22.

Der *Eisenstein*sche Satz über Reihen-Entwickelung algebraischer Functionen.

(Von Herrn Prof. *Heine* zu Bonn.)

In dem Monatsberichte der Akademie der Wissenschaften zu Berlin, vom Juli 1852, S. 441, findet sich eine kurze Notiz, in welcher *Eisenstein* einen wichtigen Satz über algebraische Functionen ohne Beweis aufstellt, indem er die weitere Ausführung einer künftigen Mittheilung vorbehält, die sein früher Tod vereitelte. Die *Eisenstein*sche Notiz enthält Folgendes:

„Entwickelt man die Quadratwurzel aus $1+x$, etwa nach dem bi„nomischen Satze für gebrochene Exponenten, in eine unendliche Reihe „nach steigenden Potenzen von x, und sucht die sich ergebenden ratio„nalen Coëfficienten auf ihre *kleinste Benennung* zu bringen, so be„merkt man, dafs nur Potenzen von 2 in den Nennern derselben zurück„bleiben, während alle übrigen Factoren des Nenners gegen Factoren „des Zählers aufgehoben werden können; auch ist der Exponent der im „Nenner des allgemeinen Gliedes verbleibenden Potenz von 2 immer „kleiner als der doppelte Exponent von x (und zwar beiläufig gesagt „um so viel, als die Anzahl der Einheiten beträgt, mit denen der Ex„ponent von x nach dem Dual-System geschrieben wird), so dafs es „genügt, $4x$ statt x zu setzen, um alle Nenner wegzuschaffen und die „Coëfficienten der Reihe in ganze Zahlen zu verwandeln. Die Betrach„tung dieses, wahrscheinlich längst bekannten speciellen Falles führte mich „auf die Entdeckung einer merkwürdigen, allen algebraischen Functionen „gemeinschaftlichen Eigenthümlichkeit. In jeder Reihen-Entwickelung „dieser Art, wenn sie nur aus einer *algebraischen Function* stammt, „mag dieselbe übrigens explicite oder implicite gegeben sein, kommen in „sämmtlichen Coëfficienten, so fern dieselben rational sind, als nothwendige „Nenner, d. h. als solche, die sich nicht weiter gegen Factoren des „Zählers aufheben lassen, stets nur eine *endliche Anzahl ganz be-„stimmter Primfactoren* und deren Potenzen vor; es sind diese Prim„zahlen zugleich die Divisoren einer aus der algebraischen Gleichung,

„welcher die Function Genüge leistet, leicht zu bildenden characteristischen „Zahl, nämlich ihrer dem speciellen Werthe $x=0$ entsprechenden, von „*Gaufs* sogenannten Determinante, welche bekanntlich nicht verschwinden „darf, wenn die Reihen-Eutwicklung überhaupt möglich sein soll; endlich „kann statt x immer ein solches Vielfache von x gesetzt werden, dafs „alle Coëfficienten der Reihe in ganze Zahlen übergehen. Nachdem diese „allgemeine Eigenschaft erst bekannt war, fiel es nicht schwer, dieselbe „durch die Methode der unbestimmten Coëfficienten zu erweisen und „auch auf die aus der Auflösung eines Systems von beliebig vielen „algebraischen Gleichungen hervorgehenden Entwicklungen auszudehnen. „Die wichtigsten Anwendungen der so erhaltenen Sätze habe ich auf „Fälle gemacht, in welchen die algebraischen Functionen als Integrale von „Differential-Gleichungen definirt werden, und wo diese Differential-Glei„chungen für eine einfache Reihen-Entwicklung geeignet sind, während die, „vielleicht sehr complicirte Darstellung in endlicher Form ganz unbekannt „bleibt und für diesen Zweck auch wirklich ganz aus dem Spiele ge„lassen werden kann. Das Einzelne der hierauf bezüglichen Unter„suchungen mag für eine künftige Mittheilung vorbehalten bleiben. Eine „andere sehr einfache Art der Anwendung beruht darauf, dafs jede „Reihen-Entwicklung mit rationalen Coëfficienten, für welche die obi„gen Bedingungen nicht erfüllt werden, sicher aus einer transcendenten, „d. h. *nicht* algebraischen Function, hervorgegangen sein mufs. Da z. B. in „der bekannten logarithmischen Reihe

$$\log(1+x) = x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 - \cdots,$$

„wenn man hinreichend weit fortgeht, jede beliebige, noch so grofse „Primzahl als Nenner eines Coëfficienten angetroffen wird, so folgt hier„aus, dafs der Logarithmus keine algebraische, sondern eine wesentlich „transcendente Function ist. Ähnliches gilt von der Reihe für e^x, und „unendlich vielen andern."

Nachdem der Urheber des Theorems die in demselben ausgesprochene Eigenschaft algebraischer Functionen einmal entdeckt hatte, war es nicht schwer, den nachfolgenden Beweis desselben zu finden.

1.

Wir gehen von der Betrachtung der Reihe aus, welche $(1+x)^n$, nach aufsteigenden Potenzen von x entwickelt, giebt. Es bedeutet n eine positive oder negative rationale Zahl, die gleich $\frac{g}{h}$ sein mag, indem unter g und h ganze Zahlen ohne gemeinschaftlichen Theiler verstanden werden, so dafs in der binomischen Reihe der Bruch

$$b = \frac{g(g-h)(g-2h)\dots(g-(m-1)h)}{1.2.3\dots\dots\dots m}$$

der Coëfficient von $\left(\frac{x}{h}\right)^m$ ist. Bringt man diesen Bruch auf die kleinste Benennung, so wird sein Nenner nur durch solche Primzahlen theilbar sein, welche auch h (den Nenner von n) theilen. Zunächst ist nämlich klar, dafs, wenn eine Primzahl q, die in dem Nenner von b explicite oder implicite (als Vielfaches von q) vorkommt, h theilt, diese Primzahl gegen keinen Factor des Zählers sich aufheben kann, also im Nenner, *nach* der Reduction des Bruchs, grade so oft als Factor erscheint, wie *vorher*. Jede andere Primzahl p wird aber, wie sogleich gezeigt werden soll, eben so oft, oder einmal mehr, im Zähler als im Nenner enthalten sein; hebt sich also aus diesem weg.

