Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen.

Von Herrn *G. Pólya* in Zürich.

Eine rationale Funktion, deren Potenzreihenentwicklung um den Punkt $z = 0$ nur rationale Koeffizienten enthält, ist der Quotient zweier Polynome $P(z)$ und $Q(z)$, wo $P(z)$ und $Q(z)$ ganzzahlige Koeffizienten, keine gemeinsame Wurzel und auch keinen gemeinsamen Zahlenfaktor (außer ± 1) besitzen. Ich setze

$$\frac{P(z)}{Q(z)} = \frac{s_0}{t_0} + \frac{s_1}{t_1} z + \frac{s_2}{t_2} z^2 + \cdots + \frac{s_n}{t_n} z^n + \cdots,$$

wo die beiden ganzen Zahlen s_n und t_n teilerfremd sind $(n = 0, 1, 2 \ldots)$.

Die arithmetische Natur der Nenner $t_0, t_1, t_2, \ldots t_n, \ldots$ ist durch den *Eisenstein*schen Satz (der in unserem Falle, d. h. für rationale Funktionen, auf der Hand liegt) genügend klargelegt. Es gibt nämlich eine ganze Zahl T von der Eigenschaft, daß T^n durch t_n teilbar ist $(n = 1, 2, 3, \ldots)$, d. h. die Zahl T ist so beschaffen, daß die Potenzreihe

$$\frac{P(Tz)}{Q(Tz)} - \frac{s_0}{t_0} = \frac{s_1 T}{t_1} z + \frac{s_2 T^2}{t_2} z^2 + \cdots$$

nur ganzzahlige Koeffizienten hat. Die Zahlen $t_0, t_1, \ldots t_n, \ldots$ sind also aus endlich vielen Primfaktoren, nämlich aus den Primfaktoren von T, zusammengesetzt.

Die arithmetische Natur der Zähler $s_0, s_1, s_2, \ldots s_n, \ldots$ scheint hingegen noch nicht untersucht und auch verwickelter zu sein. Wie die Beispiele

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n, \qquad \frac{1}{(1-z)^2} = \sum_{n=0}^{\infty} (n+1)\, z^n$$

zeigen, können die Zähler endlich viele (eventuell keine) oder auch unendlich viele Primfaktoren enthalten. Ich werde in vorliegender Arbeit *alle rationalen Funktionen bestimmen, in deren Reihenentwicklung die Zähler aus endlich vielen Primfaktoren zusammengesetzt sind.*

Es wird sich herausstellen, daß im allgemeinen die Zahlen $s_0, s_1, s_2, \ldots s_n, \ldots$ unendlich viele Primfaktoren enthalten. Dafür daß sie nur aus endlich vielen Primfaktoren aufgebaut sein sollen, ist nämlich notwendig (aber noch lange nicht hinreichend), daß alle Wurzeln von $Q(z)$ voneinander verschieden und von der Form $\sqrt[n]{\frac{a}{b}}$ sind, wo a, b, n rationale ganze Zahlen sind. Ferner ist notwendig, daß $Q(z)$, wenn es nicht vom ersten Grade ist, zwei verschiedene Wurzeln hat, deren Quotient eine Einheitswurzel ist. Letztere Bedingung besagt neben der ersterwähnten nur dann etwas Neues, wenn alle Wurzeln von $Q(z)$ rational sind; ich wollte aber diese Bedingung hervorheben, denn ihr Beweis bildet in der Begründung des vollen Satzes den springenden Punkt (vgl. den Satz II im zweiten Teile).

Man kann sich noch mit der Art und Weise befassen, wie die verschiedenen Primfaktoren in die Zahlen $s_0, s_1, s_2, \ldots s_n, \ldots$ eingehen. Das prägnanteste Resultat, zu dem ich in dieser Richtung gelangt bin, spricht sich in folgendem Satze aus:

Besitzt das Integral einer rationalen Funktion eine Potenzreihenentwicklung, deren sämtliche Koeffizienten rationale ganze Zahlen sind, so ist dies Integral notwendigerweise selber eine rationale Funktion.

Vorliegende Arbeit zerfällt in zwei Teile. Der erste Teil bringt den Beweis des eben ausgesprochenen Satzes über das Integral einer rationalen Funktion, der zweite Teil stellt das angedeutete Kriterium auf, das die beiden Fälle, wo $s_0, s_1, s_2, \ldots s_n, \ldots$ aus endlich vielen bzw. aus unendlich vielen Primfaktoren aufgebaut sind, auseinanderhält. Die beiden Teile sind von einander völlig unabhängig, so daß auch die Numerierung der Formeln, Sätze usw. in beiden Teilen getrennt erfolgen konnte.

Erster Teil.

Die Potenzreihe des Integrals.

1. Die uns bekannten Funktionen, deren Potenzreihenentwicklung nur ganzzahlige Koeffizienten besitzt, sind von sehr verschiedener analytischer Natur. Es sind einerseits rationale oder algebraische Funktionen, andererseits sind es Funktionen mit singulären Linien oder unendlichvieldeutige Funktionen. Daß uns nur solche extremen Fälle bekannt sind, scheint nicht bloß auf einer Zufälligkeit des augenblicklichen Standes unserer Kenntnisse zu beruhen. Neuere Untersuchungen*) haben gezeigt, daß gewisse mittlere Fälle wirklich nicht vorkommen können. Es gibt z. B. keine meromorphen Funktionen, deren Potenzreihe nur ganzzahlige Koeffizienten enthält.

Die einfachsten unendlichvieldeutigen Funktionen entspringen aus der Integration der rationalen Funktionen. Ich zeige im folgenden, daß diese einfachen Transzendenten (sie sind gleich der Summe von endlichvielen Logarithmen und einer rationalen Funktion) *nicht* durch Potenzreihen mit ganzzahligen Koeffizienten dargestellt werden können, d. h. ich zeige den schon in der Einleitung erwähnten

Satz I. *Besitzt das Integral einer rationalen Funktion eine Potenzreihenentwicklung, deren sämtliche Koeffizienten rationale ganze Zahlen sind, so ist dies Integral notwendigerweise selber eine rationale Funktion.*

Es waren funktionentheoretische Gesichtspunkte, die zur Auffindung von Satz I führten. Satz I bringt aber eigentlich nur eine einfache zahlentheoretische Eigenschaft der Reihenentwicklungen rationaler Funktionen zum Ausdruck. Es sei

$$(1.) \qquad \frac{P(z)}{Q(z)} = a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \cdots$$

eine solche Reihenentwicklung mit rationalen ganzzahligen Koeffizienten $a_0, a_1, \ldots a_n, \ldots$. (Wären die Koeffizienten nur rational, nicht ganzzahlig, so läßt sich die Ganzzahligkeit, nach *Eisenstein*, leicht erreichen.) Es

*) Vgl. *Borel*, Sur une application d'un théorème de M. Hadamard, Bulletin des sciences mathématiques Bd. 18 (2. Folge), S. 22—25; ferner zwei Arbeiten des Verfassers: Über ganzwertige ganze Funktionen, Rendiconti, Palermo Bd. 40 und Über Potenzreihen mit ganzzahligen Koeffizienten, Mathematische Annalen Bd. 77.

handelt sich um die Frage: wann können die Koeffizienten

$$a_0, a_1, a_2, \ldots a_n$$

der Reihe nach durch die Glieder einer arithmetischen Progression

$$a, a+d, a+2d, \ldots a+nd, \ldots$$

teilbar sein? Die Zahlen a und d sind rational ganz, und es kann ohne Beschränkung $d > 0$ angenommen werden. Ist ein Glied $a + n_0 d = 0$, so wollen wir natürlich von a_{n_0} absehen, d. h. die um $a_{n_0} x^{n_0}$ verminderte rationale Funktion (1.) betrachten. Die erwähnte Frage kann auch so formuliert werden: wann enthält die Potenzreihenentwicklung

$$(2.) \qquad \sum_{n=0}^{\infty} \frac{a_n}{a+nd} z^{a+nd} = \int_0^z z^{a-1} \frac{P(z^d)}{Q(z^d)} dz$$

nur ganzzahlige Koeffizienten? Satz I besagt, daß dies höchstens dann der Fall sein kann, wenn alle Residua in der Partialbruchentwicklung der rationalen Funktion, die in (2.) rechts unter dem Integralzeichen steht, verschwinden, d. h. wenn die Funktion (2.) selber rational ist. Tritt letzteres ein, so sind auch die Koeffizienten der Potenzreihe (2.) wenigstens „im wesentlichen" ganzzahlig, dem *Eisenstein*schen Satz gemäß.

2*). Alle Funktionen $P(z), Q(z), R(z), \ldots p(z), q(z), r(z), \ldots$, die ich unter gegenwärtiger Nummer 2. betrachte, sind Polynome mit rationalen Koeffizienten. Mein Zweck ist, den Bruch

$$(3.) \qquad \frac{P(z)}{Q(z)},$$

dessen Zähler und Nenner keine gemeinschaftliche Wurzel haben, auf rationalem Wege zur Integration vorzubereiten. Dies geschieht in zwei Schritten.

1) Ich nehme an, daß $Q(z)$ in zwei teilerfremde Faktoren $S(z)$ und $T(z)$ zerfällt,

$$Q(z) = S(z)\, T(z).$$

Man bestimme $s(z)$ und $t(z)$ so, daß

$$s(z)\, S(z) + t(z)\, T(z) = 1$$

wird. Daraus folgt

*) Vgl. *Hermite*, Cours d'Analyse, Première partie (Paris 1873), S. 265—270.

$$\frac{P(z)}{Q(z)} = \frac{s(z)\,P(z)}{T(z)} + \frac{t(z)\,P(z)}{S(z)}.$$

Durch wiederholte Anwendung dieses Verfahrens zerlegt man (3.) in eine Summe von rationalen Funktionen, wo der Nenner jedes Summanden die Potenz eines irreduziblen Polynoms ist. Dies will ich durch die Formel

$$\frac{P(z)}{Q(z)} = \sum_{\nu} \frac{P_\nu(z)}{Q_\nu(z)^{n_\nu}} \tag{4.}$$

andeuten. $Q_\mu(z)$ und $Q_\nu(z)$ sind teilerfremd, wenn $\mu \leqq \nu$.

