen $r=s$, so sind beide Werte endlich und von 0 verschieden, und wir haben daher in allen Fällen

$$\left(\frac{\alpha-\alpha_0}{\beta-\beta_0}\right)_0=\left(\frac{d\alpha}{d\beta}\right)_0. \tag{8}$$

Hierin sind α_0, β_0 die Werte von α, β in $\mathfrak{P}$, wenn diese Werte endlich sind, sonst beliebige Konstanten, z. B. 0.

9. Sind a, b die Ordnungszahlen von $\alpha-\alpha_0$, $\beta-\beta_0$ in $\mathfrak{P}$, so kommt, falls a, b positiv sind, der Punkt $\mathfrak{P}$ $(a-1)$-mal resp. $(b-1)$-mal in den Verzweigungspolygonen $\mathfrak{Z}_\alpha$, $\mathfrak{Z}_\beta$ in α, β vor. Ist aber a negativ, so enthält $\mathfrak{Z}_\alpha$ den Punkt $\mathfrak{P}$ $(-a-1)$-mal, und Entsprechendes gilt, wenn b negativ ist (§ 16, 1.). Bezeichnet man also mit $\mathfrak{A}$, $\mathfrak{B}$ die Unterecke von α, β, so erhält man, weil die Ordnungszahl von $\frac{d\alpha}{d\beta}$ (wie eben bewiesen) immer gleich $a-b$ ist, für diese Funktion folgenden Ausdruck als Polygonquotienten

$$\frac{d\alpha}{d\beta}=\frac{\mathfrak{Z}_\alpha\mathfrak{B}^2}{\mathfrak{Z}_\beta\mathfrak{A}^2}. \tag{9}$$

§ 24.

Das Geschlecht des Körpers Ω.

1. Bezeichnet man mit w_α, w_β die Verzweigungszahlen, mit n_α, n_β die Ordnungen der Variablen α, β, so folgt aus der Formel (9) des vorigen §, da Zähler und Nenner von $\frac{d\alpha}{d\beta}$ gleichviel Punkte enthalten müssen, die wichtige Relation

$$\mathrm{w}_\alpha - 2n_\alpha = \mathrm{w}_\beta - 2n_\beta;$$

wenn man also

(1) $$p = \tfrac{1}{2}\mathrm{w} - n + 1$$

setzt, welches nach § 22, 4. eine ganze Zahl ist, so ist diese von der Wahl der Variablen unabhängig und eine für den Körper Ω charakteristische Zahl, welche das Geschlecht des Körpers Ω genannt wird. Daß diese Zahl niemals negativ ist, ergibt sich, wenn man für $\frac{1}{2}\mathrm{w}$ den Wert $r_1 + r_2 + \cdots + r_n$ aus § 22 einsetzt. Man erhält dann

(2) $$p = (r_2 - 1) + (r_3 - 1) + \cdots + (r_n - 1),$$

was, da $r_2, r_3, \ldots r_n \geqq 1$ sind, nicht negativ werden kann.

2. Es seien α, β zwei Funktionen in Ω von den Ordnungen m, n, von der Beschaffenheit, daß alle Funktionen in Ω rational durch α, β darstellbar sind. Es ist dann

$$\begin{aligned} F(\alpha, \beta) &= a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n \\ &= b_0\beta^m + b_1\beta^{m-1} + \cdots + b_{m-1}\beta + b_m = 0 \end{aligned}$$

die zwischen α, β bestehende irreduktible Gleichung, worin $a_0, a_1, \ldots a_n$ ganze rationale Funktionen von β, ebenso $b_0, b_1, \ldots b_m$ ganze rationale Funktionen von α sind.

Es sei ferner

$$\alpha = \frac{\mathfrak{A}_1}{\mathfrak{A}}, \quad \beta = \frac{\mathfrak{B}_1}{\mathfrak{B}}$$

und $\mathfrak{A}_1$ relativ prim zu $\mathfrak{A}$, $\mathfrak{B}_1$ zu $\mathfrak{B}$, so daß $\mathfrak{A}$, $\mathfrak{A}_1$ von der Ordnung m, $\mathfrak{B}$, $\mathfrak{B}_1$ von der Ordnung n sind. Nun ist

$$F'(\alpha) = n a_0\alpha^{n-1} + (n-1)a_1\alpha^{n-2} + \cdots + a_{n-1},$$

$$\alpha F'(\alpha) = -a_1\alpha^{n-1} - 2a_2\alpha^{n-2} - \cdots - n a_n,$$

woraus hervorgeht, daß

$$F'(\alpha) = \frac{\mathfrak{K}}{\mathfrak{A}^{n-2}\mathfrak{B}^m}$$

und ebenso

$$F'(\beta) = \frac{\mathfrak{L}}{\mathfrak{A}^n \mathfrak{B}^{m-2}}$$

sein muß. Es ist nun nachzuweisen, daß das Polygon $\mathfrak{K}$ durch $\mathfrak{Z}_\beta$, $\mathfrak{L}$ durch $\mathfrak{Z}_\alpha$ teilbar ist.

Für $\mathfrak{K}$ ist dies leicht einzusehen unter der Voraussetzung, daß in sämtlichen Punkten von $\mathfrak{Z}_\beta$ die Funktion β einen endlichen, und a_0 einen von Null verschiedenen Wert hat; denn es ist

$$\alpha' = a_0 \alpha$$

eine ganze Funktion von β, und wenn man

$$f(\alpha') = a^{n-1} F(\alpha, \beta)$$

setzt, so ist

$$f'(\alpha') = a_0^{n-2} F'(\alpha).$$

Da nun nach § 11, 5. $\mathfrak{o}_\beta f'(\alpha')$ durch das von $\mathfrak{Z}_\beta$ erzeugte Verzweigungsideal in β teilbar ist, so folgt hieraus die Richtigkeit der Behauptung. Analoges gilt für $F'(\beta)$.

Macht man nun für α, β beliebige lineare Substitutionen:

$$\alpha = \frac{c + d\alpha'}{a + b\alpha'}; \quad \beta = \frac{c' + d'\beta'}{a' + b'\beta'},$$

$$(a + b\alpha')(d - b\alpha) = ad - bc,$$

$$(a' + b'\beta')(d' - b'\beta) = a'd' - b'c',$$

so ist nach § 16, 2.

$$\mathfrak{Z}_\alpha = \mathfrak{Z}_{\alpha'}; \quad \mathfrak{Z}_\beta = \mathfrak{Z}_{\beta'},$$

und die zwischen α', β' bestehende irreduktible Gleichung lautet:

$$F_1(\alpha', \beta') = (a + b\alpha')^n (a' + b'\beta')^m F(\alpha, \beta) = 0.$$

Es lassen sich aber unter allen Umständen die Konstanten a, b, c, d; a', b', c', d' so wählen, daß die oben angegebenen Voraussetzungen sowohl für α' als für β' erfüllt sind.

Denn setzt man die Koeffizienten a'_0, b'_0 von α'^n, β'^m in $F_1(\alpha', \beta')$ in die Form

$$\begin{aligned} a'_0 &= (a' + b'\beta')^m (a^0 d^n + a_1 d^{n-1} b + \cdots + a_n b^n) \\ &= \left(\frac{a'd' - b'c'}{d' - b'\beta}\right)^m (a_0 d^n + a_1 d^{n-1} b + \cdots + a_n b^n), \\ b'_0 &= (a + b\alpha')^n (b_0 d'^m + b_1 d'^{m-1} b' + \cdots + b_m b'^m) \\ &= \left(\frac{ad - bc}{d - b\alpha}\right)^n (b_0 d'^m + b_1 d'^{m-1} b' + \cdots + b_m b'^m), \end{aligned}$$

so erkennt man leicht, daß nur für eine endliche Anzahl von Werten der Verhältnisse $d:b$, $d':b'$ die Funktionen a'_0, $d'-b'\beta$ in einem Punkte von $\mathfrak{Z}_\beta$, b'_0, $d-b\alpha$ in einem Punkte von $\mathfrak{Z}_\alpha$ verschwinden können.

Setzen wir nun

$$\alpha' = \frac{\mathfrak{A}'_1}{\mathfrak{A}'}, \quad \beta' = \frac{\mathfrak{B}'_1}{\mathfrak{B}'},$$

so folgt (§ 19, 1.)

$$d - b\alpha = \frac{\mathfrak{A}_2}{\mathfrak{A}}, \quad a + b\alpha' = \frac{\mathfrak{A}'_2}{\mathfrak{A}'},$$

also:

$$\mathfrak{A}_2 \mathfrak{A}'_2 = \mathfrak{A}\mathfrak{A}'.$$

Ist aber, wie angenommen, b von Null verschieden, so ist $\mathfrak{A}_2$ relativ prim zu $\mathfrak{A}$, weil in einem Punkte von $\mathfrak{A}$ die Ordnungszahl von $d-b\alpha$ dieselbe ist, wie die von α (§ 15, 5.) und folglich

$$\mathfrak{A}_2 = \mathfrak{A}', \quad \mathfrak{A}'_2 = \mathfrak{A},$$

also:

$$a + b\alpha' = \frac{\mathfrak{A}}{\mathfrak{A}'},$$

und ebenso:

$$a' + b'\beta' = \frac{\mathfrak{B}}{\mathfrak{B}'}.$$

Nun ist aber, da $F(\alpha, \beta) = 0$ ist:

$$F'_1(\alpha') = (ad - bc)(a + b\alpha')^{n-2}(a' + b'\beta')^m F'(\alpha),$$

und wenn also, wie vorausgesetzt:

$$F'_1(\alpha') = \frac{\mathfrak{R}\,\mathfrak{Z}_\beta}{\mathfrak{A}'^{\,n-2}\mathfrak{B}'^{\,m}},$$

so folgt

$$F'(\alpha) = \frac{\mathfrak{R}\,\mathfrak{Z}_\beta}{\mathfrak{A}^{n-2}\mathfrak{B}^m}$$

und in gleicher Weise

$$F'(\beta) = \frac{\mathfrak{R}\,\mathfrak{Z}_\alpha}{\mathfrak{A}^n\mathfrak{B}^{m-2}}.$$

Daß das im Zähler dieser beiden Ausdrücke auftretende Polygon $\mathfrak{R}$ in beiden Ausdrücken dasselbe sein muß, ergibt sich aus

$$\frac{d\alpha}{d\beta} = -\frac{F'(\beta)}{F'(\alpha)} = \frac{\mathfrak{B}^2\,\mathfrak{Z}_\alpha}{\mathfrak{A}^2\,\mathfrak{Z}_\beta}.$$

Nun ist die Ordnung des Polygons $\mathfrak{A}^{n-2}\mathfrak{B}^m$

$$m(n-2)+mn=2m(n-1),$$

also die Ordnung von $\mathfrak{R}$

$$2r=2m(n-1)-\mathrm{w}_\beta$$

stets eine gerade Zahl, und daraus ergibt sich

$$p=\tfrac{1}{2}\mathrm{w}_\beta-n+1=(n-1)(m-1)-r. \tag{3}$$

Das Polygon $\mathfrak{R}$ wird das Polygon der Doppelpunkte in (α, β) genannt.