Um diese Eigenschaft der p zu erweisen, theile man den *Nenner* von b in Gruppen, deren jede p aufeinanderfolgende Zahlen enthält, so dafs nur in der letzten Gruppe deren weniger als p vorkommen können; und zwar wird dieser Fall immer vorkommen, wenn m nicht durch p theilbar ist. Es bestehe z. B. die erste und die zweite Gruppe resp. aus den Gliedern $1.2.3\dots p$ und $(p+1)(p+2)\dots(2p)$. In jeder Gruppe, die letzte im Allgemeinen ausgenommen, wird *ein*, und *nur ein* durch p theilbares Glied vorkommen; und zwar ist dies immer das *letzte* Glied der Gruppe.

Theilt man den *Zähler* in ähnliche Gruppen, deren erste also $g(g-h)(g-2h)\dots(g-(p-1)h)$ ist, so wird in jeder derselben, mit Ausnahme der letzten, *ein* und *nur ein* durch p theilbares Glied vorkommen müssen (und zwar wird dasselbe in der Regel nicht erst das letzte Glied der Gruppe sein), während in der letzten ein durch p theilbares Glied vorkommen kann, und jedenfalls auch vorkommt, wenn m durch p theilbar ist. Man sieht dies leicht, wenn man erwägt, dafs g und h keinen gemeinsamen Theiler haben und daher die Congruenz

$$g - zh \equiv 0 \text{ mod. } p$$

eine Wurzel z hat, die zwischen 0 und $p-1$ liegt, *eine* zwischen p und $2p-1$, u. s. w. Es befinden sich daher im Zähler eben so viele Glieder, welche durch p theilbar sind, als im Nenner; oder sogar eins mehr.

Unter diesen durch p theilbaren Gliedern werden auch solche sein können, die durch eine höhere als die erste Potenz von p theilbar sind. Dadurch, dafs man Gruppen von p^α Gliedern bildet, findet man, mittels eines dem obigen ganz ähnlichen Verfahrens, nämlich durch Betrachtung der Congruenz

$$g - zh \equiv 0 \text{ mod. } p^\alpha,$$

dafs im Zähler eben so viele Glieder durch p^α theilbar sind, wie im Nenner, oder sogar eins mehr. Wir haben daher folgenden Satz:

Entwickelt man $(1+x)^{\frac{g}{h}}$ nach aufsteigenden Potenzen von x, so enthalten die Coëfficienten der verschiedenen Potenzen von x, in ihrer kleinsten Benennung, keine andern Nenner als solche, die in Potenzen von h aufgehen. Diese Nenner sind also nur durch solche Primzahlen theilbar, welche auch Theiler von h sind.

So z. B. können in der Entwickelung von $(1+x)^{\frac{4}{15}}$ alle Nenner, bis auf die Potenzen von 3 und 5, weggeschafft werden.

Anm. Auf folgende Art läfst sich ein Ausdruck für die höchste Potenz von p aufstellen, welche $1.2.3\ldots\ldots m$ theilt. Man zerlege m in die Form

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r,$$

wo durch die a positive ganze Zahlen kleiner als p bezeichnet werden, die auch zum Theil Null sein können. Eine solche Zerlegung kann *nur auf eine Art* geschehen. Es giebt dann unter den Zahlen von 1 bis m:

$$\begin{array}{ll}
a_r p^{r-1} + a_{r-1} p^{r-2} + a_{r-2} p^{r-3} + \cdots + a_2 p + a_1 & \text{durch } p, \\
a_r p^{r-2} + a_{r-1} p^{r-3} + a_{r-2} p^{r-4} + \cdots + a_2 & \text{durch } p^2, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
a_r p^2 + a_{r-1} p + a_{r-2} & \text{durch } p^{r-2}, \\
a_r p + a_{r-1} & \text{durch } p^{r-1}, \\
a_r & \text{durch } p^r
\end{array}$$

theilbare Zahlen, so dafs die höchste Potenz von p, welche das Product $1.2.3\ldots m$ theilt, die Gröfse

$$(a_1 + a_2 + \cdots + a_r) + (a_2 + \cdots + a_r) p + \cdots + (a_{r-1} + a_r) p^{r-2} + a_r p^{r-1}$$

zum Exponenten hat. Z. B. für $m = 131$ setze man $p = 7$. Dann ist

$$131 = m = 5 + 4.7 + 2.7^2,$$

also das Product $1.2.3\ldots 131$ noch durch 7^{20} theilbar. Die höchste Potenz von 3, die in dasselbe Product aufgeht ist 3^{62}, da

$$131 = 2 + 1.3 + 2.3^2 + 3^3 + 3^4 \text{ ist.}$$

2.

Eine irrationale Zahl nennt man eine solche, welche durch Addition, Subtraction, Multiplication, Division und Erhebung zu *positiven* Potenzen aus ganzen rationalen Zahlen entsteht. Wurde die Division nicht angedeutet, so soll die Zahl eine *ganze* heifsen; so dafs eine ganze Zahl rational, oder irrational sein kann. Dem Worte ***Primzahl*** geben wir keinen erweiterten Begriff; nur die rationalen Zahlen 2, 3, 5 etc. werden darunter verstanden. Eine ganze Zahl heifse ***theilbar*** durch eine zweite ganze Zahl, wenn die erste sich als Product der zweiten und einer dritten ganzen Zahl vorstellen läfst. Die beiden letzten Zahlen heifsen ***Theiler*** oder ***Factoren*** der ersten.

