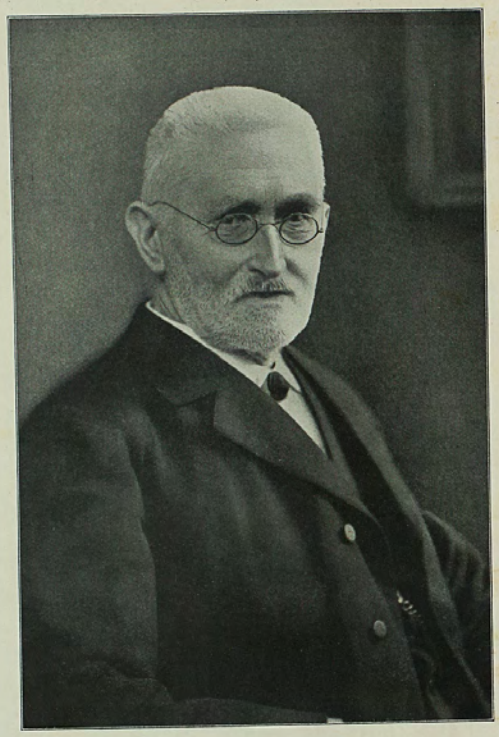

R. Dedekind.

Richard Dedekind

Gesammelte mathematische Werke

Herausgegeben von

Robert Fricke
in Braunschweig

Emmy Noether
in Göttingen

Öystein Ore
in New Haven

Erster Band

Mit einem Bildnis Dedekinds

Druck und Verlag von Friedr. Vieweg & Sohn Akt.-Ges.
Braunschweig 1930

Inhaltsverzeichnis.

I.

Über die Elemente der Theorie der Eulerschen Integrale.

[Inauguraldissertation, Göttingen 1852.]

Es ist bekannt, daß die Ausführung der indirekten Operationen in der Analysis meist auf viel bedeutendere Schwierigkeiten stößt, als die der direkten; aber gerade dieser scheinbar unglückliche Umstand hat auf die Entwicklung der Mathematik stets den günstigsten Einfluß ausgeübt. Nicht nur, daß die Besiegung dieser Schwierigkeiten, wenn sie möglich, immer einen eigentümlichen Reiz für den Mathematiker darbietet, sondern auch gerade die Fälle, in welchen dies mit den früher eingeführten Begriffen und Hilfsmitteln nicht möglich war, haben immer der weiteren Ausbildung der Mathematik ganz neue Felder eröffnet; so führen z. B. die Operationen der Subtraktion, Division und Wurzelausziehung auf die Begriffe der negativen, gebrochenen und imaginären Zahlen, von denen jeder das Gebiet der Mathematik so außerordentlich erweitert hat. Ganz ähnlich verhält es sich nun auch in der höheren Analysis mit dem ihr zugrunde liegenden Begriff der Funktion, welcher sich anfangs nur auf die in der Elementarmathematik gelehrten Operationen (die ihnen entsprechenden Funktionen könnte man füglich Elementarfunktionen nennen) und auf deren Zusammensetzung stützt. Die Differentialrechnung, der mächtigste Hebel zur Entwicklung der Theorie der Funktionen, findet in ihrer Ausführung keine Schwierigkeiten, d. h. das Differentiieren der aus den Operationen der Elementarmathematik gebildeten Funktionen führt wieder auf eben solche Funktionen. Dagegen ist es der umgekehrten Rechnungsart, welche in ihrer Gesamtheit die Integralrechnung bildet, nur in verhältnismäßig wenigen Fällen gelungen, dasselbe zu leisten; in den meisten ist es bisher nicht geglückt, oder vielleicht auch ganz unmöglich, die Integrale

gegebener Funktionen mit Hilfe eben solcher darzustellen. Aber gerade dieser Umstand hat zu einer beträchtlichen Erweiterung des Begriffs der Funktion geführt, indem man solchen nicht darstellbaren Integralen neue Namen und Bezeichnungen beigelegt, und sie dadurch in den Kreis der früheren Funktionen eingeführt hat. Bei der Entwicklung der Theorie solcher Integralfunktionen sind nun namentlich die Fälle von der größten Wichtigkeit, in denen sie sich auf die bisher allein gebräuchlichen Funktionen zurückführen lassen, indem dadurch ihr Verlauf deutlicher hervortritt, und auch oft Mittel an die Hand gegeben werden, ihre Berechnung zu erleichtern. Die Zusammenstellung dieser Fälle für die Eulerschen Integrale, mit besonderer Rücksicht auf die dabei anzuwendende Methode, ist der Hauptzweck der folgenden Abhandlung.

1.

Es ist zuerst erforderlich, die Fundamentaleigenschaften der Eulerschen Integrale kurz in Erinnerung zu bringen. Die Definitionen dieser Funktionen liegen in den Gleichungen

$$(1) \qquad B(a,b) = \int_0^1 x^{a-1}(1-x)^{b-1}\,dx; \quad \Gamma(\mu) = \int_0^\infty x^{\mu-1}e^{-x}\,dx.$$

Die Integrale rechts heißen Eulersche Integrale der ersten und der zweiten Art; die ersteren lassen sich leicht auf die letzteren zurückführen. Führt man nämlich in dem Doppelintegral

$$\int_0^\infty\int_0^\infty e^{-(x+y)}x^{a-1}y^{b-1}\,dy\,dx = \Gamma(a)\Gamma(b)$$

für x und y zwei neue Variabeln r und w ein, indem man $x+y=r$ und $x=rw$ setzt, woraus $dy\,dx = r\,dr\,dw$ folgt, so erhält man

$$\int_0^\infty e^{-r}r^{a+b-1}\,dr\int_0^1 w^{a-1}(1-w)^{b-1}\,dw = \Gamma(a)\Gamma(b)$$

und daraus zufolge der Definitionen von B und Γ

$$(2) \qquad B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)},$$

woraus sich zugleich ergibt, daß $B(b,a) = B(a,b)$ eine symmetrische Funktion von a und b ist, was man auch direkt zeigen kann, wenn man in dem Integral B $(1-x)$ statt x setzt.

Setzt man in dem Integral Γrx statt x, und nimmt r als eine positive Konstante an, so erhält man

$$(3) \qquad \int_0^\infty x^{\mu-1}e^{-rx}\,dx = \frac{\Gamma(\mu)}{r^\mu}$$

und hieraus durch $n$malige partielle Differentiation in bezug auf r die wichtige Relation

$$(4) \qquad \Gamma(\mu+n) = (\mu+n-1)(\mu+n-2)\dots(\mu+1)\mu\Gamma(\mu).$$

Es leuchtet ein, daß man $\Gamma(\mu)$ nur für jedes μ innerhalb eines Intervalls zu berechnen braucht, welches eine Einheit umfaßt, um daraus mit Hilfe dieser Gleichung $\Gamma(\mu)$ für jedes andere μ zu finden.

2.

Aus den eben entwickelten Formeln lassen sich wichtige Folgerungen für die Theorie der Eulerschen Integrale ziehen, namentlich in bezug auf die Fälle, in denen sie sich ohne Hilfe neuer Funktionen darstellen lassen. Da die der ersten Art auf die der zweiten zurückgeführt werden können, so beginnen wir mit der Untersuchung der letzteren. Nun ist bekannt, daß sich bestimmte Integrale jedesmal ermitteln lassen, wenn man die unbestimmten Integrale allgemein darstellen kann (vgl. Art. 6); die Integralrechnung lehrt aber, daß dies bei dem Integral

$$\int x^{\mu-1}e^{-x}\,dx$$

nur dann möglich ist, wenn μ eine positive ganze Zahl n ist; wir können also im voraus schließen, daß dann auch $\Gamma(n)$ sich wird angeben lassen. Nun haben wir aber in der Gleichung (4) eine Reduktionsformel gewonnen, welche uns lehrt, wie eine Gammafunktion durch eine andere dargestellt werden kann, wenn ihre Argumente um eine ganze Zahl differieren; nehmen wir also am einfachsten $\mu = 1$, so erhalten wir aus der unbestimmten Integration

$$(5) \quad \Gamma(1) = \int_0^\infty e^{-x}\,dx = 1 \text{ und folglich } \Gamma(n) = (n-1)(n-2)\dots 2.1.$$

Dies ist aber auch der einzige Fall, in welchem a priori einleuchtet, daß $\Gamma(\mu)$ sich darstellen läßt.

Einen ähnlichen Weg können wir auch bei den Eulerschen Integralen der ersten Art einschlagen, indem wir zunächst die Darstellbarkeit des unbestimmten Integrals

$$\int x^{a-1}(1-x)^{b-1}\,\mathrm{d}x$$

untersuchen; dieses gehört bekanntlich zu der Klasse der Integrale von sogenannten binomischen Differentialen, welche unter der allgemeinen Form

$$\int x^m(a+bx^n)^p\,\mathrm{d}x$$

stehen; es ist aber bekannt, daß das binomische Differential jedesmal rational und folglich auch integrabel gemacht werden kann, wenn entweder $\frac{m+1}{n}$ oder $\frac{m+1}{n}+p$ eine ganze Zahl ist, und m, n und p rational sind. Damit also das obige unbestimmte Integral darstellbar sei, muß entweder a [oder auch b, da ja $B(a,b)=B(b,a)$ ist] oder $a+b$ eine ganze Zahl sein. Der erste Fall folgt aber auch unmittelbar aus den Formeln (2) und (4); denn wenn a eine ganze Zahl m ist, so geben diese Formeln

$$B(m,b)=\frac{\Gamma(m)\Gamma(b)}{\Gamma(m+b)}=\frac{\Gamma(m)}{(m-1+b)(m-2+b)\dots(1+b)b}$$

und folglich mit Hilfe von der Formel (5)

$$(6)\qquad B(m,b)=\frac{(m-1)(m-2)\dots 2.1}{(m-1+b)(m-2+b)\dots(1+b)b}.$$

Ebenso erhält man, wenn n eine positive ganze Zahl bedeutet:

$$B(a,n)=\frac{(n-1)(n-2)\dots 2.1}{(n-1+a)(n-2+a)\dots(1+a)a},$$

$$B(m,n)=\frac{(m-1)\dots 2.1.(n-1)\dots 2.1}{(m+n-1)(m+n-2)\dots 2.1}.$$

Dagegen liefert der zweite Fall, in welchem $a+b$ eine ganze Zahl, ohne daß a und b gleichzeitig ganze Zahlen sind, unabhängig von den Eulerschen Integralen der zweiten Art, eine neue Klasse von Integralen, von denen man a priori behaupten kann, daß sie sich darstellen lassen; doch können sie alle folgendermaßen auf ein einziges zurückgeführt werden. Ist nämlich $a+b$ eine ganze positive Zahl (positive, weil als bekannt vorauszusetzen ist, daß die Eulerschen Integrale für negative Argumente stets unendlich groß ausfallen), so kann man immer $a=m+r$, $b=n-r$ setzen, worin m und n positive ganze Zahlen, und r ein positiver echter Bruch ist. Mit Benutzung der Reduktionsformel (4) findet man dann leicht

$$B(m+r,n-r)=\frac{\Gamma(m+r)\Gamma(n-r)}{\Gamma(m+n)}$$

$$=\frac{(m-1+r)(m-2+r)\dots r\Gamma(r).(n-1-r)(n-2-r)\dots(1-r)\Gamma(1-r)}{(m+n-1)(m+n-2)\dots 3.2.1}$$

oder, da aus den Gleichungen (2) und (5) $\Gamma(r)\Gamma(1-r)=B(r,1-r)$ folgt,

$$(7)\qquad B(m+r,n-r)=\frac{(m-1+r)\dots r.(n-1-r)\dots(1-r)}{(m+n-1)(m+n-2)\dots 2.1}B(r,1-r).$$

Das Integral $B(r,1-r)$, auf welches hierdurch die Integrale

$$B(m+r,\ n-r)$$

zurückgeführt werden, ist eines der interessantesten der Integralrechnung und namentlich von der größten Wichtigkeit für die Theorie der Eulerschen Integrale beider Arten, wie schon aus der letzten Gleichung hervorgeht. So einfach aber die Form ist, in welcher der Wert desselben dargestellt werden kann, so verschiedenartig untereinander und kompliziert sind die Methoden, welche diesen Wert kennen lehren. Mit diesem Integral sollen sich daher die folgenden Artikel beschäftigen.

3.

Der Gleichmäßigkeit in der Bezeichnung wegen will ich b statt r schreiben, und $B(b,1-b)=\Gamma(b)\Gamma(1-b)$ kurz mit B bezeichnen, so daß B als Funktion der einen Veränderlichen b aufgefaßt wird; zwischen b und B besteht also folgende Gleichung:

$$(8)\qquad \begin{cases} B=\int_0^1\left(\frac{x}{1-x}\right)^b\frac{\mathrm{d}x}{x}=\int_0^1\left(\frac{x}{1-x}\right)^{1-b}\frac{\mathrm{d}x}{x} \\ =\int_0^\infty\frac{x^{b-1}\,\mathrm{d}x}{x+1}=\int_0^\infty\frac{x^{-b}\,\mathrm{d}x}{x+1} \end{cases}$$

Die beiden letzten Formen erhält man, wenn man in den beiden ersten x für $\frac{x}{1-x}$ schreibt. Wenn nun schon im vorigen Artikel b auf das Intervall zwischen 0 und 1 beschränkt ist, weil sonst das Integral B als Eulersches Integral ein negatives Argument und da-

mit einen unendlich großen Wert erhielte, so soll in diesem Artikel die Notwendigkeit dieser Beschränkung unabhängig von der Theorie der Eulerschen Integrale in aller Strenge erwiesen werden. Größerer Allgemeinheit wegen will ich diese Untersuchung nicht unmittelbar an das Integral B, sondern an das allgemeinere

$$\int_0^\infty \frac{1+x+xx+\cdots+x^{m-1}}{1+x+xx+\cdots+x^{n-1}} x^{b-1}\,dx = \int_0^\infty \frac{1-x^m}{1-x^n} x^{b-1}\,dx$$

anknüpfen, welches für $m = 1$, $n = 2$ in das Integral B übergeht. Die Form rechts erfordert auch nicht einmal, daß m und n ganze Zahlen sind; ich will daher gleich zu der Betrachtung des Integrals

$$\varphi(b) = \int_0^\infty \frac{1-x^\mu}{1-x^\nu} x^{b-1}\,dx, \tag{9}$$

worin b, μ, ν beliebige reelle Konstanten bedeuten sollen, übergehen.

Zuerst wird man leicht einsehen, daß man μ und ν stets positiv annehmen darf, ohne die Allgemeinheit des Integrals zu beeinträchtigen, indem man statt $1-x^\mu$ und $1-x^\nu$ auch $x^\mu(x^{-\mu}-1)$ und $x^\nu(x^{-\nu}-1)$ schreiben kann. Zerlegt man dann $\varphi(b)$ in zwei Integrale von derselben Funktion, deren Grenzen bzw. 0, 1 und 1, ∞ sind, und setzt in dem zweiten Integral $\frac{1}{x}$ für x, so erhält auch dieses die Grenzen 0, 1, und beide lassen sich in

$$\varphi(b) = \int_0^1 \frac{1-x^\mu}{1-x^\nu}(x^b + x^{\nu-\mu-b})\frac{dx}{x} \tag{10}$$

zusammenziehen. Da nun nach der Voraussetzung μ und ν positiv sind, so ist innerhalb der Integrationsgrenzen für x, d. h. wenn x ein positiver echter Bruch ist, der Quotient $\frac{1-x^\mu}{1-x^\nu}$ fortwährend eine positive endliche Zahl; denn auch für $x = 1$ erhält dieser Quotient einen endlichen Wert, nämlich $\frac{\mu}{\nu}$. Bezeichnet man daher den größten und kleinsten Wert desselben mit M und N, so sind dies ebenfalls endliche positive Zahlen, und es ist im ganzen Integrationsintervall

$M > \frac{1-x^\mu}{1-x^\nu} > N$, und folglich auch, nach einem bekannten Satze aus der Theorie der bestimmten Integrale

$$M\int_0^1 (x^b + x^{\nu-\mu-b})\frac{dx}{x} > \varphi(b) > N\int_0^1 (x^b + x^{\nu-\mu-b})\frac{dx}{x}.$$

Da nun das Integral, welches zu beiden Seiten von $\varphi(b)$ mit den Faktoren M und N vorkommt, die Werte $\frac{\nu-\mu}{b(\nu-\mu-b)}$, $+\infty$, oder $-\infty$ erhält, je nachdem sowohl b als $\nu-\mu-b$ positiv, oder eins von beiden 0, oder negativ ist, so folgt, daß nur im ersten Falle $\varphi(b)$ einen endlichen, und zwar positiven, in jedem andern aber einen unendlich großen Wert erhält; es ist daher erforderlich, daß sowohl b als auch $\nu-\mu-b$ eine positive Zahl sei, was man durch die Bedingung $\nu-\mu > b > 0$ ausdrücken kann; hieraus geht zugleich hervor, daß $\nu > \mu$ sein muß. Wird $b = 0$ oder $b = \nu-\mu$, so wird $\varphi(b)$ nicht nur unendlich groß, sondern auch unstetig, indem $\varphi(b)$ von $+\infty$ in $-\infty$ überspringt.

Aus der Gleichung (10) läßt sich noch eine interessante Folgerung ziehen; setzt man nämlich $\nu-\mu-b$ statt b, so erhält man unmittelbar

$$\varphi(\nu-\mu-b) = \varphi(b), \tag{11}$$

und wenn man hierin $b = \frac{\nu-\mu}{2} + b'$ setzt, in bezug auf b' differentiiert und dann $b' = 0$ setzt, so folgt $\varphi'\left(\frac{\nu-\mu}{2}\right) = 0$, worin $\varphi'(b) = \frac{d\varphi(b)}{db}$ ist; um zu entscheiden, ob der Wert $b = \frac{\nu-\mu}{2}$ einem Maximum oder Minimum von $\varphi(b)$ entspricht, muß man das zweite Differentialverhältnis $\varphi''(b)$ bilden; da dieses durch das Integral

$$\int_0^\infty \frac{1-x^\mu}{1-x^\nu} x^{b-1}\,dx\,(lx)^2$$

dargestellt wird, worin lx den natürlichen Logarithmen von x bezeichnet, und folglich in dem ganzen Intervall von b positiv ist, so

wird $\varphi\left(\frac{\nu-\mu}{2}\right)$ ein Minimum von $\varphi(b)$ sein, und zwar das einzige. Dieses Minimum wird demnach

$$(12) \qquad \varphi\left(\frac{\nu}{2}-\frac{\mu}{2}\right)=\int_0^\infty \frac{x^{\frac{\mu}{2}}-x^{-\frac{\mu}{2}}}{x^{\frac{\nu}{2}}-x^{-\frac{\nu}{2}}}\frac{\mathrm{d}x}{x}=2\int_0^\infty \frac{x^\mu-x^{-\mu}}{x^\nu-x^{-\nu}}\frac{\mathrm{d}x}{x}.$$

Wenden wir das Bisherige auf unseren Fall an, in welchem $\mu=1$, $\nu=2$ zu setzen ist, so ergibt sich, daß das Integral B nur dann einen endlichen, und zwar positiven Wert besitzt, wenn b ein positiver echter Bruch ist; ferner das $B=\varphi(b)=\varphi(1-b)$ ist und für $b=\frac{1}{2}$ ein Minimum

$$(13) \qquad \varphi\left(\tfrac{1}{2}\right)=2\int_0^\infty \frac{x-\frac{1}{x}}{xx-\frac{1}{xx}}\frac{\mathrm{d}x}{x}=2\int_0^\infty \frac{\mathrm{d}x}{xx+1}=\pi$$

erreicht.

4.

Es sollen jetzt die hauptsächlichsten Beweise angegeben werden, welche bisher für den Wert des Integrals B aufgestellt sind; indessen wird es genügen, kurz den Gang derselben anzudeuten, und nur da, wo eine strengere Begründung nötig scheint, näher ins Detail zu gehen.

Da schon in Art. 2 gezeigt ist, daß sich der Wert des Integrals $B(m+r, n-r)$, von welchem B nur ein spezieller Fall ist, aus der unbestimmten Integration ergeben muß, wenn r ein echter rationaler Bruch ist, so ist es am natürlichsten, mit dieser Methode den Anfang zu machen. Nimmt man daher $b=\frac{m}{n}$ an, worin m und n positive ganze Zahlen sind, und $m<n$, so kommt es zunächst darauf an, in dem Integral

$$(14) \qquad B=\int_0^\infty \frac{x^{b-1}\mathrm{d}x}{x+1}=\int_0^\infty \frac{x^{\frac{m}{n}-1}\mathrm{d}x}{x+1}=n\int_0^\infty \frac{x^{m-1}\mathrm{d}x}{x^n+1}$$

die unbestimmte Integration auszuführen, welche bekanntlich die Zerlegung der unter dem Integralzeichen stehenden Funktion in Partialbrüche erfordert. Setzt man zur Abkürzung $\vartheta=e^{\frac{\pi}{n}i}$, worin $i=\sqrt{-1}$ ist, so ist

$$x^n+1=(x-\vartheta)(x-\vartheta^3)\dots(x-\vartheta^{2k-1})\dots(x-\vartheta^{2n-1});$$

führt man danach die Zerlegung in Partialbrüche mit linearen Nennern und die Integration jedes einzelnen Gliedes aus, so findet man

$$(15) \qquad n\int\frac{x^{m-1}\,\mathrm{d}x}{x^n+1}=-\sum_{k=1}^{k=n}\vartheta^{m(2k-1)}\,l(\vartheta^{2k-1}-x).$$

Die Summe rechts kann man auch so schreiben:

$$-\sum_{k=1}^{k=n}\vartheta^{m(2k-1)}\;l\left(\frac{\vartheta^{2k-1}}{x}-1\right)-lx\cdot\sum_{k=1}^{k=n}\vartheta^{m(2k-1)},$$

worin $\Sigma\vartheta^{m(2k-1)}=\vartheta^m\Sigma(\vartheta^{2m})^{k-1}=\vartheta^m\frac{\vartheta^{2mn}-1}{\vartheta^{2m}-1}=0$ ist, so daß auch

$$(16) \qquad n\int\frac{x^{m-1}\,\mathrm{d}x}{x^n+1}=-\sum_{k=1}^{k=n}\vartheta^{m(2k-1)}\;l\left(\frac{\vartheta^{2k-1}}{x}-1\right)$$

ist; hierbei ist wohl zu bemerken, daß die Summen in (15) und (16) vollkommen gleich, nicht etwa um eine Konstante verschieden sind. Setzt man daher in (16) $x=\infty$ und in (15) $x=0$, so gibt die Differenz das bestimmte Integral B, nämlich

$$(17) \qquad \begin{cases} B=\sum_{k=1}^{k=n}\vartheta^{m(2k-1)}\,l(\vartheta^{2k-1}) \\ =\frac{\pi i}{n}\sum_{k=1}^{k=n}(2k-1)\,\vartheta^{m(2k-1)}=\frac{\pi}{\sin b\pi}, \end{cases}$$

womit also der Wert von B für rationale b gefunden ist. Durch die Umformung von (15) in (16) glaube ich am kürzesten gezeigt zu haben, daß die Summe in (15) für $x=\infty$ verschwindet, und hinsichtlich seiner Strenge scheint dieser Weg denen wenigstens nicht nachzustehen, welche in den meisten Lehrbüchern der Integralrechnung befolgt sind.

5.

Ein zweiter Beweis ist der folgende, welcher, so viel mir bekannt ist, von Schlömilch gegeben ist. Aus der Gleichung

$$B = \int_0^1 \frac{x^{b-1} + x^{-b}}{x+1} \, \mathrm{d}x,$$

welche sich aus der Formel (10) in Art. 3 ergibt, wenn man $\mu = 1$, $\nu = 2$ setzt, erhält man durch Entwicklung von $\frac{1}{x+1}$ nach Potenzen von x mit Berücksichtigung des Restes und durch Ausführung der Integrationen für B die $n$gliedrige Reihe

$$(18) \quad \frac{1}{b} + \frac{2b}{1-bb} - \frac{2b}{4-bb} + \frac{2b}{9-bb} - \cdots + (-1)^n \frac{2b}{(n-1)^2 - bb}$$

nebst dem Reste

$$\frac{(-1)^{n-1}}{n-b} + (-1)^n \int_0^1 \frac{(x^{b-1} + x^{-b})\, x^n}{x+1} \, \mathrm{d}x.$$

Durch ähnliche Betrachtungen, wie die in Art. 3 über die Endlichkeit von $\varphi(b)$ angestellten, läßt sich zeigen, daß dieser Rest für unendlich wachsende n gleich Null wird, so daß B der unendlich fortgesetzten Reihe (18) gleich zu setzen ist. Nimmt man aber in der als bekannt vorausgesetzten Formel

$$\mathrm{cosec}\, u = \frac{1}{u} + \frac{2u}{\pi\pi - uu} - \frac{2u}{4\pi\pi - uu} + \text{usw.}$$

$u = b\pi$, so findet man unmittelbar für B denselben Wert, wie im vorigen Artikel.

6.

Ein dritter Beweis (von Cauchy) stützt sich auf einen Satz über die sogenannte Umkehrung der Integrationsordnung bei Doppelintegralen. Da die hierhergehörigen Betrachtungen sehr feiner Natur sind, und sich öfters noch Unklarheiten darüber finden, so möge es mir vergönnt sein, hier etwas weiter auszuholen, um ein sicheres Fundament für diese Untersuchung zu gewinnen. Dazu ist aber erforderlich, auf die Grundlagen der Theorie der bestimmten Integrale zurückzugehen.

Das bestimmte Integral wird meistens definiert als Differenz zweier Werte des unbestimmten Integrals, welche zwei speziellen

Werten der Integrationsvariabelen entsprechen; die letztern heißen die Grenzen des Integrals. So einfach aber diese Definition scheint, so wenig kann sie strengeren Anforderungen Genüge leisten, die immer gemacht werden müssen, wenn es sich um die Festlegung einer Basis für eine ganze Theorie handelt. Der Hauptgrund für die Verwerfung dieser Definition liegt vorzüglich in dem Umstande, daß sie nicht unmittelbar auf der eigentlich gegebenen Funktion fußt, sondern als Mittelglied noch eine andere Funktion, nämlich das unbestimmte Integral voraussetzt; und dies ist ein Übelstand in mehrfacher Hinsicht. Einmal ist die Existenz des bestimmten Integrals nicht eher evident, als bis die des unbestimmten nachgewiesen ist; gesetzt aber auch, daß dies allgemein möglich wäre, so fragt sich andererseits, ob nach dieser Definition das bestimmte Integral wirklich ein bestimmtes zu nennen ist, d. h. ob es nur von der gegebenen Funktion und den Grenzen abhängt. Es ist schon mehrfach gezeigt, daß dies keineswegs der Fall ist, und es sind Fälle bekannt, in welchen diese Definition zu Zweideutigkeiten führt, welche auf diesem Wege allein gar nicht zu heben sind. Ich hoffe nun zeigen zu können, daß das nach dieser Definition aufgefaßte bestimmte Integral in jedem Falle vollkommen so unbestimmt ist wie das sogenannte unbestimmte Integral.