§ 25.

Die Differentiale in Ω.

Sind z, z_1 irgend zwei Variable in Ω von den Ordnungen n, n_1 und den Verzweigungszahlen w, w_1, ferner $\mathfrak{Z}$, $\mathfrak{Z}_1$ die Verzweigungspolygone, $\mathfrak{U}$, $\mathfrak{U}_1$ die Unterecke von z, z_1, so ist (§ 23)

$$\frac{dz}{dz_1}=\frac{\mathfrak{Z}\mathfrak{U}_1^2}{\mathfrak{Z}_1\mathfrak{U}^2}. \tag{1}$$

Jede Funktion ω in Ω läßt sich in die Form setzen

$$\omega=\frac{\mathfrak{U}^2\mathfrak{A}}{\mathfrak{Z}\mathfrak{B}}, \tag{2}$$

worin $\mathfrak{A}$, $\mathfrak{B}$ Polygone bedeuten, deren Ordnungen a, b der Bedingung genügen

$$2n+a=\mathrm{w}+b$$

oder (§ 24)

$$a=b+2p-2. \tag{3}$$

Wenn man nun eine Funktion ω_1 durch die Gleichung erklärt

$$\omega\, dz=\omega_1\, dz_1,$$

so erhält nach (1) ω_1 die Bezeichnung

$$\omega_1=\frac{\mathfrak{U}_1^2\mathfrak{A}}{\mathfrak{Z}_1\mathfrak{B}}.$$

Wir nennen in der Folge solche Ausdrücke, wie

$$\omega\, dz=\omega_1\, dz_1$$

Differentiale in Ω, und bezeichnen dieselben in symbolischer Weise durch ein Zeichen wie $d\varpi$. Ein solches Differential ist hierdurch invariant, d. h. unabhängig von der Wahl der Veränderlichen z erklärt und ist durch die beiden Polygone $\mathfrak{A}$, $\mathfrak{B}$ vollständig bestimmt.

Wir können ohne Gefahr eines Mißverständnisses die symbolische Bezeichnung

$$d\widetilde{\omega} = \frac{\mathfrak{A}}{\mathfrak{B}},$$

also beispielsweise auch

$$dz = \frac{\mathfrak{Z}}{\mathfrak{U}^2}$$

anwenden. Diese Bezeichnung eines Differentials durch einen Polygonquotienten unterscheidet sich von der ähnlichen Bezeichnung der Funktionen in Ω (§ 17) dadurch, daß bei letzterer Zähler und Nenner von gleicher Ordnung sind, während bei den Differentialen die Ordnung des Zählers die des Nenners um $2p-2$ übertrifft. Wie bei der Bezeichnung in § 17, können auch hier gemeinschaftliche Teiler, welche $\mathfrak{A}$ und $\mathfrak{B}$ etwa enthalten, unterdrückt werden. Sind $\mathfrak{A}$ und $\mathfrak{B}$ relativ prim, so heißt $\mathfrak{A}$ das Obereck, $\mathfrak{B}$ das Untereck des Differentials $d\widetilde{\omega}$.

Unter den hier aufgestellten allgemeinen Begriff des Differentials in Ω fallen als spezielle Fälle auch die in § 23, 4. erkärten Differentiale der Funktionen des Körpers Ω. Diese nennen wir eigentliche Differentiale, während die anderen, welche nicht als Differentiale von in Ω existierenden Funktionen dargestellt werden können, uneigentliche oder Abelsche Differentiale genannt werden.

Funktionen von der Form (2), die nach unserer jetzt getroffenen Festsetzung mit $\dfrac{d\widetilde{\omega}}{dz}$ bezeichnet werden können, nennen wir Differentialquotienten nach z und unterscheiden gleichfalls zwischen eigentlichen und uneigentlichen Differentialquotienten, je nachdem $d\widetilde{\omega}$ ein eigentliches oder uneigentliches Differential ist*).

Es entsteht nun die Aufgabe, den Umfang des Begriffs der Differentiale festzustellen, d. h. alle Polygone $\mathfrak{A}$, $\mathfrak{B}$ zu finden, welche Ober- und Untereck eines Differentials sein können. Wir schicken darüber die folgenden allgemeinen Bemerkungen voraus:

---

*) Der Quotient irgend zweier eigentlichen oder uneigentlichen Differentiale $\dfrac{d\widetilde{\omega}}{d\widetilde{\omega}'}$ hat stets die Bedeutung einer bestimmten Funktion in Ω. Wir beschränken uns im folgenden aber auf die Betrachtung solcher Quotienten, bei denen wenigstens der Nenner ein eigentliches Differential ist.

Die notwendige und hinreichende Bedingung dafür, daß $\frac{\mathfrak{A}}{\mathfrak{B}}$ ein Differential sei, ist die, daß für eine beliebige Variable z

$$\frac{\mathfrak{U}^2\mathfrak{A}}{\mathfrak{Z}\mathfrak{B}}$$

eine Funktion in Ω ist, also daß $\mathfrak{U}^2\mathfrak{A}$ mit $\mathfrak{Z}\mathfrak{B}$ äquivalent ist. Dies Verhältnis bleibt aber bestehen, wenn $\mathfrak{A}$, $\mathfrak{B}$ selbst durch äquivalente Polygone $\mathfrak{A}'$, $\mathfrak{B}'$ ersetzt werden. Halten wir $\mathfrak{B}$ fest, und ist $\frac{\mathfrak{A}}{\mathfrak{B}}$ ein Differential, so werden hiernach

$$\frac{\mathfrak{A}'}{\mathfrak{B}}, \quad \frac{\mathfrak{A}''}{\mathfrak{B}}, \ldots$$

dann und nur dann Differentiale darstellen, wenn die Polygone $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, ... alle derselben Klasse A angehören. Bilden die Polygone $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$, ... eine Basis von A, ist also

$$A = (\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \ldots),$$

so bilden die zugehörigen Differentialquotienten in bezug auf eine beliebige Variable z, $\frac{d\tilde{\omega}_1}{dz}, \frac{d\tilde{\omega}_2}{dz}, \frac{d\tilde{\omega}_3}{dz}, \cdots$ die Basis einer Funktionenschar von endlicher Dimension, und dementsprechend werden wir auch $d\tilde{\omega}_1, d\tilde{\omega}_2, d\tilde{\omega}_3, \ldots$ die Basis einer Schar von Differentialen

$$(d\tilde{\omega}_1, d\tilde{\omega}_2, d\tilde{\omega}_3, \ldots)$$

von derselben Dimension nennen. Dies besagt, daß jedes Differential $d\tilde{\omega}$, dessen Untereck $\mathfrak{B}$ oder ein Teiler von $\mathfrak{B}$ ist, in der Form dargestellt werden kann

$$d\tilde{\omega} = c_1 d\tilde{\omega}_1 + c_2 d\tilde{\omega}_2 + c_3 d\tilde{\omega}_3 + \cdots$$

mit konstanten Koeffizienten $c_1, c_2, c_3, \ldots$

§ 26.

Die Differentiale erster Gattung.

Wir betrachten zunächst die einfachsten unter den Differentialen in Ω, nämlich die, deren Untereck das Nulleck $\mathfrak{O}$ ist. Solche Differentiale (deren Existenz freilich erst noch nachzuweisen ist) heißen Differentiale erster Gattung. Das Obereck $\mathfrak{W}$ eines solchen Differentials dw, dessen Ordnung $2p-2$ ist, wird als das Grundpolygon von

dw bezeichnet und heißt ein vollständiges Polygon erster Gattung, während jeder Teiler eines solchen ein Polygon erster Gattung schlechtweg genannt wird. Ist $\mathfrak{W} = \mathfrak{A}\mathfrak{B}$, so heißen $\mathfrak{A}$, $\mathfrak{B}$ Ergänzungspolygone voneinander. Ein Polygon, welches nicht Teiler eines vollständigen Polygons erster Gattung ist, also insbesondere jedes Polygon von mehr als $2p-2$ Punkten heißt ein Polygon zweiter Gattung.

1. Nach dem oben Bemerkten bilden alle vollständigen Polygone erster Gattung eine Polygonklasse W, deren Dimension zu bestimmen ist; ergibt sich diese Dimension > 0, so ist damit zugleich die Existenz der Polygone erster Gattung nachgewiesen. Diese Dimension ist aber dieselbe wie die Dimension der Schar der Differentiale erster Gattung oder auch, für eine beliebige Variable z, der Schar der Differentialquotienten erster Gattung, wenn wir als Differentialquotienten erster Gattung nach z die Funktionen

$$u = \frac{dw}{dz}$$

bezeichnen. Eine solche Funktion u hat nach § 25, (2) den Ausdruck

$$u = \frac{\mathfrak{U}^2 \mathfrak{W}}{\mathfrak{Z}},$$

und man erkennt leicht aus der Betrachtung der Ordnungszahlen in den verschiedenen Punkten, daß ein solcher Differentialquotient erster Gattung durch folgende beiden Eigenschaften vollkommen definiert ist:

I. In jedem Punkte $\mathfrak{P}$, in welchem z einen endlichen Wert z_0 hat, ist

$$(u(z-z_0))_0 = 0.$$

II. In einem Punkte $\mathfrak{P}$, in welchem z unendlich ist, ist

$$(z\,u)_0 = 0.$$

Bedeutet wie in § 11, 4.

$$r = (z-c)(z-c_1)(z-c_2)\ldots$$

das Produkt sämtlicher voneinander verschiedenen Linearfaktoren der Diskriminante $\Delta_z(\Omega)$, $\mathfrak{r}$ das Produkt sämtlicher voneinander verschiedenen in r aufgehenden Primideale, so ist die Bedingung I. vollkommen gleichbedeutend mit der, daß ru eine Funktion in $\mathfrak{r}$, oder daß u eine Funktion des zu $\mathfrak{o}$ komplementären Moduls $\mathfrak{e}$ sein muß [§ 11, 4. (6)]. Um also die Gesamtheit der Funktionen u zu erhalten, hat man unter den Funktionen in $\mathfrak{e}$ diejenigen aufzusuchen, welche der Bedingung II. genügen.