Man sieht leicht, dafs sich jede irrationale Zahl als Quotient zweier ganzen Zahlen darstellen läfst, deren eine ihr ***Zähler,*** die andere ihr ***Nenner*** heifst. So z. B. ist $\sqrt{(1-\sqrt{\frac{2}{3}})}$ gleich dem Quotienten von $\sqrt{(\sqrt{3}-\sqrt{2})}$ und $\sqrt[4]{3}$; $\sqrt[4]{3}$ ist der Nenner von $\sqrt{(1-\sqrt{\frac{2}{3}})}$. Verbindet man zwei ganze Zahlen durch Addition, Subtraction und Multiplication, oder erhebt man eine solche Zahl zu einer positiven Potenz, so entsteht wieder eine ganze Zahl.

3.

Entwickelt man das Polynom

$$(a_0+a_1x+a_2x^2+\cdots+a_mx^m)^n$$

nach aufsteigenden Potenzen von x, so wird der Coëfficient einer jeden Potenz von x, *erstens* aus Binomialcoëfficienten, *zweitens* aus ganzen positiven Potenzen der a, und endlich auch aus negativen Potenzen non a_0 durch Addition, Subtraction und Multiplication zusammengesetzt sein. Beachtet man, dafs nach (§. 1.) die erwähnten Binomialcoëfficienten in ihrer kleinsten Benennung keine andern Nenner enthalten können, als Potenzen des Nenners von n, so findet man folgenden Satz:

> Bedeuten die Gröfsen a rationale oder irrationale Zahlen, so werden sich die Coëfficienten sämmtlicher Potenzen von x in der Entwickelung von
>
> $$(a_0+a_1x+a_2x^2\ldots+a_mx^m)^n$$
>
> nach aufsteigenden Potenzen von x, als Quotienten zweier ganzen Zahlen darstellen lassen, deren eine (der Nenner) ein Product aus Potenzen der Nenner der a, des Zählers von a_0 und des Nenners von n ist.

4.

Durch Addition, Subtraction und Multiplication zweier Reihen oder ganzen Functionen von x kommen keine neuen Primzahlen in die Nenner; durch

Erhebung einer nach x geordneten Function zu einer positiven oder negativen Potenz (§. 3.), nur eine beschränkte Anzahl derselben. Da sich aber jede algebraische Function einer Veränderlichen x durch eine gewisse Anzahl der vorgenannten Operationen aus x und Constanten (die man sich nicht als transcendent vorstellen darf, wie z. B. sin 2, sondern höchstens als irrational) zusammensetzen läfst, so findet man (§. 2.) folgenden Satz:

Läfst sich eine algebraische Function einer Veränderlichen x nach aufsteigenden Potenzen derselben entwickeln, so können die mit den Potenzen von x multiplicirten constanten Coëfficienten als Brüche dargestellt werden, deren Nenner Producte aus Potenzen einer beschränkten Anzahl ganzer Zahlen sind.

Man darf nicht glauben, dafs dieser Satz schon unmittelbar mit dem ersten Theile des zu beweisenden Satzes übereinstimmt. Es ist nämlich zu zeigen, dafs in solchen Reihen die Coëfficienten, *insofern sie rational sind,* eine endliche Anzahl bestimmter Primfactoren und deren Potenzen enthalten. (Die *Exponenten* dieser Potenzen können natürlich in unendlicher Anzahl vorkommen). Es wäre nun wohl denkbar, dafs eine Reihe von Brüchen, deren Zähler und Nenner irrationale ganze Zahlen und deren Nenner aufserdem Producte aus Potenzen einer *endlichen* Anzahl gegebener ganzer Zahlen sind, dennoch, wenn die Brüche rational werden, Nenner enthalte, die durch alle möglichen Primzahlen getheilt werden können. Das gewonnene Resultat stimmt aber offenbar mit dem gesuchten überein, wenn folgende Eigenschaften irrationaler Zahlen erwiesen werden können:

a) Sind Z und N irgend welche ganze Zahlen, g und h rationale ganze Zahlen, die keinen gemeinschaftlichen rationalen Theiler haben: so kann $\frac{Z}{N}$ nur dann gleich $\frac{g}{h}$ sein, wenn Z durch g und N durch h theilbar ist.

b) Eine Zahl N, und ihre Potenzen, sind nur durch eine endliche Anzahl verschiedener Primzahlen theilbar.

Mit dem Beweise dieser Sätze, welche einer Theorie der irrationalen Zahlen angehören, werden wir die gegenwärtige Abhandlung schliefsen; zunächst aber zu dem allgemeinen Falle der Reihen-Entwickelung impliciter Functionen uns wenden, welcher den eben behandelten umfafst, ohne die Eigenschaften irrationaler Zahlen vorauszusetzen.

5.

Der zweite Theil des *Eisenstein*schen Satzes beschäftigt sich mit dem Falle, wo eine Function von x, welche die Wurzel einer algebraischen Gleichung im weiteren Sinne ist, in eine nach Potenzen von x aufsteigende Reihe mit rationalen Coëfficienten entwickelt werden kann. Es wird behauptet, dafs die nothwendigen Nenner dieser Coëfficienten nur durch eine endliche Anzahl verschiedener Primzahlen theilbar sind.

Die allgemeinste Form einer algebraischen Gleichung zwischen einer unabhängigen Veränderlichen x und einer abhängigen y ist die, dafs eine gegebene algebraische Function von x und y Null sein soll. Wir müssen annehmen, dafs die Constanten, welche in dieser Function vorkommen, höchstens irrationale Zahlen, aber nicht transcendente sind. Unter dieser Voraussetzung kann die gegebene Gleichung, wie man weifs, durch Multiplication mit geeigneten Factoren auf die Form einer algebraischen Gleichung im engern Sinne gebracht werden, d. h. auf die Form

$$f(y,x) = 0,$$

wo $f(y,x)$ eine ganze Function von x und y, mit rationalen ganzzahligen Coëfficienten ist. Jede Wurzel der ursprünglichen Gleichung wird auch eine Wurzel der letzten sein, die wir uns schon von gleichen Wurzeln befreit vorstellen. Hierdurch wird allerdings noch nicht die Möglichkeit ausgeschlossen, dafs einige Wurzeln für besondere Werthe von x, z. B. für $x=0$, einander gleich seien.

