

Carl Friedrich Gauss

Werke

Band III

Ein neuer Beweis des Satzes, dass jedes Polynom in einer Variablen
in reelle Faktoren ersten oder zweiten Grades zerlegt werden kann

Vollständige Dissertation von 1799 und vollständiger zweiter Beweis
von 1815

Moderne deutsche Übersetzung

Es folgen die historischen Titelblätter und die vollständige Dissertation von 1799, Artikel 1–24, mit den zehn historischen Fußnoten von Gauss und allen vier Figuren. Es folgt der vollständige zweite Beweis, Artikel 1–20 mit beiden historischen Fußnoten und seinem Titelblatt. Er wurde 1815 vorgelegt und 1816 veröffentlicht. Spätere Texte des dritten Bandes sind in diesem Leseband nicht enthalten. Historische Verweise behalten die Nummerierung der Vorlage bei.

Historische Vorlage: Carl Friedrich Gauss, *Werke*, dritter Band, Göttingen, 1866; Dissertation erstmals 1799 bei C. G. Fleckeisen in Helmstedt erschienen. Die ursprünglich deutschen Titelblätter sind in modernem Deutsch wiedergegeben; das historische Original wird gesondert bewahrt.

Mit OpenAI GPT-6.1 Sol KI-übersetzt ins Deutsche; KI-erzeugter Satz.

Quellen und Terminologie

Historischer Text: Carl Friedrich Gauss, *Werke*, dritter Band, Göttingen, 1866. Diese englischen und deutschen Texte sind aus der originalsprachlichen Ausgabe KI-übersetzt. Die folgenden menschlichen Übersetzungen und Schriften werden für die angegebene Terminologie und den Sprachgebrauch herangezogen; ihr fortlaufender Wortlaut wird nicht übernommen. Die ursprünglichen mathematischen Formulierungen von Gauss bleiben maßgeblich.

Paul Taylor; Bernard Leak. Taylors englische Übersetzung des zweiten Beweises von Gauss für den Fundamentalsatz der Algebra, mit Korrekturen von Leak, 1983. Die entsprechenden Passagen des zweiten Beweises von 1815 wurden für die englische Terminologie zu Polynomen, Teilern, Graden, symmetrischen Funktionen und Beweisen herangezogen. Verwandte Terminologie wurde auch für die Dissertation von 1799 herangezogen, zu der diese Arbeit keine Parallelübersetzung ist. Fortlaufender Text aus dieser menschlichen Übersetzung wird nicht übernommen. Ihr späterer Gebrauch komplexer Größen ersetzt hier nicht die Definition imaginärer Größen von Gauss. Die herangezogene Online-Ausgabe nennt Dezember 1983 als Übersetzungsdatum, August 2003 für die LaTeX-Fassung und den 8. Juni 2007 als letztes Änderungsdatum der zugrunde liegenden Quelle. Ihre Danksagung nennt Mark Wainwright für die Rückgabe von Taylors Notizen und Nikita Danilov für die Korrektur von Tippfehlern.
<https://www.paultaylor.eu/misc/gauss.html>

H. Maser. Deutscher Übersetzer und Herausgeber, *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*, Berlin: Julius Springer, 1889. Verwandte deutsche Terminologie für algebraische Funktionen, Wurzeln, Teilbarkeit, Quotienten und Grade; keine Parallelübersetzung dieser Dissertation.
<https://archive.org/details/carlfriedrichga00gausgoog>

James Caddall Morehead und Adam Miller Hildebeitel. Übersetzer von Gauss' *General Investigations of Curved Surfaces of 1827 and 1825*, Princeton University Library, 1902; Project Gutenberg 36856, TeX-Ausgabe. Verwandte englische Terminologie für Geometrie, Koordinaten und unendlich kleine Größen; keine Parallelübersetzung der Dissertation von 1799.
<https://www.gutenberg.org/ebooks/36856>

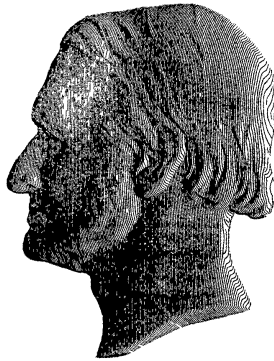
Ulrich Görtz. *Algebra*, Wintersemester 2021/22, Abschnitt 3.1.1, Beispiele 3.1–3.2. Verwandter zeitgenössischer deutscher Sprachgebrauch zu Polynomen, Unbestimmten, Summen, Zählern und Nennern sowie zur mathematischen Argumentation. Diese Quelle dient der Terminologie; sie ist keine Parallelübersetzung der beiden Beweise. Fortlaufender Text und moderne ringtheoretische Argumente werden nicht übernommen.
<https://math.ug/a-ws2122/sect0006.html>

KI-Urheberschaft und Quellen. Mit OpenAI GPT-6.1 Sol KI-übersetzt; KI-erzeugter Satz. Gauss ist der Autor des historischen mathematischen Textes. Die genannten menschlichen Übersetzungen werden für ihre angegebenen Beiträge zu Terminologie und Sprachgebrauch gewürdigt.

Bibliografische Metadaten: CITATIONS.bib.

CARL FRIEDRICH GAUSS: WERKE
BAND III.

CARL FRIEDRICH GAUSS
WERKE
DRITTER BAND



HERAUSGEGEBEN
VON DER
KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
ZU GÖTTINGEN
1866.

EIN NEUER BEWEIS
DES SATZES,
DASS JEDES POLYNOM

IN EINER VARIABLEN
IN REELLE FAKTOREN ERSTEN ODER ZWEITEN GRADES
ZERLEGT WERDEN KANN

ZUR ERLANGUNG
DER HÖCHSTEN WÜRDEN IN DER PHILOSOPHIE
DER HOCHBERÜHMTE PHILOSOPHISCHE FAKULTÄT
DER ACADEMIA JULIA CAROLINA

VORGELEGT VON
CARL FRIEDRICH GAUSS

HELMSTEDT
BEI C. G. FLECKEISEN. MDCCLXXXIX.

EIN NEUER BEWEIS DES SATZES,
DASS JEDES POLYNOM
IN EINER VARIABLEN
IN REELLE FAKTOREN ERSTEN ODER ZWEITEN GRADES ZERLEGT
WERDEN KANN.

1.