2) Behandeln wir nunmehr den Bruch

$$\frac{R(z)}{S(z)^n},$$

wo $S(z)$ irreduzibel und $n \geqq 2$ ist. $S(z)$ ist gewiß teilerfremd zu seiner Derivierten $S'(z)$, und daher existieren $s(z)$ und $s_1(z)$, so daß

$$s(z)\,S(z) + s_1(z)\,S'(z) = R(z).$$

Ich führe die Polynome $H(z)$ und $R_1(z)$ durch die Formeln

$$s_1(z) = -(n-1)\,H(z),$$
$$s(z) = H'(z) + R_1(z)$$

ein. Es folgt

$$R(z) = (H'(z) + R_1(z))\;S(z) - (n-1)\,H(z)\,S'(z),$$

$$\frac{R(z)}{S(z)^n} = \frac{d}{dz}\left(\frac{H(z)}{S(z)^{n-1}}\right) + \frac{R_1(z)}{S(z)^{n-1}}.$$

Durch wiederholte Anwendung dieses Verfahrens entsteht

$$\frac{R(z)}{S(z)^n} = \frac{d}{dz}\left(\frac{H(z)}{S(z)^{n-1}}\right) + \frac{d}{dz}\left(\frac{H_1(z)}{S(z)^{n-2}}\right) + \cdots + \frac{d}{dz}\left(\frac{H_{n-2}(z)}{S(z)}\right) + \frac{R_{n-1}(z)}{S(z)}.$$

Durch Division erhalte ich endlich

$$R_{n-1}(z) = S(z)\,\frac{dH_n(z)}{dz} + H_{n-1}(z),$$

wo $H_{n-1}(z)$ von niedrigerem Grade ist als $S(z)$ und $H_n(z)$ nur bis auf eine additive Konstante bestimmt ist. Es kommt

$$\frac{R(z)}{S(z)^n} = \frac{d}{dz}\left(\frac{H(z)}{S(z)^{n-1}}\right) + \cdots + \frac{d}{dz}\left(\frac{H_{n-2}(z)}{S(z)}\right) + \frac{H_{n-1}(z)}{S(z)} + \frac{d}{dz}H_n(z).$$

Wendet man dies auf (4.) an, so ergibt sich

$$\frac{P(z)}{Q(z)} = \sum_{\mu,\nu} \frac{d}{dz}\left(\frac{K_{\mu,\nu}(z)}{Q_\nu(z)^\mu}\right) + \sum_{\nu} \frac{K_\nu(z)}{Q_\nu(z)} + \frac{d}{dz}K(z). \tag{5.}$$

Das erste und dritte Glied auf der rechten Seite von (5.) lassen sich also unmittelbar integrieren, und ihr Integral ist eine rationale Funktion. Hingegen ist das Integral des mittleren Gliedes keine rationale Funktion, abgesehen von dem Falle, wo dieses mittlere Glied identisch verschwindet. Wenn es nämlich nicht verschwindet, so hat es, $Q(0) \gtrless 0$ vorausgesetzt, die Form

$$(6.) \qquad \sum_{\nu} \frac{K_\nu(z)}{Q_\nu(z)} = \frac{\alpha_1}{\frac{1}{\omega_1} - z} + \frac{\alpha_2}{\frac{1}{\omega_2} - z} + \cdots + \frac{\alpha_r}{\frac{1}{\omega_r} - z},$$

wo

$$r \geqq 1,$$

$$\alpha_i \neq 0, \qquad \omega_i \neq 0, \qquad \omega_i - \omega_k \neq 0$$

$$(i \gtrless k;\ i, k = 1, 2, 3, \ldots r),$$

und es ist

$$\int \sum_{\nu} \frac{K_\nu(z)}{Q_\nu(z)}\, dz = -\alpha_1 \lg\left(z - \frac{1}{\omega_1}\right) - \cdots - \alpha_r \lg\left(z - \frac{1}{\omega_r}\right).$$

$\frac{1}{\omega_1}, \frac{1}{\omega_2}, \ldots \frac{1}{\omega_r}$ bezeichnen gewisse Wurzeln von $Q(z)$ und sind als solche algebraische Zahlen. Die Zahlen $\alpha_1, \alpha_2, \ldots \alpha_r$ sind auch algebraisch.

3. Hat das Integral der Funktion (3.) nur ganzzahlige rationale Entwicklungskoeffizienten, so hat die Funktion (3.) selbst gewiß ganzzahlige und um so mehr rationale Entwicklungskoeffizienten. Wir können also die unter 2. dargelegte Reduktion auf (3.) anwenden und dadurch den Beweis von Satz I seinem springenden Punkte näher bringen. Wir haben zu beweisen, daß das Integral von (3.) gebrochene Entwicklungskoeffizienten enthalten muß, wenn es transzendent ist. Letzteres ist dann und nur dann der Fall, wenn das mittlere Glied der rechten Seite von (5.) nicht identisch verschwindet, sondern in die Form (6.) gesetzt werden kann.

Ich behaupte: man kann zwei rationale ganze Zahlen a und b so bestimmen, daß

1) sämtliche Koeffizienten des Polynoms

$$aK(bz)$$

ganzzahlig werden,

2) sämtliche Entwicklungskoeffizienten der rationalen Funktionen

$$\frac{aK_{\mu,\nu}(bz)}{Q_\nu(bz)^\mu}$$

ganzzahlig werden (die Potenzreihenentwicklung ist um $z = 0$ vorzunehmen),

3) sämtliche algebraische Zahlen

$$a\alpha_1, \quad a\alpha_2, \ldots a\alpha_r,$$
$$b\omega_1, \quad b\omega_2, \ldots b\omega_r$$

ganze algebraische Zahlen werden.

In der Tat, man kann a und b so wählen, daß sie irgendeiner der aufgezählten Bedingungen einzeln genügen. Bei 1) ist dies evident, bei 2) folgt es aus dem *Eisenstein*schen Satze, bei 3) aus der Bemerkung, daß jede algebraische Zahl der Quotient einer algebraischen ganzen Zahl und einer rationalen ganzen Zahl ist. Durch geeignete Produktbildung gelangt man zu zwei ganzen Zahlen a und b, die sämtlichen Bedingungen 1) 2) 3) zugleich genügen.

Wäre also das Integral von (3.) transzendent und hätte nur ganze rationale Entwicklungskoeffizienten, so hätte die Funktion

$$\begin{aligned} &a\int \frac{P(bz)}{Q(bz)}\, b\,dz - aK(bz) - \sum_{\mu,\nu} \frac{aK_{\mu,\nu}(bz)}{Q_\nu(bz)^\mu} \\ &= \int a \sum_\nu \frac{K_\nu(bz)}{Q_\nu(bz)}\, b\,dz \\ &= \int \left(\frac{a\alpha_1 b\omega_1}{1-b\omega_1 z} + \cdots + \frac{a\alpha_r b\omega_\nu}{1-b\omega_r z}\right) dz \\ &= \sum_{n=1}^{\infty} \frac{a\alpha_1(b\omega_1)^n + a\alpha_2(b\omega_2)^n + \cdots + a\alpha_r(b\omega_r)^n}{n}\, z^n \end{aligned}$$

ebenfalls nur rationale ganze Entwicklungskoeffizienten. Ich werde zeigen, daß dies unmöglich ist.

4. Es gilt also, unter Vereinfachung der Bezeichnungen, folgendes zu zeigen:

Satz II. *Die $2r$ Zahlen*

$$\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_r,$$
$$\omega_1, \omega_2, \omega_3, \ldots \omega_r$$

seien algebraische ganze Zahlen,

$$\alpha_i \neq 0, \quad \omega_i \neq 0, \quad \omega_i - \omega_k \neq 0$$
$$(i \leqq k;\ i, k = 1, 2, \ldots r).$$

Dann können nicht alle Zahlen

$$(7.) \qquad \frac{\alpha_1\omega_1^n + \alpha_2\omega_2^n + \cdots + \alpha_r\omega_r^n}{n} \qquad (n = 1, 2, 3, 4, \ldots$$

(algebraische) ganze Zahlen sein.

Mit Satz II sind wir bei dem springenden Punkte des Beweises angelangt. Ich bewies Satz II unter Anwendung gewisser einfacher Sätze der Idealtheorie (*Fermat*sche Kongruenz nach einem Primideal). Herr *Hurwitz*, dem ich meinen Beweis mitteilte, bemerkte, daß derselbe ohne wesentliche Änderung des Gedankenganges so gewendet werden kann, daß die Idealtheorie ganz entbehrlich wird. Ich will nur die auf einfacheren Prinzipien beruhende Beweisanordnung von *Hurwitz* mitteilen.

Man nennt zwei algebraische ganze Zahlen α und β teilerfremd*), wenn es zwei algebraische ganze Zahlen α_1 und β_1 gibt, so daß

$$\alpha\alpha_1 + \beta\beta_1 = 1.$$

Ist α sowohl zu β wie zu γ teilerfremd, so ist α auch zu $\beta\gamma$ teilerfremd. Denn aus

$$\alpha\alpha_1 + \beta\beta_1 = 1,$$
$$\alpha\alpha_2 + \gamma\gamma_1 = 1$$

folgt

$$\beta\gamma\,\beta_1\gamma_1 = 1 + \alpha(\alpha_1\alpha_2\alpha - \alpha_1 - \alpha_2).$$

Es sei

$$x^m + a_1 x^{m-1} + \cdots + a_{m-1}x + a_m = 0$$

die irreduzible rationale Gleichung, der die ganze Zahl α $(\alpha \neq 0)$ genügt. Geht die rationale Primzahl p in der rationalen ganzen Zahl a_m nicht auf, so sind p und α teilerfremd. In der Tat, es gibt zwei rationale ganze Zahlen u und v, so daß

$$pu + a_m v = 1$$

ist, woraus

$$pu - \alpha(a_{m-1} + \cdots + a_1\alpha^{m-2} + \alpha^{m-1})\,v = 1$$

folgt. In a_m gehen aber nur endlich viele Primzahlen auf, und daraus folgt die Tatsache: es gibt nur endlich viele rationale Primzahlen, die zu einer gegebenen algebraischen Zahl α $(\alpha \neq 0)$ nicht teilerfremd sind.

Kehren wir nun zu Satz II zurück. Es sei p eine der unendlich vielen rationalen Primzahlen, die zu sämtlichen $r+2$ ganzen Zahlen $\alpha_1, \omega_1, \omega_2, \ldots \omega_r$ und δ teilerfremd sind, wo

$$\delta = \left|\omega_k^{i-1}\right|_{\substack{i\\k}=1,2,\ldots r} = \prod_{i<k}^{1\ldots r}(\omega_k - \omega_i).$$

*) *Dirichlet-Dedekind*, Zahlentheorie, 4. Auflage, S. 532 ff.

Wären alle Zahlen ganz, die man aus (7.) erhält, wenn man

$$n = p, 2p, 3p, \ldots rp$$

setzt, so wäre umsomehr

$$(8.)\qquad \begin{aligned} &\alpha_1 \omega_1^p + \alpha_2 \omega_2^p + \cdots + \alpha_r \omega_r^p \equiv 0 \pmod{p} \\ &\alpha_1 \omega_1^{2p} + \alpha_2 \omega_2^{2p} + \cdots + \alpha_r \omega_r^{2p} \equiv 0 \pmod{p} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\alpha_1 \omega_1^{rp} + \alpha_2 \omega_2^{rp} + \cdots + \alpha_r \omega_r^{rp} \equiv 0 \pmod{p}. \end{aligned}$$

Durch Elimination aus den Gleichungen (8.) erhält man

$$\alpha_1 \omega_1^p \omega_2^p \ldots \omega_r^p \prod_{i<k}^{1\ldots r} (\omega_k^p - \omega_i^p) \equiv 0 \pmod{p},$$

und wenn man die Teilbarkeit der Binomialkoeffizienten $\binom{p}{\nu}$ durch p beachtet, und $p > 2$ annimmt,

$$\alpha_1 \omega_1^p \omega_2^p \ldots \omega_r^p \prod_{i<k}^{1\ldots r} (\omega_k - \omega_i)^p \equiv 0 \pmod{p}.$$

Die Zahl

$$\alpha_1 \omega_1^p \omega_2^p \ldots \omega_r^p \delta^p$$

ist aber zu p teilerfremd, da ihre Faktoren zu p teilerfremd sind.