Die Gleichung $f(y,x)=0$ sei nach y vom m^{ten} Grade, und habe also die Form

$$f(y,x) = A_0 y^m + A_1 y^{m-1} + \cdots + A_{m-1} y + A_m = 0,$$

wo die A ganze Functionen von x mit rationalen ganzen Coëfficienten sind, die sich für $x=0$ auf a_0, a_1, a_m reduciren mögen, so dafs für $x=0$,

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

ist. Hier sind die a rationale ganze Zahlen; es können auch einige von ihnen Null sein, aber nicht alle zugleich, wenn man die A von ihrem gröfsten, allen gemeinschaftlichen Theiler befreit hat. Diejenige Wurzel der Gleichung $f(y,x)=0$, welche wir betrachten, die also durch eine Potenzenreihe mit rationalen Coëfficienten ausgedrückt ist, sei

$$y_0 = c_0 + c_1 x + c_2 x^2 + \cdots,$$

so dafs c_0 eine rationale Wurzel der Gleichung $f(y,0)=0$ ist. Es ist nun zu bezweisen, dafs die Nenner der c nur durch eine endliche Anzahl verschiedener Primzahlen theilbar sind.

Offenbar wird es genügen, wenn man den Beweis für alle c, von einem bestimmten, dem n^{ten} an, giebt, da c_0. c_1, bis zu c_n hin, gewifs nur eine endliche Anzahl von Nennern haben, indem die Anzahl dieser Glieder endlich ist.

6.

Wir behandeln nun zunächst den Fall, dafs $f(y,0)=0$ nicht mehrere Wurzeln hat, die gleich c_0 sind, dafs also

$$ma_0 c_0^{m-1}+(m-1)a_1 c_0^{m-2}+\cdots+2a_{m-2}c_0+a_{m-1}$$

nicht verschwindet. Es ist dieser Ausdruck nämlich gleich

$$\frac{\partial f(y,0)}{\partial y},$$

für $y=c_0$.

Man gehe zunächst, von c_0 anfangend, in der Reihe der c bis zu einem solchen, dessen Index gröfser als der Grad von A_m ist (§. 5.). Es ist leicht zu sehen, welche Primzahlen p in der unendlichen Reihe der c, von dem bezeichneten an, in den Nennern vorkommen dürfen. Kommt nämlich die Primzahl p zuerst in dem Nenner von c_n als Theiler vor (wo nun n gröfser als der Grad von A_m ist), so wird sie in allen ganzen positiven Potenzen von y_0 gleichfalls zuerst in dem mit x^m multiplicirten Gliede sich zeigen können; und zwar enthalten y, y^2, y^3, ... y^m, nach dem polynomischen Lehrsatze, den Nenner p im Coëfficienten von x^n resp. in folgender Verbindung:

$$c_n,\; 2c_0c_n,\; 3c_0^2c_n,\; \ldots\; mc_0^{m-1}c_n.$$

Setzt man in die Gleichung $f(y,x)=0$ für y seinen Werth, ausgedrückt durch die Reihe, und ordnet nach Potenzen von x, so mufs der Coëfficient jeder Potenz von x, also auch von x^n, für sich verschwinden. Dieser besteht aber aus einem Theile, welcher p gewifs nicht im Nenner enthalten kann (indem er aus den in den A vorkommenden rationalen ganzen Zahlen und den c von c_0 bis c_{n-1} zusammengesetzt ist), und aus dem Theile

$$c_n(ma_0c_0^{m-1}+(m-1)a_1c_0^{m-2}\cdots+2a_{m-2}c_0+a_{m-1}).$$

Es mufs sich also auch aus diesem das p wegheben, *so dafs in den Nennern nur solche Primzahlen p vorkommen können, welche Theiler von dem*

Zähler des Ausdrucks

$$ma_0 c_0^{m-1}(m-1)a_1 c_0^{m-2} + \cdots + a_{m-1}$$

sind, der nach der Annahme nicht Null ist.

7.

Wir kommen zu dem Falle, wo $f(y,0) = 0$ *gleiche* Wurzeln hat. Es scheint mir auf einem Irrthum zu beruhen, wenn *Eisenstein* sagt, dafs die von *Gaufs* sogenannte *Determinante* von $f(y,0)$ nicht verschwinden darf, wenn eine Reihen-Entwickelung überhaupt möglich sein soll. Die Determinante dieser Function ist nach *Gaufs* (Commentat. Gotting. Classis Math. Tom. III. p. 114, „Demonstratio nova altera theor. omnem funct. algebr. etc. §. 6.") nichts anders, als das Product der m Werthe, welche

$$\frac{\partial f(y,0)}{\partial y}$$

annimmt, wenn man, nach Ausführung der Differentiation, für y der Reihe nach die m Wurzeln von $f(y,0) = 0$ setzt. Die Determinante verschwindet nur, und immer, wenn $f(y,0) = 0$ einige *gleiche* Wurzeln hat. Also müfste nach obiger Behauptung, wenn ich die betreffende Stelle nicht unrichtig deute, in gegenwärtigem Falle keine Reihen-Entwickelung einer Wurzel der Gleichung $f(y,x) = 0$ möglich sein. Man findet indessen, zunächst in speciellen Fällen, wenn auch die Determinante für $x = 0$ verschwindet, allerdings Reihen-Entwickelungen; wie es das Beispiel der Gleichung

$$f(y,x) = y^2 - 2(1+x)y + 1 + 2x + x^3 = 0$$

zeigt, deren Wurzeln

$$y = 1 + x + x\sqrt{(1-x)}$$

und

$$y = 1 + x - x\sqrt{(1-x)}$$

sich offenbar in Reihen entwickeln lassen, während die Determinante von

$$f(y,0) = y^2 - 2y + 1$$

verschwindet. Aufserdem sehe ich keinen Grund, aus welchem im vorliegenden Falle die Reihen-Entwickelung im allgemeinen unmöglich sein sollte, wenn gleich gewisse einfache Kunstgriffe angewendet werden müssen, um sie zu finden. Wie *Jacobi* in diesem Journal (Band 6. S. 273) bemerkt, hat *Laplace,* der in den „Mémoires de Mathématique et de Physique de l'Académie royale des sciences pour 1777 p. 99" zuerst die *Lagrange*'sche Umkehrungsformel bewies (Histoire, p. 54), an der Stelle wo er die Wurzel y einer Gleichung $f(y,x)=0$ in eine Reihe entwickeln will, wenn $f(y,0)=0$ gleiche Wurzeln hat (Mémoires p. 121), einen Irrthum begangen, den ***Jacobi*** am angezeigten Orte berichtigt.