2. Zu diesem Zwecke legen wir eine Normalbasis $\lambda_1, \lambda_2, \ldots \lambda_n$ von $\mathfrak{o}$ zugrunde (§ 22) und bezeichnen die dazu komplementäre Basis mit $\mu_1, \mu_2, \ldots \mu_n$, so daß jede der Bedingung I. genügende Funktion, also auch jeder Differentialquotient erster Gattung, in der Form enthalten ist

$$(1) \qquad u = y_1 \mu_1 + y_2 \mu_2 + \cdots + y_n \mu_n,$$

worin $y_1, y_2, \ldots y_n$ ganze rationale Funktionen von z sind. Aus den Grundeigenschaften der komplementären Basis ergibt sich aber (§ 10, 3.)

$$y_s = S(u \lambda_s); \qquad \frac{y_s}{z^{r_s - 1}} = S\left(uz \cdot \frac{\lambda_s}{z^{r_s}}\right).$$

Da nun $\dfrac{\lambda_s}{z^{r_s}}$ in $\mathfrak{o}'$ enthalten, also für $z = \infty$ endlich ist, und uz nach II. in jedem solchen Punkte verschwindet, so folgt (§ 16, 5.), daß $\dfrac{y_s}{z^{r_s - 1}}$ für $z = \infty$ verschwinden muß, d. h. daß die ganze rationale Funktion y_s den Grad $r_s - 2$ nicht übersteigen kann.

Es muß daher, falls $r_s < 2$ ist, y_s verschwinden, also ist unter allen Umständen (§ 22, 2.)

$$y_1 = 0; \quad S(u) = 0$$

(Abelsches Theorem für Differentiale erster Gattung) und, falls $r_s \gtreqless 2$:

$$(2) \qquad y_s = c_0 + c_1 z + c_2 z^2 + \cdots + c_{r_s - 2} z^{r_s - 2}.$$

Es ist noch zu zeigen, daß diese Bedingungen auch hinreichend sind, d. h. daß jede Funktion von der Form (1), in welcher die y_s den Ausdruck (2) haben, der Forderung II. genügt, oder, was dasselbe ist, daß, wenn $r_s \gtreqless 2$ ist, $z^{r_s - 1} \mu_s$ in allen Punkten, in welchen z unendlich wird, verschwindet. Dies ergibt sich sofort durch die Betrachtung des Systems $\mathfrak{o}'$ der ganzen Funktionen von $z' = \dfrac{1}{z}$, für welches nach § 22, 3. die Funktionen

$$\lambda_1' = \frac{\lambda_1}{z^{r_1}}, \quad \lambda_2' = \frac{\lambda_2}{z^{r_2}}, \quad \ldots \quad \lambda_n' = \frac{\lambda_n}{z^{r_n}}$$

eine Normalbasis bilden. Die hierzu komplementäre Basis ist nach § 10, 5.

$$\mu'_1 = z^{r_1}\mu_1, \quad \mu'_2 = z^{r_2}\mu_2, \quad \ldots \quad \mu'_n = z^{r_n}\mu_n,$$

und da (wegen der Eigenschaft I., auf z', μ' angewandt)

$$z'\mu'_s = 0 \quad \text{für} \quad z' = 0,$$

so folgt

$$z^{r_s - 1}\mu_s = 0 \quad \text{für} \quad z = \infty,$$

w. z. b. w.

Da aber die Funktionen $z^h\mu_s$ linear unabhängig sind (wegen der rationalen Unabhängigkeit der Funktionen μ_s), so ergibt sich hieraus nach § 24, (2) der Hauptsatz:

Die Schar der Differentiale erster Gattung ist von der Dimension

$$(r_2 - 1) + (r_3 - 1) + \cdots + (r_n - 1) = p,$$

und demnach ist auch p die Dimension der Klasse W der vollständigen Polygone erster Gattung.

Als Basis der Schar der Differentialquotienten erster Gattung nach z kann man die p Funktionen $z^h\mu_s$ $(h \lesseqgtr r_s - 2)$ wählen, und die Grundpolygone $\mathfrak{W}_1, \mathfrak{W}_2, \ldots \mathfrak{W}_p$ der zugehörigen Differentiale dw bilden eine Basis der Klasse W.

3. Wegen einer späteren Anwendung soll hier noch eine besondere Art von Differentialquotienten erster Gattung u' betrachtet werden, nämlich die, bei welchen die Bedingung II. ersetzt ist durch die dieselbe einschließende Bedingung.

III. In jedem Punkte $\mathfrak{P}$, in welchem z unendlich ist, sei

$$(z^k u')_0 = 0,$$

wo k eine gegebene positive ganze Zahl.

Die Funktionen u' lassen sich darstellen durch

$$u' = \frac{\mathfrak{U}^{k+1}\mathfrak{W}'}{\mathfrak{Z}}$$

und bilden ebenfalls eine Schar; desgleichen bilden die Polygone $\mathfrak{W}'$ eine Klasse W', deren Ordnung ist

$$\mathrm{w} - n(k+1) = 2p - 2 - n(k-1).$$

Die Polygone $\mathfrak{W}'$ sind jedoch von der Wahl der Variablen z nicht unabhängig. Die Dimension der Klasse W' läßt sich nach derselben Methode bestimmen, wie die der Klasse W. Da nämlich die Bedingung I. erfüllt ist, so sind Funktionen u' gleichfalls in der Form (1) enthalten; jedoch muß jetzt

$$\frac{y_s}{z^{r_s - k}} = S\left(u' z^k \frac{\lambda_s}{z^{r_s}}\right)$$

für $z = \infty$ verschwinden, und daher kann der Grad der ganzen rationalen Funktion y_s die Zahl $r_s - k - 1$ nicht übersteigen. Es verschwindet also y_s identisch, sobald $r_s < k + 1$; andernfalls ist

$$y_s = c_0 + c_1 z + \cdots + c_{r_s - k - 1} z^{r_s - k - 1}. \tag{3}$$

Hat umgekehrt y_s diese Form, so wird durch die Funktion

$$u' = \sum^{s} y_s \mu_s$$

der Bedingung III. genügt, denn es hat, wie in 2. bewiesen,

$$z^k(z^{r_s - k - 1} \mu_s) = z^{r_s - 1} \mu_s$$

für $z = \infty$ den Wert 0.

Daraus ergibt sich, daß die Dimension der Schar der Funktionen u' und folglich auch der Klasse W'

$$= \sum^{\iota} (r_\iota - k)$$

ist, wobei jedoch in der Summe nur diejenigen Glieder beizubehalten sind, die einen positiven Wert haben. Sind alle $r_\iota - k \overline{\gtrless} 0$, so existieren die gesuchten Funktionen überhaupt nicht.

§ 27.

Polygonklassen erster und zweiter Gattung.

Ist $\mathfrak{A}$ ein Polygon erster Gattung, so sind alle mit $\mathfrak{A}$ äquivalenten Polygone gleichfalls von der ersten Gattung. Denn wenn $\mathfrak{A}$ und $\mathfrak{B}$ Ergänzungspolygone sind und

$$\mathfrak{A}\mathfrak{B} = \mathfrak{W},$$

so ist, wenn A, B die Klassen von $\mathfrak{A}$ und $\mathfrak{B}$ sind:

$$AB = W,$$

und, wenn $\mathfrak{A}'$ mit $\mathfrak{A}$ äquivalent ist, auch $\mathfrak{A}'\mathfrak{B} = \mathfrak{W}'$ äquivalent mit $\mathfrak{W}$ (§ 18, 5.).

Wir nennen daher solche Klassen, welche Polygone erster Gattung enthalten, P o l y g o n k l a s s e n e r s t e r G a t t u n g, die übrigen P o l y g o n k l a s s e n z w e i t e r G a t t u n g. Die Klasse W der vollständigen Polygone erster Gattung heißt die Hauptklasse, und zwei Klassen A, B, die der Bedingung genügen

$$AB = W,$$

Ergänzungsklassen.

Ist

$$\eta = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

eine Funktion in Ω, und $\mathfrak{A}'$ relativ prim zu $\mathfrak{A}$, also die Klasse A von $\mathfrak{A}$ eine eigentliche, so nennen wir η eine Funktion erster oder zweiter Gattung, je nachdem die Klasse A von der ersten oder von der zweiten Gattung ist.

Ist A eine beliebige Klasse erster Gattung und q die Anzahl der voneinander unabhängigen Polygone $\mathfrak{W}$, die durch irgendein Polygon $\mathfrak{A}$ der Klasse A teilbar sind, so ist nach § 21, 2.

$$q = (A, W) = (O, B)$$

d. h. gleich der Dimension der Ergänzungsklasse B von A. Ebenso ist (B, W) gleich der Dimension der Klasse A. Ist A eine Klasse zweiter Gattung, so ist $(A, W) = 0$. Da p die Dimension von W ist, so ist nach § 20, 2., 3. jede Klasse, deren Ordnung $\overline{\gtrless} p - 1$ ist, von der ersten Gattung, und es gibt insbesondere Klassen A von der Ordnung $p - k$ derart, daß $(A, W) = (O, B) = k$ ist. Aus den gleichen Sätzen folgt, daß es Klassen von der Ordnung p gibt, welche von der zweiten Gattung sind.

§ 28.

Der Riemann-Rochsche Satz für eigentliche Klassen.

Der Riemann-Rochsche Satz, der nach seiner gewöhnlichen Ausdrucksweise die Anzahl der willkürlichen Konstanten kennen lehrt, welche eine Funktion enthält, die in einer gewissen Anzahl gegebener Punkte unendlich wird, enthält nach unserer Darstellungsweise eine Beziehung zwischen der Dimension und der Ordnung einer Klasse, resp. einer Klasse und ihrer Ergänzungsklasse. Indem wir uns zunächst auf eigentliche Klassen beschränken, schicken wir der Ableitung dieser fundamentalen Relation die folgenden Bemerkungen voraus.

1. In einer eigentlichen Klasse A kann man nach § 19, 2. stets zwei zueinander relativ prime Polygone $\mathfrak{A}$, $\mathfrak{A}'$ auswählen (eines derselben kann in der Klasse beliebig angenommen werden). Setzt man also

$$z = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

und, wenn $\mathfrak{A}''$ ein beliebiges drittes Polygon der Klasse A bedeutet:

$$\omega = \frac{\mathfrak{A}''}{\mathfrak{A}}, \quad \frac{\omega}{z} = \frac{\mathfrak{A}''}{\mathfrak{A}'},$$

so ist nach § 17 ω eine ganze Funktion von z, $\frac{\omega}{z}$ eine ganze Funktion von $\frac{1}{z}\cdot$ Es ist daher (§ 22) der Exponent von $\omega \leqq 1$.