Jede bestimmte algebraische Gleichung lässt sich auf die Form

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + M = 0$$

bringen, wobei m eine positive ganze Zahl ist. Bezeichnen wir die linke Seite dieser Gleichung mit X und nehmen wir an, dass die Gleichung $X = 0$ durch mehrere ungleiche Werte von x erfüllt wird, etwa indem wir $x = \alpha$, $x = \beta$, $x = \gamma$ usw. setzen, so ist die Funktion X durch das Produkt aus den Faktoren $x - \alpha$, $x - \beta$, $x - \gamma$ usw. teilbar. Umgekehrt: Wenn das Produkt aus mehreren linearen Faktoren $x - \alpha$, $x - \beta$, $x - \gamma$ usw. die Funktion X teilt, so wird die Gleichung $X = 0$ erfüllt, wenn man x irgendeiner der Größen α , β , γ usw. gleichsetzt. Ist schließlich X gleich einem Produkt aus m solchen linearen Faktoren (ob sie nun alle verschieden oder einige von ihnen identisch sind), so können keine anderen linearen Faktoren die Funktion X teilen. Eine Gleichung vom Grad m kann daher nicht mehr als m Wurzeln haben. Zugleich ist aber klar, dass eine Gleichung vom Grad m *weniger* Wurzeln haben kann, auch wenn sich X in m lineare Faktoren zerlegen lässt: Sind nämlich einige dieser Faktoren identisch, so ist die Anzahl der verschiedenen Möglichkeiten, die Gleichung zu erfüllen, notwendig kleiner als m . Der Einheitlichkeit halber haben es die Mathematiker dennoch vorgezogen, auch in diesem Fall zu sagen, die Gleichung habe m Wurzeln und nur einige davon seien einander gleich; was sie sich durchaus erlauben können.

2.

Was bisher dargelegt wurde, wird in den Büchern über Algebra ausreichend bewiesen und verstößt nirgends gegen die geometrische Strenge. Doch scheinen die Analysten allzu voreilig und ohne vorherigen stichhaltigen Beweis den Satz angenommen zu haben, auf dem fast die gesamte Lehre von den Gleichungen beruht: *Jede Funktion wie X lässt sich stets in m lineare Faktoren zerlegen*, oder, was damit völlig übereinstimmt, *jede Gleichung vom Grad m hat tatsächlich m Wurzeln*. Da schon bei quadratischen Gleichungen sehr häufig Fälle auftreten, die diesem Satz widersprechen, waren die Algebraiker gezwungen, um auch diese Fälle unter ihn zu bringen, eine imaginäre Größe zu erfinden, deren Quadrat -1 ist. Darauf erkannten sie: Lässt man

Größen der Form $a + b\sqrt{-1}$ ebenso zu wie reelle, so gilt der Satz nicht nur für quadratische, sondern auch für kubische und biquadratische Gleichungen. Daraus durfte man jedoch keineswegs schließen, dass sich nach Zulassung der Größen der Form $a + b\sqrt{-1}$ jede Gleichung fünften oder höheren Grades erfüllen lässt oder, wie man gewöhnlich sagt (obwohl ich diese schlüpfrige Formulierung nicht gutheißen möchte), dass die Wurzeln jeder Gleichung auf die Form $a + b\sqrt{-1}$ gebracht werden können. Der Sache nach unterscheidet sich dieser Satz in nichts von dem im Titel dieser Schrift ausgesprochenen; einen neuen strengen Beweis dafür zu geben, ist das Ziel der vorliegenden Dissertation.

Seit die Analysten erkannt haben, dass es unendlich viele Gleichungen gibt, die überhaupt keine Wurzel hätten, wenn nicht Größen der Form $a + b\sqrt{-1}$ zugelassen würden, hat man solche erdachten Größen als eine besondere Art von Größen betrachtet, sie zur Unterscheidung von den *reellen* als *imaginäre* bezeichnet und in die gesamte Analysis eingeführt. Mit welchem Recht? Das erörtere ich hier nicht. — Ich werde meinen Beweis ohne jede Hilfe imaginärer Größen durchführen, obwohl es auch mir erlaubt wäre, dieselbe Freiheit in Anspruch zu nehmen, deren sich alle neueren Analysten bedient haben.

3.

Was in den meisten elementaren Büchern als Beweis unseres Satzes angeführt wird, ist zwar so gehaltlos und von geometrischer Strenge so weit entfernt, dass es kaum der Erwähnung wert ist; damit aber nichts fehlt, will ich es dennoch kurz berühren. ‘Um zu zeigen, dass jede Gleichung

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + M = 0$$

oder $X = 0$ tatsächlich m Wurzeln hat, unternimmt man den Beweis, dass sich X in m lineare Faktoren zerlegen lässt. Dazu nimmt man m lineare Faktoren $x - \alpha$, $x - \beta$, $x - \gamma$ usw. an, wobei α , β , γ usw. noch unbekannt sind, und setzt ihr Produkt der Funktion X gleich. Durch Vergleich der Koeffizienten erhält man dann m Gleichungen, aus denen sich, wie man sagt, die Unbekannten α , β , γ usw. bestimmen lassen, da auch ihre Anzahl m ist. Man könne nämlich $m - 1$ Unbekannte eliminieren, sodass eine Gleichung übrig bleibe, die nur noch diejenige Unbekannte enthalte, die man beliebig auswählt.’ Von den übrigen Einwänden gegen eine solche Schlussweise will ich schweigen und nur fragen: Woher können wir sicher wissen, dass diese letzte Gleichung tatsächlich irgendeine Wurzel hat? Warum könnte es nicht sein, dass weder diese letzte noch die vorgelegte Gleichung durch irgendeine Größe im gesamten Bereich der reellen und imaginären Größen erfüllt wird? — Im Übrigen werden Sachkundige leicht erkennen, dass diese letzte Gleichung notwendig mit der vorgelegten *völlig identisch* ist, sofern die

Rechnung richtig durchgeführt wurde: Nach Elimination der Unbekannten β , γ usw. muss nämlich die Gleichung

$$\alpha^m + A\alpha^{m-1} + B\alpha^{m-2} + \text{usw.} + M = 0$$

entstehen. Mehr braucht über diese Schlussweise nicht gesagt zu werden.

Einige Autoren, die die Schwäche dieser Methode bemerkt zu haben scheinen, nehmen als *Axiom* an, jede Gleichung habe tatsächlich Wurzeln, wenn nicht mögliche, dann unmögliche. Was sie unter möglichen und unmöglichen Größen verstehen wollen, scheinen sie nicht hinreichend deutlich erläutert zu haben. Sollen die möglichen Größen dasselbe wie die reellen, die unmöglichen dasselbe wie die imaginären bezeichnen, so darf jenes Axiom keineswegs zugestanden werden, sondern bedarf notwendig eines Beweises. Doch scheinen die Ausdrücke nicht in diesem Sinn gemeint zu sein; vielmehr scheint der Sinn des Axioms dieser zu sein: ‘Obwohl wir noch nicht sicher sind, dass es notwendig m reelle oder imaginäre Größen gibt, die eine gegebene Gleichung vom Grad m erfüllen, wollen wir dies dennoch eine Zeit lang voraussetzen; sollte es nämlich geschehen, dass sich so viele reelle und imaginäre Größen nicht finden lassen, so bleibt uns gewiss der Ausweg zu sagen, die übrigen seien unmöglich.’ Zieht jemand diese Ausdrucksweise der einfachen Aussage vor, die Gleichung werde in diesem Fall nicht so viele Wurzeln haben, so habe ich nichts dagegen. Benutzt er dann aber diese unmöglichen Wurzeln, als wären sie etwas Wirkliches, und sagt zum Beispiel, die Summe aller Wurzeln der Gleichung $x^m + Ax^{m-1} + \text{usw.} = 0$ sei $= -A$, auch wenn sich unmögliche darunter befinden (was eigentlich bedeutet: *auch wenn einige fehlen*), so kann ich dies keineswegs gutheißen. Denn unmögliche Wurzeln, in diesem Sinn genommen, sind dennoch Wurzeln; dann darf jenes Axiom auf keinen Fall ohne Beweis zugestanden werden, und wäre es abwegig zu fragen, ob es nicht Gleichungen geben könnte, die nicht einmal unmögliche Wurzeln haben?*)