Will man eine Wurzel der Gleichung $f(y,x)$ in eine nach Potenzen von x geordnete Reihe entwickeln, so hat man y, $\frac{dy}{dx}$, $\frac{d^2y}{dx^2}$, etc. für $x=0$ zu suchen. Schreibt man zur Abkürzung f statt $f(y,x)$, und wendet das Zeichen ∂ für das ***partielle***, das Zeichen d für das ***vollständige*** Differentiiren an, so wird

$$\frac{dy}{dx}=-\frac{\frac{\partial f}{\partial x}}{\frac{\partial f}{\partial y}}.$$

Hat nun $f(y,0)=0$ mehrere gleiche Wurzeln c_0, so wird $\frac{\partial f}{\partial y}$ für $x=0$ verschwinden und $\frac{dy}{dx}$ für $x=0$ die Form $\frac{0}{0}$ bekommen; den wahren Werth des Bruchs wird man durch $(r-1)$malige Differentiation von Zähler und Nenner erhalten, wenn $f(y,0)=0$ eine Anzahl r gleicher Wurzeln hat. So entsteht eine Gleichung r^{ten} Grades für $\frac{dy}{dx}$, die auch die nothwendige Anzahl von Werthen dieser Gröfse, nämlich r, giebt. Ähnlich findet man $\frac{d^2y}{dx^2}$, u. s. w. für $x=0$. Hätte z. B. $f(y,0)=0$ zwei Wurzeln c_0, so wird

$$\frac{dy}{dx}=-\frac{d\frac{\partial f}{\partial x}}{d\frac{\partial f}{\partial y}}$$

für $x=0$, d. h.

$$=-\frac{\frac{\partial^2 f}{\partial x^2}+\frac{\partial^2 f}{\partial x\,\partial y}\cdot\frac{dy}{dx}}{\frac{\partial^2 f}{\partial x\,\partial y}+\frac{\partial^2 f}{\partial y^2}\cdot\frac{dy}{dx}},$$

so dafs $\frac{dy}{dx}$ für $x=0$ die Wurzel einer Gleichung ***zweiten*** Grades ist, nämlich von

$$\left(\frac{dy}{dx}\right)^2\frac{\partial^2 f}{\partial y^2}+2\left(\frac{dy}{dx}\right)\frac{\partial^2 f}{\partial x\,\partial y}+\frac{\partial^2 f}{\partial x^2}=0,$$

wenn man nach Ausführung sämmtlicher Differentiationen $x=0$ und $y=c_0$ setzt.

8.

Hat $f(y,0)=0$ *gleiche* Wurzeln, und läfst sich eine Wurzel der Gleichung $f(y,x)=0$ wieder in die Reihe

$$y_0 = c_0 + c_1 x + c_2 x^2 + \cdots$$

entwickeln, so bleibt der Satz im wesentlichen bestehen; nämlich:

Nimmt man n grofs genug an, so wird

$$y - (c_0 + c_1 x \cdots + c_{n-1} x^{n-1})$$

für keine andere Wurzel der Gleichung $f(y,x)=0$ als für $y=y_0$ durch x^n theilbar sein, d. h., durch x^n getheilt, für $x=0$ noch einen endlichen Werth geben. Sollte man gerade ein solches n angenommen haben, dafs dieser endliche Werth für $x=0$ gleich Null ist, so wird ein noch gröfseres, geeignet gewähltes n diese letzte Eigenschaft der Differenz verhindern.

Wäre nämlich auch für die Wurzel y die Differenz

$$y_1 - (c_0 + c_1 x \cdots + c_{n-1} x^{n-1}),$$

wie grofs man auch n annimmt, durch n theilbar, so müfste offenbar y_1 mit y_0 übereinstimmen.

Setzt man

$$y = (c_0 + c_1 x \cdots + c_{n-1} x^{n-1}) + x^n \eta,$$

so wird man (§. 5.) aus der Gleichung für y eine ähnliche für η erhalten; nämlich:

$$B_0 \eta^m + B_1 \eta^{m-1} + \cdots + B_{m-1} \eta + B_m = 0,$$

in welcher die B ganze Functionen von x (mit ganzen rationalen Coëfficienten) sind, die wir uns *frei von einem gemeinsamen Factor* vorstellen und die sich *daher* für $x=0$ in rationale ganze Zahlen $b_0, b_1, \ldots b_{m-1}, b_m$ verwandeln, *welche nicht sämmtlich Null sein können.* Von den m Wurzeln der vorstehenden Gleichung wird nur *eine* für $x=0$ einen endlichen Werth haben; nämlich die aus y_0 entstandene, η_0, deren Werth durch die Gleichung

$$y_0 = (c_0 + c_1 x \cdots + c_{n-1} x^{n-1}) + x^n \eta_0$$

gegeben ist, so dafs

$$b_0 z^m + b_1 z^{m-1} \cdots + b_{m-1} z + b_m = 0$$

eine Gleichung ersten Grades sein mufs. Es verschwinden daher $b_0, b_1, \ldots b_{m-2}$, nicht aber b_{m-1} und b_m. Würde nämlich b_{m-1} gleich Null, so müfsten auch b_m, also alle b verschwinden; was nicht geschehen kann (S. oben). Wäre ferner b_{m-1} nicht Null, wohl aber b_m, so würde $z = -\frac{b_m}{b_{m-1}} = 0$ sein, also der Werth von η_0 für $x = 0$, d. h. c_n verschwinden. Es war aber n so angenommen, dafs dies nicht Statt findet.