Ist umgekehrt ω eine ganze Funktion von z, deren Exponent $\leqq 1$ ist, so hat es die Form

$$\omega = \frac{\mathfrak{A}''}{\mathfrak{A}},$$

wo $\mathfrak{A}''$ ein Polygon der Klasse A ist. Wenn nämlich

$$\omega = \frac{\mathfrak{A}_1''}{\mathfrak{A}_1}, \quad \frac{\omega}{z} = \frac{\mathfrak{A}_1''\mathfrak{A}}{\mathfrak{A}_1\mathfrak{A}'}$$

und $\mathfrak{A}_1''$ relativ prim zu $\mathfrak{A}_1$ angenommen wird, so kann zunächst, da ω eine ganze Funktion von z sein soll, $\mathfrak{A}_1$ keinen Punkt enthalten, der nicht auch in $\mathfrak{A}$ enthalten wäre. Es kann aber auch $\mathfrak{A}_1$ keinen Punkt öfter als $\mathfrak{A}$ enthalten, weil sonst $\frac{\omega}{z}$ in einem solchen Punkte (der nicht in $\mathfrak{A}'$ vorkommen kann) unendlich, also keine ganze Funktion von $\frac{1}{z}$ wäre. Daher ist $\mathfrak{A}$ teilbar durch $\mathfrak{A}_1$, und ω kann in die Form $\frac{\mathfrak{A}''}{\mathfrak{A}}$ gesetzt werden.

2. Um also die Gesamtheit der Polygone der Klasse A zu erhalten, haben wir nur diejenigen ganzen Funktionen von z aufzusuchen, deren Exponent $\leqq 1$ ist.

Ist n die Ordnung der Klasse A, also auch die Ordnung der Variablen z, und bilden $\lambda_1, \lambda_2, \ldots \lambda_n$ eine Normalbasis von $\mathfrak{o}$ mit den Exponenten $r_1, r_2, \ldots r_n$, darunter r_s der letzte, welcher $\leqq 1$ ist, so kann jede Funktion ω, deren Exponent $\leqq 1$ ist, nach § 22, 2. in der Form dargestellt werden

$$\omega = c_1\lambda_1 + c_2\lambda_2 + \cdots + c_s\lambda_s + z\omega_1.$$

Da der Exponent von $z\omega_1$ aber nicht größer als 1 sein kann, so muß ω_1 eine Konstante sein, und daher

$$\omega = c_1\lambda_1 + c_2\lambda_2 + \cdots + c_s\lambda_s + c_{s+1}z.$$

Umgekehrt genügt jede Funktion von dieser Form der gestellten Forderung. Es ist also $s+1$ die Dimension der Klasse A, welche hiernach, in Übereinstimmung mit § 21, 1., stets $\overline{\gtrless}\, n+1$ ist. Die obere Grenze $n+1$ kann aber nur in dem Falle $p=0$ erreicht werden und wird auch wirklich erreicht, weil in diesem Falle $r_2, r_3, \ldots r_n = 1$ sind. Daraus ergibt sich, daß ein einzelner Punkt $\mathfrak{P}$ nur, falls $p=0$ ist, zu einer eigentlichen Klasse gehören kann.

3. Wenn von den Exponenten $r_{s+1}, r_{s+2}, \ldots r_n$ einer größer als 2 ist, so ist sicher auch $r_n > 2$, und es sind nach § 26, 2., wenn $\mathfrak{Z}$ das Verzweigungspolygon in z bedeutet,

$$\mu_n = \frac{\mathfrak{A}^2 \mathfrak{W}}{\mathfrak{Z}}, \quad \mu_n z = \frac{\mathfrak{A}^2 \mathfrak{W}_1}{\mathfrak{Z}} = \frac{\mathfrak{A}\mathfrak{A}' \mathfrak{W}}{\mathfrak{Z}}$$

Differentialquotienten erster Gattung nach z, also

$$\mathfrak{A}\mathfrak{W}_1 = \mathfrak{A}'\mathfrak{W}$$

oder, da $\mathfrak{A}$, $\mathfrak{A}'$ relativ prim sind,

$$\mathfrak{W} = \mathfrak{A}\mathfrak{B}, \quad \mathfrak{W}_1 = \mathfrak{A}'\mathfrak{B},$$

d. h. die Klasse A ist von der ersten Gattung (z eine Variable erster Gattung). Machen wir daher zunächst die Annahme, es sei A eine Klasse zweiter Gattung, so folgt

$$r_{s+1} = 2, \quad r_{s+2} = 2, \ \ldots \ r_n = 2$$

und

$$p = (r_2 - 1) + \cdots + (r_s - 1) + (r_{s+1} - 1) + \cdots + (r_n - 1) = n - s.$$

Die Dimension $s+1$ der Klasse A ist daher

$$(O, A) = n - p + 1.$$

4. Machen wir zweitens die Annahme, es sei A von der ersten Gattung und wie in § 27

$$q = (A, W),$$

so existieren q linear unabhängige, durch $\mathfrak{A}$ teilbare vollständige Polygone erster Gattung, und die diesen entsprechenden Differentialquotienten erster Gattung nach z, deren es ebenfalls q und nicht mehr linear unabhängige gibt, haben den Ausdruck

$$v = \frac{\mathfrak{A}^3 \mathfrak{B}}{\mathfrak{Z}},$$

worin $\mathfrak{B}$ ein Polygon von $2p-2-n$ Punkten bedeutet; die Klasse B von $\mathfrak{B}$ ist die Ergänzungsklasse von A, und daher ihre Dimension gleich q (§ 27).

Diese Funktionen v haben aber die Eigenschaft, daß in den Eckpunkten von $\mathfrak{A}$, d. h. für $z = \infty$ nicht nur zv, sondern auch

$$z^2 v = \frac{\mathfrak{A}\mathfrak{A}'^2\mathfrak{B}}{\mathfrak{Z}}$$

verschwindet, und sind hierdurch und durch die Forderung, Differentialquotienten erster Gattung zu sein, völlig bestimmt. Denn ist

$$v = \frac{\mathfrak{A}^2\mathfrak{W}}{\mathfrak{Z}}, \quad vz^2 = \frac{\mathfrak{A}'^2\mathfrak{W}}{\mathfrak{Z}},$$

so muß, wenn $z^2 v$ in allen Punkten von $\mathfrak{A}$ verschwinden soll, $\mathfrak{W}$ durch $\mathfrak{A}$ teilbar sein, da $\mathfrak{A}'$ relativ prim zu $\mathfrak{A}$ vorausgesetzt ist. Es ist daher nach § 26, 3.:

$$q = (r_{s+1} - 2) + (r_{s+2} - 2) + \cdots + (r_n - 2),$$

andererseits

$$p = (r_{s+1} - 1) + (r_{s+2} - 1) + \cdots + (r_n - 1),$$

folglich:

$$p - q = n - s, \quad s = n - p + q.$$

Hierin ist der Riemann-Rochsche Satz enthalten, dem wir, mit Rücksicht auf § 27, für diesen Fall folgenden Ausdruck geben können: Sind A, B Ergänzungsklassen erster Gattung, von denen wenigstens die eine eine eigentliche ist, und a, b ihre Ordnungen, also

$$a + b = 2p - 2,$$

so ist

$$(O, A) - \tfrac{1}{2}a = (O, B) - \tfrac{1}{2}b.$$

5. Wir können, wenn wir den Fall $(A, W) = 0$ nicht ausschließen, den Riemann-Rochschen Satz für beide Fälle dahin zusammenfassen:

Ist A eine eigentliche Klasse von der Ordnung n, so ist ihre Dimension

$$(O, A) = n - p + 1 + (A, W).$$

Da die Dimension einer eigentlichen Klasse (wenn sie nicht aus dem einzigen Nulleck besteht) mindestens $= 2$ sein muß, so folgt noch, wenn $(A, W) = 0$ ist,

$$n \geqq p + 1,$$

und daraus der von Riemann herrührende Satz:

Jede Funktion, deren Ordnung $\leqq p$ ist, ist eine Funktion erster Gattung.

6. Es läßt sich mit Hilfe dieser Sätze leicht beweisen, daß die Hauptklasse W der vollständigen Polygone erster Gattung stets eine eigentliche ist.

Ist nämlich $\mathfrak{M}$ der Teiler von W, so läßt sich nach § 19, 2. in W ein Polygon $\mathfrak{A}\mathfrak{M}$ derart finden, daß $\mathfrak{A}$ relativ prim zu $\mathfrak{M}$ ist Die Klasse A von $\mathfrak{A}$ ist eine eigentliche (§ 21, 3.), und zugleich ist $\mathfrak{A}\mathfrak{M}$ das einzige durch $\mathfrak{A}$ teilbare Polygon der Klasse W (weil jedes Polygon in W den Teiler $\mathfrak{M}$ hat). Also ist

$$(A, W) = 1.$$

Nun ist p die Dimension von W, also auch die von A, und mithin nach dem Riemann-Rochschen Satze die Ordnung von A gleich $2p-2$, d. h. ebenso groß wie die von W. Mithin ist $\mathfrak{M} = \mathfrak{O}$.

§ 29.

Der Riemann-Rochsche Satz für uneigentliche Klassen erster Gattung.

Ist A eine Klasse erster Gattung vom Teiler $\mathfrak{M}$ und

$$A = \mathfrak{M}A',$$

so ist A' eine eigentliche Klasse erster Gattung. Es sei B die Ergänzungsklasse von A; B' die von A'; a, b die Ordnungen der Klassen A, B; m die Ordnung von $\mathfrak{M}$. Die gesamte Klasse B erhält man, wenn man in sämtlichen durch $\mathfrak{M}$ teilbaren Polygonen der Klasse B' den Faktor $\mathfrak{M}$ unterdrückt; denn ist

$$\mathfrak{A}\mathfrak{B} = \mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{W},$$

so gehört $\mathfrak{M}\mathfrak{B}$ in die Klasse B', und umgekehrt, wenn

$$\mathfrak{A}'\mathfrak{B}' = \mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{W}$$

ist, so gehört $\mathfrak{B}$ in die Klasse B.