*) Unter einer imaginären Größe verstehe ich hier stets eine Größe der Form $a + b\sqrt{-1}$, so lange b nicht $= 0$ ist. In diesem Sinn haben alle Mathematiker ersten Ranges jenen Ausdruck stets gebraucht. Ich meine, man sollte diejenigen nicht anhören, die eine Größe $a + b\sqrt{-1}$ nur dann imaginär nennen wollen, wenn $a = 0$ ist, dagegen unmöglich, wenn nicht $a = 0$ ist; denn diese Unterscheidung ist weder nötig noch von irgendeinem Nutzen. — Sollen imaginäre Größen überhaupt in der Analysis beibehalten werden (was aus mehreren Gründen ratsamer erscheint, als sie abzuschaffen, sofern sie nur hinreichend sicher begründet werden), so muss man sie notwendig als ebenso möglich wie die reellen betrachten. Daher möchte ich die reellen und die imaginären Größen lieber unter der gemeinsamen Bezeichnung *mögliche Größen* zusammenfassen. Dagegen würde ich eine Größe *unmöglich* nennen, die Bedingungen erfüllen soll, die sich selbst bei Zulassung imaginärer Größen nicht erfüllen lassen, jedoch so, dass diese *Ausdrucksweise* dasselbe bedeutet, wie wenn man sagt, eine solche Größe gebe es im gesamten Bereich der Größen nicht. Daraus eine besondere Art von Größen zu bilden, würde ich keineswegs gestatten. Sagt jemand, ein geradliniges gleichseitiges rechtwinkliges Dreieck sei unmöglich, so wird niemand widersprechen. Wollte er aber ein solches unmögliches Dreieck als eine neue Art von Dreiecken betrachten und andere Eigenschaften der Dreiecke darauf

4.

Bevor ich die Beweise anderer Mathematiker für unseren Satz durchgehe und darlege, was mir an jedem von ihnen zu beanstanden scheint, bemerke ich: Es genügt, nur zu zeigen, dass sich jede Gleichung eines beliebigen Grades

$$x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + M = 0$$

oder $X = 0$ (wobei die Koeffizienten A, B usw. als reell vorausgesetzt werden) auf wenigstens eine Weise durch einen Wert von x der Form $a + b\sqrt{-1}$ erfüllen lässt. Bekanntlich ist X dann durch den reellen quadratischen Faktor $xx - 2ax + aa + bb$ teilbar, wenn b nicht $= 0$ ist, und durch den reellen linearen Faktor $x - a$, wenn $b = 0$ ist. In beiden Fällen ist der Quotient reell und von niedrigerem Grad als X ; und da dieser auf dieselbe Weise einen reellen Faktor ersten oder zweiten Grades haben muss, ist klar, dass die Fortsetzung dieses Verfahrens die Funktion X schließlich in reelle lineare oder quadratische Faktoren zerlegt oder, wenn man für jeden reellen quadratischen Faktor lieber zwei imaginäre lineare verwendet, in m lineare Faktoren.

5.

Der erste Beweis des Satzes stammt von dem ausgezeichneten Mathematiker D'ALEMBERT, *Recherches sur le calcul intégral, Histoire de l'Acad. de Berlin, Année 1746*, S. 182 ff. Er findet sich auch bei BOUGAINVILLE, *Traité du calcul intégral, à Paris 1754*, S. 47 ff. Die Hauptschritte dieser Methode sind folgende.

Zunächst zeigt er: Wird irgendeine Funktion X der veränderlichen Größe x entweder für $x = 0$ oder für $x = \infty$ gleich $= 0$ und kann sie einen unendlich kleinen positiven reellen Wert annehmen, wenn man x einen reellen Wert gibt, so kann diese Funktion auch einen unendlich kleinen negativen reellen Wert durch einen Wert von x annehmen, der entweder reell ist oder die imaginäre Form $p + q\sqrt{-1}$ hat. Bezeichnet nämlich Ω einen unendlich kleinen Wert von X und ω den entsprechenden Wert von x , so behauptet er, ω lasse sich durch

anwenden, wer könnte das Lachen zurückhalten? Das hieße mit Worten spielen oder vielmehr sie missbrauchen. — Zwar haben auch die größten Mathematiker häufig Wahrheiten, die die Möglichkeit der Größen, auf die sie sich beziehen, offenkundig voraussetzen, auf solche angewendet, deren Möglichkeit noch zweifelhaft war. Auch will ich nicht bestreiten, dass derartige Freiheiten meist nur die Form und gleichsam die Hülle der Schlussfolgerungen betreffen, die der Scharfblick eines wahren Mathematikers bald durchdringen kann. Dennoch scheint es ratsamer und der Erhabenheit einer Wissenschaft, die mit Recht als vollkommenstes Muster von Klarheit und Gewissheit gerühmt wird, angemessener, solche Freiheiten entweder ganz zu verbannen oder sie wenigstens sparsamer und nur dort zu gebrauchen, wo auch weniger Geübte erkennen können, dass die Sache ohne ihre Hilfe vielleicht weniger kurz, aber ebenso streng hätte erledigt werden können. — Im Übrigen will ich nicht bestreiten, dass man das, was ich hier gegen den Missbrauch der unmöglichen Größen gesagt habe, in gewisser Hinsicht auch gegen die imaginären einwenden könnte; doch behalte ich mir deren Verteidigung sowie eine ausführlichere Darstellung dieser ganzen Sache für eine andere Gelegenheit vor.

eine rasch konvergierende Reihe $a\Omega^\alpha + b\Omega^\beta + c\Omega^\gamma$ usw. ausdrücken, deren Exponenten α, β, γ usw. fortwährend zunehmende rationale Größen sind, die daher wenigstens von einer bestimmten Entfernung vom Anfang an positiv werden und die Glieder, in denen sie vorkommen, unendlich klein machen. Kommt nun unter diesen Exponenten kein Bruch mit geradem Nenner vor, so werden alle Glieder der Reihe sowohl für einen positiven als auch für einen negativen Wert von Ω reell. Finden sich dagegen unter jenen Exponenten Brüche mit geradem Nenner, so haben für einen negativen Wert von Ω die entsprechenden Glieder bekanntlich die Form $p + q\sqrt{-1}$. Wegen der unendlichen Konvergenz der Reihe genügt es aber im ersten Fall, nur das erste (das heißt größte) Glied beizubehalten; im zweiten braucht man nicht über dasjenige Glied hinauszugehen, das zuerst einen imaginären Teil hervorbringt.