Während nämlich die obige Definition schon zu Zweifeln Anlaß gibt, wenn es nicht möglich ist, mit Hilfe der bekannten Methoden das unbestimmte Integral darzustellen, so geschieht dies noch in viel höherem Maße, wenn es mehrere, ja unendlich viele Funktionen gibt, deren Differential die gegebene Funktion ist. Es läßt sich zwar strenge beweisen, daß diese Funktionen nur um sogenannte Konstanten voneinander verschieden sein können, und darauf fußt gerade die obige Definition, indem sie stillschweigend voraussetzt, daß der konstante Unterschied solcher Funktionen wirklich für alle Werte der Veränderlichen derselbe bleibt. Aber gerade dies ist durchaus nicht notwendig; man kann sich hingegen denken, daß diese Konstante in verschiedenen endlichen Intervallen der Veränderlichen x verschiedene Werte besitzt, und doch wird in jedem das Differentialverhältnis von $f(x) + C$ dieselbe Funktion $f'(x)$ sein, vorausgesetzt daß C seinen Wert nicht stetig mit x verändert, weil dann C nicht mehr eine Konstante wäre. Dies leuchtet namentlich geometrisch ein, wenn man $f(x)$ als Ordinate einer krummen Linie betrachtet; man kann beliebige Stücke dieser Linie parallel der Ordinatenachse

verschieben, ohne daß dadurch $f'(x)$ geändert würde. Mit andern Worten, das erste Differentialverhältnis einer Funktion gibt nicht den geringsten Aufschluß über die Stetigkeit derselben. Solche Unstetigkeiten lassen sich auch analytisch darstellen, namentlich mit Hilfe der Fourierschen Integrale, noch einfacher aber mit ganz elementaren Hilfsmitteln.

Bei der Zweideutigkeit, welche jeder Quadratwurzel hinsichtlich ihres Zeichens anhaftet, ist es durchaus erforderlich, durch ein bestimmtes Zeichen immer nur die eine Wurzel zu bezeichnen. So ist man auch darin übereingekommen, unter $\sqrt{x}$ stets die positive Quadratwurzel aus x zu verstehen. Die Notwendigkeit hiervon leuchtet namentlich ein, wenn statt einer Wurzelgröße ein anderer Ausdruck, z. B. die binomische Reihe gesetzt wird, welche jedenfalls immer nur eine Wurzel ausdrückt. Dies vorausgesetzt, läßt sich leicht ein Ausdruck bilden, welcher zwar mit x sich nicht stetig ändert, also eine Konstante ist, aber doch in verschiedenen Intervallen verschiedene Werte erhält. Ein solcher Ausdruck ist z. B. $C\frac{x-c}{\sqrt{(x-c)^2}}$, welcher gleich $+C$ oder $-C$ ist, je nachdem x größer oder kleiner als c genommen wird. Durch Differentiation findet man natürlich

$$\frac{\mathrm{d}\left(C\frac{x-c}{\sqrt{(x-c)^2}}\right)}{\mathrm{d}x} = C\frac{\sqrt{(x-c)^2}-(x-c)\frac{x-c}{\sqrt{(x-c)^2}}}{(x-c)^2} = 0$$

und folglich ist auch

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(f(x)+C\frac{x-c}{\sqrt{(x-c)^2}}\right) = \frac{\mathrm{d}f(x)}{\mathrm{d}x} = f'(x).$$

Wollte man daher die obige Definition des bestimmten Integrals zur Anwendung bringen, so müßte man aus dem unbestimmten Integral

$$\int f'(x)\,\mathrm{d}x = f(x)+C\frac{x-c}{\sqrt{(x-c)^2}}$$

das bestimmte Integral

$$\int_a^b f(x)\,\mathrm{d}x = f(b)-f(a)+C\frac{b-c}{\sqrt{(b-c)^2}}-C\frac{a-c}{\sqrt{(a-c)^2}}$$

erhalten; nimmt man hierin $a<c<b$, so ist die Summe der beiden letzten Glieder gleich $2C$, so daß das bestimmte Integral noch eine völlig willkürliche Konstante enthält.

Hiermit ist wohl das Ungenügende dieser Definition des unbestimmten Integrals dargetan, und wir wenden uns nun zu einer anderen, welche direkt von den gegebenen Größen ausgeht; nach ihr ist nämlich das bestimmte Integral als die Summe aller der unendlich kleinen Werte des gegebenen Differentials aufzufassen, wenn man der Veränderlichen x stetig alle Werte beilegt, welche zwischen den gegebenen Grenzen des Integrals liegen. Diese Definition läßt wenigstens keine anderen Zweideutigkeiten zu, als solche, welche schon in der Natur der gegebenen Funktion liegen. Es läßt sich ferner zeigen, daß sie mit der ersteren stets identisch ist, sobald nur das unbestimmte Integral so gewählt ist, daß es innerhalb des Integrationsintervalls keine Unstetigkeit enthält; denn dann ist die Summe, welche nach der zweiten Definition das Integral bildet, gerade die Summe aller der unendlich kleinen Inkremente, welche das unbestimmte Integral $f(x)$ erhält, wenn x das Intervall von a bis b stetig durchläuft. Ist aber $f(x)$ an irgend einer Stelle c zwischen a und b unstetig, so kann man sich eine stetige Funktion $f_1(x)$ substituiert denken, deren Differential ebenfalls $f'(x)\,\mathrm{d}x$ ist. Dann ist das bestimmte Integral $= f_1(b)-f_1(a)$, und diese Differenz unterscheidet sich von $f(b)-f(a)$ nur um den Betrag des Sprunges, welchen $f(x)$ an der Stelle $x=c$ macht, und es wird daher

$$\int_a^b f'(x)\,\mathrm{d}x = f(b)-f(a)+\lim\left(f(c-\delta)-f(c+\varepsilon)\right)$$

werden, worin δ und ε unendlich kleine, mit $(b-a)$ gleichstimmige Größen bedeuten; und statt dieser Gleichung kann man auch die folgende schreiben:

$$\int_a^b f'(x)\,\mathrm{d}x = \lim\left(\int_a^{c-\delta} f'(x)\,\mathrm{d}x+\int_{c+\varepsilon}^b f'(x)\,\mathrm{d}x\right).$$

7.

Die eben angestellten Betrachtungen sind vorzüglich wichtig bei solchen bestimmten Integralen, die noch eine andere Veränderliche enthalten, also bei Integralen von der Form

$$\int_a^b f(x,\xi)\,\mathrm{d}x,$$

worin ξ eine von x unabhängige Veränderliche bedeutet. Es kann nämlich der Fall eintreten, daß das unbestimmte Integral, wenn es im allgemeinen auch für alle Werte von x stetig ist, doch diese Eigenschaft verliert, wenn man der Veränderlichen ξ einen bestimmten Wert beilegt. Dies ist namentlich dann zu berücksichtigen, wenn das bestimmte Integral, als Funktion von ξ angesehen, einer zweiten Integration in bezug auf ξ unterworfen wird, und zwar zwischen Grenzen, innerhalb deren auch der spezielle Wert von ξ liegt, welcher das in bezug auf x genommene unbestimmte Integral unstetig macht. Sind α, β diese Grenzen, c und γ die Werte von x und ξ, für welche das Integral in bezug auf x unstetig wird, so muß man zufolge des vorigen Artikels

$$(19)\qquad \int_\alpha^\beta \mathrm{d}\xi \int_a^b f(x,\xi)\,\mathrm{d}x = \lim \int_\alpha^\beta \mathrm{d}\xi \int_a^{c-\varepsilon} f(x,\xi)\,\mathrm{d}x + \int_\alpha^\beta \mathrm{d}\xi \int_{c+\varepsilon}^b f(x,\xi)\,\mathrm{d}x$$

setzen; denn man muß erst die Integration in bezug auf x so ausführen, daß sie für alle Werte von ξ, welche bei der zweiten Integration in Betracht kommen, gültig bleibt. Ich habe diese Formel angeführt, um dadurch der unrichtigen Auffassung eines Satzes zu begegnen, der sich auf die Umkehrung der Integrationsordnung bei Doppelintegralen bezieht. In einem solchen Doppelintegral kann man nämlich die Ordnung vertauschen, also

$$(20)\qquad \int_\alpha^\beta \mathrm{d}\xi \int_a^b f(x,\xi)\,\mathrm{d}x = \int_a^b \mathrm{d}x \int_\alpha^\beta f(x,\xi)\,\mathrm{d}x$$

setzen, wenn $f(x,\xi)$ für alle Werte von x und ξ innerhalb der Integration endlich und stetig bleibt; wird aber $f(x,\xi)$ für $x = c$, $\xi = \gamma$ unstetig, so kann man noch immer

$$\int_\alpha^\beta \mathrm{d}\xi \int_a^{c-\varepsilon} f(x,\xi)\,\mathrm{d}x + \int_\alpha^\beta \mathrm{d}\xi \int_{c+\varepsilon}^b f(x,\xi)\,\mathrm{d}x = \int_a^{c-\varepsilon} \mathrm{d}x \int_\alpha^\beta f(x,\xi)\,\mathrm{d}\xi + \int_{c+\varepsilon}^b \mathrm{d}x \int_\alpha^\beta f(x,\xi)\,\mathrm{d}\xi$$

setzen; bezeichnet man die unbestimmten Integrale in bezug auf x und ξ bzw. mit $F(x,\xi)$ und $\varphi(x,\xi)$ und setzt diese als stetig zwischen den Grenzen der einzelnen Integrale voraus, so geht die letzte Gleichung in

$$\int_\alpha^\beta [F(b,\xi) - F(a,\xi)]\,\mathrm{d}\xi - \int_\alpha^\beta [F(c+\varepsilon,\xi) - F(c-\varepsilon,\xi)]\,\mathrm{d}\xi$$
$$= \int_a^{c-\varepsilon} [\varphi(x,\beta) - \varphi(x,\alpha)]\,\mathrm{d}x + \int_{c+\varepsilon}^b [\varphi(x,\beta) - \varphi(x,\alpha)]\,\mathrm{d}x$$

über; und wenn man hierin ε Null werden läßt, so erhält man

$$(21)\qquad \begin{cases} \displaystyle\int_\alpha^\beta [F(b,\xi) - F(a,\xi)]\,\mathrm{d}\xi - \lim \int_\alpha^\beta [F(c+\varepsilon,\xi) - F(c-\varepsilon,\xi)]\,\mathrm{d}\xi \\ \qquad = \displaystyle\int_a^b [\varphi(x,\beta) - \varphi(x,\alpha)]\,\mathrm{d}x \end{cases}$$

Diese Formel wird meistens so aufgefaßt, als gäbe das zweite Glied auf der linken Seite den Unterschied zwischen den beiden Doppelintegralen in (20) an; aus dem im Anfang dieses Artikels Gesagten erhellt aber, daß dies nicht richtig ist, indem erst beide Glieder der linken zusammengenommen das auf der linken Seite in (20) stehende Doppelintegral darstellen. Doch wird hierdurch die Richtigkeit der Gleichung (21) nicht beeinträchtigt, und diese ist es gerade, auf welche sich der von Cauchy gegebene Beweis stützt. Nimmt man nämlich

$$f(x,\xi) = if'(x+\xi i)$$

an, worin $i = \sqrt{-1}$ und $f'(z) = \dfrac{\mathrm{d}f(z)}{\mathrm{d}z}$ ist, so wird

$$F(x,\xi) = if(x+\xi i) \quad \text{und} \quad \varphi(x,\xi) = f(x+\xi i)$$

und die Gleichung (21) geht in die folgende über:

$$(22)\qquad \begin{cases} \quad i\displaystyle\int_\alpha^\beta [f(b+\xi i) - f(a+\xi i)]\,\mathrm{d}\xi \\ -i\lim \displaystyle\int_\alpha^\beta [f(c+\varepsilon+\xi i) - f(c-\varepsilon+\xi i)]\,\mathrm{d}\xi \\ \qquad = \displaystyle\int_a^b [f(x+\beta i) - f(x+\alpha i)]\,\mathrm{d}x. \end{cases}$$

Führt man in dem zweiten Gliede links eine neue Variabele η durch die Gleichung $\xi = \gamma + \varepsilon\eta$ ein, worin der Annahme nach $\alpha < \gamma < \beta$ ist, und setzt

$$(23)\qquad f(z) = \frac{F(z)}{z - c - \gamma i},$$

so findet man leicht

$$(24)\qquad i\lim \int_\alpha^\beta [f(c+\varepsilon+\xi i) - f(c-\varepsilon+\xi i)]\,\mathrm{d}\xi = 2\pi i F(c+\gamma i).$$

8.

Aus den eben entwickelten Formeln hat nun Cauchy den Wert des Integrals B abgeleitet, aber auf eine Weise, welche in einzelnen Punkten einer strengeren Begründung sehr bedürftig erscheint. Sie besteht in folgendem: Wenn die Funktion $f(z)$ so beschaffen ist, daß für jeden Wert von ξ $f(\pm\infty + \xi i) = 0$ und für jeden Wert von x $f(x + \infty i) = 0$ ist, so folgt aus den Gleichungen (22), (23) und (24), wenn man $\alpha = 0$, $\beta = \infty$, $a = -\infty$, $b = \infty$ setzt,

$$\int_{-\infty}^{+\infty} f(x)\,\mathrm{d}x = 2\pi i F(c + \gamma i), \tag{25}$$

worin nun γ zufolge der Bedingung $\alpha < \gamma < \beta$ notwendig positiv sein muß. Setzt man jetzt $f(z) = \frac{(-zi)^{\mu-1}}{zz+1}$, worin μ eine zwischen 0 und 2 liegende Zahl ist (unmotiviert), so sind die Bedingungen $f(\pm\infty + \xi i) = 0$ und $f(x + \infty i) = 0$ erfüllt; die Werte von x und ξ, welche $f(x + \xi i)$ unendlich machen, sind $c = 0$, $\gamma = 1$; es ist daher

$$F(z) = (z - i)\frac{(-zi)^{\mu-1}}{zz+1}; \quad F(c + \gamma i) = F(i) = \frac{1}{2i}$$

und folglich

$$\int_{-\infty}^{+\infty} \frac{(-xi)^{\mu-1}}{xx+1}\,\mathrm{d}x = \pi. \tag{26}$$

Zerlegt man dies Integral in zwei andere, deren Grenzen o, ∞ und $-\infty$, o sind, und setzt in dem zweiten $(-x)$ statt x, so findet man

$$\int_0^{\infty} \frac{x^{\mu-1}\,\mathrm{d}x}{xx+1} = \frac{\pi}{(+i)^{\mu-1} + (-i)^{\mu-1}} = \frac{\pi}{2\cos(\mu-1)\frac{\pi}{2}} = \frac{\pi}{2\sin\mu\frac{\pi}{2}},$$

und hierin braucht man bloß x statt xx, und $\mu = 2b$ (wo b zwischen 0 und 1 liegt, wenn $0 < \mu < 2$ ist) zu setzen, um die Gleichung (17) wieder zu erhalten.

Hierin scheint mir namentlich die Ableitung der Gleichung (25) nicht ganz streng zu sein; denn wenn auch die Bedingungen $f(\pm\infty + \xi i) = 0$, $f(x + \infty i) = 0$ für jedes zwischen 0 und 2 liegende μ erfüllt sind (eigentlich ist dazu nur erforderlich, daß

$\mu < 3$ ist, so daß μ auch negativ sein kann), so ist doch bekannt, daß das Verschwinden der Funktion unter dem Integralzeichen das des Integrals nicht immer zur Folge hat, namentlich dann, wenn die eine Grenze unendlich groß ist. Ich will daher versuchen, durch die folgende Darstellung diese Zweifel zu heben und zugleich zu beweisen, daß μ zwischen den Grenzen 0 und 2 liegen muß.

Setzt man in der Gleichung (22) $\alpha = 0$, $b = \beta = -a = k$, so geht sie mit Berücksichtigung der Gleichung (24) in folgende über

$$i\int_0^k [f(k + \xi i) - f(-k + \xi i)]\,\mathrm{d}\xi - 2\pi i F(c + \gamma i) = \int_{-k}^{+k} f(x + ki)\,\mathrm{d}x - \int_{-k}^{+k} f(x)\,\mathrm{d}x,$$

und wenn man in dem ersten Integral $\xi = k\eta$, im zweiten $x = ky$ setzt:

$$ik\int_0^1 [f(k(1 + \eta i)) - f(-k(1 - \eta i))]\,\mathrm{d}\eta - 2\pi i F(c + \gamma i) = k\int_{-1}^{+1} f(k(y + i))\,\mathrm{d}y - \int_{-k}^{+k} f(x)\,\mathrm{d}x.$$

Wenn nun bei unendlichem Wachsen von k die Funktionen unter den Integralzeichen verschwinden, und zwar für jeden Wert der Variabelen, so werden die Integrale selbst gleich Null. Nun ist für unseren Fall

$$kf(k(1 + \eta i)) = (-i)^{\mu-1}\frac{k^{\mu}(1 + \eta i)^{\mu-1}}{kk(1 + \eta i)^2 + 1}$$

und ähnlich die anderen Funktionen; damit diese Ausdrücke bei dem unendlichen Wachsen von k verschwinden, ist erforderlich, daß $\mu < 2$ sei, wodurch aber nicht ausgeschlossen ist, daß μ auch negativ sein kann. Jedenfalls erhält man unter dieser Annahme die Gleichung (25). Aus dem Gange des Beweises im vorigen Artikel leuchtet aber ein, daß, wenn es mehrere Paare von Werten, wie c und γ gibt, für welche $f(x, \xi)$ unendlich wird, in Gleichung (25) die Summe der ihnen entsprechenden Ausdrücke zu nehmen ist (nur mit der Bemerkung, daß, wenn $\gamma = \alpha$ ist, in Gleichung (24) $\pi i F(c + \gamma i)$ statt $2\pi i F(c + \gamma i)$ gesetzt werden muß). In unserem Falle ist aber $f(x, \xi) = if'(x + \xi i)$ und nach der obigen Spezialisierung von $f(z)$:

$$f'(z) = (-i)^{\mu-1}\frac{(\mu-3)z^{\mu} + (\mu-1)z^{\mu-2}}{(zz+1)^2},$$

und hierin sind die komplexen Werte von z aufzusuchen, welche diese Funktion unendlich machen; die ersten erhält man aus der Gleichung $zz + 1 = 0$, woraus die beiden Systeme ($c = 0$, $\gamma = 1$) und ($c = 0$, $\gamma = -1$) folgen, deren erstes oben schon behandelt ist; das zweite muß aber ausgeschlossen werden, weil dies γ der Bedingung $\alpha < \gamma < \beta$ nicht entspricht. Wenn aber, wie eben gezeigt ist, $\mu < 2$ sein muß, so ist auch ($c = 0$, $\gamma = 0$) ein solches System, und wir hätten demnach noch die Korrektion $\pi i F(0)$ anzubringen, worin $F(z) = (z - c - \gamma i) f(z)$, also in diesem Falle

$$F(z) = (-i)^{\mu-1} \frac{z^\mu}{zz+1}$$

ist; für $z = 0$ wird $F(z)$ nun entweder unendlich groß oder Null, je nachdem μ negativ oder positiv ist. Soll daher der Wert des Integrals in (25) endlich sein, so müssen wir das letztere annehmen, und dann ist in (26) eine Korrektion nicht mehr hinzuzufügen, da $F(0) = 0$ wird. Durch diese Betrachtung ist daher die Gültigkeit der Gleichung (26), aus welcher unmittelbar der Wert des Integrals B folgt, auf die Bedingung $0 < \mu < 2$ oder $0 < b < 1$ beschränkt.

9.

Ein von den bisher angeführten wesentlich verschiedener Beweis ist endlich noch in der Abhandlung „Disquisitiones generales circa seriem infinitam etc. Auctore C. F. Gauss“ enthalten. Die ganze Anlage derselben macht es aber unmöglich, diesen Beweis hier darzustellen, indem die Grundlagen, auf welche er sich stützt, mit einem Schlage eine vollständige Theorie der Eulerschen Integrale ergeben, deshalb aber auch zu bedeutend sind, um hier bloß zu diesem einzigen Zwecke entwickelt zu werden.

Zu diesen will ich nun noch einen, so viel mir bekannt ist, neuen Beweis hinzufügen, der eben nicht viel Zurüstungen erfordert und sich stets in dem Gebiete der Integralrechnung hält, wenn auch die Methode nicht eben neu ist, die darauf hinaus läuft, die Aufgabe auf die Integration einer Differentialgleichung zweiter Ordnung zurückzuführen. Setzt man in der Gleichung

$$BB = \int_0^\infty \frac{x^{b-1}\,dx}{x+1} \int_0^\infty \frac{y^{b-1}\,dy}{y+1} = \int_0^\infty \frac{dx}{x+1} \int_0^\infty \frac{(xy)^{b-1}}{y+1}\,dy$$

$y = \frac{z}{x}$, $dy = \frac{dz}{x}$, kehrt dann die Integrationsordnung um, und führt die Integration in bezug auf x aus, so findet man leicht

$$BB = \int_0^\infty \frac{z^{b-1} l z}{z-1}\,dz = \frac{d}{db} \int_0^\infty \frac{z^{b-1}\,dz}{z-1}. \tag{27}$$

Durch unbestimmte Integration in bezug auf b erhält man daher

$$\int BB\,db = \int_0^\infty \frac{z^{b-1}\,dz}{z-1},$$

worin das Integral rechts sich bloß durch die Form des Nenners von dem Integral B unterscheidet; und es ist leicht vorauszusehen, daß man das Integral B wiedererhält, wenn man das eben gewonnene derselben Behandlung unterwirft. In der Tat findet man

$$B \int BB\,db = \int_0^\infty \frac{dz}{z-1} \int_0^\infty \frac{(zy)^{b-1}}{y+1}\,dy,$$

und wenn man $y = \frac{x}{z}$, $dy = \frac{dx}{z}$ setzt, dann zufolge Art. 6 und 7 das in bezug auf z genommene Integral in zwei Integrale zerlegt, deren Grenzen 0, $1 - \delta$ und $1 + \varepsilon$, ∞ sind, die Integrationsordnung umkehrt, und die Integration in bezug auf z ausführt, so erhält man

$$B \int BB\,db = \int_0^\infty \frac{x^{b-1} l x}{x+1}\,dx + \lim \int_0^\infty \frac{x^{b-1}\,dx}{x+1} l\left(\frac{\delta}{\varepsilon}\right).$$

Hierin ist nun zwar $\lim l\left(\frac{\delta}{\varepsilon}\right)$ unbestimmt, jedenfalls aber unabhängig von x und b, und mag mit k bezeichnet werden. Dann gibt die letzte Gleichung

$$B \int BB\,db = \frac{dB}{db} + kB$$

oder, wenn man bedenkt, daß in dem Integral links doch schon eine willkürliche Konstante enthalten ist,

$$B \int BB\,db = \frac{dB}{db}, \tag{28}$$

woraus man durch Division mit B und Differentiation in bezug auf b die Differentialgleichung zweiter Ordnung

$$BB = \frac{1}{B}\frac{\mathrm{d}\,\mathrm{d}B}{\mathrm{d}b^2} - \frac{1}{BB}\left(\frac{\mathrm{d}B}{\mathrm{d}b}\right)^2$$

erhält, welche die Eigentümlichkeit besitzt, daß die unabhängige Variabele b nicht vorkommt, und sich deshalb bekanntlich auf eine Differentialgleichung erster Ordnung zurückführen läßt, wenn man das erste Differentialverhältnis als neue Variabele einführt. Bezeichnen wir dieses mit B', so ist

$$\frac{\mathrm{d}B}{\mathrm{d}b} = B', \quad \frac{\mathrm{d}\,\mathrm{d}B}{\mathrm{d}b^2} = \frac{\mathrm{d}B'}{\mathrm{d}b} = \frac{B'\mathrm{d}B'}{\mathrm{d}B},$$

und führen wir diese Transformationen in die obige Differentialgleichung ein, so geht diese in

$$BB = \frac{B'\mathrm{d}B'}{B\mathrm{d}B} - \frac{B'B'}{BB}$$

oder in

$$\mathrm{d}(BB) = \frac{BB\mathrm{d}(B'B') - B'B'\mathrm{d}(BB)}{(BB)^2} = \mathrm{d}\,\frac{B'B'}{BB}$$

über, deren Integral

$$BB = cc + \frac{B'B'}{BB} = cc + \frac{1}{BB}\left(\frac{\mathrm{d}B}{\mathrm{d}b}\right)^2$$

ist. Zu der Bestimmung der Konstanten ist nun die Kenntnis zweier Eigenschaften des Integrals erforderlich; diese nehmen wir aus Art. 3, wo gezeigt ist, das B für $b = \frac{1}{2}$ ein Minimum $= \pi$ erreicht; da gleichzeitig $\frac{\mathrm{d}B}{\mathrm{d}b} = 0$ wird, so ergibt sich unmittelbar $cc = \pi\pi$. Man erhält dann weiter

$$\pm\,\mathrm{d}b = \frac{\mathrm{d}B}{B\sqrt{(BB - \pi\pi)}} = \frac{1}{\pi}\,\frac{-\,\mathrm{d}\,\frac{\pi}{B}}{\sqrt{\left(1 - \frac{\pi\pi}{BB}\right)}},$$

folglich durch Integration

$$\pm\,(b + c) = \frac{1}{\pi}\,arc\,cos\,\frac{\pi}{B}, \quad B = \frac{\pi}{cos\,(b+c)\pi}.$$

Da B für $b = \frac{1}{2}$ den Wert π erhält, so muß

$$cos\,(\tfrac{1}{2} + c)\pi = -\,sin\,c\pi = 1, \quad cos\,c\pi = 0$$

sein; folglich ist

$$cos\,(b + c)\pi = cos\,b\pi\,cos\,c\pi - sin\,b\pi\,sin\,c\pi = sin\,b\pi,$$

wodurch man wieder $B = \frac{\pi}{sin\,b\pi}$ findet.

10.

Weil der im vorigen Artikel gegebene Beweis den Anforderungen der größten Strenge doch noch nicht Genüge leistet, namentlich insofern das Integral $\int_0^\infty \frac{x^{b-1}\,\mathrm{d}x}{x-1}$ darin eine Rolle spielt, so ist es wohl nicht unangemessen, hier eine solche Modifikation noch folgen zu lassen, in welcher die unbestimmte Integration in bezug auf b ganz vermieden wird. Da die Gleichung (28) sich auch so schreiben läßt

$$\int BB\,\mathrm{d}b = \frac{\mathrm{d}lB}{\mathrm{d}b},$$

so läßt sich vermuten, daß eine Entwicklung des rechts stehenden Ausdrucks ebenfalls zum Ziele führt. Da $B = \Gamma(b)\,\Gamma(1-b)$ ist, so reicht es hin, ein Integral für $\frac{\mathrm{d}l\Gamma(\mu)}{\mathrm{d}\mu}$ zu finden, was sich bekanntlich auf folgendem Wege erreichen läßt. Aus der Definition von $\Gamma(\mu)$ folgt

$$\frac{\mathrm{d}\Gamma(\mu)}{\mathrm{d}\mu} = \int_0^\infty x^{\mu-1}e^{-x}\,\mathrm{d}x\,lx.$$

Setzt man hierin für lx das Integral

$$lx = \int_0^\infty \frac{e^{-z} - e^{-zx}}{z}\,\mathrm{d}x,$$

welches sich aus dem Integral $\int_0^1 y^{x-1}\,\mathrm{d}y = \frac{1}{x}$ durch Integration in bezug auf x zwischen den Grenzen 1 und x, und durch Substitution von e^{-z} für y ergibt, so findet man durch Umkehrung der Integrationsordnung und mit Hilfe von Gleichung (3) sehr leicht

$$\frac{\mathrm{d}l\Gamma(\mu)}{\mathrm{d}\mu} = \int_0^\infty \frac{\mathrm{d}z}{z}\left(e^{-z} - \frac{1}{(z+1)^\mu}\right).$$

Setzt man hierin b und $(1-b)$ für μ, so ergibt sich

$$\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_0^\infty \frac{\mathrm{d}z}{z}\left(\frac{1}{(z+1)^{1-b}} - \frac{1}{(z+1)^b}\right),$$

und wenn man hierin $z = x-1$ oder $z = \frac{1}{x} - 1$ setzt:

$$\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_1^\infty \frac{x^b - x^{1-b}}{x-1}\frac{\mathrm{d}x}{x} = \int_0^1 \frac{x^b - x^{1-b}}{x-1}\frac{\mathrm{d}x}{x},$$

also auch

$$2\,\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_0^\infty \frac{x^b - x^{1-b}}{x-1}\frac{\mathrm{d}x}{x}.$$

Vergleicht man dies mit Gleichung (27), so ergibt sich augenblicklich

$$2\,\frac{\mathrm{d}lB}{\mathrm{d}b} = \int_{1-b}^{b} B B\,\mathrm{d}B = 2\int_{\frac{1}{2}}^{b} B B\,\mathrm{d}b, \tag{29}$$

indem ja zufolge Art. 3 B für $b = \frac{1}{2} + b'$ und $b = \frac{1}{2} - b'$ dieselben Werte erhält; durch Differentiation dieser Gleichung in bezug auf b erhält man wieder die im vorigen Artikel behandelte Differentialgleichung.