Der Widerspruch löst sich nur, wenn man zugibt, daß unter den r Zahlen, die man aus (7.) für $n = p, 2p, \ldots rp$ erhält, wenigstens eine nicht ganz ist, w. z. b. w.

Satz II stellt keine Bedingungen in bezug auf Rationalität. So ersieht man aus dem Beweise, daß es auch *keine transzendente Funktion gibt die Integral einer rationalen Funktion ist und deren Potenzreihe nur algebraische ganze Zahlen zu Koeffizienten hat.*

Zweiter Teil.

Die Primfaktoren in den Zählern der Koeffizienten.

1. Die Potenzreihe

$$\mathfrak{P}(z) = \frac{s_0}{t_0} + \frac{s_1}{t_1} z + \frac{s_2}{t_2} z^2 + \cdots + \frac{s_n}{t_n} z^n + \cdots$$

soll rationale Koeffizienten haben. Die beiden rationalen ganzen Zahlen s_n und t_n seien teilerfremd ($n = 0, 1, 2, \ldots$). Es sind zwei Fälle möglich: In den von Null verschiedenen unter den unendlich vielen Zahlen

$$s_0, s_1, s_2, \ldots s_n, \ldots; \quad t_0, t_1, t_2, \ldots t_n, \ldots$$

gehen entweder nur endlich viele oder unendlich viele (rationale) Primzahlen auf. Je nachdem der erste oder der zweite dieser Fälle vorliegt, sage ich von der Potenzreihe $\mathfrak{P}(z)$, daß sie endlich viele oder daß sie unendlich viele Primfaktoren enthält. Ob die Potenzreihenentwicklung einer rationalen oder algebraischen Funktion endlich viele oder unendlich viele Primfaktoren enthält, das hängt, nach dem *Eisenstein*schen Satze, bloß von der Beschaffenheit der Zähler $s_0, s_1, \ldots s_n, \ldots$ ab.

Ich werde einige einfache Operationen aufzählen, die aus einer Potenzreihe $\mathfrak{P}(z)$, die nur endlich viele Primfaktoren enthält, eine neue Potenzreihe $\mathfrak{P}^*(z)$ von derselben Eigenschaft entstehen lassen.

1) Es sei $P(z)$ ein Polynom mit rationalen Koeffizienten. Die Reihe

$$\mathfrak{P}^*(z) = \mathfrak{P}(z) + P(z)$$

entsteht aus $\mathfrak{P}(z)$ durch Addition von $P(z)$.

2) Es sei die Zahl a rational. Die Reihe

$$\mathfrak{P}^*(z) = a\,\mathfrak{P}(z)$$

entsteht aus $\mathfrak{P}(z)$ durch Multiplikation mit a.

3) Es sei die Zahl b rational. Die Reihe

$$\mathfrak{P}^*(z) = \mathfrak{P}(bz)$$

entsteht aus $\mathfrak{P}(z)$ durch Multiplikation der Variablen mit b.

4) Es sei m eine natürliche Zahl. Die Reihen

$$\mathfrak{P}_0(z), \mathfrak{P}_1(z), \mathfrak{P}_2(z), \ldots \mathfrak{P}_{m-1}(z)$$

sollen nur endlich viele Primfaktoren enthalten. Übrigens können einige von ihnen auch identisch verschwinden. Die Reihe

$$\mathfrak{P}^*(z) = \mathfrak{P}_0(z^m) + z\,\mathfrak{P}_1(z^m) + z^2\mathfrak{P}_2(z^m) + \cdots + z^{m-1}\mathfrak{P}_{m-1}(z^m),$$

die aus ihnen durch „Zusammensetzung" entsteht, enthält auch nur endlich viele Primfaktoren.

Wenn übrigens die ursprüngliche Reihe $\mathfrak{P}(z)$ eine rationale Funktion darstellte, bzw. wenn die ursprünglichen Reihen $\mathfrak{P}_0(z), \mathfrak{P}_1(z), \ldots \mathfrak{P}_{m-1}(z)$ sämtlich rationale Funktionen darstellten, so wird die durch irgendeine der Operationen 1) 2) 3) 4) neu entstehende Reihe $\mathfrak{P}^*(z)$ offenbar wieder eine rationale Funktion darstellen.

Die einfachste gebrochene rationale Funktion, deren Potenzreihe nicht unendlich viele Primzahlen enthält, ist wohl die Funktion

$$\frac{1}{1-z} = 1 + z + z^2 + \cdots + z^n + \cdots,$$

die Summe der geometrischen Reihe. Ich behaupte nun den

Satz I. *Jede rationale Funktion, deren Potenzreihe nur endlich viele Primfaktoren enthält, entsteht aus der geometrischen Reihe durch Anwendung einer endlichen Anzahl von Operationen* 1) 2) 3) 4).

Anders kann man die in Satz I ausgesprochene Tatsache so formulieren: Der Gesamtheit G sollen alle und nur diejenigen Potenzreihen angehören, die rationale Funktionen darstellen und nur endlich viele Primfaktoren enthalten. Die Gesamtheit G hat folgende Eigenschaften:

I. Die Gesamtheit enthält die geometrische Reihe.

II. Die Operationen 1) 2) 3) 4) sind in ihr unbeschränkt ausführbar.

Satz I besagt, daß G die *kleinste* unter allen Gesamtheiten von Potenzreihen ist, denen die beiden Eigenschaften I und II zukommen.

Es ist nützlich, die einfachsten Funktionen ins Auge zu fassen, die aus der geometrischen Reihe durch die Operationen 1) 2) 3) 4) entstehen. Durch Anwendung von 2) und 3) erhält man

$$\frac{a}{1-bz},$$

durch m-malige Anwendung von 2) (im allgemeinen mit verschiedenen a-Werten) und durch Anwendung von 4) entsteht

$$\frac{a_0}{1-z^m} + z\frac{a_1}{1-z^m} + z^2\frac{a_2}{1-z^m} + \cdots + z^{m-1}\frac{a_{m-1}}{1-z^m} = \frac{P(z)}{1-z^m},$$

wo also $P(z)$ ein beliebiges Polynom vom Grade $\leqq m-1$ mit rationalen Koeffizienten bedeutet usw.

Die Operationen 1) 2) 3) 4) einzeln durchgehend überzeugt man sich, daß mittelst deren aus der geometrischen Reihe nur solche rationale Funktionen entspringen können, deren sämtliche Pole einfach und von der Form $\sqrt[n]{\frac{a}{b}}$ sind, wo a, b, n natürliche ganze Zahlen sind; so folgt aus Satz I das erste in der Einleitung ausgesprochene notwendige Kriterium.

2. Man kann eine und dieselbe rationale Funktion auf verschiedene Weisen aus der geometrischen Reihe durch Anwendung von 1) 2) 3) 4) erhalten. Es ist von Wichtigkeit, eine einfachste, normale Entstehungsweise anzugeben. Dazu dient die folgende Bemerkung: Übt man die Operationen 2) 3) auf eine durch die Operation 4) entstandene Reihe aus:

$$a\mathfrak{P}^*(bz) = a\mathfrak{P}_0(b^m z^m) + zab\mathfrak{P}_1(b^m z^m) + \cdots + z^{m-1}ab^{m-1}\mathfrak{P}_{m-1}(b^m z^m),$$

so kann man sich das Resultat auch so entstanden denken: Zuerst verwandelt man die Reihen

$$\mathfrak{P}_0(z),\ \mathfrak{P}_1(z),\ \ldots\ \mathfrak{P}_{m-1}(z)$$

mittelst 2) und 3) in

$$a\mathfrak{P}_0(b^m z),\ ab\mathfrak{P}(b^m z),\ \ldots\ ab^{m-1}\mathfrak{P}_{m-1}(b^m z),$$

und dann erhält man $a\mathfrak{P}^*(bz)$ aus den letzteren m Reihen durch Anwendung von 4). Daraus geht hervor: Man kann die Entstehung einer Reihe aus der geometrischen mittelst 1) 2) 3) 4) immer so einrichten, daß *jede Operation* 4) *nach sämtlichen Operationen* 2) *und* 3) *ausgeführt wird.* Übt man andrerseits irgend eine der Operationen 2) 3) 4) nach einer Operation 1) aus, so kann man sich leicht überzeugen, daß man zu demselben Resultate kommt, wenn man zuerst die betreffende Operation 2) bzw. 3) 4) ausübt, und dann zu der neuentstandenen Reihe ein gewisses Polynom addiert, also eine Operation 1) ausführt. Mehrere Operationen 1) nacheinander ausgeführt, geben wieder eine Operation 1); also kann man die Entstehung einer Reihe aus der geometrischen mittelst 1) 2) 3) 4) immer so einrichten, daß *nur eine einzige Operation* 1) *vorkommt, und diese wird nach allen übrigen ausgeführt.*

Unser Satz I behauptet also dies: Irgend eine rationale Funktion, deren Potenzreihe nur endlich viele Primfaktoren enthält, ist auf die folgende Weise aufgebaut: Man nimmt eine endliche Anzahl Funktionen

$$\frac{a_1}{1-b_1 z},\ \frac{a_2}{1-b_2 z},\ \cdots\ \frac{a_e}{1-b_e z},$$

die aus $\frac{1}{1-z}$ mittelst 2) und 3) entstehen, man setzt einige unter ihnen mit der Operation 4) zusammen, dann setzt man einige von den entstehenden rationalen Funktionen wieder mit der Operation 4) zusammen u. s. f., bis man schließlich nach einer endlichen Anzahl von solchen Operationen 4) den Aufbau durch das Hinzufügen eines Polynoms mit rationalen Koeffizienten beendigt.

Wollen wir Satz I beweisen, so genügt es, uns auf solche rationalen Funktionen zu beschränken, bei denen der Grad des Zählers niedriger ist, als der des Nenners. Denn es läßt sich irgend eine rationale Funktion in eine solche verwandeln durch Subtraktion eines Polynoms, das durch Division auf rationalem Wege bestimmt wird.