Setzt man für η_0 den ihm zukommenden Werth

$$\eta_0 = c_n + c_{n+1}x + c_{n+2}x^2 + \cdots$$

in seine Gleichung vom m^{ten} Grade, so hat man ähnliche Betrachtungen anzustellen wie in (§. 6.), die aber hier einfacher sind. Man wird ohne Mühe sehen, dafs in dem Nenner eines hinlänglich entfernten Gliedes c_{n+s} (und zwar mufs s gröfser sein als der Grad von B_m) eine neue Primzahl p nur dann auftreten kann, wenn sie b_{m-1} theilt. Also ist auch in diesem Falle die Anzahl der Primzahlen beschränkt, welche die Nenner der Coëfficienten unserer Reihe, wenn sie auf ihre kleinste Benennung gebracht sind, theilen.

Wir schliefsen hieraus, dafs $\log x$, $\operatorname{arc\,tang} x$, $\sin x$, e^x, u. s. w. *wirkliche Transcendenten* sind, d. h. nicht algebraische Functionen, ja nicht einmal Wurzeln algebraischer Gleichungen.

9.
Beweis der Sätze in §. 4.

Hülfssätze. Bezeichnet I irgend eine irrationale Zahl, so kann man dieselbe leicht als Wurzel einer Gleichung

$$I^m - A_1 I^{m-1} + A_2 I^{m-2} - \cdots \pm A_m = 0$$

darstellen, in welcher die Coëfficienten A rational sind. War I eine ganze Zahl (§. 2.), so kann man auch immer erreichen, dafs die A rational und ganz werden.

Der Beweis des ersten Theils dieses Satzes würde keine Schwierigkeiten haben, so dafs wir nur den Fall untersuchen wollen, wo I eine *ganze* Zahl bezeichnet. Das verlangte Resultat wird sich ergeben, wenn man I in die Theile auflöset, aus welchen es entstanden ist. Dazu theile man die irrationalen Zahlen in *Ordnungen,* auf die Weise, wie es *Abel* in seinem „Beweise der Unmöglichkeit, Gleichungen von höherem als dem 4ten Grade allgemein aufzulösen" (Journal, Bd. I. S. 67) gethan hat. Der Kürze wegen mag im Folgenden der Ausdruck „ganze *Function*" auch von *Zahlen* gebraucht werden; und zwar soll ein Aggregat, welches aus Zahlen *a, b, c,* etc. durch Addition, Subtraction und Multiplication entstanden ist, ohne dafs aufser *a, b, c,* etc. noch andere als rationale ganze Zahlen benutzt wurden, eine *ganze Function* von a, b, c, etc. heifsen. So ist $2a+b$ eine *ganze* Function von a und b, nicht aber $a\sqrt{2}+b$. Zählen wir Wurzel-Ausziehungen, so nehmen wir solche, deren Exponent eine Primzahl ist, für *eine*, also z. B. eine 15^{te} Wurzel, da $15=3.5$ ist, für eine *zweifache* Wurzel-Ausziehung.

Irrational erster Ordnung heifst dann eine ganze Function von rationalen ganzen Zahlen und einfachen Wurzeln; *Irrational zweiter Ordnung* eine ganze Function rationaler ganzer Zahlen, von Irrationalen erster Ordnung und einfachen Wurzeln aus Irrationalen erster Ordnung; u. s. w. *Die Irrationalen der verschiedenen Ordnungen sind ganze Zahlen;* eine Irrationale 0^{ter} Ordnung ist eine rationale ganze Zahl. Wir werden uns dann I als Irrationale einer gewissen, der n^{ten} Ordnung, vorstellen können; und zwar seien die Wurzeln aus den Irrationalen $(n-1)^{\text{ter}}$ Ordnung, die in ihr vorkommen,

$$\sqrt[e_1]{r_1},\quad \sqrt[e_2]{r_2},\quad \sqrt[e_3]{r_3},\quad \text{etc.};$$

wo also die e Primzahlen die r Irrationalen $(n-1)^{\text{ter}}$ Ordnung vorstellen. Potenzen von $\sqrt[e]{r}$ sind von keiner höheren Ordnung als diese Wurzeln selbst, und können unter der oben befindlichen Reihe von e_1^{ten}, e_2^{ten}, etc. Wurzeln vorkommen; dagegen braucht man in diese Reihe nur die ersten $e-1$ Potenzen aufzunehmen, da für ein ganzes rationales z,

$$(\sqrt[e]{r})^{ez+\alpha}$$

gleich der α^{ten} Potenz von $\sqrt[e]{r}$, multiplicirt mit einer ganzen Potenz von r, d. h. mit einer Irrationalen $(n-1)^{\text{ter}}$ Ordnung ist. Es läfst sich also I als ganze Function von $\sqrt[e_1]{r_1}$, $\sqrt[e_2]{r_2}$, etc. und ihrer resp. e_1-1, e_2-1, etc. ersten Potenzen, aufserdem aber von Gröfsen einer niedrigeren als der n^{ten} Ordnung darstellen. Setzt man jene e_1^{ten}, e_2^{ten}, etc. Wurzeln resp. gleich ϱ_1, ϱ_2, etc., so hat I die Form

$$I = \Sigma g_{s_1, s_2, \ldots}\, \varrho_1^{s_1}\, \varrho_2^{s_2} \ldots$$

wo die g Irrationalen höchstens von der $(n-1)^{\text{ten}}$ Ordnung sind, und die Summationen sich auf alle Werthe s_1, s_2, ..., von Null bis resp. e_1-1, e_2-1, etc. beziehen.

Es genügt also I einer Gleichung

$$I - \Sigma g_{s_1, s_2, \ldots}\, \varrho_1^{s_1}\, \varrho_2^{s_2} \ldots = 0,$$

deren Form mit der oben aufgestellten übereinstimmt, indem die höchste Potenz von I, (hier I selbst), nur mit 1 multiplicirt ist, die Summe aber eine ganze Zahl vorstellt, welche allerdings noch nicht rational, sondern eine Irrationale n^{ter} Ordnung ist.