11.

Nachdem durch die angegebenen Beweise die Richtigkeit der Gleichung

$$B(r, 1-r) = \int_0^\infty \frac{x^{r-1}\,\mathrm{d}x}{x+1} = \frac{\pi}{\sin r\pi},$$

worin r einen positiven echten Bruch bezeichnet, außer Zweifel gesetzt ist, ergibt sich unmittelbar aus Art. 2, daß die Eulerschen Integrale der ersten Art, deren beide Argumente eine ganze positive Zahl zur Summe haben, sich wirklich darstellen lassen; man findet

$$\left\{\begin{aligned} &B(m+r, n-r) \\ &= \frac{(m+r-1)\cdots(1+r)r\cdot(n-1-r)\cdots(2-r)(1-r)}{(m+n-1)(m+n-2)\cdots 2\cdot 1}\,\frac{\pi}{\sin r\pi}. \end{aligned}\right. \tag{30}$$

Man kann hiervon auch noch einen wichtigen Rückschluß auf die Eulerschen Integrale der ersten Art machen; setzt man nämlich $m = 0$, $n = 1$, $r = \frac{1}{2}$, so findet man

$$\Gamma\left(\frac{1}{2}\right) = \int_0^\infty e^{-x}\frac{\mathrm{d}x}{\sqrt{x}} = 2\int_0^\infty e^{-xx}\,\mathrm{d}x = \sqrt{\pi} \tag{31}$$

und folglich nach Gleichung (4):

$$\Gamma\left(n+\frac{1}{2}\right) = (2n-1)(2n-3)\ldots 5\cdot 3\cdot 1\,\frac{\sqrt{\pi}}{2^n}. \tag{32}$$

12.

Nachdem in Artt. 2 und 11 die Fälle zusammengestellt sind, in welchen die Eulerschen Integrale beider Arten ohne Hilfe neuer Funktionen dargestellt werden können, will ich zum Schluß noch einmal zu dem Integral B zurückkehren, um noch einige Beziehungen desselben zu anderen Integralen zu entwickeln. Unter den verschiedenen Formen, in welchen es auftritt, sind die beiden folgenden

$$\int_{-\infty}^{+\infty} \frac{e^{(2b-1)z} + e^{-(2b-1)z}}{e^z + e^{-z}}\,\mathrm{d}z \quad \text{und} \quad 2\int_0^{\frac{\pi}{2}} (tg\,\varphi)^{2b-1}\,\mathrm{d}\varphi = 2\int_0^{\frac{\pi}{2}} (tg\,\varphi)^{1-2b}\,\mathrm{d}\varphi$$

ganz interessant; wichtiger sind aber die Verallgemeinerungen desselben durch Einführung neuer Konstanten. Dahin gehört das Integral

$$\int_0^\infty \frac{x^{b-1}\,\mathrm{d}x}{x+c} = \frac{\pi c^{b-1}}{\sin b\pi}, \tag{33}$$

worin c positiv sein muß; doch läßt sich nachträglich beweisen, daß c auch imaginär sein darf; multipliziert man nämlich Zähler und Nenner der Funktion $\frac{x^{b-1}}{x+i}$ mit $(x \mp i)$, so zerfällt das entsprechende Integral in zwei andere, welche sich durch die Substitution $xx = y$ auf das Integral B reduzieren lassen, und so findet man die Gültigkeit der Gleichung (33) für imaginäre c. Durch Differentiation und Integration in bezug auf c kann man dann wieder eine Reihe von anderen Integralen ableiten.

Sind $c_1, c_2, \ldots, c_n$ voneinander verschiedene positive oder imaginäre Konstanten, ferner $0 < b < n$ und

$$f(x) = (x + c_1)(x + c_2) \ldots (x + c_n), \quad f'(x) = \frac{\mathrm{d}f(x)}{\mathrm{d}x},$$

so findet man auch

$$\int_0^\infty \frac{x^{b-1}\,\mathrm{d}x}{f(x)} = \frac{\pi}{\sin b\pi} \sum_{k=1}^{k=n} \frac{c_k^{b-1}}{f'(-c_k)}, \tag{34}$$

indem man $\frac{x^\beta}{f(x)}$ in Partialbrüche zerlegt, worin β die größte in b enthaltene ganze Zahl bedeutet.

Ein Vorzug des in Art. 10 gegebenen Beweises besteht auch noch darin, daß er unmittelbar eine verwandte Klasse von Integralen bestimmen lehrt. Aus den Gleichungen (27) und (29) folgt nämlich unmittelbar

$$\int_0^\infty \frac{x^b - x^{\frac{1}{2}}}{1-x} \frac{\mathrm{d}x}{x} = \pi \cot b\pi,$$

folglich auch

$$\int_0^\infty \frac{x^a - x^b}{1-x} \frac{\mathrm{d}x}{x} = \pi(\cot a\pi - \cot b\pi), \tag{35}$$

und hieraus ergiebt sich auch das in Art. 3 mit $\varphi(b)$ bezeichnete Integral

$$\int_0^\infty \frac{1 - x^\mu}{1 - x^\nu} x^{b-1}\,\mathrm{d}x = \frac{1}{\nu} \int_0^\infty \frac{x^{\frac{b}{\nu}} - x^{\frac{\mu+b}{\nu}}}{1-x} \frac{\mathrm{d}x}{x}$$

$$= \frac{\pi}{\nu} \frac{\sin\frac{\mu\pi}{\nu}}{\sin\frac{b\pi}{\nu} \sin\frac{(\mu+b)\pi}{\nu}} = \frac{2\pi}{\nu} \frac{\sin\frac{\mu\pi}{\nu}}{\cos\frac{\mu\pi}{\nu} - \cos\frac{(\mu+2b)\pi}{\nu}}$$

und das Minimum desselben

$$\int_0^\infty \frac{x^{\frac{\mu}{2}} - x^{-\frac{\mu}{2}}}{x^{\frac{\nu}{2}} - x^{-\frac{\nu}{2}}} \frac{\mathrm{d}x}{x} = \frac{2\pi}{\nu} \operatorname{tg}\frac{\mu\pi}{2\nu}.$$

Die meisten der hierher gehörigen Integrale finden sich in der im Auftrage des preußischen Ministeriums von Minding herausgegebenen „Sammlung von Integraltafeln“ (Berlin 1849), im Anfang der vierten Abteilung. Vielleicht ist hier der Ort, um einige Fehler, welche sich daselbst finden, anzuzeigen und zu verbessern. Durch Zerlegung von $\frac{1}{(x-1)(x+c)}$ in Partialbrüche und Anwendung der Formeln dieses Artikels findet man leicht

$$\int_0^\infty \frac{x^a - 1}{(x-1)(x+c)} \mathrm{d}x = \frac{\pi}{c+1}\left(\frac{c^a - \cos a\pi}{\sin a\pi} - \frac{lc}{\pi}\right),$$

und diese Gleichung gilt für positive und negative echt gebrochene a, wovon man sich leicht überzeugt, wenn man $\frac{1}{x}$ und $\frac{1}{c}$ statt x und c schreibt. Differentiiert man in bezug auf a und setzt dann $a = 0$, so erhält man eine Reihe von Integralen, welche in jenen Tafeln unrichtig angegeben sind. Um die lästigen Differentiationen möglichst zu erleichtern, kann man folgenden Kunstgriff anwenden. Setzt man

$$\frac{lc}{\pi} + \frac{c+1}{\pi} \int_0^\infty \frac{x^a - 1}{(x-1)(x+c)} \mathrm{d}x = \frac{c^a - \cos a\pi}{\sin a\pi} = J, \quad \frac{\mathrm{d}^n J}{\mathrm{d}a^n} = {}^n\!J,$$

so erhält man für $a = 0$

$$\int_0^\infty \frac{(lx)^n\,\mathrm{d}x}{(x-1)(x+c)} = \frac{\pi}{c+1}\,{}^n\!J_0.$$

Man findet aber leicht

$$J\pi^n \sin\left(a + \frac{n}{2}\right)\pi + n\,{}^1\!J\pi^{n-1} \sin\left(a + \frac{n-1}{2}\right)\pi + \cdots$$

$$\cdots + n\,{}^{n-1}\!J\pi \sin(a + \tfrac{1}{2})\pi + {}^n\!J \sin a\pi$$

$$= \frac{\mathrm{d}^n(J \sin a\pi)}{\mathrm{d}x^n} = c^a (lc)^n - \pi^n \cos\left(a + \frac{n}{2}\right)\pi,$$

und für $a = 0$ erhält man Rekursionsformeln für die J_0 mit geraden und die mit ungeraden Indizes. So findet man

$$\int_0^\infty \frac{lx\,dx}{(x-1)(x+c)} = \frac{(lc)^2+\pi\pi}{2(c+1)},$$

$$\int_0^\infty \frac{(lx)^2\,dx}{(x-1)(x+c)} = \frac{lc((lc)^2+\pi\pi)}{3(c+1)},$$

$$\int_0^\infty \frac{(lx)^3\,dx}{(x-1)(x+c)} = \frac{((lc)^2+\pi\pi)^2}{4(c+1)},$$

$$\int_0^\infty \frac{(lx)^4\,dx}{(x-1)(x+c)} = \frac{lc((lc)^2+\pi\pi)(3(lc)^2+7\pi\pi)}{5(c+1)\cdot 3},$$

$$\int_0^\infty \frac{(lx)^5\,dx}{(x-1)(x+c)} = \frac{((lc)^2+\pi\pi)^2((lc)^2+3\pi\pi)}{6(c+1)},$$

während in jenen Tafeln statt der Divisoren 2, 3, 4, 5, 6 die Divisoren $1\cdot 2$, $1\cdot 2\cdot 3$, $1\cdot 2\cdot 3\cdot 4$, $1\cdot 2\cdot 3\cdot 4\cdot 5$, $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6$ angegeben sind.

II.

Über ein Eulersches Integral.

[Journal für reine und angewandte Mathematik, Bd. 45, S. 370—374 (1853)].

Die von Gauß und Legendre in die Analysis eingeführten Funktionen Π und Γ stehen bekanntlich in dem Zusammenhange, daß $\Gamma(a)$ mit $\Pi(a-1)$ identisch ist, so lange a einen positiven Wert hat; für negative a ist $\Gamma(a)$ stets unendlich groß, während $\Pi(a-1)$ eine bestimmte Funktion bleibt und nur dann unendlich und unstetig wird, wenn a einen der Werte 0, -1, -2 usw. erhält. Die Funktion Π wird als unendliches Produkt, Γ als bestimmtes Integral definiert. Unstreitig ist die erstere Definition umfassender und gewährt eine tiefere Einsicht in das wahre Wesen dieser Funktionen; indessen ist es für die Integralrechnung wichtig, ohne Hilfe jener Entwicklungen in unendliche Produkte und Reihen, selbständig eine Theorie dieser Funktionen aufzustellen. Dies ist auch in der Tat nach und nach vollständig gelungen, seitdem namentlich Dirichlet (im 15. Bande dieses Journals) das berühmte Multiplikationstheorem von Gauß so elegant bewiesen hat. In dieser Abhandlung wird auch der Lehrsatz

$$\Pi(a-1)\cdot\Pi(-a) = \int_0^\infty \frac{x^{a-1}\,dx}{x+1} = \frac{\pi}{\sin a\pi}$$

angewendet, für welchen sehr verschiedene Beweise von verschiedenen Mathematikern gegeben sind, die aber fast alle ihren Weg über Entwicklungen in unendliche Reihen nehmen. In meiner, Ostern 1852 gedruckten Inaugural-Dissertation (Über die Elemente der Theorie der Eulerschen Integrale) sind die hauptsächlichsten zusammengestellt; auch habe ich schon dort einen neuen Weg hinzugefügt, welcher sich ganz im Gebiet der bestimmten Integrale hält, dem ich aber eine vollkommene Strenge nur dadurch zu verleihen vermochte, daß ich die Entstehung dieses Integrals aus der Multiplikation von $\Pi(a-1)$ und $\Pi(-a)$, und den Ausdruck für $\frac{d\log\Pi(a)}{da}$ als bekannt voraussetzte. Im folgenden soll nun ein, zwar auf ganz derselben Idee beruhender, aber von anderen Theorien ganz unabhängiger

Beweis gegeben werden, der nur die allgemeinsten Sätze über die bestimmten Integrale zu Hilfe nimmt.

Zuerst muß an einen Hilfssatz erinnert werden, der nachher einige Male gebraucht wird. Es ist bekanntlich

$$\int \frac{dw}{(\alpha w+\beta)(\alpha' w+\beta')} = \frac{log\left(\frac{\alpha w+\beta}{\alpha' w+\beta'}\right)}{\alpha\beta'-\alpha'\beta},$$

wo die Logarithmen hyperbolische sind. Sind nun $\frac{\beta}{\alpha}$ und $\frac{\beta'}{\alpha'}$ positive Größen, so folgt hieraus

$$\int_0^\infty \frac{dw}{(\alpha w+\beta)(\alpha' w+\beta')} = \frac{log\frac{\alpha\beta'}{\alpha'\beta}}{\alpha\beta'-\alpha'\beta}$$

oder, wenn der Logarithme immer nur von dem absoluten Werte genommen wird:

$$(1) \qquad \int_0^\infty \frac{dw}{(\alpha w+\beta)(\alpha' w+\beta')} = \frac{log(\alpha\beta')-log(\alpha'\beta)}{\alpha\beta'-\alpha'\beta};$$

und diese Gleichung gilt selbst für den Fall, in welchem $\frac{\alpha}{\beta}=\frac{\alpha'}{\beta'}$ ist, wenn man den unter die Form $\frac{0}{0}$ tretenden Wert nach den Regeln der Differentialrechnung behandelt.

Gehen wir nun zu dem eigentlichen Gegenstande über, so ist erstens leicht zu sehen, daß das gegebene Integral

$$(2) \qquad \int_0^\infty \frac{x^{a-1}dx}{x+1} = A = \varphi(a)$$

nur dann einen endlichen, und zwar positiven Wert hat, wenn a ein positiver echter Bruch ist. Zerlegt man nämlich das Integral in zwei andere mit den Grenzen 0, 1 und 1, ∞, und schreibt im letzteren $\frac{1}{x}$ statt x, so findet man

$$(3) \qquad A = \int_0^1 \frac{x^{a-1}+x^{-a}}{x+1}\,dx.$$

Da nun im ganzen Intervall der Integration $\frac{1}{x+1}$ zwischen den Grenzen 1 und $\frac{1}{2}$ liegt, so liegt auch A zwischen den Grenzen

$$\int_0^1 (x^{a-1}+x^{-a})\,dx \quad \text{und} \quad \tfrac{1}{2}\int_0^1 (x^{a-1}+x^{-a})\,dx.$$

Dieses Integral hat aber nur dann einen endlichen und positiven Wert, $=\frac{1}{a(1-a)}$, wenn a ein positiver echter Bruch ist. Dieselbe Bedingung ist daher auch für die Endlichkeit des Integrals A nötig.

Ferner ergibt sich unmittelbar aus der Gleichung (3) der Satz

$$(4) \qquad \varphi(a) = \varphi(1-a).$$

Differentiiert man diese Gleichung in bezug auf a und setzt dann $a=\frac{1}{2}$, so findet man

$$(5) \qquad \varphi'(\tfrac{1}{2}) = 0.$$

Da ferner, wie leicht zu sehen, $\varphi''(\frac{1}{2})$ positiv ist, so erreicht $\varphi(a)$ für $a=\frac{1}{2}$ einen Minimumwert

$$(6) \qquad \varphi\left(\frac{1}{2}\right) = \int_0^\infty \frac{x^{-\frac{1}{2}}dx}{x+1} = 2\int_0^\infty \frac{d(\sqrt{x})}{1+(\sqrt{x})^2} = \pi.$$

Bezeichnet w eine positive Größe, so erhält man, wenn man in der Gleichung (2) $\frac{x}{w}$ statt x schreibt:

$$(7) \qquad \int_0^\infty \frac{x^{a-1}dx}{x+w} = A\,w^{a-1},$$

und wenn man $\frac{1}{w}$ statt w setzt,

$$(8) \qquad \int_0^\infty \frac{x^{a-1}dx}{xw+1} = A\,w^{-a}.$$

Multipliziert man die Gleichung (7) mit $\frac{dw}{w+1}$, integriert in bezug auf w zwischen den Grenzen 0 und ∞ und bedenkt, daß zufolge des Hilfssatzes (1)

$$\int_0^\infty \frac{dw}{(w+1)(w+x)} = \frac{log\,x}{x-1}$$

ist, so erhält man

$$AA = \int_0^\infty \frac{x^{a-1}\,dx}{x-1} \log x.$$

Integriert man jetzt in bezug auf a zwischen den Grenzen $(1-a)$ und a, so erhält man

$$\int_{1-a}^{a} AA\,da = \int_0^\infty \frac{x^{a-1}-x^{-a}}{x-1}\,dx = \int_0^\infty \frac{w^{a-1}-w^{-a}}{w-1}\,dw.$$

Subtrahiert man die Gleichung (8) von (7), so findet man leicht:

$$A\frac{w^{a-1}-w^{-a}}{w-1} = \int_0^\infty \frac{x^{a-1}(x-1)}{(xw+1)(w+x)}\,dx,$$

und wenn man zwischen den Grenzen $w=0$ und $w=\infty$ integriert und erwägt, daß

$$\int_0^\infty \frac{dw}{(xw+1)(w+x)} = \frac{2\log x}{xx-1}$$

ist, so folgt unmittelbar:

$$A\int_{1-a}^{a} AA\,da = A\int_0^\infty \frac{w^{a-1}-w^{-a}}{w-1}\,dw = 2\int_0^\infty \frac{x^{a-1}\,dx}{x+1}\log x.$$

Zufolge der Eigenschaft von A, daß $A = \varphi(a) = \varphi(1-a)$ ist, ergibt sich aber

$$\int_{a-1}^{a} AA\,da = 2\int_{\frac{1}{2}}^{a} AA\,da.$$

Ferner ist

$$\int_0^\infty \frac{x^{a-1}\,dx}{x+1}\log x = \frac{dA}{da},$$

und so erhält man endlich die Gleichung

$$A\int_{\frac{1}{2}}^{a} AA\,da = \frac{dA}{da}.$$

aus welcher sich durch Division mit A und Differentiation in bezug auf a die folgende ableiten läßt:

$$AA = \frac{1}{A}\frac{ddA}{da^2} - \frac{1}{AA}\left(\frac{dA}{da}\right)^2.$$

Da in derselben die unabhängige Variable a nicht vorkommt, so führe man $\frac{dA}{da} = A'$ als neue Variable ein. Dies gibt

$$AA = \frac{A'\,dA'}{A\,dA} - \frac{A'A'}{AA}, \quad A\,dA = \frac{AA\cdot A'\,dA' - A'A'\cdot A\,dA}{A^4}$$

oder

$$d(AA) = \frac{AA\cdot d(A'A') - A'A'\cdot d(AA)}{(AA)^2},$$

und das Integral dieser Gleichung ist offenbar

$$AA = Const. + \frac{A'A'}{AA} = Const. + \frac{1}{AA}\left(\frac{dA}{da}\right)^2.$$

Um die Konstante zu bestimmen, setze man $a = \frac{1}{2}$, wofür nach Gleichung (5) und (6) $\frac{dA}{da} = 0$ und $A = \pi$ ist; daraus folgt $\pi\pi$ als Wert der Konstante und

$$da = \pm\frac{dA}{A\sqrt{(AA-\pi\pi)}} = \mp\frac{1}{\pi}\frac{d\left(\frac{\pi}{A}\right)}{\sqrt{\left(1-\frac{\pi\pi}{AA}\right)}}.$$

Bezeichnet man mit c eine Konstante, so ergibt sich

$$a + c = \pm\frac{1}{\pi}\,arc\,cos\frac{\pi}{A}, \quad A = \frac{\pi}{cos\,(a+c)\,\pi}.$$

Um die Konstante c zu finden, setze man wieder $a = \frac{1}{2}$, woraus

$$1 = cos\,(\tfrac{1}{2}\pi + c\pi) = -\,sin\,c\pi, \quad cos\,c\pi = 0$$

und

$$cos\,(a+c)\,\pi = sin\,a\pi$$

folgt. Man erhält daher

$$A = \frac{\pi}{sin\,a\pi},$$

was zu beweisen war. Außerdem ergeben sich aus diesem Beweise sehr leicht noch mehrere verwandte Integrale, was ich hier nicht weiter ausführe.

Braunschweig, im September 1852.

III.

Ein Satz aus der Theorie der dreiachsigen Koordinatensysteme.

[Journal für reine und angewandte Mathematik, Bd. 50, S. 272—275 (1855)].

Wenn die Winkel YOZ, ZOX, XOY eines dreiachsigen Koordinatensystems durch a, b, c bezeichnet werden, so wird der konkave Winkel w zwischen zwei beliebigen Richtungen OM und OM' durch folgende Gleichung bestimmt:

$$(1)\quad \left\{\begin{array}{l} \alpha\alpha' \sin a^2 + \beta\beta' \sin b^2 + \gamma\gamma' \sin c^2 + (\beta\gamma' + \gamma\beta')(\cos b \cos c - \cos a) \\ + (\gamma\alpha' + \alpha\gamma')(\cos c \cos a - \cos b) + (\alpha\beta' + \beta\alpha')(\cos a \cos b - \cos c) \\ = D \cos w, \end{array}\right.$$

in welcher α, β, γ die Kosinus der konkaven Winkel MOX, MOY, MOZ, ebenso α', β', γ' die Kosinus der konkaven Winkel $M'OX$, $M'OY$, $M'OZ$ sind, und D folgende Bedeutung hat:

$$(2)\qquad D = 1 - \cos a^2 - \cos b^2 - \cos c^2 + 2 \cos a \cos b \cos c.$$

Dieser bekannte Satz schließt den anderen ein, daß drei solche Richtungskosinus, wie α, β, γ, stets der Bedingung

$$(3)\quad \left\{\begin{array}{l} \alpha\alpha \sin a^2 + \beta\beta \sin b^2 + \gamma\gamma \sin c^2 + 2\beta\gamma(\cos b \cos c - \cos a) \\ + 2\gamma\alpha(\cos c \cos a - \cos b) + 2\alpha\beta(\cos a \cos b - \cos c) = D \end{array}\right.$$

Genüge leisten müssen.

Ist das Koordinatensystem rechtwinklig, so gehen die Gleichungen (1) und (3) in die beiden folgenden über:

$$\alpha\alpha' + \beta\beta' + \gamma\gamma' = \cos w,$$
$$\alpha\alpha + \beta\beta + \gamma\gamma = 1.$$

Um daher auszudrücken, daß dann die drei Linien OM, OM', OM'' ein zweites rechtwinkliges Koordinatensystem bilden, sind folgende sechs Gleichungen nötig:

$$(4)\quad \left\{\begin{array}{llll} \alpha\alpha + \beta\beta + \gamma\gamma = 1, & & \alpha'\alpha'' + \beta'\beta'' + \gamma'\gamma'' = 0, \\ \alpha'\alpha' + \beta'\beta' + \gamma'\gamma' = 1, & & \alpha''\alpha + \beta''\beta + \gamma''\gamma = 0, \\ \alpha''\alpha'' + \beta''\beta'' + \gamma''\gamma'' = 1, & & \alpha\alpha' + \beta\beta' + \gamma\gamma' = 0. \end{array}\right.$$

Sie sind auch hinreichend zu diesem Zwecke, wenn angenommen wird, daß das erste System rechtwinklig sei.

Der in der Überschrift angekündigte Satz besteht nun darin, daß diese letztere Beschränkung weggelassen werden darf, indem die Gleichungen (4) unzweifelhaft ausdrücken, daß beide Systeme durchaus rechtwinklig sein müssen. Der Beweis dieses merkwürdigen Theorems bildet den Gegenstand des gegenwärtigen Aufsatzes.

Zunächst mögen hier ohne weiteren Beweis die bekannten Folgerungen aus den Gleichungen (4) Platz finden, nämlich:

$$(5)\quad \left\{\begin{array}{llll} \alpha\alpha + \alpha'\alpha' + \alpha''\alpha'' = 1, & & \beta\gamma + \beta'\gamma' + \beta''\gamma'' = 0, \\ \beta\beta + \beta'\beta' + \beta''\beta'' = 1, & & \gamma\alpha + \gamma'\alpha' + \gamma''\alpha'' = 0, \\ \gamma\gamma + \gamma'\gamma' + \gamma''\gamma'' = 1, & & \alpha\beta + \alpha'\beta' + \alpha''\beta'' = 0, \end{array}\right.$$

und

$$(6)\quad \left\{\begin{array}{llll} \beta'\gamma'' - \beta''\gamma' = \varepsilon\alpha, & & \gamma'\alpha'' - \gamma''\alpha' = \varepsilon\beta, & \alpha'\beta'' - \alpha''\beta' = \varepsilon\gamma, \\ \beta''\gamma - \beta\gamma'' = \varepsilon\alpha', & & \gamma''\alpha - \gamma\alpha'' = \varepsilon\beta', & \alpha''\beta - \alpha\beta'' = \varepsilon\gamma', \\ \beta\gamma' - \beta'\gamma = \varepsilon\alpha'', & & \gamma\alpha' - \gamma'\alpha = \varepsilon\beta'', & \alpha\beta' - \alpha'\beta = \varepsilon\gamma'', \end{array}\right.$$

wo bekanntlich $\varepsilon\varepsilon = 1$ ist.

Die ternäre quadratische Form

$$F \equiv xx + yy + zz + 2yz\cos a + 2zx\cos b + 2xy\cos c,$$

[welche bekanntlich das Quadrat der Entfernung eines beliebigen Punktes (xyz) von dem Nullpunkte O des Koordinatensystems $OXYZ$ ausdrückt] hat zur Determinante den oben (2) mit D bezeichneten Ausdruck (das Quadrat des Volumens des von den drei Achsen $OX = OY = OZ = 1$ als Kanten gebildeten Parallelepipedums) und zur adjungierten Form:

$$F_1 \equiv xx \sin a^2 + yy \sin b^2 + zz \sin c^2 + 2yz(\cos b \cos c - \cos a) + 2zx(\cos c \cos a - \cos b) + 2xy(\cos a \cos b - \cos c).$$

Es ist dann bekanntlich die Determinante von F_1 das Quadrat der von F, also $= DD$, und die adjungierte Form F_2 von F_1 ist $\equiv DF$.

Wenn man folgende Bezeichnung einführt:

$$xx' \sin a^2 + yy' \sin b^2 + zz' \sin c^2 + (yz' + zy')\cos b \cos c - \cos a) + (zx' + xz')(\cos c \cos a - \cos b) + (xy' + yx')(\cos a \cos b - \cos c) \equiv F_1\begin{pmatrix} x, & y, & z \\ x', & y', & z' \end{pmatrix},$$

so ist aus der Theorie der ternären Formen weiter bekannt, daß

$$F_1\begin{pmatrix} x, & y, & z \\ x, & y, & z \end{pmatrix} F_1\begin{pmatrix} x', & y', & z' \\ x', & y', & z' \end{pmatrix} - \left[F_1\begin{pmatrix} x, & y, & z \\ x', & y', & z' \end{pmatrix}\right]^2$$
$$\equiv F_2\begin{pmatrix} yz'-zy', & zx'-xz', & xy'-yx' \\ yz'-zy', & zx'-xz', & xy'-yx' \end{pmatrix},$$

also im gegenwärtigen Falle

$$\equiv D\cdot F\begin{pmatrix} yz'-zy', & zx'-xz', & xy'-yx' \\ yz'-zy', & zx'-xz', & xy'-yx' \end{pmatrix} \tag{7}$$

ist.