Durch ähnliche Überlegungen lasse sich zeigen: Kann X durch einen reellen Wert von x einen unendlich kleinen negativen Wert annehmen, so kann diese Funktion durch einen reellen Wert von x oder einen imaginären der Form $p + q\sqrt{-1}$ einen unendlich kleinen positiven reellen Wert erhalten.

Daraus schließt er zweitens, dass es auch einen endlichen reellen Wert von X gibt, im ersten Fall einen negativen, im zweiten einen positiven, der durch einen imaginären Wert von x der Form $p + q\sqrt{-1}$ hervorgebracht werden kann.

Hieraus folgt: Ist X eine solche Funktion von x , die durch einen reellen Wert v von x einen reellen Wert V erhält und durch einen reellen Wert von x auch einen um eine unendlich kleine Größe größeren oder kleineren reellen Wert annimmt, so kann sie auch einen reellen Wert erhalten, der entsprechend um eine unendlich kleine und folglich um eine endliche Größe kleiner oder größer als V ist, indem man x einen Wert der Form $p + q\sqrt{-1}$ gibt. Das ergibt sich ohne Schwierigkeit aus dem Vorhergehenden, wenn man sich für X den Ausdruck $V + Y$ und für x den Ausdruck $v + y$ eingesetzt denkt.

Schließlich behauptet der ausgezeichnete D'ALEMBERT: Nimmt man an, dass X ein ganzes Intervall zwischen zwei reellen Werten R, S durchlaufen kann (das heißt sowohl R als auch S und allen dazwischenliegenden reellen Werten gleich werden kann), indem man x stets Werte der Form $p + q\sqrt{-1}$ gibt, so kann die Funktion X noch um jede endliche reelle Größe vermehrt oder vermindert werden (je nachdem, ob $S > R$ oder $S < R$ ist), wobei x stets die Form $p + q\sqrt{-1}$ behält. Gäbe es nämlich eine reelle Größe U (zwischen der und R der Wert S liegen soll), der X durch einen solchen Wert von x nicht gleich werden könnte, so müsste es einen *größten* Wert von X geben (wenn $S > R$ ist; einen *kleinsten* dagegen, wenn $S < R$ ist), etwa T , den sie durch einen Wert $p + q\sqrt{-1}$ von x erreichte, sodass man x keinen Wert derselben Form geben könnte, der die Funktion X auch nur um den kleinsten Betrag näher an U brächte. Setzt man nun in dieser Gleichung zwischen X und x überall $p + q\sqrt{-1}$ für x ein und setzt dann sowohl den reellen Teil als

auch den Teil, der den Faktor $\sqrt{-1}$ enthält, nach Weglassung dieses Faktors gleich null, so kann man aus den beiden entstehenden Gleichungen (in denen p, q und X zusammen mit Konstanten vorkommen) durch Elimination zwei andere gewinnen. In der einen stehen p, X und Konstanten; die andere ist von p frei und enthält nur q, X und Konstanten. Da also X durch reelle Werte von p, q alle Werte von R bis T durchlaufen hat, kann X nach dem Vorhergehenden noch näher an den Wert U herankommen, wenn man p, q entsprechend Werte der Formen $\alpha + \gamma\sqrt{-1}$ und $\beta + \delta\sqrt{-1}$ gibt. Dann wird aber $x = \alpha - \delta + (\gamma + \beta)\sqrt{-1}$, hat also weiterhin die Form $p + q\sqrt{-1}$, entgegen der Voraussetzung.

Nimmt man jetzt an, dass X eine Funktion wie $x^m + Ax^{m-1} + Bx^{m-2} +$ usw. $+ M$ bezeichnet, so sieht man ohne Schwierigkeit, dass man x solche reellen Werte geben kann, dass X ein ganzes Intervall zwischen zwei reellen Werten durchläuft. Daher kann x einen Wert der Form $p + q\sqrt{-1}$ erhalten, durch den X gleich $= 0$ wird. Q. E. D.*)

6.

Die Einwände, die sich gegen den Beweis von D'ALEMBERT erheben lassen, laufen im Wesentlichen auf Folgendes hinaus.

1. Der ausgezeichnete d'A. zweifelt nicht an der *Existenz* der Werte von x , denen gegebene Werte von X entsprechen, sondern setzt sie voraus und untersucht nur die *Form* jener Werte.

Obwohl dieser Einwand für sich genommen sehr schwer wiegt, betrifft er hier doch nur die Ausdrucksweise, die sich leicht so ändern lässt, dass er vollständig entfällt.

2. Die Behauptung, ω lasse sich stets durch eine Reihe der von ihm angegebenen Art ausdrücken, ist gewiss falsch, wenn X auch eine beliebige transzendente Funktion bezeichnen soll (wie d'A. an mehreren Stellen andeutet). Das ist zum Beispiel klar, wenn man $X = e^{\frac{1}{x}}$ oder $x = \frac{1}{\log X}$ setzt. Beschränken wir jedoch den Beweis auf den Fall, dass X eine algebraische Funktion von x ist (was für die vorliegende Aufgabe genügt), so ist der Satz allerdings richtig. — Im Übrigen hat d'A. zur Bestätigung seiner Voraussetzung nichts angeführt. Der berühmte BOUGAINVILLE setzt voraus, dass X eine algebraische

*)Es ist zu beachten, dass der ausgezeichnete D'ALEMBERT in seiner eigenen Darstellung dieses Beweises geometrische Betrachtungen benutzt und X als Abszisse, x als Ordinate einer Kurve betrachtet hat (nach der Gewohnheit aller Mathematiker des ersten Teils dieses Jahrhunderts, bei denen der Begriff der Funktion weniger gebräuchlich war). Da jedoch alle seine Schlussfolgerungen, wenn man nur auf ihren wesentlichen Inhalt sieht, auf keinen geometrischen, sondern auf rein analytischen Grundlagen beruhen und die Ausdrücke imaginäre Kurven und imaginäre Ordinaten etwas hart erscheinen und den heutigen Leser leichter befremden können, habe ich hier eine rein analytische Darstellungsform vorgezogen. Diese Anmerkung habe ich hinzugefügt, damit niemand, der den eigentlichen Beweis von D'ALEMBERT mit dieser kurzen Darstellung vergleicht, vermutet, es sei etwas Wesentliches verändert worden.

Funktion von x ist, und empfiehlt zur Auffindung der Reihe das NEWTONSche Parallelogramm.