Um Satz I zu beweisen, müssen wir zeigen, daß der eben auseinandergesetzte Aufbau sich immer rückgängig machen läßt, wenn die Potenzreihe der rationalen Funktion nur endlich viele Primfaktoren enthält. Den letzten Schritt des Aufbaues, die darin vorkommende einzige Operation 1), haben wir schon rückgängig gemacht, indem wir uns auf solche Funktionen beschränkt haben, die für $z = \infty$ verschwinden. Um die übrigen Schritte rückgängig zu machen, müssen wir die rationale Funktion „zerfällen".

Zwischen der Potenzreihe

$$\mathfrak{P}^*(z) = a_0 + a_1 z + a_2 z^2 + \cdots = \sum_{\nu=0}^{\infty} a_\nu z^\nu$$

einerseits und den Potenzreihen

$$\mathfrak{P}_0(z) = a_0 + a_m z + a_{2m} z^2 + \cdots = \sum_{\nu=0}^{\infty} a_{\nu m} z^\nu$$

$$\mathfrak{P}_1(z) = a_1 + a_{1+m} z + a_{1+2m} z^2 + \cdots = \sum_{\nu=0}^{\infty} a_{1+\nu m} z^\nu$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\mathfrak{P}_{m-1}(z) = a_{m-1} + a_{2m-1} z + a_{3m-1} z^2 + \cdots = \sum_{\nu=0}^{\infty} a_{m-1+\nu m} z^\nu$$

andrerseits besteht die Identität

$$\mathfrak{P}^*(z) = \mathfrak{P}_0(z^m) + z\mathfrak{P}_1(z^m) + \cdots + z^{m-1}\mathfrak{P}_{m-1}(z^m).$$

$\mathfrak{P}^*(z)$ ist aus $\mathfrak{P}_0(z), \mathfrak{P}_1(z), \ldots \mathfrak{P}_{m-1}(z)$ mittelst Operation 4) zusammengesetzt. Ich werde sagen, daß $\mathfrak{P}^*(z)$ *nach dem Modul m in die m Potenzreihen* $\mathfrak{P}_0(z), \mathfrak{P}_1(z), \ldots \mathfrak{P}_{m-1}(z)$ *„zerfällt"*.

Ich beweise in dieser Arbeit den

Satz II. *Wenn die Potenzreihe einer rationalen Funktion mit r verschiedenen Polen* ($r \geqq 2$) *nur endlich viele Primfaktoren enthält, so zerfällt sie nach einem passenden Modul m in die Potenzreihen solcher m rationalen Funktionen, deren jede weniger als r verschiedene Pole hat.*

Enthält eine Potenzreihe nur endlich viele Primfaktoren, so enthält offenbar jede der m Potenzreihen, in welche sie mod. m zerfällt, wieder nur endlich viele Primfaktoren. Wird also Satz II als richtig angenommen, so folgt daraus, daß jede Potenzreihe, die nur endlich viele Primfaktoren enthält und eine rationale Funktion darstellt, nach und nach in eine endliche Anzahl solcher rationalen Funktionen zerfällt werden kann, die nur einen einzigen Pol haben. Dieser einzige Pol muß nun von der ersten Ordnung sein, denn es besteht der

Satz III. *Wenn eine rationale Funktion $R(z)$ für $z=\infty$ verschwindet, nur einen Pol hat und ihre Potenzreihenentwicklung nur endlich viele Primfaktoren enthält, so ist diese rationale Funktion*

$$R(z)=\frac{a}{1-bz},$$

wo a, b rational.

Bestehen also die Sätze II und III, so ist Satz I als richtig erwiesen.

3. Die rationale Funktion $R(z)$ soll für $z=\infty$ verschwinden und sie soll den einzigen Pol $z=\frac{1}{\omega}$ von der Ordnung m besitzen ($\omega \neq 0$), d. h. es soll

$$R(z)=\frac{\alpha_0}{1-\omega z}+\frac{\alpha_1}{(1-\omega z)^2}+\cdots+\frac{\alpha_{m-1}}{(1-\omega z)^m},$$
$$\alpha_{m-1}\neq 0$$

sein. Die Potenzreihenentwicklung von $R(z)$ läßt sich am einfachsten schreiben, wenn man das Polynom $(m-1)$-ten Grades

$$P(x)=\alpha_0+\alpha_1\binom{x+1}{1}+\alpha_2\binom{x+2}{2}+\cdots+\alpha_{m-1}\binom{x+m-1}{m-1}$$
$$=\alpha_0+\frac{\alpha_1}{1!}(x+1)+\frac{\alpha_2}{2!}(x+1)(x+2)+\cdots+\frac{\alpha_{m-1}}{m-1!}(x+1)\ldots(x+m-1)$$

einführt. Es ist nämlich

$$R(z)=\sum_{\nu=0}^{\infty}P(\nu)\omega^\nu z^\nu.$$

Sind die Koeffizienten von $R(z)$ rational, so ist ω rational, und die Koeffizienten $\alpha_0, \alpha_1, \ldots \alpha_{m-1}$ sind ebenfalls rational. Die ganze Zahl a sei so bestimmt, daß sämtliche Zahlen

$$a\alpha_0, a\frac{\alpha_1}{1!}, a\frac{\alpha_2}{2!}, \ldots a\frac{\alpha_{m-1}}{m-1!}$$

ganz sein sollen. Die Potenzreihenentwicklung

$$aR\left(\frac{z}{\omega}\right)=\sum_{\nu=0}^{\infty}aP(\nu)z^\nu$$

hat ganzzahlige Koeffizienten und enthält dann und nur dann endlich viele Primfaktoren, wenn dies für die Potenzreihenentwicklung von $R(z)$ der Fall ist.

Satz III behauptet also: Wenn $m\geqq 2$, d. h. wenn $m-1\geqq 1$, kurz wenn das Polynom $aP(x)$ keine Konstante ist, so können die ganzen Zahlen

$$aP(0),\ aP(1),\ aP(2),\ aP(3),\ldots$$

nicht aus endlich vielen Primfaktoren aufgebaut sein.

Ich will zur Bezeichnung dieser Sachlage eine kurze Ausdrucksweise einführen. Es sei $F(x)$ eine ganzwertige Funktion, d. h. es sei eine solche Funktion, die für $x = 0, 1, 2, 3, \ldots$ rationale ganze Zahlenwerte annimmt. Eine (rationale) Primzahl p heißt ein „Primteiler von $F(x)$" dann und nur dann, wenn es einen rationalen ganzzahligen Wert $x = \nu$ gibt ($\nu \geqq 0$), so daß $F(\nu) \gtrless 0$ und $F(\nu)$ durch p teilbar wird. Mit dieser, übrigens althergebrachten Ausdrucksweise läßt sich Satz III so aussprechen:

Satz III'. *Jedes Polynom mit ganzen rationalen Koeffizienten, das keine Konstante ist, hat unendlich viele Primteiler.*

Satz III' ist längst bekannt. Ich beabsichtige, auf seinen Beweis unter 4. zurückzukommen. —

Verschwindet die rationale Funktion $R(z)$ für $z = \infty$ und hat sie r verschiedene Pole $\frac{1}{\omega_1}, \frac{1}{\omega_2}, \ldots \frac{1}{\omega_r}$, so läßt sich ihre Potenzreihe so schreiben

$$R(z) = \sum_{\nu=0}^{\infty} F(\nu)\, z^{\nu}, \tag{1.}$$

wo

$$F(x) = P_1(x)\,\omega_1^x + P_2(x)\,\omega_2^x + \cdots + P_r(x)\,\omega_r^x$$

ist, und $P_1(x), P_2(x), \ldots P_r(x)$ Polynome vom Grade $m_1 - 1$, bezw. $m_2 - 1, \ldots m_r - 1$ sind, wenn $m_1, m_2, \ldots m_r$ die bezüglichen Ordnungen der Pole $z = \frac{1}{\omega_1}, \frac{1}{\omega_2}, \ldots \frac{1}{\omega_r}$ bedeuten. Umgekehrt, ist keines der Polynome $P_1(x), P_2(x), \ldots P_r(x)$ identisch $= 0$, und sind die r Zahlen $\omega_1, \omega_2, \ldots \omega_r$ alle voneinander und von 0 verschieden, so ist die durch die Formel (1.) definierte Funktion $R(z)$ eine rationale Funktion, die für $z = \infty$ verschwindet und r verschiedene Pole $z = \frac{1}{\omega_1}, \frac{1}{\omega_2}, \ldots \frac{1}{\omega_r}$ hat.

Aus dem Gesagten folgt sofort: Die Potenzreihe einer rationalen Funktion, die für $z = \infty$ verschwindet, zerfällt nach irgend einem Modul m in m Potenzreihen, die wieder für $z = \infty$ verschwindende rationale Funktionen darstellen.

In der Tat, setzen wir

$$F_h(x) = F(h + mx) = \omega_1^h P_1(h + mx)\,\omega_1^{mx} + \cdots + \omega_r^h P_r(h + mx)\,\omega_r^{mx}$$

$$R_h(z) = \sum_{\nu=0}^{\infty} F_h(\nu)\, z^{\nu} \tag{2.}$$

$$(h = 0, 1, 2, 3, \ldots m - 1)$$

so daß die Identität in z

$$R(z) = R_0(z^m) + zR_1(z^m) + \cdots + z^{m-1}R_{m-1}(z^m)$$

zwischen der Funktion (1.) und den eben definierten (2.) besteht, so sind die Funktionen $R_0(z), R_1(z), \ldots R_m(z)$ rational, und sie verschwinden für $z = \infty$. Sind die r Zahlen $\omega_1^m, \omega_2^m, \ldots \omega_r^m$ alle verschieden, so hat jede dieser m Funktionen r verschiedene Pole, nämlich die Pole $z = \frac{1}{\omega_1^m}, \frac{1}{\omega_2^m}, \ldots \frac{1}{\omega_r^m}$. Gibt es unter den Zahlen $\omega_1^m, \omega_2^m, \ldots \omega_r^m$ zwei oder mehr gleiche, so wird jede der m Funktionen $R_0(z), R_1(z), \ldots R_m(z)$ weniger als r verschiedene Pole haben, und einige unter ihnen können sogar identisch verschwinden. Ist $\omega_i^m = \omega_k^m$, so ist $\frac{\omega_i}{\omega_k}$ eine m-te Einheitswurzel. So ergibt sich der für unseren Zweck sehr wichtige Satz: *Die Potenzreihe einer rationalen Funktion, die r verschiedene Pole* $\frac{1}{\omega_1}, \frac{1}{\omega_2}, \ldots \frac{1}{\omega_r}$ *hat, zerfällt nach dem Modul m dann und nur dann in solche Potenzreihen, deren jede weniger als r Pole hat, wenn es unter den r Zahlen* $\omega_1, \omega_2, \ldots \omega_r$ *zwei verschiedene* ω_i *und* ω_k *gibt, deren Verhältnis eine m-te Einheitswurzel ist.*

Was behauptet also Satz II? Satz II behauptet, daß die rationale Funktion $R(z)$, wenn ihre Potenzreihe nur endlich viele Primfaktoren enthält, sicherlich zwei verschiedene Pole haben muß, deren Quotient eine Einheitswurzel ist. Oder, was dasselbe ist, Satz II behauptet dies: Wenn die rationale Funktion $R(z)$ keine zwei Pole hat, deren Quotient eine Einheitswurzel ist, so enthält die (als rationalzahlig vorausgesetzte) Potenzreihenentwicklung von $R(z)$ unendlich viele Primfaktoren.