Nach diesen Vorbemerkungen ist es nun leicht, den obigen Satz zu beweisen. $OXYZ$ sei das eine Koordinatensystem mit den Winkeln. a, b, c; $OMM'M''$ das andere mit den Winkeln m, m', m''. OM bilde mit den drei Achsen OX, OY, OZ Winkel, deren Kosinus α, β, γ usw sind. Dann finden folgende sechs Gleichungen Statt:

$$\begin{cases} F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha, & \beta, & \gamma \end{pmatrix} = D, & F_1\begin{pmatrix} \alpha', & \beta', & \gamma' \\ \alpha', & \beta', & \gamma' \end{pmatrix} = D, \\ F_1\begin{pmatrix} \alpha'', & \beta'', & \gamma'' \\ \alpha'', & \beta'', & \gamma'' \end{pmatrix} = D, & F_1\begin{pmatrix} \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{pmatrix} = D\cos m, \\ F_1\begin{pmatrix} \alpha'', & \beta'', & \gamma'' \\ \alpha, & \beta, & \gamma \end{pmatrix} = D\cos m', & F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \end{pmatrix} = D\cos m'', \end{cases} \tag{8}$$

welche allgemein die Beziehung zwischen irgend zwei dreiachsigen Koordinatensystemen ausdrücken. Wenn nun aber außerdem die Gleichungen (4), und folglich auch die (5) und (6) gelten, so erhält man durch Addition der drei ersten Gleichungen in (8):

$$\sin a^2 + \sin b^2 + \sin c^2 = 3D. \tag{9}$$

Ferner ergibt sich aus dem in (7) enthaltenen Theorem:

$$F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha, & \beta, & \gamma \end{pmatrix} F_1\begin{pmatrix} \alpha', & \beta', & \gamma' \\ \alpha', & \beta', & \gamma' \end{pmatrix} - \left[F_1\begin{pmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \end{pmatrix}\right]^2$$
$$\equiv D\cdot F\begin{pmatrix} \beta\gamma'-\beta'\gamma, & \gamma\alpha'-\gamma'\alpha, & \alpha\beta'-\alpha'\beta \\ \beta\gamma'-\beta'\gamma, & \gamma\alpha'-\gamma'\alpha, & \alpha\beta'-\alpha'\beta \end{pmatrix} = D\cdot F\begin{pmatrix} \varepsilon\alpha'', & \varepsilon\beta'', & \varepsilon\gamma'' \\ \varepsilon\alpha'', & \varepsilon\beta'', & \varepsilon\gamma'' \end{pmatrix}$$

oder

$$DD - DD\cos m''^2$$
$$= D(\alpha''\alpha'' + \beta''\beta'' + \gamma''\gamma'' + 2\beta''\gamma''\cos a + 2\gamma''\alpha''\cos b + 2\alpha''\beta''\cos c),$$

also

$$D\sin m^2 = 1 + 2\beta\ \gamma\ \cos a + 2\gamma\ \alpha\ \cos b + 2\alpha\ \beta\ \cos c,$$
$$D\sin m'^2 = 1 + 2\beta'\gamma'\cos a + 2\gamma'\alpha'\cos b + 2\alpha'\beta'\cos c,$$
$$D\sin m''^2 = 1 + 2\beta''\gamma''\cos a + 2\gamma''\alpha''\cos b + 2\alpha''\beta''\cos c,$$

und hieraus durch Addition:

$$D(\sin m + \sin m'^2 + \sin m''^2) = 3.$$

Vergleicht man diese Relation mit der in (9) enthaltenen, so ergibt sich

$$(\sin a^2 + \sin b^2 + \sin c^2)(\sin m^2 + \sin m'^2 + \sin m''^2) = 3\cdot 3,$$

und hieraus

$$\sin a^2 = \sin b^2 = \sin c^2 = \sin m^2 = \sin m'^2 = \sin m''^2 = 1;$$

d. h. alle sechs Koordinatenwinkel müssen rechte Winkel sein.

Bei diesem Beweis wurde natürlich vorausgesetzt, daß D von Null verschieden sei, d. h. daß OX, OY, OZ nicht in einer Ebene enthalten sind.

Göttingen, 15. Juli 1854.

IV.

Bemerkungen zu einer Aufgabe der Wahrscheinlichkeitsrechnung.

[Journal für reine und angewandte Mathematik, Bd. 50, S. 268—271 (1855)].

In einem der früheren Hefte des „Philosophical Magazine“ für 1854 hat G. Boole eine von A. Cayley gegebene Auflösung einer Wahrscheinlichkeitsaufgabe angegriffen. Wiewohl nicht zu zweifeln ist, daß der in diesem Angriff enthaltene Irrtum auch von anderen schon erkannt sei, so kommen doch die folgenden Bemerkungen denen, welche sich für diese schöne Theorie interessieren, vielleicht nicht unerwünscht.

> Die Aufgabe lautet: Gegeben ist die Wahrscheinlichkeit α, daß eine Ursache A (welche ein gewisses Ereignis hervorbringen kann) zur Wirkung kommt, und die Wahrscheinlichkeit p, daß, wenn A wirkt, das Ereignis eintritt; ebenso die Wahrscheinlichkeit β, daß eine Ursache B zur Wirkung gelangt, und die Wahrscheinlichkeit q, daß, wenn B wirkt, das Ereignis eintritt: gesucht wird die Wahrscheinlichkeit u des Ereignisses, unter der Annahme, daß dasselbe von keiner anderen Ursache als von A und B hervorgebracht werden kann.

Cayley löset die Aufgabe auf folgende Weise: Es sei λ die Wahrscheinlichkeit, daß, wenn A wirkt, das Ereignis auch durch A hervorgebracht wird; μ die Wahrscheinlichkeit, daß, wenn B wirkt, das Ereignis auch durch B hervorgebracht wird; dann ist

$$p = \lambda + (1-\lambda)\mu\beta, \quad q = \mu + (1-\mu)\lambda\alpha.$$

Hieraus werden λ, μ bestimmt; und die gesuchte Wahrscheinlichkeit ist

$$u = \lambda\alpha + \mu\beta - \lambda\mu\alpha\beta.$$

Nachdem nun Boole diese Auflösung bei mehreren Spezialisierungen als richtig bewährt fand, sucht er nachzuweisen, daß sie

in dem Falle $p = 1$, $q = 0$ zu einem falschen Resultat führe. Er sagt: Es ist einleuchtend, daß die Wahrscheinlichkeit des Ereignisses in diesem Falle $= \alpha$ sein muß. Denn wenn die Ursache A das Ereignis stets hervorbringt, die Ursache B niemals, und das Eintreten des Ereignisses keiner anderen Ursache zugeschrieben werden kann, so muß die Wahrscheinlichkeit des „Ereignisses gleich der des Eintretens der Ursache A sein“. Da sich gegen diesen Satz natürlich nichts einwenden läßt, und nun die Auflösung, wie sie Cayley darstellt, in diesem Falle entweder $u = 1$ oder $u = \alpha(1-\beta)$ gibt, so schließt Boole, daß die ganze Auflösung fehlerhaft sein müsse, und gibt die Endformel seiner eigenen Auflösung, mit Hinzufügung besonderer Beschränkungen, aus denen sich allerdings für diesen Fall das gewünschte Resultat $u = \alpha$ ableiten läßt.

Man sieht indessen durchaus nicht, wo Cayley einen Fehler gemacht hätte; und in der Tat ist seine Auflösung auch (bis auf gewisse Beschränkungen, durch welche sie erst eindeutig gemacht werden muß) streng richtig, selbst in dem eben angeführten Falle; denn man findet leicht, daß $\alpha(1-\beta)$ mit α übereinstimmt, indem α nichts anderes als Null sein kann. Wäre nämlich die Möglichkeit des Eintretens der Ursache A offen gelassen, d. h. wäre α nicht Null so könnte auch unmöglich die Wahrscheinlichkeit q des Ereignisses (unter der Annahme des Eintretens der Ursache B) gänzlich verschwinden, mag p noch so klein, nur nicht Null sein (in diesem Falle war aber $p = 1$ angenommen). Die gestellte Aufgabe ist daher widersinnig, wenn $q = 0$, α und p dagegen beide von Null verschieden angenommen werden. Dies ergibt sich auch durch einen Blick auf die Gleichungen von Cayley. Wenn man nämlich beachtet, daß μ, $(1-\mu)$, λ, α, der Natur ihrer Bedeutung nach, nicht negativ sein können, so folgt aus der einen Gleichung $q = 0$, sowohl $\mu = 0$, als auch $\lambda\alpha = 0$, und die andere Gleichung geht in $p = \lambda$ über. Ist nun p von Null verschieden (es ist nicht nötig, daß p gerade $= 1$ sei), so muß auch $\alpha = 0$ sein; und die gesuchte Wahrscheinlichkeit u muß stets $= 0$ sein, mag q oder p, oder mögen beide $= 0$ sein; wie man es nicht anders erwarten darf.

Wenn nun aber dieser Vorwurf auch die obige Auflösung nicht trifft, so ist sie doch wenigstens noch unvollständig zu nennen, da die Bedingungen nicht angegeben sind, unter welchen die Aufgabe wirklich einen reellen Sinn hat, und da ferner zu entscheiden übrig

bleibt, welchen der beiden Werte von u, die den obigen Gleichungen genügen, man zu wählen habe. Dies soll hier geschehen.

Man verfährt mit der meisten Symmetrie, wenn man μ aus den Gleichungen für q und u, und ebenso λ aus den Gleichungen für p und u eliminiert. Dies gibt

$$(1) \qquad u - \beta q = (1-\beta)\lambda\alpha, \quad u - \alpha p = (1-\alpha)\mu\beta,$$

und wenn man diese Werte von $\lambda\alpha$, $\mu\beta$ in die Gleichung für u substituiert, so erhält man eine quadratische Gleichung, durch deren Auflösung sich

$$(2) \qquad u = \tfrac{1}{2}(1 - \alpha\beta + \alpha p + \beta q - \varrho)$$

ergibt, worin ϱ die noch zweideutige Quadratwurzel aus

$$\varrho\varrho = (1 - \alpha\beta + \alpha p + \beta q)^2 - 4(1-\beta)\alpha p, \\ - 4(1-\alpha)\beta q - 4\alpha p \cdot \beta q$$

ist. Damit aber die Aufgabe lösbar sei, ist nötig: zuerst, daß ϱ reell, und weiter, daß u (als eine Wahrscheinlichkeit) ein positiver echter Bruch sei. Aber auch dies ist noch nicht genügend; und darin liegt eigentlich das Hauptinteresse der ganzen Aufgabe. Sie würde immer noch ohne Sinn bleiben, wenn die Hilfswahrscheinlichkeiten λ, μ nicht ebenfalls zwischen den Grenzen 0 und 1 enthalten wären, und es ist klar, daß mit diesen letzten Bedingungen auch zugleich die ersten erfüllt werden müssen. Es kommt daher nur darauf an, die Bedingungen aufzustellen, welche ausdrücken, daß λ, μ nicht außerhalb der genannten Grenzen liegen. Dies ist leicht, da man die Werte λ, μ aus den Gleichungen (1) erhält, wenn man in ihnen für u den in (2) gefundenen Ausdruck substituiert. Bei dieser Untersuchung kommt man auf die folgenden Gleichungen:

$$\begin{aligned} \varrho\varrho &= (1 - 2\alpha + \alpha\beta + \alpha p - \beta q)^2 + 4\alpha(1-\alpha)(1-\beta)(1-p) \\ &= (1 - 2\beta + \alpha\beta - \alpha p + \beta q)^2 + 4\beta(1-\beta)(1-\alpha)(1-q) \\ &= (1 - \alpha\beta + \alpha p - \beta q)^2 - 4\alpha(1-\beta)(p - \beta q) \\ &= (1 - \alpha\beta - \alpha p + \beta q)^2 - 4\beta(1-\alpha)(q - \alpha p). \end{aligned}$$

Aus den beiden ersten Formen für $\varrho\varrho$ geht hervor, daß es keiner besonderen Bedingung für die Realität von ϱ bedarf. Setzt man aber die Formen in Verbindung mit den Forderungen für λ, μ, so ergibt sich, daß in dem Ausdrucke (2) für u stets die positive Quadratwurzel für ϱ genommen werden muß. Vergleicht man endlich die beiden letzten Formen für $\varrho\varrho$ mit den Forderungen für λ und μ, so

erhält man, als die einzigen notwendig erforderlichen, aber auch vollständig genügenden Bedingungen, daß die beiden Differenzen

$$(3) \qquad p - \beta q \quad \text{und} \quad q - \alpha p$$

nicht negativ sein dürfen.

Wenn man also, um ein Beispiel zu der Aufgabe zu geben, für α, β, p, q vier beliebige Zahlen innerhalb der Grenzen 0 und 1 angenommen hat, so muß man erst untersuchen, ob sie den beiden Bedingungen in (3) Genüge leisten. Beiläufig bemerkt, kann man bei einer solchen willkürlichen Wahl ebensooft ein widersinniges Beispiel wie ein passendes treffen; denn der Wert des vierfachen Integrals $\int\int\int\int d\alpha\, d\beta\, dp\, dq$ ist $= 1$, wenn man die Integrationen über alle Werte der Veränderlichen zwischen 0 und 1 ausdehnt; dagegen $= \frac{1}{2}$, wenn man diejenigen Werte ausschließt, welche den Bedingungen (3) nicht Genüge leisten. Man kann sich hiervon auch leicht durch geometrische Betrachtungen überzeugen.

In dem von Boole untersuchten Falle $q = 0$ reduzieren sich die Bedingungen (3) auf $\alpha p = 0$; dann wird $\varrho = 1 - \alpha\beta$, und folglich $u = 0$, ganz in Übereinstimmung mit den obigen Resultaten. Auch der Fall $\alpha = 0$ ist von Interesse. Dann ist $\varrho = 1 - \beta q$, und folglich $u = \beta q$ offenbar das richtige Resultat. Hierbei ist natürlich u von q unabhängig, und dennoch bleibt die Bedingung $p - \beta q \geqq 0$ in voller Kraft, und obgleich zur Bestimmung von u auf den Wert von p gar kein Gewicht fällt, so wäre es doch widersinnig, die Wahrscheinlichkeit p des Ereignisses unter der Annahme, daß die Ursache A zur Wirkung gelangt, kleiner als die Wahrscheinlichkeit βq anzunehmen, wenn auch diese Annahme durch die Bestimmung $\alpha = 0$ faktisch verboten ist. Und mit dieser Bemerkung, die, wie ich glaube, dazu geeignet ist, auf die Eigentümlichkeit dieser Art von Aufgaben ein frappantes Licht zu werfen, will ich meine Betrachtungen abbrechen.

Göttingen, 22. Juli 1854.

V.

Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus.

[Journal für reine und angewandte Mathematik, Bd. 54, S. 1—26 (1857)].

Es ist meine Absicht, dem in der Überschrift bezeichneten Gegenstand, welcher, von Gauß[*)] zuerst angeregt, später mit Erfolg von Galois, Serret, Schönemann[**)] wieder aufgenommen ist, eine einfache zusammenhängende Darstellung zu widmen, welche sich streng an die Analogie mit den Elementen der Zahlentheorie binden soll. Diese ist in der Tat so durchgreifend, daß es mit Ausnahme einiger unserem Gegenstand eigentümlicher Untersuchungen nur einer Wortänderung in den Beweisen der Zahlentheorie bedarf. Ich folge genau dem Gange, welchen Dirichlet in seinen Vorlesungen über die Zahlentheorie (oder in seiner kurzen Darstellung der Theorie der komplexen Zahlen im 24. Bande dieses Journals) eingeschlagen hat. In Rücksicht hierauf wird man es nicht tadeln, daß ich meist nur die Hauptmomente der Beweise hervorhebe, da größere Ausführlichkeit für den Kenner der Zahlentheorie, welche hier vorausgesetzt wird, ermüdend sein müßte.

Die hier dargestellte Theorie, deren Erweiterungen auf der Hand liegen, ist vielfacher Anwendungen fähig, namentlich auf die Algebra, wie ich in einer späteren Abhandlung zeigen werde; zunächst schien es mir zweckmäßig, dieselbe ohne alle Einmischung algebraischer Prinzipien abzuhandeln.

Gebiet der Untersuchung; Definitionen und Fundamentalsätze.

1.

Unter einer Funktion einer Variabeln x wird hier immer eine ganze rationale Funktion von x verstanden, deren Koeffizienten reelle ganze Zahlen sind. Es werden die Eigenschaften solcher Funktionen

[*) Man vgl. C. F. Gauß' Werke, Bd. 2, S. 212—240.]

[**) E. Galois: Oeuvres mathématiques, S. 15—23. I. A. Serret: Cours d'algèbre, 2. Ausg., S. 343—370. Th. Schönemann, Journ. f. Math., Bd. 31, S. 269—325 und Bd. 32, S. 93—105, 1846.]

untersucht in bezug auf einen Modulus, der eine reelle Primzahl p ist. Zwei Funktionen A, B heißen kongruent in bezug auf den Modul p, in Zeichen

$$A \equiv B \pmod{p},$$

wenn sämtliche Koeffizienten der nach Potenzen von x geordneten Differenz $A - B$ durch p teilbar sind, oder, was dasselbe sagt, wenn die Koeffizienten gleich hoher Potenzen von x in den beiden Funktionen paarweise einander kongruent sind in bezug auf den Modulus p. Es ist daher diese Kongruenz nur ein Ausdruck für die Identität

$$A = B + p \cdot C,$$

in welcher C eine beliebige Funktion bedeutet. Hieraus gehen sogleich die beiden folgenden Sätze hervor:

Man darf in jeder Kongruenz zwischen zwei Funktionen die Variabeln x durch eine beliebige Funktion von x ersetzen.

Man darf jede Kongruenz beliebig oft nach der Variabeln x differentiieren.

Ebenso leuchten folgende Sätze ein, in welchen der Modulus p unveränderlich beibehalten wird:

Ist $A \equiv A'$, $B \equiv B'$, so ist auch $A \pm B \equiv A' \pm B'$, ferner $AB \equiv A'B'$, ferner $A^n \equiv A'^n$, wo n eine positive ganze Zahl bedeutet; und allgemein: Sind die beiden Seiten einer Kongruenz ganze rationale Funktionen (mit ganzen Zahlkoeffizienten) von einer Reihe von Funktionen A, B, C etc. der Variabeln x, so darf man dieselben (an beliebigen Stellen) durch ihnen resp. kongruente Funktionen A' B', C' etc. ersetzen.

2.

Der Exponent der höchsten Potenz von x in einer Funktion, deren Koeffizient nicht durch den Modul teilbar ist, heiße der Grad der Funktion. Aus dieser Definition, welche für alle Funktionen gilt, die nicht $\equiv 0 \pmod{p}$ sind, ergibt sich, daß alle die unendlich vielen einander kongruenten Funktionen einen und denselben Grad haben. Ist ferner α der Grad von A, β der Grad von B, so ist $\alpha + \beta$ der Grad von AB; denn das Produkt zweier durch eine Primzahl p nicht teilbaren Zahlen-Koeffizienten ist ebenfalls nicht teilbar

durch p. Hieraus folgt weiter: Ist $AB \equiv 0 \pmod{p}$, so ist mindestens eine der beiden Funktionen A, $B \equiv 0 \pmod{p}$; und ferner: Ist $AB \equiv A'B'$, und $A \equiv A'$ nicht $\equiv 0 \pmod{p}$, so ist $B \equiv B' \pmod{p}$; denn es ist $AB \equiv AB'$, oder $A(B - B') \equiv 0 \pmod{p}$. Dieser Satz gibt daher die Bedingung für die Berechtigung zur Division einer Kongruenz durch eine andere. Ferner ist leicht zu sehen, daß die Anzahl der einander nicht kongruenten (inkongruenten) Funktionen vom Grade α gleich $(p-1)p^{\alpha}$ ist; denn der Koeffizient von x^{α} kann $p-1$, der jeder niedrigeren Potenz kann p nach dem Modul p inkongruente Werte haben, und der Koeffizient jeder höheren Potenz ist $\equiv 0 \pmod{p}$. Dies Resultat gilt auch für den Fall $\alpha = 0$, insofern bei den Funktionen, welche $\equiv 0$ sind, überhaupt von einem Grade keine Rede ist.

3.

Sind A, B, C drei solche Funktionen von x, daß $A \equiv BC \pmod{p}$, so heißen B, C (oder alle diesen kongruente Funktionen) Divisoren oder Faktoren von A (oder jeder mit A kongruenten Funktion) in bezug auf den Modul p. Gleichbedeutend sind die Ausdrücke: A ist ein Multiplum von B, C; oder: A ist teilbar durch B, C. Diese Teilbarkeit nach einem Modulus ist natürlich nicht mit der algebraischen Teilbarkeit zu verwechseln, obwohl aus der letzteren stets die erstere folgt. Offenbar kann der Grad eines Divisors B von A nicht höher sein als der Grad von A. Jede Funktion ist teilbar durch jede der $p-1$ inkongruenten Funktionen vom Grade Null; denn jede der letzteren ist einer durch p nicht teilbaren Zahl a kongruent; bestimmt man nun a' so, daß $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a \cdot a'A$, wo A jede beliebige Funktion bedeutet. Außer diesen $p-1$ Funktionen vom Grade Null hat keine andere die Eigenschaft, Divisor von jeder beliebigen Funktion zu sein; denn eine Funktion, deren Grad höher als Null ist, kann nicht mehr Divisor der Funktionen vom Grade Null sein. Man kann deshalb (zufolge der Analogie mit ähnlichen Untersuchungen) diese $p-1$ inkongruenten Funktionenklassen vom Grade Null Einheiten nennen.

Man kann jede Funktion vom Grade α kongruent setzen dem Produkte aus einer bestimmten Funktion vom Grade Null und einer Funktion vom Grade α, in welcher der Koeffizient von $x^{\alpha} \equiv 1 \pmod{p}$ ist (solche Funktionen sollen primäre heißen); denn ist a der durch

p nicht teilbare Koeffizient von x^{α} in A, und $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a \cdot a'A$, worin $a'A$ eine primäre Funktion ist. — Die Anzahl der inkongruenten primären Funktionen vom Grade α ist gleich p^{α}.

Aus der Definition der Multipla ergeben sich unmittelbar die beiden folgenden Sätze: Ist eine Funktion ein Multiplum von einer zweiten, diese ein Multiplum von einer dritten, diese von einer vierten usw., so ist jede frühere in der Reihe dieser Funktionen ein Multiplum von jeder späteren. — Die Summe und die Differenz zweier Multipla von einer Funktion sind selbst wieder Multipla derselben Funktion.

4.

Von großer Bedeutung für die späteren Untersuchungen ist folgende Aufgabe: Zu untersuchen, ob zwei gegebene Funktionen A, A' nach dem Modul p gemeinschaftliche Divisoren haben.

Zunächst läßt sich zeigen, daß man stets eine Kongruenz von der Form

$$A \equiv QA' + A'' \pmod{p}$$

aufstellen kann, in welcher Q, A'' zwei neue Funktionen sind, deren letztere A'' einen niedrigeren Grad als A' hat, oder gar $\equiv 0 \pmod{p}$ ist. Denn es sei α der Grad von A, α' der von A'; im Falle nun $\alpha < \alpha'$ ist, braucht man nur $Q \equiv 0$, $A'' \equiv A \pmod{p}$ zu setzen; ist aber $\alpha \geqq \alpha'$, so kann man die Zahl q so bestimmen, daß $A - qx^{\alpha-\alpha'} \cdot A'$ von niedrigerem Grade α_1 als α ist; ist dann α_1 auch $< \alpha'$, so ist das Ziel schon erreicht, wenn man $Q \equiv qx^{\alpha-\alpha'}$ setzt; ist aber $\alpha_1 \geqq \alpha'$, so verfährt man mit der Funktion $A - qx^{\alpha-\alpha'} \cdot A'$ ebenso, wie bei dem ersten Schritte mit A; man bestimmt q_1 so, daß $A - qx^{\alpha-\alpha'} \cdot A' - q_1 x^{\alpha_1-\alpha'} \cdot A'$ von niedrigerem Grade ist als α_1 u. s. f., bis man zu einer Funktion von niedrigerem Grade als α' gelangt, was nach einer endlichen Anzahl von Operationen geschehen muß Man setzt dann

$$Q \equiv qx^{\alpha-\alpha'} + q_1 x^{\alpha_1-\alpha'} + \text{etc.} \pmod{p},$$

und dann ist $A'' \equiv A - QA'$ von niedrigerem Grade als α'. W. Z. B. W.

Aus der so gebildeten Kongruenz folgt nun unmittelbar, daß jeder gemeinschaftliche Divisor von A, A' auch Divisor von A'', und umgekehrt, daß jeder gemeinschaftliche Divisor von A', A'' auch

Divisor von A sein muß. Man braucht daher die Operation nur fortzusetzen und ein System von Kongruenzen zu bilden:

$$\left.\begin{aligned} A &\equiv QA' + A'' \\ A' &\equiv Q'A'' + A''' \\ &\cdots\cdots\cdots \\ A^{(\nu-2)} &\equiv Q^{(\nu-2)}A^{(\nu-1)} + A^{(\nu)} \\ A^{(\nu-1)} &\equiv Q^{(\nu-1)}A^{(\nu)} \end{aligned}\right\} \text{(mod. } p\text{)},$$

in welchem die Grade α', α'' etc. eine abnehmende Reihe bilden, woraus von selbst folgt, daß nach einer endlichen Anzahl von Operationen es geschehen muß, daß eine Funktion $A^{(\nu-1)}$ durch die nächstfolgende $A^{(\nu)}$ teilbar ist. Schreitet man von der ersten bis zur letzten Kongruenz fort, so ergibt sich, daß jeder gemeinschaftliche Divisor von A, A' auch Divisor von $A^{(\nu)}$ sein muß; verfolgt man den umgekehrten Weg, so ergibt sich, daß $A^{(\nu)}$ Divisor aller vorhergehenden Funktionen und folglich auch gemeinschaftlicher Divisor der beiden Funktionen A, A' ist. Es heiße daher $A^{(\nu)}$ ein größter gemeinschaftlicher Divisor von A, A'. Multipliziert man $A^{(\nu)}$ mit einer beliebigen Funktion vom Grade Null (mit einer Einheit), so hat das Produkt offenbar dieselbe Eigenschaft wie $A^{(\nu)}$; es gibt daher $p-1$ inkongruente größte gemeinschaftliche Divisoren desselben Grades, und ein einziger unter diesen ist primär.

Drückt man vermöge der vorletzten Kongruenz $A^{(\nu)}$ durch $A^{(\nu-1)}$ und $A^{(\nu-2)}$, diese vermöge der vorhergehenden Kongruenzen durch die vorhergehenden Funktionen aus, so kommt man zuletzt auf eine Kongruenz von der Form

$$G \cdot A + G' \cdot A' \equiv A^{(\nu)} \text{ (mod. } p\text{)},$$

welche also stets möglich ist, wenn $A^{(\nu)}$ größter gemeinschaftlicher Divisor von A, A' ist.

5.

Ist der größte gemeinschaftliche Divisor $A^{(\nu)}$ der Funktionen A, A' vom Grade Null (also $\equiv 1$ (mod. p), wenn er primär ist), so heißen A, A' relativ prim gegeneinander.