Hieraus ergibt sich aber nach § 21, 2.

$$(O, B) \geqq (O, B') - m.$$

Nun ist A' eine eigentliche Klasse von derselben Dimension wie A und von der Ordnung $a-m$, also (§ 28, 5.)

$$(O, A) = (O, A') = a - m - p + 1 + (A', W),$$

oder

$$(O, A) = (O, B') - m + a - p + 1;$$

daher

$$(O, A) \lesseqqgtr (O, B) + a - p + 1 = (O, B) + \tfrac{1}{2}(a-b),$$

also

$$(O, A) - \tfrac{1}{2}a \lesseqqgtr (O, B) - \tfrac{1}{2}b.$$

Da aber die Klassen A, B miteinander vertauscht werden können, so folgt in gleicher Weise

$$(O, B) - \tfrac{1}{2} b \gtreqless (O, A) - \tfrac{1}{2} a,$$

d. h.

$$(O, A) - \tfrac{1}{2} a = (O, B) - \tfrac{1}{2} b,$$

wodurch der Riemann-Rochsche Satz in derselben Form wie in § 28, 4. für Polygonklassen erster Gattung allgemein nachgewiesen ist*).

§ 30.

Uneigentliche Klassen zweiter Gattung.

Es soll nun die Bedingung aufgesucht werden, unter der eine Polygonklasse zweiter Gattung A von der Ordnung n überhaupt eine uneigentliche sein kann, wobei sich die allgemeine Gültigkeit des Riemann-Rochschen Satzes von selbst ergeben wird.

1. Jede Klasse A kann stets durch Multiplikation mit einer andern Klasse N von der Ordnung ν in eine eigentliche Klasse AN verwandelt werden. Denn ist $\mathfrak{A}$ ein beliebiges Polygon in A, so wähle man eine Variable z, welche in sämtlichen Punkten von $\mathfrak{A}$ endlich bleibt (§ 15, 6.). Ist dann η eine beliebige Funktion des durch $\mathfrak{A}$ erzeugten Ideals in z, so ist das Obereck von η durch $\mathfrak{A}$ teilbar, also von der Form $\mathfrak{A}\mathfrak{N}$, und die Klasse von $\mathfrak{A}\mathfrak{N}$ ist eine eigentliche.

2. Die Dimension der eigentlichen Klasse AN zweiter Gattung ist nach § 28, 3.

$$(O, AN) = n + \nu - p + 1,$$

und hieraus folgt nach § 21, 2.

$$(O, A) \geqq n - p + 1.$$

Ist nun der Teiler $\mathfrak{M}$ der Klasse A von der Ordnung m, und

$$A = \mathfrak{M} A',$$

*) Nach der Ausdrucksweise von Christoffel (Über die kanonische Form der Riemannschen Integrale erster Gattung, Annali di Matematica pura ed applicata, Serie II, Tomo IX) ist

$$(A, W) + a - p = (O, B) + a - p = (O, A) - 1$$

der „Überschuß“,

$$(A, W) - 1 = (O, B) - 1$$

der „Defekt“ des Punktsystems $\mathfrak{A}$.

so ist A' eine eigentliche Klasse von derselben Dimension wie A, und mithin (§ 28, 5.)

$$(O, A) = (O, A') = n - m - p + 1 + (A', W),$$

also

$$(A', W) \gtreqless m,$$

d. h. A' muß gewiß von der ersten Gattung sein, wenn A eine uneigentliche Klasse ist. Ist also B' die Ergänzungsklasse von A', so ist auch

$$(O, B') \gtreqless m.$$

Wäre aber $(O, B' > m$, so würde sich nach § 20, 2. in B' ein durch $\mathfrak{M}$ teilbares Polygon $\mathfrak{M}\mathfrak{B}$ finden lassen und es wäre

$$\mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{A}\mathfrak{B} = \mathfrak{W},$$

also A von der ersten Gattung, gegen die Voraussetzung. Es ist also

$$(A', W) = m$$

und folglich

$$(O, A) = n - p + 1,$$

worin wieder der Riemann-Rochsche Satz für diesen Fall, genau in der Form von § 28, 3. enthalten ist.

3. Enthält die Klasse A nur ein einziges isoliertes Polygon, so ist $(O, A) = n - p + 1 = 1$, mithin $n = p$, d. h. ein isoliertes Polygon zweiter Gattung hat stets die Ordnung p. Umgekehrt ist, nach 2. jedes Polygon zweiter Gattung von der Ordnung p ein isoliertes.

4. Unter Beibehaltung der Bezeichnung von 2. ist $(O, B') = m$ und daher läßt sich nach dem oft angewandten Satze (§ 20, 2.) in B' ein durch ein beliebiges $(m - 1)$-Eck teilbares Polygon finden. Setzt man also, indem man einen beliebigen Punkt $\mathfrak{P}$ von $\mathfrak{M}$ absondert,

$$\mathfrak{M} = \mathfrak{P}\mathfrak{M}',$$

so ist ein Polygon $\mathfrak{M}'\mathfrak{B}$ in B' enthalten und also

$$\mathfrak{A}'\mathfrak{M}'\mathfrak{B} = \mathfrak{W}.$$

Das Polygon $\mathfrak{A}'\mathfrak{M}' = \mathfrak{A}''$ und seine Klasse A'' sind daher von der ersten Gattung, und A hat, wenn P die Klasse von $\mathfrak{P}$ bedeutet die Form

$$A = PA''.$$

Zugleich muß $(A'', W) = (O, B'') = 1$ sein, d. h. die Ergänzungsklasse B'' von A'' enthält nur ein einziges isoliertes Polygon $\mathfrak{B}''$, da sonst in B'' ein durch $\mathfrak{P}$ teilbares Polygon existieren würde, und also auch A gegen die Voraussetzung von der ersten Gattung wäre.

5. Ist umgekehrt A'' eine Klasse erster Gattung, für welche $(A'', W) = 1$, so daß die Ergänzungsklasse B'' von A'' aus einem isolierten Polygon $\mathfrak{B}''$ besteht; ist ferner $\mathfrak{P}$ ein in B'' nicht aufgehender Punkt, und seine Klasse P, so ist $A = PA''$ eine uneigentliche Klasse zweiter Gattung von der Ordnung n, in deren Teiler $\mathfrak{P}$ aufgeht.

Daß A von der zweiten Gattung ist, ergibt sich zunächst aus der Annahme, daß $\mathfrak{P}$ in $\mathfrak{B}''$ nicht aufgeht. Die Dimension von A ist daher nach 2.

$$(O, A) = n - p + 1,$$

wo n die Ordnung von A bedeutet; andererseits ist die Dimension der Klasse A'' nach §§ 28 und 29:

$$(O, A'') = n - p + (A'', W) = n - p + 1;$$

also sind A und A'' von derselben Dimension. Sämtliche Polygone der Klasse A'' gehen aber durch Multiplikation mit $\mathfrak{P}$ in Polygone der Klasse A über, und wegen der Gleichheit der Dimensionen wird hierdurch auch die letzte Klasse vollständig erschöpft. Es enthalten daher sämtliche Polygone der Klasse A den Faktor $\mathfrak{P}$, der sonach auch im Teiler von A aufgeht.

6. In dem besonderen Falle, wo das Geschlecht p des Körpers Ω den Wert 0 hat, kommen Polygone und Klassen erster Gattung überhaupt nicht vor. Es existieren also in diesem Falle auch keine uneigentlichen Klassen. Die Dimension einer jeden Klasse ist um 1 größer als ihre Ordnung. Insbesondere gehört also auch jeder Punkt $\mathfrak{P}$ zu einer eigentlichen Klasse von der Dimension 2, und daher existieren in diesem Falle in Ω Funktionen z, welche von der ersten Ordnung sind. Durch eine solche läßt sich jede andere Funktion des Körpers rational ausdrücken, denn die zwischen z und einer anderen Variablen des Körpers bestehende irreduktible Gleichung ist in bezug auf letztere vom ersten Grad (§ 15, 7.).

§ 31.

Die Differentiale zweiter und dritter Gattung.

1. Ist jetzt nach der in § 25 eingeführten Bezeichnung

$$d\tilde{\omega} = \frac{\mathfrak{A}}{\mathfrak{B}}$$

ein beliebiges Differential in Ω, also, wenn a, b die Ordnungen von $\mathfrak{A}$ und $\mathfrak{B}$ sind,

$$a = b + 2p - 2,$$

und werden $\mathfrak{A}$, $\mathfrak{B}$ als relativ prim vorausgesetzt, so muß, wenn $\mathfrak{U}$, $\mathfrak{Z}$ Untereck und Verzweigungspolygon für eine beliebige Variable z bedeuten, $\mathfrak{U}^2\mathfrak{A}$ mit $\mathfrak{Z}\mathfrak{B}$ äquivalent sein (§ 25). Bezeichnet man also mit U, Z, A, B die Klassen der Polygone $\mathfrak{U}$, $\mathfrak{Z}$, $\mathfrak{A}$, $\mathfrak{B}$, so muß

$$U^2 A = Z B$$

sein. Andererseits ist aber, wenn W die Hauptklasse erster Gattung ist,

$$U^2 W = Z,$$

woraus sich die Relation

$$A = B W$$

ergibt. Ist umgekehrt $\mathfrak{A}$ ein beliebiges Polygon der Klasse BW, so folgt daraus die Äquivalenz von $\mathfrak{U}^2\mathfrak{A}$ mit $\mathfrak{Z}\mathfrak{B}$, also die Existenz eines Differentials von der Bezeichnung $\frac{\mathfrak{A}}{\mathfrak{B}}$. Daraus ergibt sich, daß $\mathfrak{B}$ dann und nur dann Untereck eines Differentials $d\tilde{\omega}$ sein kann, wenn in BW ein zu $\mathfrak{B}$ relativ primes Polygon existiert, d. h. wenn der Teiler der Klasse BW relativ prim zu $\mathfrak{B}$ ist. Die Dimension der Klasse BW gibt dann zugleich die Dimension der zum Untereck $\mathfrak{B}$ gehörigen Schar von Differentialen $d\tilde{\omega}$ (§ 25). Die Sätze § 30, 4., 5. ergeben daher, da $(W, W) = 1$ ist, das folgende Resultat.

a) Besteht $\mathfrak{B}$ aus einem einzigen Punkt (ist $b = 1$), so ist die Klasse BW eine uneigentliche mit dem Teiler $\mathfrak{B}$; also kann die Ordnung b des Untерecks eines Differentials $d\tilde{\omega}$ nicht gleich Eins sein.

b) Ist $b \geqq 2$, so ist BW stets eine eigentliche Klasse zweiter Gattung und daher ihre Dimension

$$b + p - 1.$$

Untereck eines Differentials kann also jedes beliebige Polygon von mehr als einem Punkt sein, und es existieren unter den zu einem Untereck von der Ordnung b gehörigen Differentialen $b + p - 1$ linear unabhängige.