Sind die Koeffizienten der Potenzreihe (1.) rationale Zahlen, so ist die rationale Funktion $R(z)$ der Quotient zweier Polynome mit ganzzahligen Koeffizienten, und die Zahlen $\omega_1, \omega_2, \ldots \omega_r$, die reziproken Wurzeln des Nenners von $R(z)$, sind algebraische Zahlen. Ebenso sind die Koeffizienten der Polynome $P_1(x), P_2(x), \ldots P_r(x)$ algebraische Zahlen. Jede algebraische Zahl ist der Quotient einer algebraischen ganzen Zahl und einer rationalen ganzen Zahl. Daher können wir zwei rationale ganze Zahlen a und b $(a > 0, b > 0)$ so bestimmen, daß alle Koeffizienten der Polynome

$$aP_1(x), \quad aP_2(x), \ldots \quad aP_r(x)$$

und alle r Zahlen

$$b\omega_1, \quad b\omega_2, \ldots \quad b\omega_r$$

algebraische ganze Zahlen werden. Dann wird die Funktion

$$aF(x)b^x = aP_1(x)(\omega_1 b)^x + \cdots + aP_r(x)(\omega_r b)^x$$

für $x = 0, 1, 2, 3, \ldots$ rationale ganze Zahlen darstellen, d. h. sie wird eine ganzwertige Funktion.

Die beiden Potenzreihen

$$R(z) = \sum_{\nu=0}^{\infty} F(\nu) z \qquad \text{und} \qquad aR(bz) = \sum_{\nu=0}^{\infty} aF(\nu) b^\nu z^\nu$$

enthalten nun zu gleicher Zeit unendlichviele oder endlichviele Primfaktoren. Überlegt man dies alles, so erkennt man, daß Satz II gleichbedeutend ist mit

Satz II′. *Die Zahlen $\omega_1, \omega_2, \ldots \omega_r$ und sämtliche Koeffizienten der Polynome $P_1(x), P_2(x), \ldots P_r(x)$ seien ganze algebraische Zahlen, und die Funktion*

$$F(x) = P_1(x)\omega_1^x + P_2(x)\omega_2^x + \cdots + P_r(x)\omega_r^x \tag{3.}$$

soll für $x = 0, 1, 2, 3, \ldots$ rationale, also rationale ganze Zahlenwerte annehmen.

Ist keines der $\frac{r(r-1)}{2}$ Verhältnisse

$$\frac{\omega_2}{\omega_1}, \frac{\omega_3}{\omega_1}, \cdots \frac{\omega_r}{\omega_1}, \frac{\omega_3}{\omega_2}, \cdots \frac{\omega_r}{\omega_2}, \cdots \frac{\omega_r}{\omega_{r-1}}$$

einer Einheitswurzel gleich, so hat die Funktion (3.) *unendlich viele Primteiler.*

In der Aussage des Satzes II′ ist stillschweigend vorausgesetzt, daß $r \geqq 2$ ist, daß keine der Zahlen $\omega_1, \omega_2, \ldots \omega_r$ verschwindet und keines der Polynome $P_1(x), P_2(x), \ldots P_r(x)$ identisch verschwindet.

Mit Satz II′ wird also auch Satz I bewiesen sein. Umgekehrt, Satz II′ enthält den wichtigsten Teil von Satz I, und in seinem Beweise konzentrieren sich alle wesentlichen Schwierigkeiten des Problems.

4. Satz III′ ist, wie gesagt, wohl bekannt. Sein üblicher Beweis stimmt im wesentlichen überein mit dem klassischen Verfahren *Euklids*, wodurch er die Existenz unendlich vieler Primzahlen dargetan hat, und verläuft so: Da das Polynom

$$P(x) = a_0 + a_1 x + \cdots$$

keine Konstante ist, gibt es gewiß ganzzahlige Werte von x, für welche

$P(x)$ nicht verschwindet. Man kann ohne Beschränkung der Allgemeinheit annehmen, daß

$$P(0) = a_0 \gtrless 0.$$

Es führt zu einem Widerspruch, anzunehmen, daß $P(x)$ nur die Primteiler $p_1, p_2, \dots p_l$ hat. Denn jeder Primteiler des Polynoms

$$(4.) \qquad \frac{P(p_1 p_2 \dots p_l a_0 x)}{a_0} = 1 + a_1 p_1 p_2 \dots p_l x + \cdots$$

ist Primteiler von $P(x)$. Das Polynom (4.) wird aber bei keinem ganzzahligen Wert x durch eine der Primzahlen $p_1, p_2, \dots p_l$ teilbar, da doch sein Wert $\equiv 1 \pmod{p_1 p_2, \dots p_l}$ ist. Es gibt aber ein ganzzahliges x, für welches der Wert von (4.) von allen drei Zahlen $0, +1, -1$ verschieden ausfällt, also durch eine Primzahl q teilbar ist; so hat notwendigerweise (4.) und damit $P(x)$ einen von $p_1, p_2, \dots p_l$ verschiedenen Primteiler q.

Man beachte folgende Wendung dieser klassischen Schlußweise: Es sei angenommen, daß $P(x)$ nur die Primteiler $p_1, p_2, \dots p_l$ hat. Es sei a ein ganzzahliger Wert, so daß

$$P(a) \gtrless 0$$

ausfällt, und $p_1^{m_1-1}, p_2^{m_2-1}, \dots p_l^{m_l-1}$ seien die höchsten Potenzen von p_1, bzw. von $p_2, \dots p_l$, die in $P(a)$ aufgehen, so daß

$$P(a) \not\equiv 0 \pmod{p_1^{m_1}}, \quad P(a) \not\equiv 0 \pmod{p_2^{m_2}}, \dots \quad P(a) \not\equiv 0 \pmod{p_l^{m_l}}.$$

Man setze

$$d = p_1^{m_1} p_2^{m_2} \dots p_l^{m_l}.$$

Es ist für $t = 1, 2, 3, \dots$

$$P(a + dt) \equiv P(a) \not\equiv 0 \pmod{p_1^{m_1}}, \dots P(a + dt) \equiv P(a) \not\equiv 0 \pmod{p_l^{m_l}},$$

und da $P(a + dt)$ außer $p_1, p_2, \dots p_l$ durch keine andere Primzahl teilbar sein soll, ist notwendigerweise

$$(5.) \qquad |P(a + dt)| \leqq p_1^{m_1-1} p_2^{m_2-1} \dots p_l^{m_l-1}$$

für $t = 1, 2, 3, \dots$. Wenn aber $P(x)$ keine Konstante ist, so muß $P(x)$ bei genügend großem x jeden vorgegebenen Wert übersteigen, und das ergibt einen Widerspruch mit (5.).

Mir gelang es nun, eben diese zweite Wendung des Beweises von Satz III′ sinngemäß zu verallgemeinern. Ich will die Zwischenstufen dieser Verallgemeinerung nicht völlig verwischen, und ich will daher zuerst folgenden leichter zugänglichen speziellen Fall des Satzes II′ beweisen.

Satz II''. *Es seien* $b_1, b_2, \dots b_r$ *voneinander verschiedene rationale ganze positive Zahlen*

$$0 < b_1 < b_2 < \cdots < b_r, \tag{6.}$$

und die Polynome $P_1(x), P_2(x), \dots P_r(x)$ *sollen rationale ganze Koeffizienten haben. Dann hat die Funktion*

$$F(x) = P_1(x) b_1^x + P_2(x) b_2^x + \cdots + P_r(x) b_r^x \tag{7.}$$

unendlich viele Primteiler.

Es ist wieder stillschweigend vorausgesetzt worden, daß

$$r \geqq 2, \qquad P_i(x) \not\equiv 0.$$

Ich kann ohne Beschränkung voraussetzen, daß die Zahlen $b_1, b_2, \dots b_r$ relativ prim sind. Denn wäre der größte gemeinsame Teiler der Zahlen $b_1, b_2, \dots b_r$

$$(b_1, b_2, \dots b_r) = d > 1,$$

so genügte es, von der ganzwertigen Funktion

$$F(x) d^{-x} = P_1(x) \left(\frac{b_1}{d}\right)^x + P_2(x) \left(\frac{b_2}{d}\right)^x + \cdots + P_r(x) \left(\frac{b_r}{d}\right)^x$$

nachzuweisen, daß sie unendlich viele Primteiler hat.

Wächst x durch positive Werte ins Unendliche, so strebt $|F(x)|$ auch gegen $+\infty$. Dasselbe gilt allgemeiner von den Funktionen

$$b_i^x |P_i(x)| - b_{i-1}^x |P_{i-1}(x)| - \cdots - b_1^x |P_1(x)| \qquad (i = 1, 2, \dots r) \tag{8.}$$

und man kann daher einen positiven ganzzahligen Wert $x = a$ finden, für den alle Ausdrücke (8.) positiv ausfallen.

Es sei nun angenommen, daß die Funktion (7.) nur endlich viele Primteiler $p_1, p_2, \dots p_l$ hat. Die ganzen Zahlen $b_1, b_2, \dots b_r$ zerfallen, mod. p_j betrachtet, in zwei Klassen: in die erste Klasse gehören diejenigen, die durch p_j teilbar sind, in die zweite Klasse diejenigen, die durch p_j nicht teilbar sind. Die erste Klasse kann eventuell leer sein, aber die zweite Klasse enthält gewiß einige der Zahlen b_i, sagen wir $b_{i_1}, b_{i_2}, \dots b_{i_k}$ $(i_1 < i_2 < \cdots < i_k)$, denn nach unserer kürzlich gerechtfertigten Annahme ist

$$(b_1, b_2, \dots b_r) = 1.$$

Ich setze

$$\Phi_j(x) = P_{i_1}(x) b_{i_1}^x + P_{i_2}(x) b_{i_2}^x + \cdots + P_{i_k}(x) b_{i_k}^x.$$

Es ist

$$|\Phi_j(a)| \geqq b_{i_k}^a |P_{i_k}(a)| - b_{i_{k-1}}^a |P_{i_{k-1}}(a)| - \cdots - b_{i_1}^a |P_{i_1}(a)|$$
$$\geqq b_{i_k}^a |P_{i_k}(a)| - \sum_{\nu=1}^{i_k-1} b_\nu^a |P_\nu(a)|$$
$$> 0,$$

da doch für $x = a$ alle Ausdrücke (8.) positiv ausfallen. Die ganze Zahl $\Phi_j(a)$ ist also von 0 verschieden. Es sei $p_j^{m_j-1}$ die höchste Potenz von p_j, die in $\Phi_j(a)$ aufgeht, d. h. es sei

$$\Phi_j(a) \equiv 0 \pmod{p_j^{m_j-1}}, \qquad \Phi_j(a) \not\equiv 0 \pmod{p_j^{m_j}}.$$