3. Er bedient sich unendlich kleiner Größen freier, als es mit geometrischer Strenge vereinbar ist oder wenigstens in unserer Zeit (in der sie mit Recht in schlechtem Ruf stehen) von einem gewissenhaften Analysten zugestanden würde. Auch erläutert er den Sprung von einem unendlich kleinen Wert von Ω zu einem endlichen nicht deutlich genug. Seinen Satz, dass Ω auch einen endlichen Wert annehmen kann, scheint er weniger aus der Möglichkeit eines unendlich kleinen Wertes von Ω zu folgern als vielmehr daraus: Bezeichnet Ω eine sehr kleine Größe, so komme man wegen der raschen Konvergenz der Reihe dem wahren Wert von ω umso näher, je mehr Glieder der Reihe man nimmt; oder je mehr Glieder man in die für ω genommene Summe einbezieht, desto genauer werde die Gleichung erfüllt, die die Beziehung zwischen ω und Ω beziehungsweise x und X ausdrückt. Abgesehen davon, dass diese ganze Argumentation zu unbestimmt erscheint, um daraus irgendeinen strengen Schluss zu ziehen, bemerke ich, dass es durchaus Reihen gibt, die, wie klein man auch den Wert der Größe ansetzt, nach deren Potenzen sie fortschreiten, dennoch immer divergieren, sodass man, wenn man sie nur weit genug fortsetzt, zu Gliedern gelangen kann, die größer als jede gegebene Größe sind^{*)}. Das tritt ein, wenn die Koeffizienten der Reihe eine hypergeometrische Progression bilden. Daher hätte notwendig bewiesen werden müssen, dass im vorliegenden Fall eine solche hypergeometrische Reihe nicht entstehen kann.

Im Übrigen scheint mir, dass der ausgezeichnete d'A. hier zu Unrecht zu unendlichen Reihen gegriffen hat und dass diese zur Begründung dieses Fundamentalsatzes der Gleichungslehre nicht geeignet sind.

4. Aus der Annahme, dass X den Wert S , nicht aber den Wert U annehmen kann, folgt noch nicht, dass zwischen S und U notwendig ein Wert T liegt, den X erreichen, aber nicht überschreiten kann. Es bleibt noch ein anderer Fall: Zwischen S und U könnte eine Grenze liegen, der X beliebig nahe kommen kann, ohne sie jemals zu erreichen. Aus den vom ausgezeichneten d'A. angeführten Gründen folgt nur, dass X jeden einmal erreichten Wert noch um eine endliche Größe überschreiten kann. Ist sie etwa gleich $= S$ geworden, so kann sie noch um eine endliche Größe Ω vermehrt werden; danach kommt ein neuer Zuwachs Ω' hinzu, dann wieder ein Zuwachs Ω'' usw., sodass, wie viele

^{*)}Bei dieser Gelegenheit bemerke ich nebenbei, dass sehr viele dieser Reihen auf den ersten Blick äußerst stark zu konvergieren scheinen, zum Beispiel größtenteils diejenigen, mit denen der ausgezeichnete EULER im hinteren Teil der *Inst. Calc. Diff.*, Kapitel VI, S. 441–474 die Summe anderer Reihen möglichst genau bestimmt (die übrigen Reihen auf S. 475–478 können nämlich tatsächlich konvergieren). Soweit ich weiß, hat dies bisher niemand bemerkt. Daher wäre sehr zu wünschen, dass deutlich und streng gezeigt würde, warum derartige Reihen, die anfangs sehr schnell, dann allmählich immer langsamer konvergieren und schließlich immer stärker divergieren, dennoch eine nahezu wahre Summe liefern, sofern man nur nicht zu viele Glieder nimmt, und wie weit man eine solche Summe sicher als genau ansehen darf?

Zuwächse auch schon hinzugefügt sind, keiner als der letzte angesehen werden darf, sondern stets noch ein neuer hinzukommen kann. Doch obwohl die *Anzahl* der möglichen Zuwächse durch keine Grenzen beschränkt ist, könnte es durchaus geschehen, dass bei fortwährender Abnahme der Zuwächse $\Omega, \Omega', \Omega''$ usw. die Summe $S + \Omega + \Omega' + \Omega''$ usw. dennoch eine Grenze niemals erreicht, wie viele Glieder man auch betrachtet.

Dieser Fall kann zwar nicht vorkommen, wenn X ein Polynom in x bezeichnet; ohne Beweis, dass dies nicht geschehen kann, muss die Methode dennoch notwendig als unvollständig gelten. Ist dagegen X eine transzendente oder auch eine gebrochene algebraische Funktion, so kann jener Fall durchaus eintreten, zum Beispiel immer dann, wenn einem bestimmten Wert von X ein unendlich großer Wert von x entspricht. Dann scheint sich die Methode von D'ALEMBERT nicht ohne viele Umwege und in manchen Fällen vielleicht überhaupt nicht auf unbezweifelbare Grundlagen zurückführen zu lassen.

Aus diesen Gründen kann ich den Beweis von D'ALEMBERT nicht für befriedigend halten. Dennoch scheint mir seine eigentliche Beweiskraft durch alle diese Einwände keineswegs gebrochen. Ich glaube, dass sich auf derselben Grundlage (wenn auch auf ganz andere Weise und wenigstens mit größerer Umsicht) nicht nur ein strenger Beweis unseres Satzes aufbauen lässt, sondern daraus auch alles gewonnen werden kann, was man sich für die Theorie *transzendenter* Gleichungen wünschen könnte. Über diese sehr wichtige Sache werde ich bei anderer Gelegenheit ausführlicher sprechen; man vergleiche inzwischen unten Artikel 24.

7.

Nach D'ALEMBERT veröffentlichte der ausgezeichnete EULER seine Untersuchungen über denselben Gegenstand in *Recherches sur les racines imaginaires des équations, Hist. de l'Acad. de Berlin A. 1749, S. 223 ff.* Er gab dort zwei Methoden an; der wesentliche Inhalt der ersten ist folgender.

Zunächst unternimmt der ausgezeichnete Euler den Beweis, dass, wenn m irgendeine Potenz der Zahl 2 bezeichnet, die Funktion $x^{2m} + Bx^{2m-2} + Cx^{2m-3} + \text{usw.} + M = X$ (in der der Koeffizient des zweiten Gliedes = 0 ist) stets in zwei reelle Faktoren zerlegt werden kann, in denen x bis zum Grad m aufsteigt. Dazu nimmt er zwei Faktoren an,

$$x^m - ux^{m-1} + \alpha x^{m-2} + \beta x^{m-3} + \text{usw.}, \text{ und } x^m + ux^{m-1} + \lambda x^{m-2} + \mu x^{m-3} \text{ usw.}$$

wobei die Koeffizienten u, α, β usw., λ, μ usw. noch unbekannt sind, und setzt ihr Produkt der Funktion X gleich. Der Vergleich der Koeffizienten liefert dann $2m - 1$ Gleichungen. Offenbar muss nur bewiesen werden, dass man den Unbekannten u, α, β usw., λ, μ usw. (deren Anzahl ebenfalls $2m - 1$ ist) solche reellen Werte geben kann, die jene Gleichungen erfüllen. Euler behauptet nun: Betrachtet man zunächst u als bekannt, sodass die Anzahl der Unbekannten