Aus dieser Definition folgt der Hauptsatz: Sind A, A' zwei relative Primfunktionen, und ist M eine beliebige Funktion, so ist jeder gemeinschaftliche Divisor der beiden Funktionen AM, A' zugleich gemeinschaftlicher Divisor von M, A'. Denn multipliziert man

die Reihe der Kongruenzen, durch welche die Funktionen A, A', $A'', \cdots, A^{(\nu)}$ zusammenhängen, mit M, so ergibt sich unmittelbar, daß jeder gemeinschaftliche Divisor von AM, A' auch Divisor von $A''M$, $A'''M, \cdots, A^{(\nu)}M$ und folglich auch (da der Annahme nach $A^{(\nu)}$ vom Grade Null ist) von M, also gemeinschaftlicher Divisor von M, A' ist. (Dies folgt auch unmittelbar aus der Kongruenz $GAM + G'MA' \equiv A^{(\nu)}M$.)

Die wichtigsten Spezialfälle dieses Satzes sind die folgenden: Ist auch M relativ prim gegen A', so ist der größte gemeinschaftliche Divisor von M und A', und folglich auch der von AM und A' eine Funktion vom Grade Null, d. h. AM und A' sind relativ prim gegeneinander; und hieraus ergibt sich der Satz: Wenn zwei Reihen von Funktionen so beschaffen sind, daß jede Funktion der einen Reihe relativ prim gegen jede Funktion der anderen Reihe ist, so ist das Produkt aus sämtlichen Funktionen der einen Reihe relativ prim gegen das Produkt aus sämtlichen Funktionen der anderen Reihe.

Eine zweite Spezialisierung ist die folgende. Ist wieder A relativ prim gegen A', und ist AM durch A' teilbar, so ist A' als gemeinschaftlicher Divisor von AM, A' auch gemeinschaftlicher Divisor von M, A', also Divisor von M.

Hieraus folgt weiter: Ist jede der Funktionen A, B, C etc. relativ prim gegen jede der anderen, und ist ferner eine Funktion M durch jede der Funktionen A, B, C etc. teilbar, so ist M auch durch das Produkt $ABC\cdots$ teilbar. Denn der Annahme nach ist $M \equiv GA$ durch B teilbar, folglich ist, da A relativ prim gegen B ist, $G \equiv HB$, also $M \equiv HAB$ usw.

6.

Eine Funktion, welche nach dem Modul p nur solche Divisoren hat, die entweder ihr selbst oder Funktionen vom Grade Null (d. h. Einheiten) oder Produkten aus beiden kongruent sind (denn jede Funktion hat alle diese Divisoren), heißt (irreduktibel oder) eine Primfunktion nach dem Modul p; jede andere heißt (reduktibel oder) zusammengesetzt. Es leuchtet ein, daß eine beliebige Funktion entweder durch eine bestimmte Primfunktion teilbar, oder relativ prim gegen dieselbe ist. Ist daher ein Produkt AB durch eine Primfunktion P teilbar, so ist mindestens einer der Faktoren A, B für sich allein durch P teilbar; denn ist A nicht durch P

teilbar, so ist A relativ prim gegen P, und folglich B durch P teilbar. Derselbe Satz gilt für ein Produkt aus beliebig vielen Funktionen.

Es leuchtet ein, daß jede beliebige Funktion M sich darstellen läßt als Produkt aus Potenzen von Primfunktionen, welche untereinander inkongruent sind, und deren Anzahl eine endliche ist (wenn der Grad von M endlich ist); und zwar ist wesentlich nur eine einzige solche Darstellung möglich; d. h. wenn in der einen Zerfällung a Faktoren vorkommen, welche einer und derselben Primfunktion A kongruent sind, so werden auch in jeder anderen Zerfällung a Faktoren vorkommen, welche derselben Primfunktion A oder einem Produkt aus A in eine Einheit kongruent sind. Man kann die Primfunktionen sämtlich primär annehmen; ist dann

$$M \equiv z A^a B^b C^c \cdots \pmod{p},$$

wo z eine Einheit, A, B, C etc. inkongruente primäre Primfunktionen, a, b, c etc. positive ganze Zahlen bedeuten, so ist jeder primäre Divisor D von M von der Form

$$D \equiv A^{a'} B^{b'} C^{c'} \cdots \pmod{p},$$

wo a', b', c' etc. die Null oder positive ganze Zahlen bedeuten, welche resp. nicht größer als a, b, c etc. sind. Die Anzahl der inkongruenten primären Divisoren von M ist demnach $= (a+1)(b+1)(c+1)\cdots$.

Wenn eine Funktion M einen Divisor D $m$mal enthält, d. h. wenn $M \equiv G D^m \pmod{p}$, so folgt durch Differentiation

$$\frac{dM}{dx} \equiv \left(G \cdot m \frac{dD}{dx} + D \cdot \frac{dG}{dx}\right) D^{m-1} \pmod{p};$$

also enthält die Derivierte von M denselben Divisor D mindestens $(m-1)$mal (sie kann ihn auch öfter enthalten). Ist daher eine Funktion relativ prim gegen ihre erste Derivierte, so ist sie einem Produkt aus lauter inkongruenten Primfunktionen kongruent.

Allgemeine Sätze über die Kongruenzen, welche sich auf einen doppelten Modulus beziehen.

7.

Die vorhergehenden Sätze entsprechen vollständig denen über die Teilbarkeit der Zahlen in der Weise, daß das ganze System der unendlich vielen einander nach dem Modulus p kongruenten Funktionen

einer Variabeln sich hier verhält, wie eine einzige bestimmte Zahl in der Zahlentheorie, indem jede einzelne Funktion eines solchen Systems jede beliebige andere desselben Systems in jeder Beziehung vollständig ersetzt; eine solche Funktion ist der Repräsentant der ganzen Klasse; jede Klasse hat ihren bestimmten Grad, ihre bestimmten Divisoren usw., und alle diese Merkmale kommen jedem einzelnen Gliede einer Klasse in derselben Weise zu. Das System der unendlich vielen inkongruenten Klassen — unendlich vielen, da der Grad unbegrenzt wachsen kann — entspricht der Reihe der ganzen Zahlen in der Zahlentheorie. Der Kongruenz der Zahlen entspricht hier Kongruenz von Funktionenklassen nach einem doppelten Modulus in der folgenden Weise.

Zwei Funktionenklassen oder deren Repräsentanten A, B heißen kongruent in bezug auf die Funktionenklasse, deren Repräsentant M, in Zeichen

$$A \equiv B \pmod{p, M} \quad \text{oder} \quad A \equiv B \pmod{M},$$

wenn die Differenz $A - B$ nach dem Modul p durch M teilbar ist.

Eine solche Kongruenz zweier Funktionen A, B in bezug auf eine dritte M ist also nur ein anderer Ausdruck für die Kongruenz

$$A \equiv B + CM \pmod{p},$$

und hieraus ergibt sich, daß man A, B, M durch beliebige Funktionen A', B', M' ersetzen kann, welche resp. jenen nach dem Modul p kongruent sind. Ferner leuchtet ein, daß man in einer solchen Kongruenz die Variable x in den drei Funktionen A, B, M durch eine beliebige Funktion von x ersetzen kann.

Aus der Definition dieser Kongruenzen ergeben sich folgende Sätze: Ist $A \equiv A' \pmod{M}$, $B \equiv B' \pmod{M}$, so ist $A \pm B \equiv A' \pm B' \pmod{M}$, ferner $AB \equiv A'B' \pmod{M}$, ferner $A^n \equiv A'^n \pmod{M}$, wo n eine positive ganze Zahl bedeutet. Und allgemein: Sind die beiden Seiten einer Kongruenz nach dem Modulus M ganze rationale Funktionen (mit ganzen Zahlenkoeffizienten) von Funktionen, so darf man jede der letzteren (an beliebigen Stellen) durch eine andere ersetzen, welche ihr nach dem Modul M kongruent ist.

Ist ferner $AB \equiv 0 \pmod{M}$ und A relativ prim gegen M, so ist auch $B \equiv 0 \pmod{M}$; allgemeiner: ist $AB \equiv A'B' \pmod{M}$ und $A \equiv A' \pmod{M}$ und A relativ prim gegen M, so ist auch $B \equiv B' \pmod{M}$.

Sind endlich A, A' kongruent nach dem Modul M, und beide von niedrigerem Grade als M, so müssen A, A' auch nach dem einfachen Modul p einander kongruent sein.

8.

Man kann nun ein System von Funktionen aufstellen, so daß irgend eine beliebige Funktion einer von diesen Funktionen, aber auch nur einer einzigen nach dem Modulus M kongruent ist. Es sei A eine beliebige Funktion, so kann man, wie früher gezeigt ist, stets eine Kongruenz von der Form

$$A \equiv QM + A' \pmod{p}$$

aufstellen, in welcher A' von niedrigerem Grade ist als M. Stellt man daher sämtliche nach dem Modul p inkongruente Funktionen von niedrigerem Grade als M auf, so ist jede beliebige Funktion einer von diesen nach dem Modulus M kongruent, aber auch nur einer einzigen von ihnen, weil zwei nach dem Modul p inkongruente Funktionen von niedrigerem Grade als M auch in bezug auf M inkongruent sind. Ist μ der Grad von M, so ist p^μ die Anzahl dieser Funktionen, welche also ein System der verlangten Art bilden. Jedes solche System heiße ein vollständiges System inkongruenter Funktionen in bezug auf den Modul M. Multipliziert man jedes Glied eines solchen Systems mit einer und derselben Funktion, welche gegen den Modulus M relativ prim ist, so bilden die Produkte wieder ein solches System, wie sich leicht beweisen läßt.

9.

Seien N, N' etc. beliebige Funktionen, deren erste durch den Modulus M nicht teilbar ist, ferner n eine positive ganze Zahl, so heißt die Bedingung

$$Ny^n + N'y^{n-1} + \text{etc.} + N^{(n)} \equiv 0 \pmod{M}$$

eine Kongruenz vom Grade n mit einer Unbekannten y; und jede Funktion, welche für y substituiert diese Bedingung befriedigt, heißt eine Wurzel derselben. Ist eine solche Wurzel gefunden, so ist jede mit ihr nach dem Modul M kongruente Funktion ebenfalls eine Wurzel; die Hauptaufgabe ist daher, sämtliche nach dem Modul M inkongruente Wurzeln zu finden.

Wir betrachten zunächst die Kongruenz ersten Grades, welche auf die Form

$$Ay \equiv B \pmod{M}$$

gebracht werden kann. Nehmen wir zuerst an, A sei relativ prim gegen den Modul M, so gibt es (zufolge der Schlußbemerkung des vorigen Artikels) in jedem vollständigen System inkongruenter Funktionen eine, aber auch nur eine Funktion y, für welche $Ay \equiv B$ wird; die Kongruenz hat daher in diesem Falle nur eine einzige Wurzel (d. h. alle Wurzeln sind dieser einen nach M kongruent). Hat aber A mit M den größten gemeinschaftlichen Divisor D, so muß, wenn die Kongruenz lösbar sein soll, auch B durch D teilbar sein; in diesem Falle sei $A \equiv A'D$, $B \equiv B'D$, $M \equiv M'D \pmod{p}$, so folgt aus der obigen Kongruenz

$$A'y \equiv B' \pmod{M'}$$

und umgekehrt jene aus dieser. Da nun hierin A' relativ prim gegen den Modulus M', so hat die letztere Kongruenz eine, aber auch nur eine einzige Wurzel W nach dem Modulus M'. Alle Wurzeln der ersten Kongruenz sind daher in der Form

$$y \equiv W + HM' \pmod{p}$$

enthalten, und alle in dieser Form enthaltenen Funktionen y sind auch Wurzeln der ersten Kongruenz; und zwei in dieser Form enthaltene Funktionen $W + HM'$, $W + GM'$ sind stets, aber auch nur dann nach dem Modulus M inkongruent, wenn H und G nach dem Modulus D inkongruent sind. Mithin hat in diesem Falle die erste Kongruenz ebensoviel nach M inkongruente Wurzeln, als es nach dem Modul D inkongruente Funktionen gibt, also p^δ, wenn δ der Grad von D ist.

Für die späteren Untersuchungen ist auch noch die Lösung der folgenden Aufgabe wichtig: Seien M, N relativ prim gegeneinander; es soll die allgemeine Form der Funktionen y gefunden werden, welche die beiden Kongruenzen $y \equiv A \pmod{M}$, $y \equiv B \pmod{N}$ befriedigen. Aus der ersten Form folgt $y \equiv A + zM \pmod{p}$, wo z eine beliebige Funktion ist, welche aber der Bedingung $A + zM \equiv B \pmod{N}$ genügen muß; diese Kongruenz hat nach dem Vorhergehenden eine einzige Wurzel nach dem Modul N, und es folgt daraus die allgemeine Lösung $y \equiv W \pmod{MN}$.

10.

Hat man ein vollständiges System inkongruenter Funktionen in bezug auf den Modul M aufgestellt, so drängen sich die beiden folgenden Fragen auf: Wieviele dieser Funktionen haben mit M einen bestimmten Divisor D gemeinschaftlich? und: Wieviele unter diesen haben D zum größten gemeinschaftlichen Divisor mit M? — Die Beantwortung dieser Fragen ist unabhängig von der besonderen Wahl des vollständigen Systems inkongruenter Funktionen, da jede von zwei einander nach M kongruenten Funktionen denselben größten Divisor mit M gemeinschaftlich hat, wie die andere.

Die erste Frage ist im vorigen Artikel schon mit beantwortet; zwei Funktionen GD, HD sind stets, aber auch nur dann nach dem Modul $M \equiv ND$ inkongruent, wenn G, H nach dem Modul N inkongruent sind; ist daher ν der Grad von N, so gibt es $p^{\nu} = p^{\mu-\delta}$ nach M inkongruente Funktionen, welche mit M den Divisor D gemeinsam haben.

Irgend eine dieser Funktionen GD hat ferner stets, aber auch nur dann D zum größten gemeinschaftlichen Divisor mit M, wenn G relativ prim gegen N ist. Bezeichnen wir daher allgemein mit $\varphi(A)$ die Anzahl der in bezug auf A inkongruenten Funktionen, welche gegen A relativ prim sind, so ist die zweite von uns gesuchte Anzahl $= \varphi(N)$.

Schreiben wir nun sämtliche Divisoren von M auf, mit der Beschränkung, daß keiner von ihnen dem Produkt aus einem anderen in eine Einheit kongruent ist, also z. B. sämtliche inkongruente primäre Divisoren von M; so hat irgend eine Funktion einen dieser Divisoren, aber auch nur einen einzigen zum größten gemeinschaftlichen Divisor mit M, woraus in Verbindung mit dem Vorhergehenden der Satz

$$\Sigma\varphi(N) = p^{\mu}$$

folgt, wo das Summenzeichen sich auf ein so definiertes System von Divisoren N der Funktion M bezieht.

Aus diesem Satze ergibt sich sogleich der Ausdruck für $\varphi(M)$ in dem Falle, wenn M einer Potenz A^{α} einer einzigen Primfunktion kongruent ist. Ist α der Grad von A, so hat man zufolge des Satzes

$$\varphi(1) + \varphi(A) + \varphi(A^2) + \cdots + \varphi(A^{\alpha-1}) + \varphi(A^{\alpha}) = p^{\alpha\alpha},$$

und ebenso

$$\varphi(1) + \varphi(A) + \varphi(A^2) + \cdots + \varphi(A^{\alpha-1}) = p^{\alpha(\alpha-1)};$$

folglich

$$\varphi(A^{\alpha}) = p^{\alpha\alpha} - p^{\alpha(\alpha-1)} = p^{\alpha\alpha}\left(1 - \frac{1}{p^{\alpha}}\right).$$

Auf diesen Fall wird aber jeder andere durch folgenden Satz zurückgeführt: Sind M, N relativ prim gegeneinander, so ist $\varphi(MN) = \varphi(M)\varphi(N)$; welcher sich so beweisen läßt. Man bilde das vollständige System der gegen M relativ primen und nach M inkongruenten Funktionen G, deren Anzahl $\varphi(M)$; ebenso bilde man in bezug auf den Modulus N ein entsprechendes System von $\varphi(N)$ Funktionen H, und in bezug auf MN ein solches System von $\varphi(MN)$ Funktionen F. Es ergibt sich dann mit Hilfe der Schlußbemerkung des vorigen Artikels, daß allen $\varphi(M)\varphi(N)$ Kombinationen von Kongruenzen $y \equiv G$ (mod. M) und $y \equiv H$ (mod. N) eine, aber auch nur eine Lösung von der Form $y \equiv F$ (mod. MN), und umgekehrt jeder der $\varphi(MN)$ Kongruenzen der letzteren Form eine, aber auch nur eine Kombination der ersteren Form entspricht; woraus unmittelbar $\varphi(MN) = \varphi(M)\varphi(N)$ folgt.

Seien nun A, B, C etc. sämtliche einander inkongruente Primfunktionen resp. von den Graden α, β, γ etc., welche in einer Funktion M vom Grade μ als Faktoren enthalten sind, und zwar so, daß keine dieser Primfunktionen etwa einem Produkt aus einer anderen von ihnen in eine Einheit kongruent ist, was man z. B. dadurch erreicht, daß man sie alle als primär annimmt; dann ist

$$\varphi(M) = p^{\mu}\left(1 - \frac{1}{p^{\alpha}}\right)\left(1 - \frac{1}{p^{\beta}}\right)\left(1 - \frac{1}{p^{\gamma}}\right)\cdots,$$

wie sich aus den vorhergehenden Sätzen leicht ergibt.

11.

Man schreibe das vollständige System der gegen M relativ primen und in bezug auf M inkongruenten Funktionen auf, deren Anzahl wir mit $\varphi(M)$ bezeichnet haben. Multipliziert man sie sämtlich mit einer und derselben F, welche sich in ihrem Komplex findet, so bilden die $\varphi(M)$ Produkte wieder ein solches System, so daß jedes Glied des einen Systems einem, aber auch nur einem einzigen Gliede des anderen Systems nach dem Modul M kongruent

ist. Multipliziert man daher alle diese $\varphi(M)$ Kongruenzen miteinander, und berücksichtigt, daß das Produkt der $\varphi(M)$ gegen M relativ primen Funktionen ebenfalls gegen M relativ prim ist, so erhält man den Satz

$$F^{\varphi(M)} \equiv 1 \pmod{M},$$

welcher dem verallgemeinerten Satze von Fermat in der Zahlentheorie entspricht.

Ist M eine Primfunktion P vom Grade π, so ist $\varphi(P) = p^\pi - 1$, und folglich

$$F^{p^\pi - 1} \equiv 1 \pmod{P},$$

wenn F eine durch P nicht teilbare Funktion bedeutet, und allgemein ist ohne alle Beschränkung für F

$$F^{p^\pi} \equiv F \pmod{P},$$

wie unmittelbar einleuchtet.

Hieraus folgt, daß die Auflösung der Kongruenz ersten Grades

$$Ay \equiv B \pmod{M}$$

in dem Falle, wo A gegen M relativ prim ist, durch die Formel

$$y \equiv BA^{\varphi(M)-1} \pmod{M}$$

gegeben wird.

12.

Von nun an wenden wir uns zu dem besonderen Falle, in welchem der Modulus der Kongruenzen eine Primfunktion P vom Grade π ist. Dann besteht folgender Satz: Eine Kongruenz $F(y) = Ny^n + N'y^{n-1} + \text{etc.} \equiv 0 \pmod{P}$ kann nicht mehr als n nach dem Modul P inkongruente Wurzeln haben. — Beweis: Wir nehmen an, der Satz sei für Kongruenzen vom Grade $n-1$ bewiesen, und zeigen, daß er dann auch für Kongruenzen vom Grade n gilt. Gesetzt dann, unsere Kongruenz $n$ten Grades hätte mehr als n inkongruente Wurzeln, also mindestens $n+1$. Sei W eine derselben, so ist für jede andere von dieser verschiedene y

$$F(y) - F(W) = (y - W)F_1(y) \equiv 0 \pmod{P},$$

wo $F_1(y)$ ein Polynom vom Grade $n-1$ ist, und folglich hätte, da $y - W$ nicht $\equiv 0 \pmod{P}$ sein kann, die Kongruenz $F_1(y) \equiv 0 \pmod{P}$ vom Grade $n-1$ gegen unsere Annahme mindestens n Wurzeln. — Nun ist der Satz für die Kongruenz ersten Grades schon früher bewiesen, folglich gilt er für jeden Grad.

Hat aber unsere Kongruenz $n$ten Grades wirklich n inkongruente Wurzeln W, W', W'' etc., so müssen die Koeffizienten gleich hoher Potenzen von y in den beiden Polynomen

$$F(y) = Ny^n + N'y^{n-1} + \cdots,$$
$$G(y) = N(y - W)(y - W')(y - W'') \cdots$$

einander paarweise nach dem Modul P kongruent sein; denn sonst hätte die Kongruenz

$$F(y) - G(y) \equiv 0 \pmod{P},$$

deren Grad jedenfalls niedriger als n ist, n inkongruente Wurzeln sie darf daher gar keinen Grad haben, d. h. alle Koeffizienten derselben müssen durch P teilbar sein.

Nun haben wir im vorigen Artikel gesehen, daß die Kongruenz

$$y^{p^\pi - 1} \equiv 1 \pmod{P}$$

durch jede der $p^\pi - 1$ inkongruenten gegen P relativ primen Funktionen F befriedigt wird; mithin ist identisch

$$y^{p^\pi - 1} - 1 \equiv \Pi(y - F) \pmod{P},$$

wo $\Pi(y - F)$ das Produkt aus allen Faktoren $(y - F)$ bezeichnet Daraus folgt als Analogon zu dem Satze von Wilson in der Zahlentheorie das Theorem

$$\Pi(F) + 1 \equiv 0 \pmod{P},$$

wo $\Pi(F)$ das Produkt aus allen $p^\pi - 1$ nach P inkongruenten und durch P nicht teilbaren Funktionen bedeutet. Und umgekehrt muß P eine Primfunktion sein, wenn dieser Satz gilt; denn hätte P einen von einer Einheit verschiedenen Divisor D von niedrigerem Grade als π, so fände sich unter den $p^\pi - 1$ Funktionen F eine (im Art. 10 bestimmte) Anzahl solcher, welche mit P den Divisor D gemeinsam hätten; daraus würde aber folgen, daß auch die Einheit diesen Divisor hätte, was unmöglich ist.

Potenzreste.

13.

Sei M wieder ein beliebiger Modulus, A relativ prim gegen denselben, so sind auch alle Glieder der Reihe $1, A, A^2 \ldots$ in inf. relativ prim gegen M; es muß daher geschehen, daß $A^{m+n} \equiv A^m \pmod{M}$ und folglich $A^n \equiv 1 \pmod{M}$ wird. Sei a der kleinste

Wert von n, für welchen dies eintritt, so sagt man: A gehört zum Exponenten a; und es sind die a Funktionen

$$1, \quad A, \quad A^2, \quad \cdots, \quad A^{a-1}$$

inkongruent nach dem Modul M, woraus folgt, daß jede Zahl n, für welche $A^n \equiv 1 \pmod{M}$ wird, durch a teilbar ist. Zufolge des Art. 11 ist aber $A^{\varphi(M)} \equiv 1 \pmod{M}$, also ist a ein Divisor von $\varphi(M)$. Doch kann dies leicht direkt bewiesen werden, und daraus ergibt sich dann ein neuer Beweis des Satzes $A^{\varphi(M)} \equiv 1 \pmod{M}$. Man braucht zu dem Zwecke sich nur der bekannten Exhaustionsmethode zu bedienen, durch welche man die $\varphi(M)$ gegen M relativ primen Funktionen in $\frac{\varphi(M)}{a}$ Gruppen, jede von a Glieder zerfällt, deren allgemeine Form

$$F, \quad FA, \quad FA^2, \quad \cdots, \quad FA^{a-1}$$

ist, wo F irgend eine gegen M relativ prime Funktion bedeutet; denn es ist leicht zu zeigen, daß zwei solche Gruppen entweder ganz identisch oder ganz verschieden in bezug auf den Modulus M sind.

Wir verlassen den allgemeinen Fall und nehmen nun an, daß der Modulus eine Primfunktion P vom Grade π ist. Ist dann A irgend eine durch P nicht teilbare Funktion, welche in bezug auf P zum Exponenten a gehört, so ist a ein Divisor von $p^\pi - 1$; es fragt sich: gehören zu jedem Divisor a von $p^\pi - 1$ wirklich Funktionen A? und wieviele? —

Nehmen wir zuerst an, es gebe mindestens eine Funktion A, welche zu a gehört, so sind die a inkongruenten Funktionen $1, A, A^2, \cdots, A^{a-1}$ sämtliche Wurzeln der Kongruenz $y^a \equiv 1 \pmod{P}$; alle zum Exponenten a gehörenden Funktionen müssen daher Gliedern dieser Gruppe kongruent sein, und es ergibt sich leicht, daß eine Funktion $A^{a'}$ stets, aber auch nur dann zum Exponenten a gehört, wenn a' relativ prim gegen a ist. Wenden wir daher die Charakteristik φ in der Bedeutung an, wie sie in der Zahlentheorie gebräuchlich ist, so ist die Anzahl der zu einem Divisor a von $p^\pi - 1$ gehörenden Funktionen entweder $= 0$, oder $= \varphi a$. Da aber jede der $p^\pi - 1$ durch P nicht teilbaren Funktionen zu einem, aber auch nur zu einem einzigen der Divisoren $a, a', a'', \cdots$ von $p^\pi - 1$ gehören muß, und außerdem bekanntlich $\varphi a + \varphi a' + \varphi a'' + \cdots = p^\pi - 1$ ist, so ergibt sich leicht, daß zu jedem Divisor a von $p^\pi - 1$ wirklich φa Funktionen gehören.

Es gibt daher auch $\varphi(p^\pi - 1)$ inkongruente durch den Modul P nicht teilbare Funktionen, welche zum Exponenten $p^\pi - 1$ gehören. Sei G irgend eine derselben, so sind die $p^\pi - 1$ Funktionen

$$1, \quad G, \quad G^2, \quad G^3, \quad \cdots, \quad G^{p^\pi - 2}$$

sämtlich inkongruent, und sie bilden daher das vollständige System der inkongruenten durch P nicht teilbaren Funktionen, so daß also jede durch P nicht teilbare Funktion einer von ihnen, aber auch nur einer einzigen kongruent ist. Diese $\varphi(p^\pi - 1)$ Funktionen G heißen primitive Wurzeln der Primfunktion P. Nimmt man eine derselben G als Basis an, und ist F eine beliebige durch P nicht teilbare Funktion, so kann man stets

$$F \equiv G^n \pmod{P}$$

setzen, wo $n = 0$ oder eine positive ganze Zahl $< p^\pi - 1$ ist. Diese Zahl n heißt dann der Index der Funktion F bezüglich der Basis G, in Zeichen

$$F \equiv G^{\text{Ind. } F} \pmod{P}.$$

Dann leuchten folgende Sätze ein, in welchen A, B Funktionen bedeuten, welche durch P nicht teilbar sind, und in denen die Basis der Indizes unverändert bleibt: Ind. $(AB) \equiv$ Ind. $A +$ Ind. $B \pmod{p^\pi - 1}$, Ind. $(A^n) \equiv n$ Ind. $A \pmod{p^\pi - 1}$; ferner folgt aus $A \equiv B \pmod{P}$ notwendig Ind. $A =$ Ind. B und umgekehrt.

Ein anderer Satz, welcher seiner Natur nach von der Wahl der Basis unabhängig ist, lautet folgendermaßen: Gehört eine Funktion A zum Exponenten a, so ist $\frac{p^\pi - 1}{a}$ der größte gemeinschaftliche Divisor von $p^\pi - 1$ und Ind. A; und umgekehrt.

Binomische Kongruenzen.

14.