2. Wir suchen jetzt unter der Voraussetzung, daß $b \gtrless 2$ ist, für die Klasse A eine Basis derart auf, daß jedes Element $\mathfrak{A}_r$ dieser Basis ein Differential $d\tilde{\omega}_r$ von möglichst einfacher Beschaffenheit liefert, nämlich ein solches, dessen Untereck eine Potenz eines einzelnen Punktes oder das Produkt aus nur zwei verschiedenen Punkten ist.

Angenommen, es sei für die Klasse BW eine solche Basis bereits gefunden

(1) $$\mathfrak{A}_1,\ \mathfrak{A}_2,\ \mathfrak{A}_3,\ \ldots\ \mathfrak{A}_{b+p-1},$$

so bilden wir daraus, wenn P die Klasse eines beliebigen Punktes $\mathfrak{P}$ bedeutet, eine ebensolche Basis für die Klasse BPW von der Dimension $b+p$, nämlich

(2) $$\mathfrak{P}\mathfrak{A}_1,\ \mathfrak{P}\mathfrak{A}_2,\ \ldots\ \mathfrak{P}\mathfrak{A}_{b+p-1},\ \mathfrak{A}'.$$

Die ersten $b+p-1$ dieser Polygone gehören wirklich der Klasse BPW an und sind voneinander unabhängig, weil es die Polygone (1) sind; zugleich sind die aus ihnen gebildeten Differentiale

$$d\widetilde{\omega}_r = \frac{\mathfrak{P}\mathfrak{A}_r}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{A}_r}{\mathfrak{B}}$$

mit den aus (1) gebildeten identisch. Es kommt also nur noch auf die Bildung von $\mathfrak{A}'$ an, wobei zwei Fälle zu unterscheiden sind.

a) Geht $\mathfrak{P}$ in $\mathfrak{B}$ auf und ist $\mathfrak{B} = \mathfrak{M}\mathfrak{P}^m$, $\mathfrak{M}$ nicht durch $\mathfrak{P}$ teilbar, so ist $P^{m+1}W$ eine eigentliche Klasse (weil $m+1 \geqq 2$, § 30, 4.), in welcher folglich ein durch $\mathfrak{P}$ nicht teilbares Polygon $\mathfrak{N}$ existiert; setzt man nun $\mathfrak{A}' = \mathfrak{M}\mathfrak{N}$, so gehört $\mathfrak{A}'$ der Klasse BPW an und ist durch $\mathfrak{P}$ nicht teilbar, folglich auch nicht in der Schar $(\mathfrak{P}\mathfrak{A}_1,\ \mathfrak{P}\mathfrak{A}_2,\ \ldots\ \mathfrak{P}\mathfrak{A}_{b+p-1})$, deren Teiler $\mathfrak{P}$ ist, enthalten; mithin sind die Polygone (2) unabhängig voneinander, und da ihre Anzahl $b+p$ ist, so bilden sie eine Basis der Klasse BPW. Das aus $\mathfrak{A}'$ gebildete Differential

$$d\widetilde{\omega}' = \frac{\mathfrak{A}'}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{N}}{\mathfrak{P}^{m+1}}$$

hat die geforderte Form, da sein Untereck eine Potenz eines einzelnen Punktes ist.

b) Geht $\mathfrak{P}$ nicht in $\mathfrak{B}$ auf, so wähle man ein für allemal einen in $\mathfrak{B}$ aufgehenden Punkt $\mathfrak{P}_1$ und setze $\mathfrak{B} = \mathfrak{M}\mathfrak{P}_1$ (gleichgültig ob $\mathfrak{M}$ durch $\mathfrak{P}_1$ teilbar ist oder nicht). Man wähle sodann in der eigentlichen Klasse PP_1W ein durch $\mathfrak{P}$ und $\mathfrak{P}_1$ nicht teilbares Polygon $\mathfrak{N}$, so gehört $\mathfrak{A}' = \mathfrak{M}\mathfrak{N}$ wieder in die Klasse PBW, und da $\mathfrak{A}'$ nicht durch $\mathfrak{P}$ teilbar ist, so folgt wie oben, daß die Polygone (2) eine Basis von BPW bilden. Zugleich ist

$$d\widetilde{\omega}' = \frac{\mathfrak{A}'}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{N}}{\mathfrak{P}\mathfrak{P}_1},$$

also von der verlangten Form.

Es bleibt noch übrig, den Anfang dieser Operation zu beschreiben. Ist $b = 0$, also $\mathfrak{B} = \mathfrak{O}$, so ist

$$BW = W = (\mathfrak{W}_1, \mathfrak{W}_2, \ldots \mathfrak{W}_p)$$

(die Hauptklasse erster Gattung).

Ist $b = 2$, so wähle man aus der eigentlichen Klasse BW ein Polygon $\mathfrak{R}$, welches relativ prim zu $\mathfrak{B}$ ist; dann ist

$$BW = (\mathfrak{B}\mathfrak{W}_1, \mathfrak{B}\mathfrak{W}_2, \ldots \mathfrak{B}\mathfrak{W}_p, \mathfrak{R}).$$

Geht man von dieser Basis aus, um in der oben beschriebenen Weise eine Basis (1) zu bestimmen, die dem beliebig gegebenen Polygon

$$\mathfrak{B} = \mathfrak{P}_1^{m_1} \mathfrak{P}_2^{m_2} \mathfrak{P}_3^{m_3} \ldots$$

entspricht, und bestimmt die beiden Polygone $\mathfrak{A}'_r$, $\mathfrak{B}'_r$ aus der Bedingung

$$d\tilde{\omega}_r = \frac{\mathfrak{A}_r}{\mathfrak{B}} = \frac{\mathfrak{A}'_r}{\mathfrak{B}'_r},$$

so daß sie keinen gemeinschaftlichen Teiler haben, so sind die Polygone $\mathfrak{B}'_r$, die als Unterecke der Differentiale $d\tilde{\omega}_r$ auftreten, folgende:

a) p-mal tritt der Nenner $\mathfrak{O}$ auf, und die zugehörigen Differentiale $d\tilde{\omega}_r$ sind die Differentiale erster Gattung.

b) Je einmal treten die Unterecke $\mathfrak{P}_1^2, \mathfrak{P}_1^3, \ldots \mathfrak{P}_1^{m_1}$ (wenn $m_1 \geqq 2$), $\mathfrak{P}_2^2, \mathfrak{P}_2^3, \ldots \mathfrak{P}_2^{m_2}$; $\mathfrak{P}_3^2, \mathfrak{P}_3^3, \ldots \mathfrak{P}_3^{m_3}, \ldots$ auf.

Die zu den Unterecken $\mathfrak{P}^r$ gehörigen Differentiale $d\omega_r$ werden, wenn eine genauere Unterscheidung nötig ist, mit $dt_{(\mathfrak{P}^{r-1})}$ bezeichnet und heißen Differentiale zweiter Gattung.

c) Endlich treten die Produkte $\mathfrak{P}_1\mathfrak{P}_2, \mathfrak{P}_1\mathfrak{P}_3, \ldots$ (bei festgehaltenem $\mathfrak{P}_1$) je einmal auf. Die zugehörigen Differentiale $d\tilde{\omega}_r$ werden mit $d\pi_{(\mathfrak{P}_1,\, \mathfrak{P}_r)}$ bezeichnet und heißen Differentiale dritter Gattung.

Jedes Differential $d\tilde{\omega}$, dessen Untereck $\mathfrak{B}$ ist, kann in der Form dargestellt werden

$$(3) \qquad d\tilde{\omega} = \sum^{r} c_r \, d\tilde{\omega}_r$$

mit konstanten Koeffizienten c_r, welche die Normalform des Differentials $d\tilde{\omega}$ genannt wird. Hat man jedes der einzelnen Differentiale $d\tilde{\omega}_r$ auf eine bestimmte Art gewählt, so läßt sich die Normalform auch nur auf eine einzige Weise herstellen, was unmittelbar aus der linearen Unabhängigkeit der Differentiale $d\tilde{\omega}_r$ folgt.

§ 32.

Die Residuen.

1. Ist $d\tilde{\omega}$ ein beliebiges Differential in Ω und $\mathfrak{P}$ ein Punkt, der m-mal im Untereck $\mathfrak{B}$ desselben vorkommt ($m \overline{\gtrless} 0$), so wähle man eine Variable z so, daß sie in $\mathfrak{P}$ ∞^1 wird. Es läßt sich dann (nach § 15, 4.), und zwar nur auf eine Weise, setzen

$$(1) \qquad \frac{d\tilde{\omega}}{dz} = a_{m-2} z^{m-2} + a_{m-3} z^{m-3} + \cdots + a_1 z + a_0 + a_{-1} z^{-1} + \eta z^{-2},$$

worin die a Konstanten, η eine Funktion in Ω, die in $\mathfrak{P}$ endlich ist. Der Koeffizient $-a_{-1}$ von $-z^{-1}$ in diesem Ausdruck heißt das Residuum des Differentials $d\tilde{\omega}$ in bezug auf den Punkt $\mathfrak{P}$. Aus dieser Definition ergeben sich die folgenden Sätze:

2. Das Residuum in bezug auf einen Punkt $\mathfrak{P}$ kann nur dann von Null verschieden sein, wenn $m > 0$, d. h. wenn der Punkt $\mathfrak{P}$ im Untereck von $d\tilde{\omega}$ wirklich vorkommt, und ist daher für die Differentiale erster Gattung immer gleich 0.

3. Das Residuum einer Summe von Differentialen ist gleich der Summe der Residuen der einzelnen Differentiale.

4. Das Residuum eines eigentlichen Differentials ist stets gleich 0. Ist nämlich σ eine Funktion in Ω, und wenn die b Konstanten, σ' eine in $\mathfrak{P}$ endliche Funktion bedeuten,

$$\sigma = b_m z^m + b_{m-1} z^{m-1} + \cdots + b_1 z + \sigma',$$

so ergibt sich durch Differentiation dieses Ausdruckes nach z, da $\frac{d\sigma'}{dz}$ in $\mathfrak{P}$ unendlich klein von mindestens zweiter Ordnung ist (§ 23, 10.), daß in dem Ausdruck für $\frac{d\sigma}{dz}$ ein Glied mit z^{-1} gar nicht vorkommt, womit die Behauptung erwiesen ist.