Multiplicirt man nun diese Gleichung ersten Grades mit den $e_1 e_2 \cdots - 1$ Factoren, die man erhält, wenn man in der Differenz

$$I - \Sigma g_{s_1, s_2, \ldots} \varrho_1^{s_1} \varrho_2^{s_2}$$

den ϱ alle möglichen Werthe giebt, deren solche Wurzelgröfsen fähig sind, so bekommt man für I eine Gleichung vom $e_1 e_2 \ldots^{\text{ten}}$ Grade, von der verlangten Form; mit Coëfficienten, die höchstens von der $(n-1)^{\text{ten}}$ Ordnung sind. Wie man von der Gleichung ersten Grades auf die $e_1 e_2 \ldots^{\text{ten}}$ Grades kam, so wird man von dieser zu immer neuen Gleichungen von derselben Form, von einem immer höheren Grade, mit Coëfficienten immer niedrigerer Ordnung gelangen, bis man endlich zur 0^{ten} Ordnung kommt.

Es genügt demnach jede ganze Zahl I einer Gleichung

$$I^m - A_1 I^{m-1} + \cdots \pm A_m = 0,$$

deren Coëfficienten A rational und ganz sind.

10.

F o l g e r u n g e n. Sollte I nur in irrationaler Form aufgetreten, aber rational sein, so ist es eine *ganze* rationale Zahl, wenn es früher die Gestalt einer ganzen Zahl hatte. Genügt nämlich der Gleichung für I mit ganzen rationalen Coëfficienten eine rationale Zahl, so mufs dieselbe nach bekannten Sätzen *ganz* sein.

Die obige Gleichung für I ist nicht nothwendig irreductibel; man sieht aber, dafs jeder ihrer irreductibeln Factoren von derselben Form ist, wie sie selbst, und ganze Coëfficienten A hat. (Der Beweis folgt aus Disq. arithm. p. 37, §. 42.) Wir haben daher folgenden Satz:

Jede irrationale Zahl I genügt einer irreductibeln Gleichung

$$I^m - A_1 I^{m-1} + A_2 I^{m-2} - \cdots \pm A_m = 0.$$

Ist I ganz, so sind die A nicht nur rational, sondern auch ganz.

Da eine Gröfse I nur *einer* irreductibeln Gleichung genügen kann, so sind alle A bestimmt; also ist es auch A_m. *Norm einer Zahl I heifst die Gröfse* A_m. Die Norm einer jeden Zahl ist daher rational, *die Norm einer ganzen ganz.*

Die p^{te} Potenz der Norm einer ganzen Zahl ist durch die Norm der p^{ten} Potenz derselben theilbar. Setzt man nämlich $I = \sqrt[p]{K}$ in die Gleichung für I, so erhält man, indem man die p^{ten} Wurzeln wegschafft, eine

Gleichung für K, die mit K^m anfängt und mit $\pm A_m^p$ schliefst. Diese Gleichung ist entweder irreductibel, oder nicht; im ersten Falle ist sie identisch mit der irreductibeln Gleichung

$$K^n - B_1 K^{n-1} \cdots \pm B_n = 0,$$

welcher K als irrationale ganze Zahl genügt; im zweiten Falle ist sie wenigstens durch sie theilbar. Es ist also B_n (und das ist nach der Erklärung die Norm von K oder von I^p) ein Theiler von A_m^p der p^{ten} Potenz der Norm von I.

11.

Beweis des Satzes *b.* in §. 4. Den Arbeiten von *Abel* (Journal Bd. I. S. 65 et seq., Oeuvres complètes Tome II. „Sur la résolution algébrique des équations, p. 185 et seq.") entnehmen wir einige Resultate, deren Beweise in den angezeigten Stellen vollständig enthalten sind. Man kann auch die Arbeiten von *Malmstèn* und *Luther* (Journal Bd. 34. und 37.) vergleichen. Es ist dort gezeigt, dafs jede irrationale Gröfse I auf eine Hauptform gebracht werden kann, in welcher sie als rationale Function gewisser Wurzelgröfsen $\sqrt[\mu]{y}$, $\sqrt[\mu_1]{y_1}$, etc. sich zeigt. Diese Function genügt dann immer derselben irreductibeln Gleichung, welche μ^{ten}, μ_1^{ten}, etc. Wurzeln man auch nehmen mag. (Oeuvres complètes, II. p. 199.) Man findet dort auch (p. 200) den Satz, dafs eine irreductibele Gleichung mit *einer* algebraischen Wurzel nur algebraische Wurzeln hat.

Bringt man daher eine Wurzel unserer irreductibeln Gleichung für I (§. 10.) auf die Hauptform und verändert die Wurzelgröfsen $\sqrt[\mu]{y}$, etc. auf alle mögliche Arten, so erhält man *alle* Wurzeln; so dafs das Product der auf diese Art gefundenen verschiedenen Ausdrücke die Norm von I wird.

Das „Théorème I." in den „Oeuvres complètes" von *Abel* p. 196 lehrt, dafs zwei algebraische Ausdrücke in der Hauptform, welche dieselben Wurzelgröfsen $\sqrt[\mu]{y}$, etc. enthalten, für *alle* Werthe, die man den Wurzelzeichen giebt, gleich sein müssen, wenn sie für *einen* der Werthe übereinstimmen. Ist nun eine ganze irrationale Zahl I das Product zweier anderen ganzen K und L, so bringe man diese auf die Hauptform. Es wird I nur die Wurzelgröfsen enthalten können, die in K und L vorkommen, obgleich einige der letztern sich durch die Multiplication wegheben, und daher in I fehlen können. Verändert man auf der Seite rechts der Gleichung

$$I = KL$$

die Wurzelzeichen $\sqrt[\mu]{y}$ etc. auf alle mögliche Art, so wird das Gleiche auch auf der Seite links Statt finden, während *verschiedenen* Veränderungen auf der Seite rechts *dieselben* auf der Seite links entsprechen können. Multiplicirt man die so entstehenden Gleichungen miteinander, so wird auf der Seite rechts das Product der Normen von K und L (nämlich aller Wurzeln der irreductibeln Gleichungen, denen K und L genügen) links die Norm von I oder eine Potenz derselben erhalten. Wir haben daher folgenden Satz:

Die Norm eines jeden Factors einer ganzen Zahl theilt die Norm der ganzen Zahl, oder eine Potenz derselben.