Soll die binomische Kongruenz $y^n \equiv A \pmod{P}$, in welcher A eine durch P nicht teilbare Funktion bedeutet, lösbar sein, so muß n Ind. $y \equiv$ Ind. $A \pmod{p^\pi - 1}$ sein; ist nun δ der größte gemeinschaftliche Divisor von n und $p^\pi - 1$, so muß auch Ind. A durch δ teilbar sein, wenn diese Kongruenz möglich sein soll, und dann hat sie in der Tat δ nach dem Modul $p^\pi - 1$ inkongruente Wurzeln Ind. y, denen ebenso viele nach dem Modul P inkongruente Wurzeln y der binomischen Kongruenz entsprechen.

Die erforderliche und hinreichende Bedingung für die Möglichkeit dieser Kongruenz, daß nämlich Ind. A durch den größten gemeinschaftlichen Divisor δ von n und $p^\pi - 1$ teilbar sein muß, ist unabhängig von der Wahl der Basis und offenbar identisch mit der Bedingung, daß A eine Wurzel der Kongruenz $y^{\frac{p^\pi-1}{\delta}} \equiv 1 \pmod{P}$ ist; und man hätte dieses Kriterium auch leicht ohne Hilfe der Theorie der Indizes ableiten können. Zugleich leuchtet nun ein, daß die vorgelegte binomische Kongruenz für $\frac{p^\pi - 1}{\delta}$ inkongruente Funktionen A möglich ist, und nur für diese.

Quadratische Reste.

15.

Wenden wir die letzten Resultate auf den Fall an, in welchem $n = 2$ und p ungerade ist (der Fall $p = 2$ ist leicht zu absolvieren), so ergibt sich, daß die Kongruenz

$$y^2 \equiv A \pmod{P}$$

stets, aber auch nur dann möglich ist, wenn A eine der $\frac{1}{2}(p^\pi - 1)$ Wurzeln der Kongruenz

$$y^{\frac{1}{2}(p^\pi-1)} \equiv 1 \pmod{P}$$

ist, die wir quadratische Reste der Primfunktion P nennen während die übrigen $\frac{1}{2}(p^\pi - 1)$ inkongruenten durch P nicht teilbaren Funktionen quadratische Nichtreste von P heißen; und jedesmal, wenn A quadratischer Rest von P ist, hat die vorgelegte Kongruenz zwei inkongruente Wurzeln. Die $\frac{1}{2}(p^\pi - 1)$ Nichtreste sind offenbar die Wurzeln der Kongruenz

$$y^{\frac{1}{2}(p^\pi-1)} \equiv -1 \pmod{P}.$$

Doch lassen sich alle diese Sätze auch unmittelbar aus den ersten Elementen ableiten, und zugleich ergeben sich dann neue Beweise für die beiden Sätze, welche denen von Fermat und Wilson in der Zahlentheorie analog sind. Ist A eine bestimmte, der $p^\pi - 1$ durch P nicht teilbaren Funktionen, so gehört zu jeder beliebigen F derselben eine, aber auch nur eine F', so daß $FF' \equiv A \pmod{P}$; wenn nun erstens A quadratischer Nichtrest von P ist (d. h. wenn die Kongruenz $y^2 \equiv A \pmod{P}$ unmöglich), so sind F und F' stets

inkongruent, und es zerfällt das System sämtlicher $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare F, F'; woraus leicht folgt, daß

$$\Pi(F) \equiv A^{\frac{1}{2}(p^\pi-1)} \pmod{P}$$

ist, wo das Zeichen Π dieselbe Bedeutung hat, wie im Art. 12. Ist aber zweitens A quadratischer Rest, d. h. ist die Kongruenz $y^2 \equiv A \pmod{P}$ möglich, so ist einleuchtend, daß diese zwei Wurzeln von der Form W und $-W$ hat, und das Produkt dieser beiden Funktionen ist $\equiv -A \pmod{P}$; die übrigen $p^\pi - 3$ Funktionen F zerfallen aber, wie im ersten Falle, in $\frac{1}{2}(p^\pi - 3)$ Paare inkongruenter Funktionen F, F'; woraus folgt, daß in diesem Falle

$$\Pi(F) \equiv -A^{\frac{1}{2}(p^\pi-1)} \pmod{P}$$

ist. Da nun 1 quadratischer Rest von P ist, so folgt aus dem zweiten Falle zunächst der Satz

$$\Pi(F) + 1 \equiv 0 \pmod{P},$$

sodann, daß

$$A^{\frac{1}{2}(p^\pi-1)} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{P},$$

je nachdem A quadratischer Rest oder Nichtrest von P ist, und endlich, daß in beiden Fällen

$$A^{p^\pi-1} \equiv 1 \pmod{P}$$

ist. Die Anzahl der quadratischen Reste bestimmt sich endlich folgendermaßen. Man kann die $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare von der Form $F, -F$ zerlegen, woraus folgt, daß es höchstens $\frac{1}{2}(p^\pi - 1)$ inkongruente Quadrate, also auch höchstens ebenso viel inkongruente quadratische Reste gibt; da aber außerdem je zwei verschiedenen Paaren, wie leicht zu beweisen ist, wirklich inkongruente Quadrate entsprechen, so gibt es in der Tat $\frac{1}{2}(p^\pi - 1)$ quadratische Reste und ebenso viele Nichtreste.

16.

Das Zeichen $\left(\frac{A}{P}\right)$ möge $+1$ oder -1 bedeuten, je nachdem (die durch die Primfunktion P nicht teilbare Funktion) A quadratischer Rest oder Nichtrest von P ist. Dann leuchten folgende Sätze ein:

1. Ist $A \equiv B \pmod{P}$, so ist $\left(\frac{A}{P}\right) = \left(\frac{B}{P}\right)$.

2. $\left(\frac{AB}{P}\right) = \left(\frac{A}{P}\right)\left(\frac{B}{P}\right)$ oder allgemeiner: das Produkt aus einer beliebigen Anzahl von Funktionen (die durch P nicht teilbar sind) ist quadratischer Rest oder Nichtrest, je nachdem die Anzahl der Faktoren, welche Nichtreste sind, gerade oder ungerade ist.

Man kann auch noch ein anderes Kriterium aufstellen, um zu entscheiden, ob eine Funktion A quadratischer Rest oder Nichtrest von P ist. Teilt man nämlich sämtliche $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare von der Form F, $-F$, und nimmt aus jedem Paare willkürlich eine Funktion, so erhält man eine Gruppe von $\frac{1}{2}(p^\pi - 1)$ Funktionen F, deren Quadrate sämtlich inkongruent sind, und ebenso bilden die übrigen $\frac{1}{2}(p^\pi - 1)$ Funktionen $-F$ eine solche Gruppe. Nun bilde man die Produkte aus jeder Funktion der einen Gruppe in die Funktion A und bezeichne mit μ die Anzahl derjenigen unter diesen Produkten, welche Funktionen der anderen Gruppe kongruent sind; so ist leicht zu zeigen, daß

$$A^{\frac{1}{2}(p^\pi - 1)} \equiv (-1)^\mu \pmod{P}$$

oder $\left(\frac{A}{P}\right) = (-1)^\mu$ ist. Je nachdem also μ gerade oder ungerade, ist A quadratischer Rest oder Nichtrest von P.

17.

Die Frage: „Von welchen Primfunktionen P ist eine gegebene Funktion A quadratischer Rest?“, welche für die Theorie der quadratischen Formen (mit Funktionen einer Variablen x) von Wichtigkeit ist, wird vermöge des vorigen Artikels auf den Fall reduziert, in welchem A eine Primfunktion R (vom Grade ϱ) ist. Die analoge Frage in der Zahlentheorie wird bekanntlich durch den (zuerst von Gauß bewiesenen) sogenannten Reziprozitäts-Satz von Legendre beantwortet. Diese Analogie, welche sich bisher in allen Prinzipien und Beweisen bewährt hat, läßt keinen Zweifel an der Existenz eines entsprechenden Satzes in unserer Theorie übrig. Dieses Theorem lautet in der Tat

$$\left(\frac{P}{R}\right)\left(\frac{R}{P}\right) = \left(\frac{-1}{p}\right)^{\pi \cdot \varrho},$$

worin P, R primäre Primfunktionen resp. von den Graden π, ϱ bedeuten, und $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ das Zeichen von Legendre ist. Der Fall, in welchem P, R nicht primär sind, läßt sich unmittelbar auf diesen zurückführen. Denn bedeutet E irgend eine der $p-1$ Einheiten, so ist stets $\left(\frac{A}{EP}\right) = \left(\frac{A}{P}\right)$, wo A irgend eine durch P nicht teilbare Funktion ist; und außerdem ist $\left(\frac{E}{P}\right) = \left(\frac{e}{p}\right)^\pi$, wo e eine Zahl $\equiv E \pmod{p}$ und $\left(\frac{e}{p}\right)$ das Zeichen von Legendre ist. Beide Sätze sind leicht zu beweisen.

Der Beweis unseres Theorems kann ganz analog dem fünften Gaußschen für den Satz von Legendre geführt werden und stützt sich dann auf das am Schlusse des vorigen Artikels bewiesene Lemma. Man betrachtet die vollständigen Systeme inkongruenter Funktionen (mit Ausnahme derer, welche $\equiv 0$ sind) in bezug auf die drei Moduli P, R, PR, und wählt dazu immer die inkongruenten Funktionen, deren Grade kleiner sind als der des entsprechenden Moduls. Jedes dieser drei Systeme teilt man in zwei Gruppen von gleich viel Gliedern ein, deren erstere sämtliche Funktionen F enthält, deren höchster Koeffizient einer der Zahlen $1, 2, \cdots, \frac{1}{2}(p-1)$ kongruent ist, während die andere Gruppe die übrigen Funktionen $-F$ enthält, deren höchster Koeffizient einer der Zahlen $-1, -2, \cdots, -\frac{1}{2}(p-1)$ kongruent ist. Die weitere Einteilung der beiden Gruppen des dritten Systems, welches sich auf den Modulus PR bezieht, in jedesmal acht Klassen mit Bezug auf die Moduli P, R und die Schlußfolgerungen daraus bis zu dem letzten Resultat hin, in welchem der Beweis des Theorems enthalten ist, sind denen der zitierten Abhandlung von Gauß so ähnlich, daß die vollständige Durchführung Niemandem entgehen kann. Und hiermit wollen wir diesen Teil unserer Theorie verlassen, da seine weitere Entwicklung sich von selbst ergibt.

Bestimmung der Primfunktionen.

18.

Sei P eine Primfunktion vom Grade π, A eine beliebige Funktion; bildet man die unendliche Reihe A, A^p, A^{p^2}, A^{p^3}, $\cdots$, so muß es natürlich geschehen, daß ein Glied $A^{p^{m+n}}$ einem früheren Gliede A^{p^m}

nach dem Modul P kongruent ist (im Falle A der Null oder einer Einheit kongruent ist, wird schon $A^p \equiv A \pmod P$); da ferner allgemein $A^{p^\pi} \equiv A \pmod P$ ist, so kann man annehmen, daß $m < \pi$ ist; erhebt man daher die Kongruenz $A^{p^m+n} \equiv A^{p^m}$ zur Potenz $p^{\pi-m}$, so ergibt sich leicht $A^{p^n} \equiv A \pmod P$. Sei nun $\varrho > 0$ der niedrigste Wert von n, für welchen dies eintritt, so wollen wir sagen: Die Funktion A paßt zur Zahl ϱ. Dann sind die ϱ Funktionen

$$(\mathfrak{A}.) \qquad A,\ A^p,\ A^{p^2},\ \ldots,\ A^{p^{\varrho-1}}$$

sämtlich inkongruent, denn aus $A^{p^{m+n}} \equiv A^{p^m}$ würde wieder $A^{p^n} \equiv A$ folgen. Daraus ergibt sich dann leicht, daß, wenn $A^{p^n} \equiv A$ ist, n notwendig durch ϱ teilbar sein muß. Also ist jedenfalls ϱ ein Divisor von π.

Es fragt sich nun: Passen zu jedem Divisor ϱ von π wirklich Funktionen? und wieviele? — Zunächst leuchtet ein, daß die Anzahl der (inkongruenten) Funktionen, welche zu ϱ passen, ein Multiplum $\varrho \cdot \psi(\varrho)$ von ϱ sein muß (die Null vorläufig nicht ausgeschlossen). Denn wenn A zu ϱ paßt, so passen auch die ϱ in dem Komplex ($\mathfrak{A}$.) enthaltenen Funktionen zu ϱ; ebenso die ϱ Funktionen

$$(\mathfrak{B}.) \qquad B,\ B^p,\ B^{p^2},\ \ldots,\ B^{p^{\varrho-1}},$$

wenn B zu ϱ paßt; und endlich sind zwei solche Komplexe ($\mathfrak{A}$.) und ($\mathfrak{B}$.) entweder ganz identisch, oder ganz verschieden in bezug auf den Modulus P.

Ferner ist klar, daß alle zu ϱ passenden Funktionen unter den Wurzeln der Kongruenz

$$y^{p^\varrho} \equiv y \pmod P$$

zu suchen sind, und jede Wurzel dieser Kongruenz paßt zu einem bestimmten Divisor von ϱ. Endlich hat diese Kongruenz in der Tat p^ϱ inkongruente Wurzeln, was sich unmittelbar daraus ergibt, daß $y^{p^\pi} - y$ algebraisch durch $y^{p^\varrho} - y$ teilbar ist. Und da unter diesen p^ϱ Wurzeln auch sämtliche Funktionen enthalten sind, die zu einem beliebigen Divisor δ von ϱ passen, so ergibt sich die Gleichung

$$\Sigma\delta \cdot \psi(\delta) = p^\varrho,$$

wo sich das Summenzeichen auf sämtliche Divisoren δ von ϱ bezieht. Stellt man nun diese Gleichung für jeden Divisor ϱ von π auf, so erhält man offenbar ebensoviel Gleichungen, als unbekannte Zahlen $\psi(\delta)$ zu bestimmen sind. Für den Fall, daß π eine Potenz a^α

einer Primzahl a ist, ergibt sich die Auflösung unmittelbar; denn dann ist, wenn α' eine der Zahlen 1, 2, 3, $\cdots$, α bedeutet,

$$1 \cdot \psi(1) + a \cdot \psi(a) + \cdots + a^{\alpha'} \cdot \psi(a^{\alpha'}) = p^{a^{\alpha'}},$$
$$1 \cdot \psi(1) + a \cdot \psi(a) + \cdots + a^{\alpha'-1}\, \psi(a^{\alpha'-1}) = p^{a^{\alpha'-1}},$$

folglich $a^{\alpha'} \cdot \psi(a^{\alpha'}) = p^{a^{\alpha'}} - p^{a^{\alpha'-1}}$ die Anzahl der inkongruenten Funktionen, welche zu dem Divisor $a^{\alpha'}$ von $\pi = a^\alpha$ passen.

Doch läßt sich auch die allgemeine Auflösung des Problems vermöge des folgenden allgemeinen Theorems leicht hinschreiben: Seien $f(m)$ und $F(m)$ zwei von der ganzen Zahl m in der Weise abhängige Funktionen, daß die letztere gleich ist der Summe der Werte der ersteren für alle Divisoren von m; so läßt sich umgekehrt $f(m)$ als algebraische Summe einer Reihe von Werten der Funktion $F(m)$ darstellen. Seien a, b, c, $\cdots$ sämtliche voneinander verschiedenen Primzahlen, welche in m aufgehen, so ist

$$f(m) = F(m) - \Sigma F\left(\frac{m}{a}\right) + \Sigma F\left(\frac{m}{ab}\right) - \Sigma F\left(\frac{m}{abc}\right) + \cdots,$$

wo die Summenzeichen auf der rechten Seite sich der Reihe nach auf alle Kombinationen zu 1, 2, 3 usw. aus den Primzahlen $a, b, c, \cdots$ beziehen. Und es ist leicht zu sehen, daß dasselbe Theorem auch gilt, wenn die Funktionen f, F sich auf irgendwelche Elemente m beziehen, denen jedesmal bestimmte andere Elemente nach denselben Prinzipien entsprechen, wie die Divisoren einer ganzen Zahl dieser Zahl selbst entsprechen.

So folgt aus diesem Satze unmittelbar die Bestimmung der in der Zahlentheorie gebräuchlichen Funktion

$$\varphi(m) = m - \Sigma\frac{m}{a} + \Sigma\frac{m}{ab} - \Sigma\frac{m}{abc} + \cdots$$
$$= m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots$$

aus dem Satze $\Sigma\varphi(\delta) = m$, wo δ alle Divisoren von m zu durchlaufen hat.

Ebenso ergibt sich aus dem in Art. 10 bewiesenen Satze $\Sigma\varphi(N) = p^\mu$ die Umkehrung

$$\varphi(M) = p^\mu - \Sigma p^{\mu-\alpha} + \Sigma p^{\mu-(\alpha+\beta)} - \Sigma p^{\mu-(\alpha+\beta+\gamma)} + \cdots$$
$$= p^\mu\left(1-\frac{1}{p^\alpha}\right)\left(1-\frac{1}{p^\beta}\right)\left(1-\frac{1}{p^\gamma}\right)\cdots;$$

denn in diesem Falle war $F(M) = p^\mu$.

In unserem Falle haben wir $f(m) = m \cdot \psi(m)$ und $F(m) = p^m$, und es ergibt sich also

$$m \cdot \psi(m) = p^m - \Sigma p^{\frac{m}{a}} + \Sigma p^{\frac{m}{ab}} - \Sigma p^{\frac{m}{abc}} + \cdots$$

als die Anzahl der nach dem Modul P inkongruenten Funktionen, welche zu dem Divisor m des Grades π von P passen; und hier bezeichnen wieder $a, b, c \cdots$ sämtliche voneinander verschiedene Primzahlen, welche in m aufgehen.

Die Unabhängigkeit dieses Ausdrucks von dem Multiplum π der Zahl m und der besonderen Natur der Primfunktion P läßt vermuten, daß derselbe eine allgemeinere Bedeutung hat, was sich auch bald herausstellen wird.

19.

Satz: Die Funktion $x^{p^\pi} - x$ ist nach dem Modul p kongruent dem Produkt aus allen primären inkongruenten Primfunktionen, deren Grade Divisoren von π sind. —

Beweis: 1. Die vorgelegte Funktion kann keine einander kongruenten Faktoren enthalten, da ihre Derivierte einer Einheit kongruent ist.

2. Sie ist durch jede Primfunktion R teilbar, deren Grad ϱ ein Divisor von π ist. Denn es ist $x^{p^\varrho} \equiv x \pmod{R}$, und wenn man beide Seiten immer wieder zur Potenz p^ϱ erhebt

$$x \equiv x^{p^\varrho} \equiv x^{p^{2\varrho}} \equiv \cdots \equiv x^{p^\pi} \pmod{R}.$$

3. Sie kann keinen Primfaktor von höherem Grade als π enthalten. Denn bezeichnet $f(x)$ eine beliebige Funktion, so ist, wie leicht zu zeigen, für jede positive ganze Zahl h:

$$f(x)^{p^h} \equiv f(x^{p^h}) \pmod{p}.$$

Ist nun Q irgend ein Primfaktor von $x^{p^\pi} - x$, so ist also

$$f(x)^{p^\pi} \equiv f(x^{p^\pi}) \equiv f(x) \pmod{Q};$$

mithin sind alle in bezug auf Q inkongruenten Funktionen $f(x)$ Wurzeln der Kongruenz $y^{p^\pi} \equiv y \pmod{Q}$, und folglich kann die Anzahl dieser in bezug auf Q inkongruenten Funktionen nicht größer als p^π, folglich der Grad von Q nicht größer als π sein.

4. Der Grad jedes Primfaktors von $x^{p^\pi} - x$ ist ein Divisor von π. Denn es folgt aus 3., daß die Funktion x in bezug auf eine Primfunktion Q vom Grade μ zur Zahl μ selbst paßt (so daß die μ

Funktionen $x, x^p, x^{p^2}, \cdots, x^{p^{\mu-1}}$ in bezug auf Q inkongruent sind); ist daher $x^{p^\pi} \equiv x \pmod{Q}$, so muß μ ein Divisor von π sein.

5. Die Funktion $x^{p^\pi} - x$ enthält daher alle Primfunktionen, deren Grade Divisoren von π sind, und nur solche, ferner jede nur einmal, und da ihr höchster Koeffizient $\equiv 1 \pmod{p}$ ist, so ist sie dem Produkt aus allen primären Primfunktionen kongruent, deren Grade Divisoren von π sind. W. z. b. w.

20.

Bezeichnet man daher die Anzahl der primären Primfunktionen von irgend einem Grade ϱ mit $\psi(\varrho)$, so ist

$$\Sigma \varrho \cdot \psi(\varrho) = p^\pi,$$

worin sich das Summenzeichen auf alle Divisoren ϱ der Zahl π bezieht. Vergleicht man diese Formel mit der im Art. 18, wo die allgemeine Auflösung solcher Gleichungen gelehrt ist, so ergibt sich, daß die Funktion ψ hier wie dort für gleiche Argumente stets denselben Wert hat; und es ist nun auch nicht schwer, die Identität der Bedeutung derselben in beiden Untersuchungen nachzuweisen.

Zunächst ziehen wir aus der im Art. 18 entwickelten Form für $m \cdot \psi(m)$ den Schluß, daß es in der Tat Primfunktionen von jedem Grade m gibt; denn wäre die rechte Seite $= 0$, so könnte man sie durch ihr letztes Glied $p^{\frac{m}{abc\cdots}}$ dividieren, woraus folgen würde, daß die Zahl 1 als algebraische Summe einer Reihe von Potenzen einer Primzahl $p(>1)$ darstellbar wäre, was unmöglich ist, da 1 nicht durch p teilbar ist; und negativ kann $m \cdot \psi(m)$ seiner Bedeutung nach nicht sein.

Sei nun P eine Primfunktion vom Grade π, und A eine Funktion, welche in bezug auf den Modulus P zu dem Divisor ϱ von π paßt. Dann sind die Koeffizienten sämtlicher Potenzen von y in dem Produkte

$$(y - A)(y - A^p)(y - A^{p^2}) \cdots (y - A^{p^{\varrho-1}})$$

nach dem Modulus P Zahlen kongruent. Denn jeder Koeffizient ist eine symmetrische Funktion der ϱ Funktionen $A, A^p, \cdots, A^{p^{\varrho-1}}$ und bleibt daher sich selbst kongruent, wenn man x durch x^p ersetzt, d. h. er ist eine Wurzel der Kongruenz $y^p \equiv y \pmod{P}$. Mit anderen Worten, diese Gruppe von ϱ Funktionen, welche zu dem

Divisor ϱ passen, bildet das vollständige Wurzelsystem einer Kongruenz

$$R(y) \equiv 0 \pmod{P}$$

vom Grade ϱ, deren Koeffizienten von x unabhängig sind. Umgekehrt läßt sich aber auch leicht zeigen, daß, wenn eine Kongruenz, deren Koeffizienten von x unabhängig sind, eine Wurzel A besitzt, welche zu dem Divisor ϱ von π paßt, sie auch die übrigen $\varrho - 1$ Funktionen $A^p, A^{p^2}, \ldots, A^{p^{\varrho-1}}$ zu Wurzeln haben muß (ein Satz, der sich leicht verallgemeinern läßt). Daraus folgt, daß $R(y)$ nach dem Modul p nicht in Faktoren niedrigen Grades zerlegt werden kann, oder, mit anderen Worten, daß $R(x)$ eine Primfunktion vom Grade ϱ ist. Die identische Kongruenz

$$y^{p^\pi} - y \equiv \Pi(y - F) \pmod{P}$$

führt daher, wenn man die Faktoren, welche eine Gruppe zusammengehöriger zu einer und derselben Zahl passender Funktionen F bilden, jedesmal in einen Faktor zusammenzieht, zur Zerlegung der Funktion $y^{p^\pi} - y$ in ihre irreduzibeln Faktoren in bezug auf den Modulus p. Auf diese Weise ist der Zusammenhang der Betrachtungen des Art. 18 mit der Bestimmung der Anzahl der Primfunktionen vollständig dargelegt.

21.

Sei nun M eine beliebige Funktion vom Grade μ, und zwar

$$M \equiv E A^a B^b C^c \cdots \pmod{p},$$

worin E eine Einheit, A, B, C etc. inkongruente primäre Primfunktionen resp. von den Graden α, β, γ etc. sind. Sei ferner π irgend eine durch sämtliche Zahlen α, β, γ etc. teilbare Zahl und P eine Primfunktion vom Grade π. Dann hat nach dem Vorhergehenden jede der Kongruenzen

$$A(y) \equiv 0 \pmod{P}, \qquad B(y) \equiv 0 \pmod{P}, \quad \text{etc.}$$

ebensoviel inkongruente Wurzeln, als ihr Grad beträgt, und zwar ist der Grad die Zahl, zu welcher die Wurzeln passen. Daraus folgt, daß man stets eine identische Kongruenz von der Form

$$M(y) \equiv E\{\Pi(y - A')\}^a \{\Pi(y - B')\}^b \cdots \pmod{P}$$

aufstellen kann, in welcher

$$\Pi(y - A') = (y - A')(y - A'^p) \cdots (y - A'^{p^{\alpha-1}})$$

und A' eine Funktion ist, welche zum Divisor α von π paßt.

22.

Man kann endlich auch das Produkt aller primären Primfunktionen eines bestimmten Grades m isoliert darstellen, mit Hilfe eines Satzes, welcher dem im Art. 18 ohne Beweis angeführten analog ist und durch einen logarithmischen Übergang leicht aus diesem abgeleitet werden kann. Dazu führt folgender Gedankengang. Sind a, b zwei ganze positive Zahlen, und ist $c < b$ der bei der Division von a durch b bleibende (nicht negative) Rest, so ist $x^c - 1$ der Rest, welcher bei der algebraischen Division von $x^a - 1$ durch $x^b - 1$ bleibt; und dies bleibt auch noch richtig, wenn man für x eine beliebige positive ganze Zahl p einsetzt. Ist daher h der größte gemeinschaftliche Teiler von a, b, so ist algebraisch $x^h - 1$ der größte gemeinschaftliche Teiler von $x^a - 1$, $x^b - 1$; und ebenso ist im gewöhnlichen Sinne $p^h - 1$ der größte gemeinschaftliche Teiler von $p^a - 1$, $p^b - 1$. Daraus folgt durch abermalige Anwendung desselben Satzes, daß algebraisch $x^{p^h-1} - 1$ der größte gemeinschaftliche Teiler von $x^{p^a-1} - 1$, $x^{p^b-1} - 1$, und also auch $x^{p^h} - x$ der größte gemeinschaftliche Teiler von $x^{p^a} - x$, $x^{p^b} - x$ ist.

Sei nun m irgend eine positive ganze Zahl, welche durch keine anderen Primzahlen als a, b, c, $\cdots$ teilbar ist, so folgt aus den vorhergehenden Prinzipien, daß

$$(x^{p^m} - x) : \Pi(x^{p^{\frac{m}{a}}} - x) \times \Pi(x^{p^{\frac{m}{ab}}} - x) : \Pi(x^{p^{\frac{m}{abc}}} - x) \times \cdots$$

eine ganze Funktion ist; hierin bezieht sich das Produkt-Zeichen Π der Reihe nach auf die verschiedenen Kombinationen zu 1, 2, 3 usw.; und die mit einander abwechselnden Divisions- und Multiplikationszeichen beziehen sich jedesmal nur auf das zunächst folgende Produkt.