5. Das Residuum eines Differentials $d\tilde{\omega}$ ist unabhängig von der Wahl der Veränderlichen z. Ist nämlich z_1 eine zweite Veränderliche von derselben Beschaffenheit wie z, also, wenn a konstant, ζ in $\mathfrak{P}$ endlich ist:

$$(2) \qquad z = a z_1 + \zeta,$$

so ergibt sich, wenn zur Abkürzung

$$\alpha = \frac{a_{m-2} z^{m-1}}{m-1} + \frac{a_{m-3} z^{m-2}}{m-2} + \cdots + a_0 z$$

gesetzt wird:

$$\frac{d\tilde{\omega}}{dz_1} = \frac{d\tilde{\omega}}{dz}\frac{dz}{dz_1} = \frac{d\alpha}{dz_1} + a_{-1}z^{-1}\frac{dz}{dz_1} - \eta\,\frac{dz^{-1}}{dz_1}.$$

Nun ist, wenn ζ', ζ'' in $\mathfrak{P}$ endliche Funktionen sind, wie sich nach § 23 und § 15, 4. leicht ergibt:

$$z^{-1}\frac{dz}{dz_1} = z_1^{-1} + z_1^{-2}\zeta', \qquad \frac{dz^{-1}}{dz_1} = z_1^{-2}\zeta'',$$

und daraus folgt nach 3., 4. die Richtigkeit der aufgestellten Behauptung*).

6. Die Summe der Residuen eines jeden Differentials $d\tilde{\omega}$ in bezug auf alle Punkte $\mathfrak{P}$ ist stets gleich Null.

Beim Beweise dieses wichtigen Satzes können wir uns auf die Betrachtung der Residuen beschränken, welche zu den sämtlichen im Untereck $\mathfrak{B}$ von $d\tilde{\omega}$ aufgehenden voneinander verschiedenen Punkten gehören; wir fügen jedoch zu diesen noch so viele voneinander verschiedene willkürliche Punkte mit verschwindenden Residuen hinzu, bis wir ein aus lauter einfachen Punkten bestehendes einer eigentlichen Klasse angehöriges Polygon $\mathfrak{P}_1\mathfrak{P}_2\ldots\mathfrak{P}_n$ erhalten. Dann wählen wir eine Variable z von der Ordnung n, deren Untereck eben dies Polygon ist, welche also in jedem der Punkte $\mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}_n$ und nur in diesen ∞^1 wird. Unter diesen finden sich dann sämtliche voneinander verschiedene in $\mathfrak{B}$ aufgehende Punkte. Es ergibt sich unter dieser Voraussetzung für $\iota = 1, 2, \ldots n$

$$(3)\quad \frac{d\tilde{\omega}}{dz} = a^{(\iota)}_{m-2}z^{m-2} + a^{(\iota)}_{m-3}z^{m-3} + \cdots + a^{(\iota)}_0 + a^{(\iota)}_{-1}z^{-1} + \eta^{(\iota)}z^{-2},$$

wo $\eta^{(\iota)}$ eine in $\mathfrak{P}_\iota$ endliche Funktion bedeutet. Lassen wir für die Konstanten $a^{(\iota)}$ auch den Wert 0 zu, so kann der Exponent m unabhängig von ι angenommen werden (m ist dann, wenn nicht alle $a^{(\iota)}_{m-2}$ verschwinden, der Exponent der höchsten Potenz eines einzelnen Punktes, welche in $\mathfrak{B}$ vorkommt). Der zu beweisende Satz besteht dann darin, daß $\sum\limits^{\iota} a^{(\iota)}_{-1} = 0$ ist. Um ihn zu beweisen, bilden wir die Spur der Funktion $\dfrac{d\tilde{\omega}}{dz}$ für die Variable z (§ 2) und bedienen

---

*) Man kann bei der Definition des Residuums auch eine Veränderliche r zugrunde legen, die in $\mathfrak{P}$ unendlich klein in der ersten Ordnung ist. Ist dann

$$\frac{d\tilde{\omega}}{dr} = a_m r^{-m} + \cdots + a_1 r^{-1} + \eta$$

und η in $\mathfrak{P}$ endlich, so ist a_1 das Residuum von $d\tilde{\omega}$ in bezug auf $\mathfrak{P}$.

uns dabei einer Erweiterung des Verfahrens § 16, 4. Wir wählen ein Funktionensystem $\varrho_1, \varrho_2, \ldots \varrho_n$ in Ω folgendermaßen: Es sei

$\varrho_1 = 0^m$ in $\mathfrak{P}_2, \mathfrak{P}_3, \ldots \mathfrak{P}_n$, endlich und von Null verschieden in $\mathfrak{P}_1$,
$\varrho_2 = 0^m$ in $\mathfrak{P}_1, \mathfrak{P}_3, \ldots \mathfrak{P}_n$, „ „ „ „ „ „ $\mathfrak{P}_2$,
. . . .
$\varrho = 0^m$ in $\mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}_{n-1}$, „ „ „ „ „ „ $\mathfrak{P}_n$.

Sind nun $x_1, x_2, \ldots x_n$ rationale Funktionen von z, und ist

$$\eta = x_1 \varrho_1 + x_2 \varrho_2 + \cdots + x_n \varrho_n$$

eine Funktion in Ω, welche für $z = \infty$, d. h. in $\mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}_n$ endlich ist, so müssen $x_1, x_2, \ldots x_n$ für $z = \infty$ endlich sein. Sind nämlich die $x_1, x_2, \ldots x_n$ für $z = \infty$ nicht alle endlich, so existiert ein positiver Exponent r von der Beschaffenheit, daß die Produkte $x_1 z^{-r}, x_2 z^{-r}, \ldots x_n z^{-r}$ für $z = \infty$ alle endlich sind, und mindestens eines von ihnen, etwa $x_1 z^{-r}$ von Null verschieden; dann enthält aber die Gleichung

$$\eta z^{-r} = x_1 z^{-r} \varrho_1 + \cdots + x_n z^{-r} \varrho_n$$

den Widerspruch, daß im Punkte $\mathfrak{P}_1$ die linke Seite und alle Glieder der rechten Seite mit Ausnahme des ersten verschwinden.

Hieraus ergibt sich zugleich, wenn man $\eta = 0$ setzt, daß die Funktionen $\varrho_1, \varrho_2, \ldots \varrho_n$ eine Basis von Ω bilden. Setzt man daher, indem man mit $x_{\iota, \iota'}$ rationale Funktionen von z bezeichnet,

$$(4) \qquad \frac{d\widetilde{\omega}}{dz} \varrho_\iota = x_{\iota,1} \varrho_1 + x_{\iota,2} \varrho_2 + \cdots + x_{\iota,n} \varrho_n, \qquad (\iota = 1, 2, \ldots n)$$

so ist (§ 2)

$$(5) \qquad S\left(\frac{d\widetilde{\omega}}{dz}\right) = x_{1,1} + x_{2,2} + \cdots + x_{n,n}.$$

Nun ist, wie aus (3) hervorgeht, $z^{-m+2} \dfrac{d\widetilde{\omega}}{dz} \varrho_\iota$ für $z = \infty$ endlich und daraus ergibt sich nach der soeben bewiesenen Eigenschaft der Funktionen ϱ, daß auch

$$z^{-m+2} x_{\iota, \iota'}$$

für $z = \infty$ endlich sind. Nun sind z. B. in dem Punkte $\mathfrak{P}_2$ die Funktionen $\varrho_1, \varrho_3, \ldots \varrho_n$ unendlich klein in der m^{ten} Ordnung, während ϱ_2 dort endlich und von Null verschieden ist. Daher werden in $\mathfrak{P}_2$ die Funktionen

$$z \frac{d\widetilde{\omega}}{dz} \varrho_1, \quad z x_{1,1} \varrho_1, \quad z x_{1,3} \varrho_3, \ \ldots \ z x_{1,n} \varrho_n$$

alle verschwinden, und es muß mithin auch $z x_{1,2}$ für $z = \infty$ verschwinden. Das gleiche folgt für $z x_{1,3}, \ldots z x_{1,n}$ und allgemein für $z x_{\iota,\iota'}$, sobald ι, ι' voneinander verschieden sind. Daher wird $z^2 x_{\iota,\iota'}$ für $z = \infty$ endlich sein.

Setzt man nun, indem man x_ι eine neue rationale Funktion bedeuten läßt,

$$(6) \qquad x_{\iota,\iota} = a_{m-2}^{(\iota)} z^{m-2} + a_{m-3}^{(\iota)} z^{m-3} + \cdots + a_{-1}^{(\iota)} z^{-1} + x_\iota z^{-2},$$

so folgt aus (3)

$$x_{\iota,\iota} - \frac{d\tilde{\omega}}{dz} = z^{-2}(x_\iota - \eta^{(\iota)}),$$

und aus (4)

$$(\eta^{(\iota)} - x_\iota)\varrho_\iota = z^2 x_{\iota,1}\varrho_1 + \cdots + z^2 x_{\iota,\iota-1}\varrho_{\iota-1} + z^2 x_{\iota,\iota+1}\varrho_{\iota+1} + \cdots + z^2 x_{\iota,n}\varrho_n.$$

Da nun in $\mathfrak{P}_\iota$ $\eta^{(\iota)}$ endlich und ϱ_ι von Null verschieden, ferner alle Glieder der rechten Seite Null sind, so folgt, daß auch x_ι im Punkte $\mathfrak{P}_\iota$, und mithin, da es rational ist, für $z = \infty$ endlich ist. Aus (5) und (6) ergibt sich dann

$$(7) \; S\left(\frac{d\tilde{\omega}}{dz}\right) = \sum^{\iota} a_{m-2}^{(\iota)} z^{m-2} + \sum^{\iota} a_{m-3}^{(\iota)} z^{m-3} + \cdots + \sum^{\iota} a_{-1}^{(\iota)} z^{-1} + \sum^{\iota} x_\iota z^{-2}.$$

Nun ist aber andererseits, wenn wieder $\mathfrak{U}$ das Untereck, $\mathfrak{Z}$ das Verzweigungspolygon von z ist:

$$\frac{d\tilde{\omega}}{dz} = \frac{\mathfrak{U}^2 \mathfrak{A}}{\mathfrak{Z}\mathfrak{B}},$$

und $\mathfrak{B}$ enthält keinen Punkt, der nicht auch in $\mathfrak{U}$ enthalten ist. Daraus ergibt sich wie in § 26, daß $\frac{d\tilde{\omega}}{dz}$, als Funktion von z aufgefaßt, eine Funktion des zu $\mathfrak{o}$ komplementären Moduls $\mathfrak{e}$ ist, und mithin ist

$$S\left(\frac{d\tilde{\omega}}{dz}\right)$$

eine g a n z e rationale Funktion von z (§ 11, 4.). Beachtet man dies, so folgt aus (7) $\sum^{\iota} x_\iota = 0$ und ferner der zu beweisende Satz

$$\sum^{(\iota)} a_{-1}^{(\iota)} = 0.$$

Wir können diesem Satze auch den folgenden Ausdruck geben: Das Residuum eines Differentials zweiter Gattung $dt_{(\mathfrak{P}^r)}$ in bezug auf den Punkt $\mathfrak{P}$ ist Null.