Denken wir uns alle Funktionen $\Phi_1(x), \Phi_2(x), \ldots \Phi_l(x)$ und alle Zahlen $m_1, m_2, \ldots m_l$ auf die besagte Weise bestimmt, und setzen wir

$$d = p_1^{m_1} p_2^{m_2} \ldots p_l^{m_l} (p_1 - 1)(p_2 - 1) \ldots (p_l - 1).$$

Erteilen wir t die Werte $t = 1, 2, 3, \ldots$. Es ist

$$P_i(a + dt) \equiv P_i(a) \pmod{p_j^{m_j}}, \tag{9.}$$

da dt durch $p_j^{m_j}$ teilbar ist. Ist

$$b_i \not\equiv 0 \pmod{p_j},$$

so ist

$$b_i^{a+dt} \equiv b_i^a \pmod{p_j^{m_j}}, \tag{10.}$$

da doch dt teilbar ist durch

$$p_j^{m_j} - p_j^{m_j-1} = \varphi(p_j^{m_j}).$$

Ist hingegen

$$b_k \equiv 0 \pmod{p_j},$$

so ist

$$b_k^{a+dt} \equiv 0 \pmod{p_j^{m_j}}, \tag{11.}$$

da

$$a + dt \geqq d \geqq p_j^{m_j} > m_j$$

ist. Aus (11.), (9.), (10.) folgt nun nacheinander

$$F(a + dt) \equiv \Phi_j(a + dt) \equiv \Phi_j(a) \not\equiv 0 \pmod{p_j^{m_j}}.$$

Die ganze Zahl $F(a + dt)$ kann also höchstens durch die $(m_1 - 1)$-te, bzw. $(m_2 - 1)$-te, $\ldots$ $(m_l - 1)$-te Potenz von $p_1, p_2, \ldots p_l$ teilbar sein. Da sie durch keine andere Primzahl teilbar sein soll, folgt

$$|F(a + dt)| \leqq p_1^{m_1-1} p_2^{m_2-1} \ldots p_l^{m_l-1}$$

für $t = 1, 2, 3, \ldots$, ein offenbarer Widerspruch, da doch

$$\lim_{x=+\infty} |F(x)| = +\infty.$$

Somit ist Satz II'' bewiesen. Die Beweisidee, die wir nun schon an zwei Beispielen erläutert haben, muß aber eingehend umgearbeitet und ausgebildet werden, bevor sie zum Beweise des vollen Satzes II' tauglich wird. Es gilt hauptsächlich zwei Schwierigkeiten zu überwinden. Erstens muß die Befreiung der Zahlen $b_1, b_2, \ldots b_r$ vom größten gemeinsamen Teiler mittels einfacher Division im Falle der allgemeinen algebraischen Zahlen $\omega_1, \omega_2, \ldots \omega_r$, die in (3.) auftreten, durch einen umständlicheren Prozeß ersetzt werden. Zweitens sind die Wachstumsverhältnisse der allgemeinen Funktion (3.) viel verwickelter als die der speziellen Funktion (7.). Dieser Komplikation muß durch eine ganze Reihe von Hilfssätzen Rechnung getragen werden (vgl. unter 6).

Beachtet der Leser diese Bemerkungen, so wird er den Leitfaden der nun folgenden etwas längeren Schlußreihe nicht verlieren.

5. Hilfssatz I*). *Die elementaren symmetrischen Funktionen der r ganzen algebraischen Zahlen $\omega_1, \omega_2, \ldots \omega_r$ sollen sämtlich rational (also rational ganz) sein.*

Es existiert dann eine natürliche ganze Zahl e, so daß der größte gemeinschaftliche Teiler von $\omega_1^e, \omega_2^e, \ldots \omega_r^e$ eine rationale ganze Zahl ist.

Die elementaren symmetrischen Funktionen $C_1, C_2, \ldots C_r$ von $\omega_1, \omega_2, \ldots \omega_r$ sind durch die Identität in u

$$(u-\omega_1)(u-\omega_2)\ldots(u-\omega_r) = u^r - C_1 u^{r-1} + C_2 u^{r-2} - \cdots + (-1)^r C_r$$

definiert, und sie sind, gemäß Voraussetzung, rationale ganze Zahlen.

Nach der Theorie der algebraischen ganzen Zahlen existiert eine ganze Zahl δ, so daß die r Zahlen

$$\omega_1' = \frac{\omega_1}{\delta}, \ \omega_2' = \frac{\omega_2}{\delta}, \ \ldots \ \omega_r' = \frac{\omega_r}{\delta}$$

ganz sind und 1 zum größten gemeinschaftlichen Teiler haben. Die Zahlen $\omega_1', \omega_2', \ldots \omega_r'$ genügen der Gleichung

$$(12.) \qquad u^r - \frac{C_1}{\delta} u^{r-1} + \frac{C_2}{\delta^2} u^{r-2} - \cdots + (-1)^r \frac{C_r}{\delta^r} = 0.$$

Die Zahlen $\frac{C_1}{\delta}, \frac{C_2}{\delta^2}, \ldots \frac{C_r}{\delta^r}$ sind ersichtlich ganze Zahlen.

Es sei die rationale ganze Zahl d der größte gemeinschaftliche Teiler der r Zahlen

*) Vgl. *Hilbert*, Die Theorie der algebraischen Zahlkörper, S. 247—249.

$$C_1^{r!},\ C_2^{\frac{r!}{2}},\ C_3^{\frac{r!}{3}},\ \dots\ C_r^{\frac{r!}{r}}.$$

Da die Zahlen

$$\text{(13.)} \qquad \left(\frac{C_1}{\delta}\right)^{r!} = \frac{C_1^{r!}}{\delta^{r!}},\ \left(\frac{C_2}{\delta^2}\right)^{\frac{r!}{2}} = \frac{C_2^{\frac{r!}{2}}}{\delta^{r!}},\ \dots \left(\frac{C_r}{\delta^r}\right)^{\frac{r!}{r}} = \frac{C_r^{\frac{r!}{r}}}{\delta^{r!}}$$

ganze Zahlen sind, muß $\delta^{r!}$ in d aufgehen. Ich behaupte, daß $\frac{d}{\delta^{r!}}$ eine Einheit ist.

Angenommen, es wäre nicht so, dann betrachten wir einen Körper K, der die $r+1$ Zahlen $\omega_1, \omega_2, \dots \omega_r$ und δ enthält. Jedes Primideal dieses Körpers K, das in $\frac{d}{\delta^{r!}}$ aufgeht, müßte alle Zahlen (13.), folglich alle Koeffizienten der Gleichung (12.), folglich alle Zahlen $\omega_1'^r, \omega_2'^r, \dots \omega_r'^r$ und daher endlich alle Zahlen $\omega_1', \omega_2', \dots \omega_r'$ teilen. Letzteres ist sicherlich ausgeschlossen, da

$$(\omega_1', \omega_2', \dots \omega_r') = 1.$$

Daher ist $\frac{d}{\delta^{r!}}$ eine Einheit und die Zahlen

$$\omega_1^{r!}, \omega_2^{r!}, \dots \omega_r^{r!}$$

haben zum größten gemeinschaftlichen Teiler die ganze rationale Zahl d, w. z. b. w.

Bezeichnen wir mit e den kleinstmöglichen Wert ($e \geqq 1$), für den $(\omega_1^e, \omega_2^e, \dots \omega_r^e)$ rational wird, so ist e nach dem Vorangehenden ein Teiler von $r!$. Im allgemeinen ist $e > 1$.

Kehren wir nun zu unserer Funktion (3.) zurück. Die elementaren symmetrischen Funktionen der in (3.) auftretenden Zahlen $\omega_1, \omega_2, \dots \omega_r$ sind rational, denn diese r Zahlen sind die verschiedenen Wurzeln des Nenners der rationalen Funktion

$$R(z) = \sum_{\nu=0}^{\infty} F(\nu) z^\nu,$$

die rationale Entwicklungskoeffizienten hat und folglich der Quotient zweier Polynome mit rationalen Koeffizienten ist. Hilfssatz I ist also anwendbar, und es sei die rationale ganze Zahl d der größte gemeinschaftliche Teiler der Potenzen $\omega_1^e, \omega_2^e, \dots \omega_r^e$.

Die e Funktionen

$$F(h+ex)\,d^{-x} = \omega_1^h P_1(h+ex)\left(\frac{\omega_1^e}{d}\right)^x + \dots + \omega_r^h P_r(h+ex)\left(\frac{\omega_r^e}{d}\right)^x$$

$$(h = 0, 1, 2, \dots r-1)$$

sind ganzwertig, und ihre Primteiler sind die Primteiler der Funktionen (3.). Die ganzen Zahlen

$$\frac{\omega_1^e}{d}, \frac{\omega_2^e}{d}, \cdots \frac{\omega_r^e}{d}$$

erfüllen die Bedingung, daß der Quotient von irgend zweien keine Einheitswurzel ist, und überdies ist

$$\left(\frac{\omega_1^e}{d}, \frac{\omega_2^e}{d}, \cdots \frac{\omega_r^e}{d}\right) = 1.$$

Es genügt uns also, Satz II′ unter der Annahme zu beweisen, daß $\omega_1, \omega_2, \ldots \omega_r$ teilerfremd sind.

6. Ich beweise nun eine Reihe von Hilfssätzen, die ich dann später in umgekehrter Reihenfolge zur Anwendung bringen will.

Hilfssatz II*). *Die rationale Funktion $R(z)$ soll im Innern des Einheitskreises keine Pole haben, am Rande des Einheiskreises nur Pole erster Ordnung, und die Koeffizienten $a_0, a_1, a_2, \ldots a_n, \ldots$ ihrer Potenzreihenentwicklung*

$$R(z) = a_0 + a_1 z + a_2 z^2 + \cdots$$

seien rationale ganze Zahlen. — Dann ist

$$R(z) = \frac{P(z)}{1 - z^h}, \tag{14.}$$

wo $P(z)$ ein Polynom mit ganzzahligen Koeffizienten bezeichnet.

Sind die Pole von $R(z)$ am Einheitskreise $e^{i\varphi_1}, \ldots e^{i\varphi_k}$ ($\varphi_1, \varphi_2, \ldots \varphi_k$ reell), so ist

$$R(z) = \frac{B_1}{1 - z e^{-i\varphi_1}} + \cdots + \frac{B_k}{1 - z e^{-i\varphi_k}} + \sum_{n=0}^{\infty} b_n z^n,$$

wo

$$\lim_{n=\infty} b_n = 0. \tag{15.}$$

Es ist

$$a_n = B_1 e^{-i\varphi_1 n} + B_2 e^{-i\varphi_2 n} + \cdots + B_k e^{-i\varphi_k n} + b_n$$
$$|a_n| \leqq |B_1| + |B_2| + \cdots + |B_k| + |b_n|.$$

Wegen (15.) ist also die Folge

$$a_0, a_1, a_2, \ldots a_n, \ldots \tag{16.}$$

---

*) Vgl. *Fatou*, Sur les séries entières à coefficients entiers, Comptes Rendus, Bd. 138 (1904, 1) S. 342—344. *Landau*, Solution de la Question 1852 (Laguerre), Nouvelles Annales, Bd. 3, 4te Folge (1903).

beschränkt. Da nun alle Zahlen (16.) rational ganz sind, gibt es unter ihnen nur endlich viele verschiedene.