Nehmen wir nun hierin p als Primzahl an, so ergibt sich aus den vorhergehenden Artikeln, daß die nach dem soeben bezeichneten Gesetz gebildete ganze Funktion in bezug auf den Modul p kongruent ist dem Produkte aus allen inkongruenten primären Primfunktionen vom Grade m. Der Grad dieser Funktion ist, übereinstimmend mit Art. 18, gleich

$$p^m - \Sigma p^{\frac{m}{a}} + \Sigma p^{\frac{m}{ab}} - \Sigma p^{\frac{m}{abc}} + \cdots.$$

Die gemeinschaftliche Quelle des im Art. 18 angeführten und des analogen soeben benutzten Satzes ist folgende. Sei m irgend

eine ganze Zahl, ferner a, b, c, ..., k sämtliche voneinander verschiedene in m aufgehende Primzahlen; man bilde zwei getrennte Komplexe D, D' von Divisoren der Zahl m nach folgendem Prinzip. In den Komplex D nehme man zunächst alle Divisoren der Zahl m auf; in den Komplex D' alle Divisoren von $\frac{m}{a}$, alle Divisoren von $\frac{m}{b}$ usw.; dann wieder in den Komplex D alle Divisoren von $\frac{m}{ab}$, von $\frac{m}{ac}$, von $\frac{m}{bc}$ usw.; dann wieder in den Komplex D' alle Divisoren von $\frac{m}{abc}$ usw., bis man endlich auch alle Divisoren von $\frac{m}{abc\ldots k}$ entweder in den Komplex D oder in den Komplex D' aufgenommen hat, je nachdem die Anzahl der Primzahlen a, b, c, ..., k eine gerade oder ungerade ist. Dann ist leicht zu zeigen, daß jeder Divisor der Zahl m ebenso oft in dem einen wie in dem anderen Komplex vorkommt, mit Ausnahme des Divisors m selbst, der lediglich und nur ein einziges Mal in dem Komplex D vorkommt. Es bedarf nur eines Blickes, um hieraus die Umkehrungen der Gleichungen

$$\Sigma f(\delta) = F(m) \quad \text{oder} \quad \Pi f(\delta) = F(m)$$

abzuleiten, in welchen das Summen- oder Produkt-Zeichen Σ oder Π sich auf sämtliche Divisoren δ einer beliebigen Zahl m bezieht; diese Auflösungen sind in den Formeln

$$f(m) = F(m) - \Sigma F\left(\frac{m}{a}\right) + \Sigma F\left(\frac{m}{ab}\right) - \cdots$$

oder

$$f(m) = F(m) : \Pi F\left(\frac{m}{a}\right) \times \Pi F\left(\frac{m}{ab}\right) : \cdots$$

enthalten.

Göttingen, im Oktober 1856.

Erläuterungen zur vorstehenden Abhandlung.

Die Resultate dieser Abhandlung befinden sich schon zum größten Teil in den in der Einleitung erwähnten Abhandlungen von Galois, Serret und Schönemann; bei Galois und Serret werden aber die Resultate unter Anwendung der Galoisschen Imaginären, bei Schönemann durch eine algebraische Betrachtungsweise unter Anwendung des Fundamentalsatzes der Algebra abgeleitet. Dedekind

reduziert hier die Theorie auf ihre einfachste, rein zahlentheoretische Form, wodurch auch die ganze Theorie der Galoisschen Imaginären überflüssig gemacht wird.

Der Restbereich für den Doppelmodul (modd. p, $P(x)$) [$P(x)$ Primfunktion (mod. p) vom Grade π] bilden offenbar einen endlichen Körper (Galoissches Feld) von der Charakteristik p mit p^π Elementen. Nach einem bekannten Satz von E. H. Moore (Papers read at the international mathematical congress, Chicago 1893 (1896), S. 208—226) ist jeder endliche Körper mit einem solchen Restbereich (modd. p, $P(x)$) isomorph und die vorstehende Dedekindsche Abhandlung gibt daher sogleich die arithmetische und zum Teil die algebraische Theorie der endlichen Körper. Für die algebraischen Eigenschaften der endlichen Körper und ihre Erweiterungen muß auf die Arbeit von E. Steinitz, Algebraische Theorie der Körper, Journ. f. Math., Bd. 137 (1910) hingewiesen werden.

Zuletzt sei noch erwähnt, daß diese Abhandlung eine wichtige Grundlage für die spätere Arbeit: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, bildet.

Ore.

VI.

Beweis für die Irreduktibilität der Kreisteilungs-Gleichungen.

[Journal für reine und angewandte Mathematik, Bd. 54, S. 27—30 (1857)].

Nachdem Gauß[*)] zuerst die Irreduktibilität der Gleichung $\frac{x^p - 1}{x - 1} = 0$ für den Fall bewiesen hatte, daß p eine Primzahl ist, lag es nahe, einen ähnlichen Satz zu vermuten, welcher sich auf die Teilung des Kreisumfangs in eine beliebige Anzahl m gleicher Teile bezieht. Dieser Satz wird so lauten:

„Die Gleichung vom Grade $\varphi(m)$, welche sämtliche $\varphi(m)$ primitive Wurzeln der Gleichung $x^m = 1$ zu Wurzeln hat, ist irreduktibel."

Dem Beweis von Gauß folgte zunächst eine Reihe anderer von Kronecker, Schönemann, Eisenstein, die auf wesentlich verschiedenen Prinzipien beruhen, sich aber sämtlich auf denselben einfachsten Fall beziehen, in welchem m eine Primzahl ist. Doch sieht man leicht, daß diese Prinzipien auch noch auf den Fall anwendbar sind, in welchem m nur durch eine einzige Primzahl teilbar, also eine Potenz dieser Primzahl ist, und namentlich wurden die Beweise von Kronecker und Eisenstein in diesem Sinne von Serret verallgemeinert. Allein diese Prinzipien reichen nicht mehr aus, sobald die Zahl m durch mehrere Primzahlen teilbar ist, weil dann die in Rede stehende Gleichung in verschiedener Hinsicht einen wesentlich anderen Charakter annimmt. Auf diesen Punkt hat zuerst Kronecker[**)] in einer Abhandlung aufmerksam gemacht, welche zugleich den ersten Beweis des obigen, und zwar noch verallgemeinerten Theorems enthält. Obgleich nun dieser Satz für die algebraische Auflösung der Gleichung $x^m = 1$ nicht gerade erforderlich ist, da diese bekanntlich immer auf den Fall zurückgeführt werden kann, in welchem m die Potenz einer einzigen Primzahl ist, so verdient doch vielleicht

[*) Ein vollständiges Literaturverzeichnis über die verschiedenen Beweise für die Irreduzibilität der Kreisteilungsgleichung findet man in: Dickson, Mitchell, Vandiver, Wahlin, Algebraic numbers § 13. Bulletin of the National Research Council, Vol. 5, part 3, no. 28 (1923)].

[**) L. Kronecker, Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$. Journ. de Math. Bd. 19, S. 177—192 (1854)].

ein neuer Beweis desselben, der sich durch seine Einfachheit auszeichnet, die Aufmerksamkeit derjenigen Mathematiker, welche sich mit diesem Teile der Algebra beschäftigen.

1.

Der neue Beweis stützt sich auf elementare Sätze über die Kongruenzen höherer Grade, und ich werde mich in dieser Beziehung auf den vorstehenden Aufsatz über die Theorie derselben berufen; außerdem benutze ich noch den folgenden zuerst von Schönemann[*)] bewiesenen Satz: Ist

$$f(x) = (x - \alpha)(x - \beta) \cdots (x - \lambda)$$

eine ganze rationale Funktion mit reellen ganzzahligen Koeffizienten, p eine absolute Primzahl und

$$f_1(x) = (x - \alpha^p)(x - \beta^p) \cdots (x - \lambda^p),$$

so sind die Koeffizienten dieser letzteren Funktion ebenfalls ganze reelle Zahlen, und zwar den entsprechenden Koeffizienten von $f(x)$ kongruent nach dem Modulus p, in Zeichen

$$f_1(x) \equiv f(x) \pmod{p}.$$

Für den direkten Beweis dieses Satzes, welcher eigentlich nur eine sehr spezielle algebraische Anwendung der genannten Theorie der höheren Kongruenzen ist, mag hier folgende Bemerkung genügen. Sieht man $\alpha, \beta, \ldots, \lambda$ als ganz unbestimmte Größen an und bezeichnet mit A und A_1 irgend zwei einander entsprechende Koeffizienten der beiden Funktionen $f(x)$ und $f_1(x)$, so leuchtet ein, daß man $A^p = A_1 + pA_2$ setzen kann, worin A_1 und A_2 ganze, ganzzahlige und zugleich symmetrische Funktionen von $\alpha, \beta, \ldots, \lambda$ und folglich auch (nach dem Fundamentalsatze über die Transformation symmetrischer Funktionen) ganze und ganzzahlige Funktionen der Koeffizienten A von $f(x)$ sind. Sind daher diese Koeffizienten ganze reelle Zahlen, so erhält man $A^p \equiv A_1 \pmod{p}$, und nach dem Fermatschen Satze also auch $A \equiv A_1 \pmod{p}$, was zu beweisen war.

2.

Es sei nun α irgend eine primitive Wurzel der Gleichung $x^m = 1$ und $f(x)$ der durch $x - \alpha$ teilbare irreduktibele Faktor von $x^m - 1$, dessen rationale Koeffizienten sämtlich ganze Zahlen sein müssen,

[*) Th. Schönemann, Grundzüge einer allgemeinen Theorie der höheren Kongruenzen, deren Modul eine reelle Primzahl ist; § 13. Journ. f. Math. Bd. 31, S. 269—325 (1846)].

wenn der der höchsten Potenz von x gleich Eins angenommen wird (Disqu. Arithm. Art. 42). Der zu beweisende Satz ist dann identisch mit dem folgenden: „Die Gleichung $f(x) = 0$ hat zu Wurzeln sämtliche $\varphi(m)$ primitive $m$te Wurzeln der Einheit, und keine anderen.“ Der Beweis des letzteren Teiles dieses Satzes hat keine Schwierigkeit, soll aber doch der Vollständigkeit halber hier nicht übergangen werden. Ist α^r irgend eine Wurzel der Gleichung $f(x) = 0$ — und in dieser Form sind ja alle ihre Wurzeln enthalten —, so folgt in bekannter Weise aus der Irreduktibilität von $f(x)$, daß jedes Glied der Reihe α^r, α^{r^2}, α^{r^3}, $\cdots$ eine Wurzel der Gleichung ist, und daß in dieser Reihe früher oder später einmal ein Glied α^{r^n} kommen muß, welches $= \alpha$ ist; daraus folgt aber $r^n \equiv 1 \pmod{m}$, und es ist daher r relative Primzahl gegen m, und folglich α^r ebenfalls eine primitive $m$te Wurzel der Einheit.

Ungleich schwieriger ist der Nachweis des ersten Teiles, daß nämlich umgekehrt jede primitive $m$te Wurzel der Einheit (d. h. jedes α^r, wenn r relative Primzahl gegen m ist) der Gleichung $f(x) = 0$ genügt; doch kann man das Problem sogleich auf den einfachsten Fall reduzieren, in welchem r eine absolute Primzahl ist, die natürlich nicht in m aufgehen darf. Ist nämlich bewiesen, daß α^r, α^s der Gleichung $f(x) = 0$ genügen, so muß auch $\alpha^{r \cdot s}$ ihr genügen; denn da der Annahme nach α der rationalen Gleichung $f(x^r) = 0$ genügt, so muß ihr auch jede andere Wurzel α^s der irreduktibeln Gleichung $f(x) = 0$ genügen. Offenbar braucht also nur noch gezeigt zu werden, daß jedes α^p der Gleichung $f(x) = 0$ genügt, wenn p eine absolute Primzahl ist, welche nicht in m aufgeht.

3.

Um dies zu beweisen, bemerken wir, daß die Wurzeln der irreduktibeln Gleichung $f_1(x) = 0$, welcher α^p genügt, mit den $p$ten Potenzen der Wurzeln der Gleichung $f(x) = 0$ übereinstimmen müssen; denn da α^p ebensowohl eine rationale Funktion von α, wie umgekehrt α von α^p ist (nämlich $= (\alpha^p)^{p'}$, wenn $pp' \equiv 1 \pmod{m}$), so müssen die Grade der beiden Funktionen $f(x)$ und $f_1(x)$ einander gleich sein. Setzt man daher

$$f(x) = (x - \alpha)(x - \beta) \cdots (x - \lambda),$$

so ist

$$f_1(x) = (x - \alpha^p)(x - \beta^p) \cdots (x - \lambda^p)$$

und folglich nach dem oben bewiesenen Satze von Schönemann

$$f_1(x) \equiv f(x) \pmod{p}.$$

Und aus dieser Kongruenz zwischen den beiden Funktionen $f(x)$ und $f_1(x)$ folgt auch ihre Identität. Denn nehmen wir an, die beiden irreduktibeln Funktionen $f(x)$ und $f_1(x)$ sind nicht identisch, so können sie auch keinen gemeinschaftlichen Faktor haben, und folglich ist $x^m - 1$ durch ihr Produkt teilbar, da $x^m - 1$ sowohl durch $f(x)$ als auch durch $f_1(x)$ teilbar ist. Es wäre daher $x^m - 1$ einem Produkt von Faktoren gleich, unter denen mindestens zwei einander nach dem Modulus p kongruent wären. Dann müßte (zufolge Art. 6 des vorstehenden Aufsatzes über die höheren Kongruenzen) die Funktion $x^m - 1$ mit ihrer ersten Derivierten mx^{m-1} nach dem Modulus p gemeinschaftliche Divisoren haben; da aber m nicht durch p teilbar, und folglich mx^{m-1} auch nicht $\equiv 0 \pmod{p}$ ist, so hat mx^{m-1} nach dem Modulus p nur solche primäre Primfaktoren, welche $\equiv x$ sind; und offenbar hat $x^m - 1$ keinen solchen Primfaktor nach dem Modulus p, da sonst für $x \equiv 0$ auch $x^m - 1 \equiv 0$ werden müßte, was ja nicht der Fall ist.

Mithin sind die beiden Funktionen $f(x)$ und $f_1(x)$ identisch; jedes α^p und folglich auch jedes α^r genügt also einer und derselben irreduktibeln Gleichung $f(x) = 0$, wenn r relative Primzahl gegen m ist. W. Z. B. W.

Göttingen, im Oktober 1856.

Erläuterungen zur vorstehenden Abhandlung.

Der vorliegende Dedekindsche Beweis der Irreduzibilität der allgemeinen Kreisteilungsgleichung ist in bezug auf Einfachheit dem S. 68 zitierten Kroneckerschen Beweise überlegen, obwohl die Verallgemeinerung auf die Irreduzibilität in Körpern, deren Diskriminante zu m relativ prim ist, nicht so einfach wird. Der Dedekindsche Beweis ist in H. Weber, Algebra, 2. Aufl. (1898), Bd. 1, S. 596—600 reproduziert.

F. Mertens (Sitzungsber. d. Akad. d. Wiss. in Wien 1905, IIa, S. 1293—96) hat eine Vereinfachung des Dedekindschen Beweises vorgeschlagen, indem er direkt beweist, daß wenn r zu m relativ prim ist, dann $f(x^r)$ algebraisch durch $f(x)$ teilbar sein muß (Bezeichnung von § 2). Das Dedekindsche Prinzip ist auch im Beweise von H. Späth (Math. Zeitschr. Bd. 26, S. 442—444 (1927)) angewandt. Aber die Dedekindsche Vereinfachung, daß r als Primzahl angenommen werden darf, ist von diesen Autoren nicht übernommen.

Ore.

VII.

Ableitung der allgemeinen Form der Kugelfunktionen.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1859, S. 346–362.]

1.

Dieses Problem ist auf verschiedene Arten von Laplace, Jacobi, Dirichlet behandelt; im folgenden soll ein mehr elementarer Weg eingeschlagen werden. Wir gehen von nachstehender Definition aus: „Unter einer Kugelfunktion n^{ter} Ordnung wird jede ganze rationale Funktion Y der drei Kugelkoordinaten

$$\cos\Theta,\quad \sin\Theta\cos\varphi,\quad \sin\Theta\sin\varphi$$

verstanden, welche der partiellen Differentialgleichung

$$(I)\qquad n(n+1)\sin\Theta\cdot Y+\frac{d}{d\Theta}\Big(\sin\Theta\frac{dY}{d\Theta}\Big)+\frac{1}{\sin\Theta}\frac{d^2Y}{d\varphi^2}=0$$

Genüge leistet.“ Bekanntlich ist dann sowohl $v=\varrho^n Y$, als auch $v=\varrho^{-(n+1)}Y$ eine Lösung der Differentialgleichung

$$(II)\qquad \sin\Theta\cdot\frac{d}{d\varrho}\Big(\varrho^2\frac{dv}{d\varrho}\Big)+\frac{d}{d\Theta}\Big(\sin\Theta\frac{dv}{d\Theta}\Big)+\frac{1}{\sin\Theta}\frac{d^2v}{d\varphi^2}=0$$

oder, als Funktion der drei rechtwinkligen Parallelkoordinaten $\xi=\varrho\cos\Theta$, $\eta=\varrho\sin\Theta\cos\varphi$, $\zeta=\varrho\sin\Theta\sin\varphi$ angesehen, eine Lösung der Gleichung

$$(III)\qquad \frac{d^2v}{d\xi^2}+\frac{d^2v}{d\eta^2}+\frac{d^2v}{d\zeta^2}=0.$$

Wir wollen indessen lediglich die Gleichung (I) unserer Untersuchung zugrunde legen.

2.

Da Y eine ganze rationale Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$, also eine Summe von Gliedern der Form

$$Const\cdot\cos\Theta^\alpha\sin\Theta^{\beta+\gamma}\cos\varphi^\beta\sin\varphi^\gamma$$

sein soll, worin α, β, γ ganze positive Zahlen oder Null sind, eine solche Funktion aber infolge der Identität

$$\cos\Theta^2+(\sin\Theta\cos\varphi)^2+(\sin\Theta\sin\varphi)^2=1$$

auf unendlich viele verschiedene Arten umgeformt werden kann, ohne diesen Charakter zu verlieren, so ist es zweckmäßig, zunächst eine Normalform festzusetzen, in welche jede solche Funktion stets, und auch nur auf eine einzige Weise, gebracht werden kann, und welche umgekehrt auch keine anderen als solche Funktionen enthält.

Zu einer solchen Darstellungsform gelangen wir leicht durch die folgende Bemerkung. Aus den Formeln für die Umwandlung der Produkte $2\sin a\sin b$, $2\cos a\cos b$, $2\sin a\cos b$ in eine Summe zweier Kosinus oder Sinus ergibt sich bekanntlich, daß man stets, je nachdem γ gerade oder ungerade ist,

$$\cos\varphi^\beta\sin\varphi^\gamma=a\cos(\beta+\gamma)\varphi+a_1\cos(\beta+\gamma-2)\varphi+a_2\cos(\beta+\gamma-4)\varphi+\cdots$$

oder

$$\cos\varphi^\beta\sin\varphi^\gamma=b\sin(\beta+\gamma)\varphi+b_1\sin(\beta+\gamma-2)\varphi+b_2\sin(\beta+\gamma-4)\varphi+\cdots$$

setzen kann, worin $a, a_1, a_2\ldots$ und $b, b_1, b_2\ldots$ bestimmte Zahlkoeffizienten bedeuten. Da nun ferner

$$\sin\Theta^{\beta+\gamma}=(1-\cos\Theta^2)\sin\Theta^{\beta+\gamma-2}=(1-\cos\Theta^2)^2\sin\Theta^{\beta+\gamma-4}=\cdots$$

ist, so leuchtet ein, daß man jedes einzelne Glied einer rationalen ganzen Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$ und folglich auch die ganze Funktion selbst in die Form

$$(1)\qquad \sum_{s=0}^{s=k}(y_s\cos s\varphi+z_s\sin s\varphi)\sin\Theta^s$$

bringen kann, wo y_s und z_s rationale Funktionen von $\cos\Theta$ sind und k den größten Wert von $\beta+\gamma$ bedeutet.

Daß eine rationale ganze Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$ nur auf eine einzige Weise in diese Form gebracht werden kann, d. h. daß zwei solche Summen von der vorstehenden Form (1) nur dann identisch sein können, wenn die einzelnen Glieder, also auch die Funktionen y_s, z_s der einen Summe mit den entsprechenden der anderen Summe identisch sind, ist bekannt und läßt sich am kürzesten durch Multiplikation mit $\cos s\varphi\cdot d\varphi$, oder mit $\sin s\varphi\cdot d\varphi$ und Integration zwischen den Grenzen 0 und 2π beweisen.

Daß endlich umgekehrt jede solche Summe von der Form (1) auch eine ganze rationale Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$ ist, folgt unmittelbar aus dem Moivreschen Satze

$$\sin\Theta^s\cos s\varphi + i\sin\Theta^s\sin s\varphi = (\sin\Theta\cos\varphi + i\sin\Theta\sin\varphi)^s,$$

worin $i = \sqrt{-1}$ ist.

Also ist die Form (1) eine solche oben verlangte Normalform.

3.

Wir haben jetzt die allgemeinste Form der rationalen ganzen Funktionen y_s, z_s von $\cos\Theta$ zu suchen, für welche der Ausdruck (1) eine Kugelfunktion n^{ter} Ordnung wird, d. h. der Differentialgleichung (I) genügt. Bezeichnen wir zur Abkürzung $\cos\Theta$, soweit diese Größe in den Funktionen y_s, z_s vorkommt, mit x, so daß also $dx = -\sin\Theta\cdot d\Theta$ ist, und unterwerfen wir den Ausdruck (1) der Differentialgleichung (I), so erhalten wir (da nach dem Vorhergehenden der Koeffizient von $\cos s\varphi$, sowie der von $\sin s\varphi$ in der entstehenden Gleichung für sich $= 0$ sein muß) das Resultat, daß die beiden rationalen ganzen Funktionen y_s, z_s von $x = \cos\Theta$ Lösungen der linearen Differentialgleichung 2^{ter} Ordnung

$$[s] \qquad [n(n+1) - s(s+1)]u - 2(s+1)x\frac{du}{dx} + (1-x^2)\frac{d^2u}{dx^2} = 0$$

sein müssen. Und umgekehrt leuchtet ein, daß dann der Ausdruck (1) eine Kugelfunktion n^{ter} Ordnung sein wird.

Diese Differentialgleichung $[s]$ wollen wir nun untersuchen, dabei aber auch die Fälle betrachten, in welchen s eine negative ganze Zahl ist, während wir n stets als ganze positive Zahl oder Null voraussetzen. Durch Differentiation der Gleichung $[s]$ erhalten wir

$$[n(n+1) - (s+1)(s+2)]\frac{du}{dx} - 2(s+2)x\frac{d^2u}{dx^2} + (1-x^2)\frac{d^3u}{dx^3} = 0,$$

woraus unmittelbar der Satz folgt: Genügt u der Gleichung $[s]$, so genügt $\frac{du}{dx}$ der Gleichung $[s+1]$, und folglich $\frac{d^ru}{dx^r}$ der Gleichung $[s+r]$, wenn r eine beliebige ganze positive Zahl bedeutet.

Nun finden wir aber für $s = -(n+1)$, daß das allgemeine Integral der Gleichung

$$[-(n+1)] \qquad 2nx\frac{du}{dx} + (1-x^2)\frac{d^2u}{dx^2} = 0$$

die Funktion

$$c\int(x^2-1)^n dx + c_1$$

ist, folglich ist nach dem eben bewiesenen Satz

$$c\frac{d^{n+s}(x^2-1)^n}{dx^{n+s}} = cD^{n+s}(x^2-1)^n$$

eine Lösung der Gleichung $[s]$, und zwar ist diese Lösung eine ganze rationale Funktion von x. Sie gilt für alle ganzen Zahlenwerte von s zwischen $-n$ und $+n$.

Jetzt soll noch bewiesen werden, daß für alle ganzen Zahlwerte von s zwischen 0 und $+n$ jede rationale ganze Auflösung der Gleichung $[s]$ in der eben gefundenen Form enthalten ist. Denn, wenn y und z irgend zwei von Null verschiedene Lösungen der Gleichung $[s]$ sind, also

$$[n(n+1) - s(s+1)]y - 2(s+1)x\frac{dy}{dx} + (1-x^2)\frac{d^2y}{dx^2} = 0$$

$$[n(n+1) - s(s+1)]z - 2(s+1)x\frac{dz}{dx} + (1-x^2)\frac{d^2z}{dx^2} = 0$$

ist, so folgt hieraus unmittelbar

$$-2(s+1)x\left\{z\frac{dy}{dx} - y\frac{dz}{dx}\right\} + (1-x^2)\left\{z\frac{d^2y}{dx^2} - y\frac{d^2z}{dx^2}\right\} = 0,$$

und da

$$z\frac{d^2y}{dx^2} - y\frac{d^2z}{dx^2} = \frac{d}{dx}\left\{z\frac{dy}{dx} - y\frac{dz}{dx}\right\}$$

ist, so erhält man durch Integration

$$z\frac{dy}{dx} - y\frac{dz}{dx} = \frac{Const}{(x^2-1)^{s+1}}.$$

Sind nun y und z ganze rationale Funktionen von x, und ist s eine der Zahlen 0, 1, 2, … n, so kann diese Gleichung nur bestehen, wenn $Const = 0$ ist; daraus folgt

$$z\frac{dy}{dx} = y\frac{dz}{dx}, \quad z = Const.\,y,$$

was zu beweisen war.

Da auf diese Weise die allgemeinste Form der Funktionen y_s, z_s für ein positives $s \gtreqless n$ gefunden ist, so fragt sich nur noch, ob auch für $s > n$ ganze rationale Lösungen der Gleichung $[s]$ existieren. Nimmt man an, daß r der Grad einer solchen Lösung sei, so erhält man unmittelbar durch Einsetzen in die Differentialgleichung $[s]$ und Vergleichung der Koeffizienten von x^r die Gleichung

$$n(n+1) - s(s+1) - 2(s+1)r - r(r-1) = 0$$

oder

$$n(n+1)-(r+s)(r+s+1)=0,$$

woraus

$$r+s=n \quad \text{oder} \quad =-(n+1)$$

folgt. Ist daher $s>n$, so würde in beiden Fällen r negativ ausfallen; also existiert keine solche Lösung.

Auf diese Weise haben wir als die allgemeinste Form einer Kugelfunktion n^{ter} Ordnung

$$Y=\sum_{s=0}^{s=n}(\alpha_s \cos s\varphi+\beta_s \sin s\varphi)\, D^{n+s}(x^2-1)^n \cdot \sin\Theta^s$$

gefunden, in welcher α_s, β_s ganz willkürliche Konstanten bedeuten, deren Anzahl $=2n+1$ ist, und wo $x=\cos\Theta$ ist.

4.

Obgleich im vorhergehenden die ursprüngliche Aufgabe ihre vollständige Lösung erhalten hat, so wird es doch nicht unangemessen sein, die schönen Sätze von Jacobi u. a. aus derselben Quelle, aus der Differentialgleichung $[s]$ abzuleiten.

Ist s eine ganze Zahl zwischen 0 und $+n$, so folgt aus dem vorigen Artikel, daß

$$D^{n-s}(x^2-1)^n$$

eine Lösung der Differentialgleichung $[-s]$ ist; diese ganze Funktion ist offenbar teilbar durch $(x^2-1)^s$; setzen wir daher

$$D^{n-s}(x^2-1)^n=(x^2-1)^s w,$$

und suchen wir die ganze Funktion w zu bestimmen.

Setzen wir, ganz abgesehen von der dem w beigelegten speziellen Bedeutung, den Ausdruck $(x^2-1)^s w$ in die Differentialgleichung $[-s]$ ein, so ergibt sich, daß w der Gleichung $[s]$ genügen muß, woraus der allgemeine Satz folgt: Wenn w der Differentialgleichung $[s]$ genügt, so genügt $(x^2-1)^s w$ der Differentialgleichung $[-s]$, und umgekehrt.

Dies auf unseren Fall angewendet (in welchem $0 \lessgtr s \lessgtr +n$) gibt das Resultat, daß die ganze Funktion

$$w=Const\cdot D^{n+s}(x^2-1)^n$$

sein muß.

Setzt man dies in die vorige Gleichung ein, so erhält man durch Vergleichung der Koeffizienten von x^{n+s} auf beiden Seiten, den Satz von Jacobi:

$$D^{n-s}(x^2-1)^n=\frac{\Pi(n-s)}{\Pi(n+s)}(x^2-1)^s D^{n+s}(x^2-1)^n,$$

der zwar nur für $0 \leqq s \leqq n$ bewiesen ist, dessen Richtigkeit aber unmittelbar auf das ganze Intervall $-n \lessgtr s \lessgtr +n$ übertragen werden kann.