Die Residuen eines Integrals dritter Gattung $d\pi_{(\mathfrak{P}_1, \mathfrak{P}_2)}$ in bezug auf $\mathfrak{P}_1$, $\mathfrak{P}_2$ sind einander gleich und entgegengesetzt, und sicher von

Null verschieden, da sonst $d\pi$ ein Differential erster Gattung sein würde.

Aus diesen Bemerkungen ergibt sich noch mittelst 4., daß ein eigentliches Differential $d\sigma$, in der Normalform dargestellt, kein Differential dritter Gattung enthalten kann. Es verdient ferner erwähnt zu werden, daß die Residuen des logarithmischen Differentials $\frac{d\sigma}{\sigma}$ ganze Zahlen, nämlich die Ordnungszahlen der Funktion σ sind (zufolge § 23).

§ 33.

Relationen zwischen Differentialen erster und zweiter Gattung.

1. Es sei σ eine Funktion in Ω mit dem Untereck

$$\mathfrak{B}' = \mathfrak{P}_1^{m_1-1}\mathfrak{P}_2^{m_2-1}\ldots \qquad (m_1, m_2, \ldots \geqq 2)$$

und dem Verzweigungspolygon (§ 16)

$$\mathfrak{S} = \mathfrak{S}'\mathfrak{P}_1^{m_1-2}\mathfrak{P}_2^{m_2-2}\ldots,$$

worin $\mathfrak{S}'$ durch die als verschieden vorausgesetzten Punkte $\mathfrak{P}_1, \mathfrak{P}_2 \ldots$ nicht teilbar ist. Demnach ist in der symbolischen Bezeichnung von § 25 das eigentliche Differential

$$d\sigma = \frac{\mathfrak{S}}{\mathfrak{B}'^2} = \frac{\mathfrak{S}'}{\mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\ldots},$$

woraus zunächst hervorgeht, daß ein eigentliches Differential niemals von der ersten Gattung sein kann.

2. Das eigentliche Differential $d\sigma$, welches in seiner Darstellung durch die Normalform nur Differentiale erster und zweiter Gattung enthalten kann, gehört zu der Schar derjenigen Differentiale, deren Untereck

$$\mathfrak{B} = \mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\ldots = \mathfrak{B}'\mathfrak{P}_1\mathfrak{P}_2\ldots$$

ist. Umgekehrt wird man also auch in einer solchen Schar, vorausgesetzt daß $m_1, m_2, \ldots \geqq 2$ sind, und daß $\mathfrak{B}'$ zu einer eigentlichen Polygonklasse gehört, stets mindestens ein eigentliches Differential $d\sigma$ finden. Denn dazu ist nach 1. nur erforderlich, daß in Ω eine Funktion σ mit dem Untereck $\mathfrak{B}'$ existiert.

3. Hieraus ergibt sich nun der folgende wichtige Satz. Alle Differentiale zweiter Gattung lassen sich linear mit konstanten Koeffizienten darstellen durch p besondere passend gewählte Differentiale zweiter Gattung, durch Differentiale erster Gattung und durch eigentliche Differentiale.

Um dies einzusehen, wähle man ein beliebiges Polygon zweiter Gattung $\mathfrak{A}$ von der Ordnung p. Ist nun $\mathfrak{P}$ ein beliebiger Punkt, r ein positiver Exponent, so ist das Polygon $\mathfrak{A}\mathfrak{P}^r$ gleichfalls von der zweiten Gattung, und folglich kann der Teiler $\mathfrak{M}$ der zugehörigen Klasse nicht durch $\mathfrak{P}$ teilbar sein, weil sonst $\mathfrak{A}\mathfrak{P}^{r-1}$, also auch $\mathfrak{A}$ ein Polygon erster Gattung wäre (§ 30, 4.). Setzt man daher

$$\mathfrak{A}\mathfrak{P}^r = \mathfrak{M}\mathfrak{B}',$$

so wird $\mathfrak{P}$ nicht in $\mathfrak{M}$ aufgehen, und folglich enthält $\mathfrak{B}'$ den Faktor $\mathfrak{P}$ genau r-mal öfter als $\mathfrak{A}$. Zugleich gehört $\mathfrak{B}'$ in eine eigentliche Klasse. Ist nun

$$\mathfrak{B}' = \mathfrak{P}^{m+r}\mathfrak{P}'^{m'}\mathfrak{P}''^{m''}\ldots,$$

so gehen die Punktpotenzen $\mathfrak{P}^m$, $\mathfrak{P}'^{m'}$, $\mathfrak{P}''^{m''}$, ... alle in $\mathfrak{A}$ auf. Setzen wir also

$$\mathfrak{B} = \mathfrak{P}^{m+r+1}\mathfrak{P}'^{m'+1}\mathfrak{P}''^{m''+1}\ldots = \mathfrak{B}'\mathfrak{P}\mathfrak{P}'\mathfrak{P}''\ldots,$$

so existiert nach 2. in der zu dem Untereck $\mathfrak{B}$ gehörigen Differentialschar gewiß ein eigentliches Differential $d\sigma$. Die Darstellung desselben durch die Normalform enthält sicher das Differential

$$dt_{(\mathfrak{P}^{m+r})} \tag{1}$$

und außerdem alle oder einige der Differentiale

$$\left\{\begin{array}{l} dt_{(\mathfrak{P})},\ dt_{(\mathfrak{P}^2)},\ \ldots\ dt_{(\mathfrak{P}^m)}\ \ldots\ dt_{(\mathfrak{P}^{m+r-1})}, \\ dt_{(\mathfrak{P}')},\ dt_{(\mathfrak{P}'^2)},\ \ldots\ dt_{(\mathfrak{P}'^{m'})}, \\ dt_{(\mathfrak{P}'')},\ dt_{(\mathfrak{P}''^2)},\ \ldots\ dt_{(\mathfrak{P}''^{m''})} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right. \tag{2}$$

nebst Differentialen erster Gattung. Es läßt sich also das Differential (1) linear und mit konstanten Koeffizienten durch (2), durch Differentiale erster Gattung und durch $d\sigma$ ausdrücken.

Ist daher das p-Eck zweiter Gattung

$$\mathfrak{A} = \mathfrak{P}_1^{m_1}\mathfrak{P}_2^{m_2}\ldots,$$

so erkennt man durch wiederholte Anwendung des hier beschriebenen Verfahrens, daß alle Differentiale zweiter Gattung in der Weise, wie unser Satz es ausspricht, darstellbar sind durch die p Differentiale

$$\left\{\begin{array}{l} dt_{(\mathfrak{P}_1)}\ldots dt_{(\mathfrak{P}_1^{m_1})}, \\ dt_{(\mathfrak{P}_2)}\ldots dt_{(\mathfrak{P}_2^{m_2})}, \\ \ldots\ldots\ldots \end{array}\right. \tag{3}$$

Braunschweig und Königsberg i. Pr., im Oktober 1880.

Erläuterungen zur vorstehenden Abhandlung.

In der vorstehenden Abhandlung, mit der die arithmetische Theorie der algebraischen Funktionen geschaffen wurde, zerfällt der Aufbau der Theorie in drei Stufen. Der erste, formale Teil bezieht sich auf den Bereich der ganzen und gebrochenen algebraischen Funktionen einer Unbestimmten; im zweiten Teil bildet die arithmetisch definierte, absolute Riemannsche Fläche die Grundlage. Der dritte Teil — der nur am Schluß des Vorworts erwähnt, aber nicht erschienen ist — sollte von der arithmetischen zur topologischen absoluten Riemannschen Fläche übergehen: ein Begriff, der auf anderer Grundlage erst mehr als dreißig Jahre später in der Weylschen „Idee der Riemannschen Fläche" entwickelt wurde. Es verdient daher besonders hervorgehoben zu werden, daß (§ 16) scharf darauf hingewiesen ist, daß die absolute Riemannsche Fläche ein zu dem Körper gehöriger invarianter Begriff ist, von dem aus sich der Übergang zur Riemannschen Auffassung vollziehen läßt.

Der erste Teil läßt sich dadurch charakterisieren, daß der algebraische Funktionenkörper als hyperkomplexes System über dem Grundkörper der rationalen Funktionen einer Unbestimmten betrachtet wird. Tatsächlich sind die Methoden zur Definition von Norm, Spur, Diskriminante usw. diejenigen der Darstellungstheorie hyperkomplexer Systeme; die Betrachtungen aus § 6 und § 22 etwa sind solche über reduzible Darstellungen.

Die um die absolute Riemannsche Fläche sich gruppierenden Entwicklungen des zweiten Teils — insbesondere die Begriffe des „Punktes" und des „Divisors" (Polygons) — sind allgemeiner bekannt geworden durch das Buch von Hensel-Landsberg, wo aber die idealtheoretischen Grundlagen des ersten Teils durch funktionentheoretische ersetzt sind. Hensel-Landsberg führen die Gruppe aller ganzen und gebrochenen Divisoren ein, was Vereinfachungen beim Beweis des Riemann-Rochschen Satzes nach sich zieht. Der einfachste Beweis ergibt sich aber erst, wenn man die bei Dedekind-Weber, § 22, gegebene Konstruktion der Normalbasis auf gebrochene Ideale überträgt, und dann nach Hensel-Landsberg weiter schließt.

Die wesentlichsten Entwicklungen von Hensel-Landsberg wurden von Jung (Rend. Palermo 26, und spätere Arbeiten) auf algebraische Funktionenkörper von zwei Veränderlichen übertragen. Eine rein arithmetische Begründung der Divisoren, die erst nach Weiterentwicklung der Idealtheorie möglich war, wurde von Schmeidler (Math. Zeitschr. 28) und v. d. Waerden (Math. Ann. 101) für n Veränderliche gegeben. Es handelt sich dort immer um Divisoren der Höchstdimension; arithmetische Definition und Existenzbeweis für den allgemeinen invarianten Punktbegriff bei algebraischen Mannigfaltigkeiten findet sich bei v. d. Waerden (Math. Ann. 97).

Noether.