Soll nun eine Primzahl q eine ganze Zahl N oder eine Potenz derselben, z. B. die g^{te} theilen, so mufs die Norm von q, d. h. q selbst. die Norm von N^g zu irgend einer Potenz, also die Norm von N^g, mithin die g^{te} Potenz der Norm von N oder diese selbst theilen. *Eine ganze Zahl N und ihre Potenzen sind folglich nur durch die Primzahlen theilbar, welche die Norm von N theilen.* So ist also der Beweis des Satzes (4. *b.*) geliefert.

12.

Ein Hülfssatz. *Hat die Gleichung*

$$I^m + A_1 I^{m-1} + A_2 I^{m-2} \ldots + A_m = 0,$$

in welcher die A rationale ganze Zahlen bezeichnen, eine irrationale Wurzel, so ist dieselbe ganz.

Beweis. Es sei Z der Zähler, N der Nenner von I, so dafs $\frac{Z}{N} = I$ ist. Man kann aber nicht annehmen, dafs Z und N keinen gemeinschaftlichen Theiler haben. Wäre nämlich δ ein solcher, so würden $\frac{Z}{\delta}$ und $\frac{N}{\delta}$ wieder einen Theiler haben können, und so könnte es in's Unendliche fortgehen. Es kann ja eine Zahl N unendlich viele Theiler haben; nur über die *Normen* derselben haben wir einen Satz aufgestellt. Wir werden zeigen, dafs wenn $\frac{Z}{N}$ der vorstehenden Gleichung genügt, es gleich $\frac{Z_1}{N_1}$, dieses gleich $\frac{Z_2}{N_2}$, etc. sein mufs, wo die Z und N ganze Zahlen bezeichnen, welche sich unbestimmt der Einheit nähern; woraus man dann schliefst, dafs der Bruch sich als ganze Zahl darstellen läfst.

Setzt man nämlich in die Gleichung für I seinen Werth, so findet sich

$$Z^m + N(A_1 Z^{m-1} + A_2 Z^{m-2} N + \cdots + A_m N^{m-1}) = 0,$$

so dafs Z^m durch N theilbar ist. Macht man

$$Z^m = N Z_1^m,$$

so wird

$$I = \frac{Z}{N} = \frac{Z_1}{N^{\frac{m-1}{m}}},$$

wo Z_1 eine ganze irrationale Zahl bezeichnet und $N^{\frac{m-1}{m}}$ Das ist, was früher N_1 genannt wurde. So schreitet man nach und nach von dem Nenner N zu

$$N_1 = N^{\frac{m-1}{m}},$$
$$N_2 = N_1^{\frac{m-1}{m}} = N^{\left(\frac{m-1}{m}\right)^2},$$
$$N_3 = N_2^{\frac{m-1}{m}} = N^{\left(\frac{m-1}{m}\right)^3}$$
$$\cdots\cdots\cdots\cdots\cdots$$

fort und nähert sich also beliebig einem der Einheit gleichen Nenner.

13.

Beweis des Satzes *a.* in §. 4. Ist nun

$$\frac{Z}{N} = \frac{g}{h},$$

so genüge Z der irreductibeln Gleichung

$$(1.)\quad Z^m + B_1 Z^{m-1} + B_2 Z^{m-2} + \cdots + B_m = 0$$

mit ganzen rationalen Coëfficienten, und N der folgenden:

$$(2.)\quad N^r + C_1 N^{r-1} + C_2 N^{r-2} + \cdots + C_r = 0.$$

Setzt man in die erste Gleichung:

$$Z = \frac{g}{h} N,$$

so ergiebt sich

$$(3.)\quad N^m + B_1 \frac{h}{g} N^{m-1} + B_2 \frac{h^2}{g^2} N^{m-2} + \cdots + B_m = 0;$$

was mit der Gleichung r^{ten} Grades für N übereinstimmen mufs. Denn (2.) ist irreductibel; eben so (3.) (welches aus der irreductibeln Gleichung (1.) entstand), weil jeder Factor, der (3.) theilt, offenbar auch Z zu der Wurzel einer Gleichung von niedrigerem Grade als dem m^{ten} machen würde. Die Gleichungen (2. und 3.) sind folglich identisch, also ist $m = r$ und

$$B_1 h = g\, C_1,$$
$$B_2 h^2 = g^2 C_2,$$
$$\cdots\cdots\cdots$$

Da g und h keine gemeinschaftlichen Theiler haben, so sind B_1, B_2, etc. resp. durch g, g^2, etc., ferner C_1, C_1, etc. resp. durch h, h^2, etc. theilbar. Macht man

$$B_1 = g A_1,$$
$$B_2 = g^2 A_2,$$
$$\dots\dots\dots,$$

so geben die Gleichungen für Z und N:

$$Z^m + g A_1 Z^{m-1} + g_2^2 A_2 Z^{m-2} + \dots + g^m A_m = 0,$$
$$N^m + h A_1 Z^{m-1} + h^2 A_2 Z^{m-2} + \dots + h^m A_m = 0.$$

Es genügen also $\frac{Z}{g}$ und $\frac{N}{h}$ einer und derselben Gleichung mit ganzen Coëfficienten A, nämlich:

$$\left(\frac{Z}{g}\right)^m + A_1\left(\frac{Z}{g}\right)^{m-1} + \dots + A_m = 0,$$
$$\left(\frac{N}{h}\right)^m + A_2\left(\frac{N}{h}\right)^{m-1} + \dots + A_m = 0;$$

sie sind ferner irrational, also nach (§. 12.) *ganz*, d. h. es ist Z durch g, und N durch h theilbar.

Bonn, im November 1852.