um eins kleiner ist als die der Gleichungen, so lassen sich durch geeignete Verbindung dieser Gleichungen nach bekannten algebraischen Methoden alle α, β usw., λ, μ usw. rational und ohne irgendein Wurzelziehen durch u und die Koeffizienten B, C usw. bestimmen; sie erhalten also reelle Werte, sobald u reell wird. Außerdem kann man alle α, β usw., λ, μ usw. eliminieren, sodass eine Gleichung $U = 0$ entsteht, in der U ein Polynom allein in u und den bekannten Koeffizienten ist. Diese Gleichung selbst nach der gewöhnlichen Eliminationsmethode zu entwickeln, wäre eine ungeheure Arbeit, wenn die vorgelegte Gleichung $X = 0$ von etwas höherem Grad ist, und für einen unbestimmten Grad ganz unmöglich (nach Eulers eigenem Urteil, S. 239). Hier genügt es jedoch, eine Eigenschaft dieser Gleichung zu kennen: Das konstante Glied in U (das die Unbekannte u nicht enthält) ist notwendig negativ. Daraus folgt bekanntlich, dass die Gleichung wenigstens eine reelle Wurzel hat oder dass sich u und somit auch α, β usw., λ, μ usw. auf wenigstens eine Weise reell bestimmen lassen. Jene Eigenschaft lässt sich durch die folgenden Überlegungen bestätigen. Da $x^m - ux^{m-1} + \alpha x^{m-2} +$ usw. ein Faktor der Funktion X sein soll, muss u die Summe von m Wurzeln der Gleichung $X = 0$ sein und daher ebenso viele Werte haben, wie man auf verschiedene Weise aus $2m$ Wurzeln m auswählen kann, also nach den Grundsätzen der Kombinatorik $\frac{2m \cdot 2m-1 \cdot 2m-2 \cdot \dots \cdot m+1}{1 \cdot 2 \cdot 3 \cdot \dots \cdot m}$ Werte. Diese Zahl ist stets das Doppelte einer ungeraden Zahl (den nicht schwierigen Beweis lasse ich weg). Setzt man sie also $= 2k$, so ist ihre Hälfte k ungerade; die Gleichung $U = 0$ hat aber den Grad $2k$. Da nun in der Gleichung $X = 0$ das zweite Glied fehlt, ist die Summe aller $2m$ Wurzeln 0. Ist also die Summe irgendwelcher m Wurzeln $+p$, so ist die Summe der übrigen $-p$; das heißt: Gehört $+p$ zu den Werten von u , so gehört auch $-p$ dazu. Hieraus schließt Euler, dass U das Produkt aus k quadratischen Faktoren wie $uu - pp$, $uu - qq$, $uu - rr$ usw. ist, wobei $+p$, $-p$, $+q$, $-q$ usw. alle $2k$ Wurzeln der Gleichung $U = 0$ bezeichnen. Wegen der ungeraden Anzahl dieser Faktoren ist daher das konstante Glied in U das Quadrat des Produkts pqr usw. mit negativem Vorzeichen. Das Produkt pqr usw. lässt sich aber stets aus den Koeffizienten B, C usw. rational bestimmen und ist deshalb notwendig eine reelle Größe. Sein Quadrat mit negativem Vorzeichen ist somit gewiss eine negative Größe. Q. E. D.

Da diese beiden reellen Faktoren von X den Grad m haben und m eine Potenz der Zahl 2 ist, lässt sich jeder auf dieselbe Weise erneut in zwei reelle Faktoren vom Grad $\frac{1}{2}m$ zerlegen. Durch wiederholte Halbierung der Zahl m muss man schließlich zu zwei gelangen; daher erhält man durch Fortsetzung des Verfahrens die Funktion X offenbar in reelle quadratische Faktoren zerlegt.

Wird dagegen eine Funktion vorgelegt, in der das zweite Glied nicht fehlt, etwa $x^{2m} + Ax^{2m-1} + Bx^{2m-2} +$ usw. $+ M$, wobei $2m$ weiterhin eine Zweierpotenz bezeichnet, so geht sie durch die Substitution $x = y - \frac{A}{2m}$ in eine

ähnliche Funktion ohne zweites Glied über. Daraus folgt leicht, dass auch diese Funktion in reelle quadratische Faktoren zerlegt werden kann.

Ist schließlich eine Funktion vom Grad n vorgelegt, wobei n eine Zahl bezeichnet, die keine Zweierpotenz ist, so setze man die nächstgrößere Zweierpotenz über n gleich $= 2m$ und multipliziere die vorgelegte Funktion mit beliebigen $2m - n$ reellen linearen Faktoren. Aus der Zerlegbarkeit des Produkts in reelle quadratische Faktoren ergibt sich ohne Schwierigkeit, dass auch die vorgelegte Funktion in reelle Faktoren zweiten oder ersten Grades zerlegbar sein muss.

8.

Gegen diesen Beweis lässt sich Folgendes einwenden.

1. Die Regel, nach der Euler schließt, dass sich aus $2m - 1$ Gleichungen alle $2m - 2$ Unbekannten α, β usw., λ, μ usw. rational bestimmen lassen, ist keineswegs allgemein, sondern lässt sehr häufig Ausnahmen zu. Betrachtet man zum Beispiel in Artikel 3 eine der Unbekannten als bekannt und versucht, die übrigen durch sie und die gegebenen Koeffizienten rational auszudrücken, so findet man leicht, dass dies unmöglich ist und keine unbekannte Größe anders als durch eine Gleichung vom Grad $m - 1$ bestimmt werden kann. Obwohl sich hier unmittelbar a priori erkennen lässt, dass dies notwendig so geschehen musste, könnte man doch mit Recht bezweifeln, ob sich die Sache nicht auch im vorliegenden Fall für manche Werte von m ebenso verhält, so dass sich die Unbekannten α, β usw., λ, μ usw. aus u, B, C usw. nur durch eine Gleichung von vielleicht höherem Grad als $2m$ bestimmen lassen. Für den Fall, dass die Gleichung $X = 0$ vierten Grades ist, leitet Euler rationale Werte der Koeffizienten durch u und die gegebenen Koeffizienten her; dass dies aber auch bei allen höheren Gleichungen möglich ist, bedurfte gewiss einer ausführlicheren Erklärung. — Im Übrigen scheint es der Mühe wert, jene Formeln, die α, β usw. rational durch u, B, C usw. ausdrücken, tiefer und in größter Allgemeinheit zu untersuchen. Dies und andere zur Eliminationstheorie gehörende Dinge (ein keineswegs erschöpftes Thema) werde ich bei einer anderen Gelegenheit ausführlicher behandeln.