Es genügt, den Fall zu betrachten, wo alle $a_n \geqq 0$ sind. Denn die beiden Reihen

$$R(z) \quad \text{und} \quad R(z) + \frac{m}{1-z}$$

sind zugleich von der Form (14.) oder nicht, und, da die Zahlen (16.) ein Minimum besitzen, läßt sich die natürliche ganze Zahl m immer so bestimmen, daß die letztere Reihe keine negativen Koeffizienten hat.

Es sei also $g-1$ das Maximum der positiven Zahlen $a_0, a_1, a_2, \ldots$

$$0 \leqq a_n \leqq g-1.$$

Da $R(z)$ der Quotient zweier Polynome mit ganzzahligen Koeffizienten ist, muß die Zahl

$$R\left(\frac{1}{g}\right) = a_0 + \frac{a_1}{g} + \frac{a_2}{g^2} + \frac{a_3}{g^3} + \cdots$$

rational sein. Sie ist im g-adischen System aufgeschrieben, und daher muß die Folge ihrer Ziffern $a_0, a_1, a_2, \ldots$ von einem gewissen Gliede an periodisch sein. Ist die Länge dieser Periode h, so ist $R(z)$ von der Form (14.), w. z. b. w. —

Betrachten wir die Potenzreihenentwicklung einer rationalen Funktion

$$R(z) = a_0 + a_1 z + a_2 z^2 + \cdots. \tag{17.}$$

Es sei s der Grad des Nenners von $R(z)$, wobei $R(z)$ als der Quotient zweier teilerfremder Polynome gedacht wird. Die Zahl s ist also die Summe der Ordnungen aller (im Endlichen liegenden) Pole von $R(z)$. Ich betrachte die Größe

$$A_n = \text{Max}\,(|a_n|, |a_{n+1}|, \ldots |a_{n+s-1}|).$$

A_n heißt also der absolute Betrag des absolut größten unter den s sukzessiven Koeffizienten $a_n, a_{n+1}, a_{n+2}, \ldots a_{n+s-1}$ der Reihe (17.). Sei ϱ der Konvergenzradius der Reihe (17.). Ich beweise den

Hilfssatz III. *Es ist*

$$\lim_{n=\infty} \sqrt[n]{A_n} = \frac{1}{\varrho}. \tag{18.}$$

Es ist evident, daß

$$\overline{\lim_{n=\infty}} \sqrt[n]{A_n} = \frac{1}{\varrho}, \tag{19.}$$

und der springende Punkt des Hilfssatzes III ist eben der, daß der Grenzwert (18.) existiert.

Hilfssatz III ist offenbar richtig in dem Falle, wo an dem Konvergenzkreise von (17.) nur ein Pol $z = \varrho e^{i\varphi}$ u. zw. von der ersten Ordnung liegt. Dann ist nämlich

$$R(z) = \frac{A}{1 - \frac{z}{\varrho e^{i\varphi}}} + \sum_{n=0}^{\infty} b_n z^n, \tag{20.}$$

wo die Reihe $\Sigma b_n z^n$ für $|z| = \varrho$ konvergiert, wo also

$$\lim_{n=\infty} b_n \varrho^n = 0.$$

Es ergibt sich aus (20.)

$$a_n = \frac{A}{\varrho^n e^{in\varphi}} + b_n = \frac{A e^{-in\varphi} + b_n \varrho^n}{\varrho^n},$$

woraus, wie wohl bekannt,

$$\lim_{n=\infty} \sqrt[n]{|a_n|} = \frac{1}{\varrho}$$

folgt. Nun beweist

$$\overline{\lim_{n=\infty}} \sqrt[n]{A_n} \geqq \lim_{n=\infty} \sqrt[n]{|a_n|} = \frac{1}{\varrho}$$

zusammen mit (19.) die Gleichung (18.).

Auf den eben behandelten speziellen Fall läßt sich nun der allgemeine Fall folgendermaßen zurückführen: Es sei k die Summe der Ordnungen derjenigen Pole von $R(z)$, die am Rande des Konvergenzkreises $|z| = \varrho$ liegen. Es ist $k \leqq s$. Es läßt sich ein Polynom $(k-1)$-ten Grades

$$z^{k-1} + c_1 z^{k-2} + c_2 z^{k-3} + \cdots + c_{k-1}$$

so bestimmen, daß die rationale Funktion

$$(z^{k-1} + c_1 z^{k-2} + \cdots + c_{k-1}) R(z) = \Sigma x^{n+k-1} (a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1})$$

nur einen Pol erster Ordnung am Kreise $|z| = \varrho$ hat. Daher ist

$$\lim_{n=\infty} \sqrt[n]{|a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}|} = \frac{1}{\varrho}.$$

Es ist aber

$$\begin{aligned} |a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}| &\leqq (1 + |c_1| + \cdots + |c_{k-1}|) \operatorname{Max}(|a_n|, \ldots |a_{n+k-1}|) \\ &\leqq (1 + |c_1| + \cdots + |c_{k-1}|) A_n, \end{aligned}$$

woraus

$$\overline{\lim_{n=\infty}} \sqrt[n]{A_n} \geqq \lim_{n=\infty} \sqrt[n]{\frac{|a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}|}{1 + |c_1| + \cdots + |c_{k-1}|}} = \frac{1}{\varrho}$$

folgt, was zusammen mit (19.) den vollen Hilfssatz III ergibt.

Hilfssatz IV. *Es sei* $\varrho = 1$, *und* $R(z)$ *soll am Kreise* $|z| = 1$ *mindestens einen Pol haben, der nicht von der ersten Ordnung ist. Dann ist*

$$\lim_{n=\infty} A_n = +\infty.$$

Man betrachte zuerst den speziellen Fall, wo $R(z)$ am Kreise $|z| = 1$ nur einen Pol $z = e^{i\varphi}$, u. zw. von der Ordnung 2 besitzt. Dieser Fall ist leicht zu erledigen und übrigens auch wohl bekannt. Den allgemeinen Fall, wo die Summe der Ordnungen aller am Einheitskreise liegenden Pole von $R(z)$ etwa k ist $(2 \leqq k \leqq s)$, führt man auf den erwähnten speziellen durch Multiplikation mit einem geeignet gewählten Polynom $(k-2)$-ten Grades zurück, also mit Hilfe des im Beweise von Hilfssatz III angewandten Kunstgriffes.

Betrachten wir nun eine Funktion

$$\Phi(x) = P_1(x)\,\omega_1^x + P_2(x)\,\omega_2^x + \cdots + P_k(x)\,\omega_k^x$$

der ganzzahligen Variablen x, wo $P_1(x), P_2(x), \ldots P_k(x)$ Polynome bedeuten, deren Koeffizienten algebraische ganze Zahlen sind, und wo die Zahlen $\omega_1, \omega_2, \ldots \omega_k$ ebenfalls algebraische ganze Zahlen sind. Es sei K ein Körper, der alle diese ganzen Zahlen enthält, und $\mathfrak{p}$ ein in keiner der Zahlen $\omega_1, \omega_2, \ldots \omega_k$ aufgehendes Primideal des Körpers K.

Es sei vorausgesetzt, daß keines der $\frac{k(k-1)}{2}$ Verhältnisse

$$\frac{\omega_2}{\omega_1}, \frac{\omega_3}{\omega_1}, \ldots \frac{\omega_k}{\omega_1}, \frac{\omega_3}{\omega_2}, \ldots \frac{\omega_k}{\omega_2}, \ldots \frac{\omega_k}{\omega_{k-1}}$$

einer Einheitswurzel gleichkommt. Unter dieser Bedingung besteht der

Hilfssatz V. *Es sei eine arithmetische Progression*

(21.) $\qquad a,\ a+d,\quad a+2d,\quad a+3d, \ldots$

vorgegeben, deren Anfangsglied a *und Differenz* d *natürliche ganze Zahlen sind. Dann läßt sich eine arithmetische Progression*

(22.) $\qquad a_1,\quad a_1+d_1,\quad a_1+2d_1,\quad a_1+3d_1, \ldots \qquad (d_1 > 0)$

deren jedes Glied auch ein Glied der Progression (21.) *ist, und eine natürliche ganze Zahl* m *finden, so daß*

$$\Phi(a_1 + t d_1) \not\equiv 0 \pmod{\mathfrak{p}^m}$$

wird für $t = 0, 1, 2, 3, \ldots$.

Ist jedes Glied von (22.) in (21.) enthalten, so existieren zwei verschiedene nicht negative rationale ganze Zahlen u und v, so daß

$$a_1 = a + ud, \qquad a_1 + d_1 = a + vd,$$

also

$$d_1 = (v-u)d,$$

d. h. ein Multiplum von d wird. Ich werde die Progression (22.) kurz als eine „Teilprogression" der arithmetischen Progression (21.) bezeichnen.

Die k Zahlen

$$\omega_1^d, \omega_2^d, \ldots \omega_k^d$$

sind alle voneinander verschieden, denn wäre $\omega_i^d = \omega_j^d$, so wäre $\frac{\omega_i}{\omega_j}$ eine d-te Einheitswurzel. Daraus folgt, wie den Ausführungen unter 3 zu entnehmen ist, daß die Funktion

$$\Phi(a+xd) = \omega_1^a P_1(a+xd)\omega_1^{dx} + \cdots + \omega_k^a P_k(a+xd)\omega_k^{dx}$$

nicht für jeden Wert $x = 0, 1, 2, 3, \ldots$ verschwinden kann. Es sei also

$$\Phi(a+ud) \neq 0.$$

Ich setze

$$a + ud = a_1.$$

Es sei $\mathfrak{p}^{m-1}$ die höchste Potenz des Primideals $\mathfrak{p}$ $(m \geqq 1)$, die in der dem Körper K angehörigen ganzen Zahl $\Phi(a_1)$ aufgeht, so daß

$$\Phi(a_1) \not\equiv 0 \pmod{\mathfrak{p}^m}.$$

Ich setze

$$d_1 = d\,N(\mathfrak{p}^m)\,\varphi(\mathfrak{p}^m),$$

wo $N(\mathfrak{p}^m)$ die Norm von $\mathfrak{p}^m$ und

$$\varphi(\mathfrak{p}^m) = N(\mathfrak{p}^m)\left(1 - \frac{1}{N(\mathfrak{p})}\right)$$

bedeutet.