Durch wiederholte teilweise Integration findet man leicht, daß

$$\int_{-1}^{+1} D^m(x^2-1)^m D^n(x^2-1)^n dx=(-1)^s\int_{-1}^{+1} D^{m-s}(x^2-1)^m D^{n+s}(x^2-1)^n dx$$

$$=(-1)^m\int_{-1}^{+1}(x^2-1)^m D^{n+m}(x^2-1)^n dx$$

ist. Hieraus folgt unmittelbar

$$\int_{-1}^{+1} D^m(x^2-1)^m D^n(x^2-1)^n dx=0,$$

wenn $m>n$, und folglich auch, da die linke Seite symmetrisch in bezug auf m und n ist, wenn $m<n$. Ist aber $m=n$, so folgt

$$\int_{-1}^{+1}[D^n(x^2-1)^n]^2 dx=\Pi(2n)\cdot\int_{-1}^{+1}(1-x^2)^n dx;$$

da nun

$$\int(1-x^2)^n dx=\frac{x(1-x^2)^n}{2n+1}+\frac{2n}{2n+1}\int(1-x^2)^{n-1}dx$$

ist, so ist

$$\int_{-1}^{+1}(1-x^2)^n dx=\frac{2n}{2n+1}\int_{-1}^{+1}(1-x^2)^{n-1}dx=\frac{2n(2n-2)\cdots 4\cdot 2}{(2n+1)(2n-1)\cdots 5\cdot 3}\cdot 2,$$

folglich

$$\int_{-1}^{+1}[D^n(x^2-1)^n]^2 dx=\frac{2}{2n+1}\cdot[2^n\Pi(n)]^2.$$

Wir bedürfen endlich noch des Wertes von $D^{n+s}(x^2-1)^n$ für $x=1$, den wir mit h_s bezeichnen wollen. Da $D^{n+s}(x^2-1)^n$ der Differentialgleichung $[s]$ genügt, so ergibt sich

$$[n(n+1)-s(s+1)]h_s-2(s+1)h_{s+1}=0,$$

also

$$h_s=\frac{2(s+1)}{(n-s)(n+s+1)}h_{s+1}=\frac{\Pi(n+s)}{\Pi(n-s)}\cdot\frac{2^n\Pi(n)}{2^s\Pi(s)},$$

da $h_n=\Pi(2n)$ ist.

5.

Nehmen wir auf einer mit einem Radius $= 1$ beschriebenen Kugelfläche einen bestimmten Punkt p als Pol eines Polarkoordinatensystems, indem wir mit Θ die Polardistanz $p\mu$ irgend eines Punktes μ der Kugelfläche, mit φ den Winkel bezeichnen, den der Meridian $p\mu$ mit einem festen Meridian bildet, so kann jede Funktion $f(\Theta, \varphi)$ von Θ, φ innerhalb der Grenzen $0 < \Theta < \pi$, $0 < \varphi < 2\pi$, als Funktion des Ortes eines Punktes μ auf dieser Kugelfläche angesehen werden. Es sei nun σ ein beliebig begrenzter Teil dieser Kugelfläche, ds ein unendlich kleines Element seiner Begrenzung, N die in ds nach innen errichtete sphärische Normale; ferner mögen Y, Z zwei Funktionen von Θ, φ sein, welche nebst ihren ersten partiellen Derivierten innerhalb des Gebietes σ endlich und stetig sind. Dann findet man

$$\iint \left\{ \frac{d}{d\Theta}\left(Z \sin\Theta \frac{dY}{d\Theta}\right) + \frac{d}{d\varphi}\left(Z \frac{1}{\sin\Theta}\frac{dY}{d\varphi}\right)\right\} d\Theta\, d\varphi = -\int Z \frac{dY}{dN}\, ds,$$

worin das Doppelintegral linker Hand über alle Werte Θ, φ auszudehnen ist, denen Punkte innerhalb σ entsprechen, während rechts die Integration sich über die ganze Begrenzung s von σ erstreckt und $\frac{dY}{dN}$ die in der Richtung der nach innen errichteten Normale N genommene Derivierte von Y bedeutet. Um sich von der Richtigkeit dieses Satzes zu überzeugen, braucht man nur an jedem der beiden Teile links eine Integration auszuführen.

Andererseits ist aber

$$\frac{d}{d\Theta}\left(Z \sin\Theta \frac{dY}{d\Theta}\right) + \frac{d}{d\varphi}\left(Z \frac{1}{\sin\Theta}\frac{dY}{d\varphi}\right)$$
$$= Z\left\{\frac{d}{d\Theta}\left(\sin\Theta \frac{dY}{d\Theta}\right) + \frac{1}{\sin\Theta}\frac{d^2Y}{d\varphi^2}\right\} + \sin\Theta \frac{dZ}{d\Theta}\frac{dY}{d\Theta} + \frac{1}{\sin\Theta}\frac{dZ}{d\varphi}\frac{dY}{d\varphi};$$

ist daher Y eine Kugelfunktion n^{ter} Ordnung, also

$$\frac{d}{d\Theta}\left(\sin\Theta \frac{dY}{d\Theta}\right) + \frac{1}{\sin\Theta}\frac{d^2Y}{d\varphi^2} = -n(n+1)\sin\Theta \cdot Y,$$

so erhalten wir folgenden Satz:

(IV) $$n(n+1)\int ZY\, d\sigma - \int \left\{\frac{dZ}{d\Theta}\frac{dY}{d\Theta} + \frac{1}{\sin\Theta^2}\frac{dZ}{d\varphi}\frac{dY}{d\varphi}\right\} d\sigma = \int Z\frac{dY}{dN}\, ds,$$

worin $d\sigma = \sin\Theta\, d\Theta\, d\varphi$ ein unendlich kleines Element von σ bedeutet, und die Integrationen links über σ, rechts über die Begrenzung s von σ auszudehnen sind. Für $Z = 1$ erhalten wir das Resultat

(V) $$n(n+1)\int Y\, d\sigma = \int \frac{dY}{dN}\, ds,$$

und diese Gleichung ist nur als eine Transformation der Fundamentalgleichung (I) anzusehen, welche sich umgekehrt wieder aus (V) ableiten läßt, sobald man für σ das von zwei unendlich nahen Parallelkreisen (Θ und $\Theta + d\Theta$) und zwei unendlich nahen Meridianen (φ und $\varphi + d\varphi$) begrenzte Flächenelement $d\sigma = \sin\Theta\, d\Theta\, d\varphi$ wählt. Diese Gleichung (V) spricht aber eine, von dem zufällig gewählten Polarkoordinatensystem (Θ, φ) ganz unabhängige, geometrische Eigenschaft der Ortsfunktion Y aus; nimmt man daher ein beliebiges anderes Polarkoordinatensystem, d. h. einen neuen Pol p' und einen neuen Anfangsmeridian, und bezeichnet mit ω die neue Polardistanz $p'\mu$, mit ψ den Winkel, den der Meridian $p'\mu$ mit dem neuen Anfangsmeridian bildet, so muß Y, als Funktion der neuen Koordinaten ω, ψ, der partiellen Differentialgleichung

(VI) $$n(n+1)\sin\omega\, Y + \frac{d}{d\omega}\left(\sin\omega \frac{dY}{d\omega}\right) + \frac{1}{\sin\omega}\frac{d^2Y}{d\psi^2} = 0$$

Genüge leisten. Ferner ist aus der Theorie der Transformation orthogonaler Koordinaten bekannt, daß jede der drei Größen

$$\cos\Theta, \quad \sin\Theta\cos\varphi, \quad \sin\Theta\sin\varphi$$

eine homogene lineare Funktion der drei Größen

$$\cos\omega, \quad \sin\omega\cos\psi, \quad \sin\omega\sin\psi$$

ist (und umgekehrt). Also ist Y auch eine ganze rationale Funktion dieser drei letzten Größen. Wir sehen also, daß die ursprünglich aufgestellte Definition einer Kugelfunktion ganz unabhängig ist von dem zugrunde gelegten Koordinatensystem. Bezeichnen wir daher zur Abkürzung $\cos\omega$ mit λ, so findet stets eine Identität von folgender Form statt:

$$Y = \sum_0^n (\alpha_s \cos s\varphi + \beta_s \sin s\varphi)\sin\Theta^s \cdot D^{n+s}(x^2-1)^n$$
$$= \sum_0^n (a_s \cos s\psi + b_s \sin s\psi)\sin\omega^s \cdot D^{n+s}(\lambda^2-1)^n.$$

6.

Wir benutzen die Resultate des vorigen Artikels, um folgende Aufgabe zu lösen: Die allgemeinste Form einer Kugelfunktion n^{ter} Ordnung

$$P = \sum_0^n (\alpha_s \cos s\varphi + \beta_s \sin s\varphi) \sin\Theta^s \cdot D^{n+s}(x^2-1)^n$$

zu finden, welche auf jedem einzelnen eines Systems von Parallelkreisen von gegebener Lage einen konstanten Wert hat.

Die Lage des Systems von Parallelkreisen ist durch die Lage des Pols p' derselben gegeben; bezeichnen wir die Koordinaten Θ, φ von p' mit Θ', φ' und nehmen wir p' zum Pol eines neuen Polarsystems ω, ψ, so ist

$$\cos\omega = \cos\Theta\cos\Theta' + \sin\Theta\sin\Theta'\cos(\varphi-\varphi') = \lambda.$$

Da nun die Kugelfunktion P lediglich von ω, nicht aber von ψ abhängen soll, so ist (nach der Endformel des vorigen Artikels)

$$P = Const \cdot D^n(\lambda^2-1)^n.$$

Es bleibt also noch die Aufgabe zu lösen, die Koeffizienten α_s, β_s in der Identität

$$D^n(\lambda^2-1)^n = \sum_0^n (\alpha_s \cos s\varphi + \beta_s \sin s\varphi)\sin\Theta^s D^{n+s}(x^2-1)^n$$

als Funktionen von Θ', φ' zu bestimmen. Da nun die linke Seite eine ganze rationale Funktion von

$$\lambda = \cos\omega = \cos\Theta\cos\Theta' + \sin\Theta\sin\Theta'\cos(\varphi-\varphi'),$$

also symmetrisch in bezug auf Θ, φ und Θ', φ', und folglich auch in bezug auf Θ', φ' eine Kugelfunktion n^{ter} Ordnuug ist, so sieht man voraus, daß

$$D^n(\lambda^2-1)^n = \sum_0^n \gamma_s \sin\Theta^s D^{n+s}(x^2-1)^n \sin\Theta'^s \cdot D^{n+s}(x'^2-1)^n \cos s(\varphi-\varphi')$$

sein muß, worin γ_s absolute Zahlenkoeffizienten bedeuten, welche allein noch zu bestimmen bleiben, und wo $x' = \cos\Theta'$ gesetzt ist.

7.

Statt diese Aufgabe durch die Bemerkung anzugreifen, daß die beiden partiellen Derivierten dieser Kugelfunktion, nach Θ und nach Θ' genommen, sich verhalten müssen, wie $\frac{d\lambda}{d\Theta}$ und $\frac{d\lambda}{d\Theta'}$, wodurch

man ebenfalls zum Ziele kommen würde, schlagen wir einen anderen Weg ein, indem wir zunächst mit den uns zu Gebote stehenden Hilfsmitteln den bekannten Satz beweisen, daß, wenn $Y = f(\Theta, \varphi)$ eine beliebige Kugelfunktion n^{ter} Ordnung bedeutet,

$$\int Y D^n(\lambda^2-1)^n d\sigma = \frac{4\pi}{2n+1} \cdot 2^n \Pi(n) \cdot Y'$$

ist, worin die Integration links über die ganze Kugelfläche auszudehnen, und $Y' = f(\Theta', \varphi')$ ist.

Zu dem Zwecke denken wir uns Y als Funktion von ω, ψ in die Form

$$Y = \sum_0^n (a_s \cos s\psi + b_s \sin s\psi)\sin\omega^s \cdot D^{n+s}(\lambda^2-1)^n$$

entwickelt, und zerlegen die Kugelfläche diesen Koordinaten ω, ψ gemäß in unendlich kleine Elemente $d\sigma = \sin\omega\, d\omega\, d\psi$; so erhalten wir

$$\int Y D^n(\lambda^2-1)^n d\sigma = \int_0^\pi D^n(\lambda^2-1)^n \sin\omega\, d\omega \int_0^{2\pi} Y\, d\psi$$

$$= \int_0^\pi D^n(\lambda^2-1)^n \sin\omega\, d\omega \cdot 2\pi \cdot a_0 \cdot D^n(\lambda^2-1)^n$$

$$= 2\pi a_0 \int_{-1}^{+1} [D^n(\lambda^2-1)^n]^2 d\lambda = \frac{4\pi}{2n+1} \cdot [2^n \Pi(n)]^2 \cdot a_0.$$

Setzen wir aber in der obigen Form für Y die Variable $\omega = 0$, also $\lambda = 1$, so wird $Y = f(\Theta', \varphi') = Y'$, und folglich (Art. 4)

$$Y' = a_0 \cdot D^n(\lambda^2-1)^n]_{\lambda=1} = a_0 h_0 = a_0 \cdot 2^n \Pi(n).$$

Wir erhalten daher

$$\int Y D^n(\lambda^2-1)^n d\sigma = \frac{4\pi}{2n+1} \cdot 2^n \Pi(n) \cdot Y';$$

was zu beweisen war.

Dieser Satz bildet die Ergänzung zu dem anderen Satze, daß, über die ganze Kugelfläche ausgedehnt,

$$\int ZY\, d\sigma = 0$$

ist, wenn Z und Y Kugelfunktionen von verschiedenen Ordnungen bedeuten. Dieses folgt unmittelbar aus der Gleichung (IV), wenn

man bedenkt, daß in diesem Falle das dort stehende Integral rechts wegfällt, und daß das zweite Integral links symmetrisch in bezug auf Y und Z ist; denn daraus folgt

$$n(n+1)\int ZY\,d\sigma = \int\left\{\frac{dZ}{d\Theta}\frac{dY}{d\Theta} + \frac{1}{\sin\Theta^2}\frac{dZ}{d\varphi}\frac{dY}{d\varphi}\right\}d\sigma = m(m+1)\int ZY\,d\sigma,$$

wenn m die Ordnung der Kugelfunktion Z ist. Wenn nun m und n verschieden sind, so ergibt sich unmittelbar der zuletzt aufgestellte Satz.

8.

Wir können nun leicht die Koeffizienten γ_s in der Entwicklung von $D^n(\lambda^2-1)^n$ in Art. 6 bestimmen, nach einem von Dirichlet angegebenen Verfahren. Setzen wir nämlich in dem ersten Satze des vorigen Artikels die spezielle Funktion

$$Y = \cos s\varphi \cdot \sin\Theta^s \cdot D^{n+s}(x^2-1)^n,$$

also

$$Y' = \cos s\varphi' \cdot \sin\Theta'^s \cdot D^{n+s}(x'^2-1)^n,$$

ein, so wird, wenn wir die Entwicklung von $D^n(\lambda^2-1)^n$ substituieren, die Kugelfläche, dem Polarsystem Θ, φ gemäß, in unendlich kleine Elemente $d\sigma = \sin\Theta\,d\Theta\,d\varphi$ zerlegen, und die Variabeln $x = \cos\Theta$ einführen,

$$\int YD^n(\lambda^2-1)^n d\sigma = \gamma_s \sin\Theta'^s D^{n+s}(x'^2-1)^n \cos s\varphi' \cdot \frac{2\pi}{2n+1}\cdot\frac{\Pi(n+s)}{\Pi(n-s)}[2^n\Pi(n)]^2$$

für ein von Null verschiedenes s, während für $s=0$ der doppelte Wert zu nehmen ist. Da nun dies Resultat mit

$$\frac{4\pi}{2n+1}\,2^n\Pi(n)Y' = \frac{4\pi}{2n+1}\cdot 2^n\Pi(n)\cdot\cos s\varphi'\cdot\sin\Theta'^s D^{n+s}(x'^2-1)^n$$

identisch sein muß, so folgt, wenn s von Null verschieden,

$$\gamma_s = 2\cdot\frac{1}{2^n\Pi(n)}\cdot\frac{\Pi(n-s)}{\Pi(n+s)},$$

dagegen

$$\gamma_0 = \frac{1}{2^n\Pi n}.$$

Folglich ist

$$D^n(\lambda^2-1)^n = \frac{2}{2^n\Pi(n)}\sum_0^n\frac{\Pi(n-s)}{\Pi(n+s)}\cdot\sin\Theta^s D^{n+s}(x^2-1)^n \sin\Theta'^s D^{n+s}(x'^2-1)^n\cos s(\varphi-\varphi'),$$

worin aber für $s=0$ das entsprechende Glied auf die Hälfte zu reduzieren ist; diesen Übelstand vermeidet man in der Form

$$D^n(\lambda^2-1)^n = \frac{1}{2^n\Pi(n)}\cdot\sum_{-n}^{+n}\frac{\Pi(n-s)}{\Pi(n+s)}\sin\Theta^s D^{n+s}(x^2-1)^n \sin\Theta'^s D^{n+s}(x'^2-1)^n\cos s(\varphi-\varphi'),$$

die man leicht aus der vorhergehenden ableitet.

9.

Zum Schluß wollen wir noch den Zusammenhang der letzten Untersuchung mit gewissen Reihenentwicklungen bemerken.

Bezeichnet r die Entfernung eines Punktes, dessen rechtwinklige Koordinaten

$$\xi = \varrho\cos\Theta,\quad \eta = \varrho\sin\Theta\cos\varphi,\quad \zeta = \varrho\sin\Theta\sin\varphi$$

sind, von einem festen Punkte, so genügt bekanntlich die Funktion $v = \frac{1}{r}$ der partiellen Differentialgleichung (III) und folglich auch der Gleichung (II). Nehmen wir als festen Punkt einen Punkt der mit dem Radius $= 1$ beschriebenen Kugelfläche, dessen Koordinaten

$$\xi' = \cos\Theta',\quad \eta' = \sin\Theta'\cos\varphi',\quad \zeta' = \sin\Theta'\sin\varphi'$$

sind, so ist

$$r^2 = 1 - 2\lambda\varrho + \varrho^2,$$

worin

$$\lambda = \cos\omega = \cos\Theta\cos\Theta' + \sin\Theta\sin\Theta'\cos(\varphi-\varphi')$$

ist. Entwickelt man daher $\frac{1}{r}$ in eine unendliche Reihe:

$$\frac{1}{r} = \frac{1}{\sqrt{1-2\lambda\varrho+\varrho^2}} = \sum_0^\infty P_n(\lambda)\cdot\varrho^n,\quad \text{für } \varrho<1,$$

worin $P_n(\lambda)$ eine rationale ganze Funktion von λ bezeichnet, so ist

$$\frac{1}{r} = \frac{\frac{1}{\varrho}}{\sqrt{1-2\lambda\frac{1}{\varrho}+\left(\frac{1}{\varrho}\right)^2}} = \sum_0^\infty\frac{P_n(\lambda)}{\varrho^{n+1}},\quad \text{für } \varrho<1,$$

und $P_n(\lambda)$ ist eine rationale ganze Funktion von $\cos\Theta$, $\sin\Theta\cos\varphi$, $\sin\Theta\sin\varphi$, welche der partiellen Differentialgleichung (I) Genüge leistet, folglich eine Kugelfunktion n^{ter} Ordnung ist. Da sie aber

die Variabeln Θ, φ nur in der Form $\lambda = \cos\omega$ enthält, so ist (nach Art. 6)

$$P_n(\lambda) = Const \cdot D^n(\lambda^2 - 1)^n = k_n D^n(\lambda^2 - 1)^n,$$

worin nur noch die Konstante k_n zu bestimmen ist; diese ergibt sich für $\lambda = 1$; denn man erhält

$$P_n(1) = k_n \cdot h_0 = 2^n \Pi(n) \cdot k_n.$$

Andererseits ist $P_n(1)$ der Koeffizient von ϱ^n in der Entwicklung

$$\frac{1}{\sqrt{1 - 2\varrho + \varrho^2}} = \frac{1}{1 - \varrho} = \sum_0^\infty \varrho^n,$$

also

$$P_n(1) = 1, \quad \text{folglich} \quad k_n = \frac{1}{2^n \Pi(n)}$$

und

$$P_n(\lambda) = \frac{D^n(\lambda^2 - 1)^n}{2^n \Pi(n)}.$$

Mit Hilfe dieses Satzes kann man die vorletzte Gleichung des vorigen Artikels auch so schreiben:

$$P_n(\lambda) = 2 \sum_0^n \frac{\Pi(n-s)}{\Pi(n+s)} \cdot \sin\Theta^s D^s P_n(x) \cdot \sin\Theta'^s D^s P_n(x') \cdot \cos s(\varphi - \varphi'),$$

worin nur das $s = 0$ entsprechende Glied auf die Hälfte zu reduzieren ist. Ferner nimmt der Satz des Art. 7 die Gestalt

$$\int Y P_n(\lambda) \, d\sigma = \frac{4\pi}{2n+1} \cdot Y'$$

an, in welcher er gewöhnlich geschrieben wird. Als spezieller Fall desselben ist bemerkenswert

$$\int P_n(\lambda) P_n(\mu) \, d\sigma = \frac{4\pi}{2n+1} \cdot P_n(\nu),$$

worin

$$\lambda = \cos\omega = \cos\Theta \cos\Theta' + \sin\Theta \sin\Theta' \cos(\varphi - \varphi')$$
$$\mu = \cos\omega' = \cos\Theta \cos\Theta'' + \sin\Theta \sin\Theta'' \cos(\varphi - \varphi'')$$
$$\nu = \cos\omega'' = \cos\Theta' \cos\Theta'' + \sin\Theta' \sin\Theta'' \cos(\varphi' - \varphi'')$$

die Kosinus der drei Seiten eines sphärischen Dreiecks sind, dessen drei Ecken die beiden festen Punkte (Θ', φ'), (Θ'', φ'') und der bewegliche Punkt (Θ, φ) sind.

VIII.

Über Kreisevolventen.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1859, S. 363—365.]

Die Betrachtung der sukzessiven Evolventen des Kreises führt zu einer einfachen mechanischen Konstruktion der Glieder der Exponentialreihe, welche, soviel ich weiß, noch nicht bemerkt ist. Beschreibt man mit dem Radius r einen Kreis K_1 und wählt auf seiner Peripherie einen bestimmten Punkt m_0, von welchem aus der (in einem bestimmten Sinne positiv genommene) Drehungswinkel φ gerechnet wird, so ist das Stück der Peripherie von dem Punkte m_0 bis zu dem Punkte m_1, welcher dem Winkel φ entspricht,

$$m_0 m_1 = r\varphi.$$

Wickelt man dieses Stück ab, vom Punkte m_0 aus, so beschreibt m_0 ein Stück $m_0 m_2$ der Kreisevolvente K_2, welches

$$m_0 m_2 = \frac{r\varphi^2}{1 \cdot 2}$$

ist. Wickelt man abermals dies Stück ab, so daß die Ablösung des Fadens am Punkte m_0 beginnt, so beschreibt m_0 ein Stück

$$m_0 m_3 = \frac{r\varphi^3}{1 \cdot 2 \cdot 3}$$

der Evolvente K_3 der Kurve K_2, und so fort. Der Radius r und die Kurvenstücke $m_0 m_1$, $m_0 m_2$, $m_0 m_3$ ... bilden die sukzessiven Glieder der unendlichen Reihe, in welche re^{φ} entwickelt wird.

Der Beweis läßt sich am einfachsten durch Betrachtung der komplexen Größen und ihrer geometrischen Bedeutung führen, wie folgt.

Wir betrachten die beiden reellen Funktionen x_n und y_n der reellen Variabeln φ, welche durch die Gleichung

$$x_n + y_n i = re^{\varphi i} + \frac{r\varphi}{1} e^{\left(\varphi - \frac{\pi}{2}\right) i} + \cdots + \frac{r\varphi^{n-1}}{1 \cdot 2 \cdot 3 \cdots (n-1)} e^{\left(\varphi - (n-1)\frac{\pi}{2}\right) i}$$

definiert sind ($i = \sqrt{-1}$), als zusammengehörige rechtwinklige Koordinaten eines Punktes m_n einer Ebene; der Ort aller dieser Punkte, welche allen reellen Werten von φ entsprechen, bildet eine Kurve K_n; für $\varphi = 0$ erhält man den Punkt $x_n = r$, $y_n = 0$; wir wollen ihn mit m_0 bezeichnen und rechnen von ihm aus den Bogen $s_n = m_0 m_n$ der Kurve nach der Seite hin, welche positiven Werten von φ entspricht. Nun ist für $h \geqq 1$:

$$d\left(\frac{r\varphi^h}{1\cdot 2\cdots h} e^{\left(\varphi - h\frac{\pi}{2}\right)i}\right)$$

$$= \frac{r\varphi^{h-1}}{1\cdot 2\cdots(h-1)} e^{\left(\varphi - h\frac{\pi}{2}\right)i} d\varphi - \frac{r\varphi^h}{1\cdot 2\cdots h} e^{\left(\varphi - (h+1)\frac{\pi}{2}\right)i} d\varphi,$$

und

$$d(re^{\varphi i}) = -re^{\left(\varphi - \frac{\pi}{2}\right)i} d\varphi,$$

woraus sogleich durch paarweise Destruktion der Glieder

$$dx_n + i\,dy_n = -\frac{r\varphi^{n-1}}{1\cdot 2\cdots(n-1)} e^{\left(\varphi - n\frac{\pi}{2}\right)i} d\varphi;$$

$$ds_n = \frac{r\varphi^{n-1}d\varphi}{1\cdot 2\cdots(n-1)}; \quad s_n = \frac{r\varphi^n}{1\cdot 2\cdots n} = m_0 m_n$$

folgt; außerdem leuchtet ein, daß $t_n = \varphi - n\frac{\pi}{2}$ die Neigung der Tangente im Punkte m_n ist, in dem Sinne genommen, nach welchem φ und s_n abnehmen. Man kann daher die erste Gleichung so schreiben

$$x_n + y_n i = re^{\varphi i} + s_1 e^{t_1 i} + s_2 e^{t_2 i} + \cdots + s_{n-1} e^{t_{n-1} i}$$

oder

$$x_n + y_n i = x_{n-1} + y_{n-1} i + s_{n-1} e^{t_{n-1} i},$$

wodurch unmittelbar ausgedrückt ist, daß die Kurve K_n die Evolvente der Kurve K_{n-1} ist.

Für $n = 1$ erhält man die Gleichungen

$$x_1 = r\cos\varphi, \quad y_1 = r\sin\varphi$$

des Kreises K_1; für $n = 2$ die Gleichungen

$$x_2 = r\cos\varphi + r\varphi\sin\varphi, \quad y_2 = r\sin\varphi - r\varphi\cos\varphi$$

der Kreisevolvente K_2 usf.

Ich bemerke nur noch, daß man die allgemeine Gleichung auch so schreiben kann

$$x_n + y_n i = re^{\varphi i}\left\{1 + \frac{-\varphi i}{1} + \frac{(-\varphi i)^2}{1\cdot 2} + \cdots + \frac{(-\varphi i)^{n-1}}{1\cdot 2\cdots(n-1)}\right\}$$

$$= re^{\varphi i}[e^{-\varphi i}]_n,$$

wo der letzte Faktor auf der rechten Seite die Summe der ersten n Glieder der Entwicklung von $e^{-\varphi i}$ bedeutet. Mag φ noch so groß sein, so wird für unendlich wachsende Werte von n stets $\lim s_n = 0$, $\lim(x_n + y_n i) = r$, d. h. der Punkt m_n nähert sich unbegrenzt wieder dem Punkte m_0.