2. Selbst wenn bewiesen worden ist, dass sich unabhängig vom Grad der Gleichung $X = 0$ stets Formeln finden lassen, die α, β usw., λ, μ usw. rational durch u, B, C usw. ausdrücken, ist doch sicher, dass diese Formeln für manche bestimmten Werte der Koeffizienten B, C usw. *unbestimmt* werden können. Dann ist es nicht nur unmöglich, jene Unbekannten aus u, B, C usw. rational zu bestimmen, sondern in manchen Fällen entsprechen einem reellen Wert von u tatsächlich keine reellen Werte von α, β usw., λ, μ usw. Zur Bestätigung verweise ich den Leser der Kürze halber auf Eulers Abhandlung selbst, in der die Gleichung vierten Grades auf S. 236 ausführlicher behandelt wird. Jeder wird sofort sehen, dass die Formeln für die Koeffizienten α, β unbestimmt werden, wenn $C = 0$ ist und für u der Wert 0 angenommen wird, und dass

sich ihre Werte nicht nur nicht ohne Wurzelziehen angeben lassen, sondern nicht einmal reell sind, wenn $BB - 4D$ eine negative Größe ist. Zwar lässt sich in diesem Fall leicht erkennen, dass u noch andere reelle Werte hat, denen reelle Werte von α, β entsprechen; dennoch könnte man befürchten, dass die Auflösung dieser Schwierigkeit (die Euler überhaupt nicht berührt hat) bei höheren Gleichungen weit größere Mühe macht. Gewiss darf diese Sache in einem genauen Beweis keineswegs stillschweigend übergangen werden.

3. Der ausgezeichnete Euler setzt stillschweigend voraus, dass die Gleichung $X = 0$ insgesamt $2m$ Wurzeln hat, und setzt ihre Summe $= 0$, weil das zweite Glied in X fehlt. Wie ich über diese Freiheit denke (deren sich alle Autoren zu diesem Gegenstand bedienen), habe ich schon oben in Artikel 3 erklärt. Der Satz, dass die Summe aller Wurzeln einer Gleichung ihrem ersten Koeffizienten mit umgekehrtem Vorzeichen gleich ist, scheint nur auf Gleichungen anwendbar, die Wurzeln haben. Da nun gerade durch diesen Beweis gezeigt werden soll, dass die Gleichung $X = 0$ tatsächlich Wurzeln hat, scheint es nicht zulässig, ihre Existenz vorauszusetzen. Ohne Zweifel werden diejenigen, die den Fehlschluss in dieser Argumentation noch nicht durchschaut haben, antworten, *hier werde nicht bewiesen, dass die Gleichung $X = 0$ erfüllt werden kann* (denn das bedeutet der Ausdruck, sie habe Wurzeln), *sondern nur, dass sie durch Werte von x erfüllt werden kann, die in der Form $a + b\sqrt{-1}$ enthalten sind; das Erstere werde dagegen als Axiom vorausgesetzt*. Da sich aber außer der reellen und der imaginären Form $a + b\sqrt{-1}$ keine anderen Formen von Größen denken lassen, scheint nicht hinreichend klar, wie sich das, was bewiesen werden soll, von dem unterscheidet, was als Axiom vorausgesetzt wird. Selbst wenn es möglich wäre, noch andere Formen von Größen zu ersinnen, etwa die Form F, F', F'' usw., dürfte man dennoch nicht ohne Beweis zugestehen, dass eine Gleichung durch irgendeinen Wert von x erfüllt werden kann, der entweder reell oder in der Form $a + b\sqrt{-1}$ oder in der Form F oder in F' usw. enthalten ist. Jenes Axiom kann daher keinen anderen Sinn haben als diesen: Jede Gleichung lässt sich *entweder* durch einen reellen Wert der Unbekannten erfüllen *oder* durch einen imaginären Wert in der Form $a + b\sqrt{-1}$ *oder* vielleicht durch einen Wert in einer anderen, bisher unbekannten Form *oder* durch einen Wert, der überhaupt in keiner Form enthalten ist. Wie sich aber solche Größen, von denen man sich nicht einmal eine Vorstellung machen kann — ein wahrer Schatten eines Schattens —, addieren oder multiplizieren lassen, versteht man gewiss nicht mit der Klarheit, die in der Mathematik stets gefordert wird^{*)}.

^{*)}Diese ganze Sache wird durch eine andere, bereits im Druck befindliche Untersuchung sehr erhellt werden. Dort hätte ich bei einem zwar ganz anderen, aber dennoch analogen Gegenstand eine ähnliche Freiheit mit genau demselben Recht gebrauchen können, wie es hier bei den Gleichungen von allen Analysten geschehen ist. Obwohl ich mithilfe solcher Fiktionen die Beweise mehrerer Wahrheiten mit wenigen Worten hätte abschließen können, die ohne

Im Übrigen will ich die Schlussfolgerungen, die Euler aus seiner Voraussetzung gezogen hat, durch diese Einwände keineswegs verdächtig machen. Vielmehr bin ich sicher, dass sie sich durch eine weder schwierige noch von der EULERSCHEN sehr verschiedene Methode so bestätigen lassen, dass niemandem auch nur der geringste Zweifel bleiben dürfte. Ich beanstande allein die *Form*, die zwar beim *Finden* neuer Wahrheiten von großem Nutzen sein kann, beim *Beweisen* vor der Öffentlichkeit aber keineswegs billigenswert erscheint.

4. Zum Beweis der Behauptung, das Produkt pqr usw. lasse sich aus den Koeffizienten in X rational bestimmen, hat der ausgezeichnete Euler überhaupt nichts angeführt. Alles, was er hierzu bei Gleichungen *vierten Grades* erläutert, ist Folgendes (wobei a, b, c, d die Wurzeln der vorgelegten Gleichung $x^4 + Bxx + Cx + D = 0$ sind):

‘Man wird mir ohne Zweifel einwenden, ich hätte hier vorausgesetzt, die Größe pqr sei eine reelle Größe und ihr Quadrat $ppqqrr$ sei positiv; das sei noch zweifelhaft gewesen, da die Wurzeln a, b, c, d imaginär seien und es daher sehr wohl geschehen könne, dass das Quadrat der aus ihnen zusammengesetzten Größe pqr negativ sei. Darauf antworte ich, dass dieser Fall niemals eintreten kann; denn wie imaginär auch die Wurzeln a, b, c, d sein mögen, weiß man doch, dass $a + b + c + d = 0$ gelten muss: $ab + ac + ad + bc + bd + cd = B$; $abc + abd + acd + bcd = -C^*$; $abcd = D$, wobei diese Größen B, C, D reell sind. Da aber $p = a + b$, $q = a + c$, $r = a + d$ ist, lässt sich ihr Produkt $pqr = (a + b)(a + c)(a + d)$, wie man weiß, durch die Größen B, C, D bestimmen und wird folglich reell sein, ebenso wie wir gesehen haben, dass tatsächlich $pqr = -C$ und $ppqqrr = CC$ ist. Ebenso wird man leicht erkennen, dass derselbe Umstand bei höheren Gleichungen eintreten muss und man mir von dieser Seite keine Einwände machen kann.’ Die Bedingung, dass sich das Produkt pqr usw. rational durch B, C usw. bestimmen lässt, hat Euler nirgends hinzugefügt; doch scheint er sie stets mitverstanden zu haben, da der Beweis ohne sie keine Beweiskraft haben kann. Nun ist zwar bei Gleichungen *vierten Grades* richtig, dass die Entwicklung des Produkts $(a + b)(a + c)(a + d)$ den Ausdruck $aa(a + b + c + d) + abc + abd + acd + bcd = -C$ ergibt; doch scheint nicht hinreichend klar, wie sich das Produkt bei allen höheren Gleichungen rational durch die Koeffizienten bestimmen lässt. Der berühmte DE FONCENEX, der dies zuerst bemerkt hat (*Miscell. phil. math. soc. Taurin.*, Bd. I, S. 117), behauptet mit Recht, dass die Methode ohne einen strengen Beweis dieses Satzes ihre ganze Beweiskraft verliert. Er gesteht aber, dass ihm dieser Beweis ziemlich schwierig erscheint, und berichtet, welchen Weg