Man gebe der Variablen t die Werte $t = 0, 1, 2, 3, \ldots$. Es ist

$$P_i(a_1 + td_1) \equiv P_i(a_1) \pmod{\mathfrak{p}^m},$$

da td_1 teilbar durch $N(\mathfrak{p}^m)$, also durch $\mathfrak{p}^m$ ist. Es ist ferner

$$\omega_i^{a_1+td_1} \equiv \omega_i^{a_1} \pmod{\mathfrak{p}^m},$$

da td_1 teilbar durch $\varphi(\mathfrak{p}^m)$ und, nach Voraussetzung,

$$\omega_i \not\equiv 0 \pmod{\mathfrak{p}}$$

ist. Daher ist

$$\Phi(a_1 + td_1) \equiv \Phi(a_1) \not\equiv 0 \pmod{\mathfrak{p}^m},$$

w. z. b. w.

7. Nun ist ersichtlich, wie der Beweis für Satz II′, für den Hauptsatz dieser Arbeit, zu führen ist.

Es sei K ein Körper, etwa der kleinste Körper, der alle in (3.) auftretenden ganzen Zahlen, also alle Koeffizienten von $P_1(x), P_2(x), \ldots P_r(x)$

und die Zahlen $\omega_1, \omega_2, \dots \omega_r$ enthält. Es sei angenommen, daß in den von Null verschiedenen unter den Zahlen

$$F(0), F(1), F(2), \dots F(n), \dots$$

nur endlich viele Primideale von K, nämlich die Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \dots \mathfrak{p}_l$ aufgehen.

Die Zahlen $\omega_1, \omega_2, \dots \omega_r$ können, auf Grund der Ausführungen unter 5., als teilerfremd vorausgesetzt werden. Sie verteilen sich, mod. $\mathfrak{p}_j$ betrachtet, in zwei Klassen: erstens diejenigen, die durch $\mathfrak{p}_j$ teilbar sind, und zweitens diejenigen, die durch $\mathfrak{p}_j$ nicht teilbar sind. Die erste Klasse kann leer sein, aber die zweite Klasse muß einige der Zahlen $\omega_1, \omega_2, \dots \omega_r$ enthalten, sagen wir die Zahlen $\omega_{i_1}, \omega_{i_2}, \dots \omega_{i_k}$. Ich setze

$$\Phi_j(x) = P_{i_1}(x)\,\omega_{i_1}^x + P_{i_2}(x)\,\omega_{i_2}^x + \dots + P_{i_k}(x)\,\omega_{i_k}^x .$$

Die Funktion $\Phi_j(x)$ genügt in bezug auf $\mathfrak{p}_j$ den dem Hilfssatze V vorausgeschickten Bedingungen. — Ist die natürliche Zahl $x \geqq m$, so ist

$$F(x) \equiv \Phi_j(x) \pmod{\mathfrak{p}_j^m}.$$

Ich bezeichne mit $s - r$ die Summe der Grade aller Polynome $P_1(x), P_2(x), \dots P_r(x)$. Anders gesagt, s ist der Grad des Nenners der rationalen Funktion

$$R(z) = \sum_{n=0}^{\infty} F(n)\, z^n .$$

Gemäß Hilfssatz V greife man aus der arithmetischen Progression

$$0, s, 2s, 3s, \dots ns, \dots$$

eine Teilprogression

$$a_1,\ a_1 + d_1,\ a_1 + 2d_1,\ a_1 + 3d_1, \dots$$

heraus, und man bestimme die natürliche ganze Zahl m_1, so daß

$$\Phi_1(a_1 + t d_1) \not\equiv 0 \pmod{\mathfrak{p}_1^{m_1}},$$

wobei der Variablen t, wie immer im folgenden, die Werte $t = 0, 1, 2, 3, \dots$ zuerteilt werden.

Man greife aus der arithmetischen Progression

$$a_1,\ a_1 + d_1,\ a_1 + 2d_1,\ a_1 + 3d_1, \dots$$

eine Teilprogression

$$a_2,\ a_2 + d_2,\ a_2 + 2d_2,\ a_2 + 3d_2, \dots$$

heraus, und man bestimme m_2 so, daß

$$\Phi_2(a_2 + d_2 t) \not\equiv 0 \pmod{\mathfrak{p}_2^{m_2}}$$

usf.

Nach l Schritten hat man eine arithmetische Progression

$$a_l,\quad a_l+d_l,\quad a_l+2d_l,\quad a_l+3d_l,\ldots \tag{23.}$$

und l ganze Zahlen $m_1, m_2, \ldots m_l$ von folgenden Eigenschaften bestimmt:

Die Progression (23.) ist als Teilprogression in der arithmetischen Progression

$$0, s, 2s, 3s, 4s, \ldots$$

enthalten.

Es ist

$$\Phi_j(a_l+td_l) \not\equiv 0 \pmod{\mathfrak{p}_j^{m_j}}$$
$$(t=0,1,2,3,\ldots;\ j=1,2,3,\ldots l).$$

Ist a_l+td_l größer als die größte der Zahlen $m_1, m_2, \ldots m_l$, so ist

$$F(a_l+td_l) \equiv \Phi_j(a_l+td_l) \not\equiv 0 \pmod{\mathfrak{p}_j^{m_j}}. \tag{24.}$$

Es seien nun

$$p_1, p_2, \ldots p_l$$

die natürlichen Primzahlen, die bzw. unter den Zahlen der Primideale

$$\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_l$$

enthalten sind. $p_1, p_2, \ldots p_l$ brauchen nicht alle verschieden zu sein. Ist x eine natürliche ganze Zahl, so ist $F(x)$ bloß aus den Primfaktoren $p_1, p_2, \ldots p_l$ zusammengesetzt. Es folgt aus (24.), daß

$$F(a_l+td_l) \not\equiv 0 \pmod{p_j^{m_j}}. \tag{25.}$$

Die linke Seite von (25.) soll aber außer $p_1, p_2, \ldots p_l$ durch keine Primzahl teilbar sein, also folgt aus (25.)

$$|F(a_l+td_l)| \leqq p_1^{m_1-1} p_2^{m_2-1} \ldots p_l^{m_l-1}.$$

Ich setze der Kürze halber

$$a_l = A,\ d_l = D.$$

Unser Resultat lautet also: Die unendliche Folge

$$F(A),\quad F(A+D),\quad F(A+2D),\quad F(A+3D),\ldots$$

ist beschränkt.

Durch das beschriebene Verfahren greife man aus der arithmetischen Progression

$$1+A,\quad 1+A+D,\quad 1+A+2D,\quad 1+A+3D,\ldots$$

eine Teilprogression

$$1+A',\quad 1+A'+D',\quad 1+A'+2D',\quad 1+A'+3D',\ldots$$

heraus, von der Eigenschaft, daß auch die Folge

$$F(1+A'),\quad F(1+A'+D'),\quad F(1+A'+2D'),\ldots$$

beschränkt ist. Und so gelangt man nach insgesamt s Schritten (oder in kleinere Schritte zerlegt, nach insgesamt ls Schritten) zu s unendlichen arithmetischen Progressionen

$$\begin{array}{lllll} A^{(s-1)}, & A^{(s-1)}+D^{(s-1)}, & A^{(s-1)}+2D^{(s-1)}, & \dots \\ 1+A^{(s-1)}, & 1+A^{(s-1)}+D^{(s-1)}, & 1+A^{(s-1)}+2D^{(s-1)}, & \dots \\ \dots & \dots & \dots & \dots \\ s-1+A^{(s-1)}, & s-1+A^{(s-1)}+D^{(s-1)}, & s-1+A^{(s-1)}+2D^{(s-1)}, & \dots \end{array} \tag{26.}$$

mit der gemeinsamen Differenz $D^{(s-1)}$ und von der Eigenschaft, daß *die Menge der Werte, die die Funktion $F(x)$ annimmt, wenn man x alle Werte der Tafel* (26.) *zuerteilt, beschränkt ist.*

Nennt man

$$F_n = \operatorname{Max}\big(F(n), F(n+1), \dots F(n+s-1)\big),$$

so folgt daraus, daß $\overline{\lim_{n=\infty}} F_n$ endlich ist.

Die Funktion

$$R(z) = \sum_{n=0}^{\infty} F(n) z^n$$

ist aber eine rationale Funktion, deren Nenner vom Grade s ist. Wendet man die Hilfssätze III, IV, II (in dieser Reihenfolge) auf die Funktion $R(z)$ an, so erhält man nacheinander: $R(z)$ hat keine Pole im Innern des Einheitskreises — $R(z)$ hat am Rande des Einheitskreises nur Pole erster Ordnung — alle Pole von $R(z)$ sind gewisse h-te Einheitswurzeln; und da liegt der Widerspruch. Denn $R(z)$ hat wenigstens zwei verschiedene Pole, und das Verhältnis dieser beiden Pole müßte selbst eine h-te Einheitswurzel sein, entgegen unserer Voraussetzung, daß keines der Verhältnisse $\frac{\omega_i}{\omega_k}$ einer Einheitswurzel gleich ist.

Der Widerspruch löst sich nur dann, wenn man zugibt, daß $F(x)$ unendlich viele Primteiler hat, w. z. b. w.

8. Ich will einige Anwendungen der vorangehenden Resultate kurz erwähnen.

Man kann leicht folgende Aufgabe erledigen: „Alle rationalen Funktionen $R(z)$ zu finden, deren Nenner nur reelle Wurzeln hat und deren Potenzreihenentwicklung nur endlich viele Primfaktoren enthält".

$R(z)$ ist nämlich entweder von der Form

$$\frac{a}{1-bz} \tag{27.}$$

(a, b rational) oder von der Form

$$\frac{a}{1-bz^2} + \frac{a'z}{1-b'z^2} \tag{28.}$$

(a, a' rational, b, b' rational und positiv), oder es unterscheidet sich von einer der beiden Funktionen (27.) (28.) nur um ein additives Polynom.

Die Anwendung des Satzes II′ (es genügt schon II″) auf die Funktion

$$F(x) = 2^{n^x} - m$$

ergibt den Satz: Es gibt unendlich viele Primzahlen, für welche eine vorgegebene Zahl m n-ter Potenzrest ist. Letzterer Satz folgt übrigens auch aus der Existenz unendlich vieler Primzahlen in arithmetischen Progressionen.

Es drängt sich die Frage auf, ob die rationalkoeffizientigen Potenzreihenentwicklungen algebraischer Funktionen stets unendlich viele Primfaktoren enthalten oder nicht. Für die Binomialreihen mit rationalen gebrochenen Exponenten ist die Frage schnell geklärt: In den Zählern gehen unendlich viele Primzahlen auf, nämlich alle Primzahlen mit Ausnahme derjenigen endlich vielen, die in den Nennern aufgehen. Die allgemeine Frage anzufassen scheint keine leichte Aufgabe zu sein.

(Abgeschlossen im Dezember 1915.)