sie sehr schwierig wurden und die feinsten Kunstgriffe erfordern, habe ich doch vorgezogen, ganz darauf zu verzichten, und hoffe, dass ich nur wenige zufriedengestellt hätte, wenn ich die Methode der Analysten nachgeahmt hätte.

*Euler hat irrtümlich C und setzt daher auch später fälschlich $pqr = C$.

er vergeblich versucht hat^{*)}. Dennoch lässt sich die Sache ohne große Schwierigkeit durch die folgende Methode erledigen (deren wesentlichen Inhalt ich hier nur andeuten kann). Obwohl bei Gleichungen vierten Grades nicht hinreichend klar ist, dass sich das Produkt $(a+b)(a+c)(a+d)$ durch die Koeffizienten B, C, D bestimmen lässt, sieht man doch leicht, dass dasselbe Produkt auch $= (b+a)(b+c)(b+d)$ sowie $= (c+a)(c+b)(c+d)$ und schließlich auch $= (d+a)(d+b)(d+c)$ ist. Das Produkt pqr ist daher ein Viertel der Summe $(a+b)(a+c)(a+d) + (b+a)(b+c)(b+d) + (c+a)(c+b)(c+d) + (d+a)(d+b)(d+c)$. Dass diese nach der Entwicklung ein Polynom in den Wurzeln a, b, c, d sein wird, in das alle auf dieselbe Weise eingehen, lässt sich ohne Mühe a priori erkennen. Solche Funktionen lassen sich aber stets rational durch die Koeffizienten der Gleichung ausdrücken, deren Wurzeln a, b, c, d sind. — Dasselbe ist auch klar, wenn man das Produkt pqr auf die Form

$$\frac{1}{2}(a+b-c-d) \times \frac{1}{2}(a+c-b-d) \times \frac{1}{2}(a+d-b-c)$$

bringt; denn man kann leicht voraussehen, dass dieses Produkt nach der Entwicklung alle a, b, c, d auf dieselbe Weise enthalten wird. Zugleich werden Sachkundige hieraus leicht entnehmen, wie dies auf höhere Gleichungen anzuwenden ist. — Eine vollständige Darstellung des Beweises, die ich der Kürze wegen hier nicht beifügen kann, behalte ich mir zusammen mit einer ausführlicheren Untersuchung von Funktionen, die mehrere Veränderliche auf dieselbe Weise enthalten, für eine andere Gelegenheit vor.

Im Übrigen bemerke ich, dass sich außer diesen vier Einwänden noch manches andere an Eulers Beweis beanstanden ließe. Das übergehe ich jedoch stillschweigend, um nicht etwa als allzu strenger Kritiker zu erscheinen, zumal das Vorhergehende hinreichend zu zeigen scheint, dass der Beweis jedenfalls in der von Euler vorgelegten Form keineswegs als vollständig gelten kann.

Nach diesem Beweis hat Euler noch einen anderen Weg gezeigt, den Satz für Gleichungen, deren Grad keine Zweierpotenz ist, auf die Auflösung solcher Gleichungen zurückzuführen. Da diese Methode aber für Gleichungen, deren Grad eine Zweierpotenz ist, nichts lehrt und außerdem allen vorigen Einwänden (außer dem vierten) ebenso ausgesetzt ist wie der erste allgemeine Beweis, ist es nicht nötig, sie hier ausführlicher zu erläutern.

^{*)}In diese Darstellung scheint sich ein Fehler eingeschlichen zu haben: Auf S. 118, Zeile 5, muss man nämlich anstelle des Zeichens p ("man wählte nur diejenigen, in denen p vorkam", usw.) notwendig *ein und dieselbe beliebige Wurzel der vorgelegten Gleichung* oder etwas Ähnliches lesen, da das Erstere keinen Sinn hat.

9.

In derselben Abhandlung hat der ausgezeichnete Euler auf S. 263 versucht, unseren Satz noch auf einem anderen Weg zu bestätigen, dessen wesentlicher Inhalt Folgendes ist. Für eine vorgelegte Gleichung $x^n + Ax^{n-1} + Bx^{n-2}$ usw. $= 0$ konnte bisher zwar kein analytischer Ausdruck gefunden werden, der ihre Wurzeln darstellt, wenn der Exponent $n > 4$ ist; dennoch scheint sicher zu sein (wie Euler behauptet), dass er nichts anderes enthalten kann als Rechenoperationen und Wurzelziehungen, die umso verwickelter miteinander verbunden sind, je größer n ist. Gibt man dies zu, so zeigt Euler sehr gut, dass sich der Wert der Formel, wie verwickelt die Wurzelzeichen auch miteinander verbunden sein mögen, stets durch die Form $M + N\sqrt{-1}$ darstellen lässt, wobei M, N reelle Größen sind.

Gegen diese Schlussweise lässt sich einwenden, dass nach den Bemühungen so vieler großer Mathematiker nur sehr geringe Hoffnung bleibt, jemals zur allgemeinen Auflösung algebraischer Gleichungen zu gelangen, sodass es immer wahrscheinlicher wird, dass eine solche Auflösung überhaupt unmöglich und widersprüchlich ist. Dies darf umso weniger paradox erscheinen, *als das, was man gewöhnlich die Auflösung einer Gleichung nennt, eigentlich nichts anderes ist als ihre Zurückführung auf reine Gleichungen*. Denn die Auflösung reiner Gleichungen wird dadurch nicht gelehrt, sondern vorausgesetzt; und wenn man eine Wurzel der Gleichung $x^m = H$ durch $\sqrt[m]{H}$ ausdrückt, hat man sie keineswegs gelöst und nicht mehr getan, als wenn man zur Bezeichnung einer Wurzel der Gleichung $x^n + Ax^{n-1} + \text{usw.} = 0$ irgendein Zeichen ersänne und die Wurzel diesem gleichsetzte. Es ist wahr, dass reine Gleichungen wegen der Leichtigkeit, ihre Wurzeln näherungsweise zu finden, und wegen des eleganten Zusammenhangs, den alle ihre Wurzeln untereinander haben, alle übrigen weit übertreffen. Daher ist keineswegs zu tadeln, dass die Analysten ihre Wurzeln durch ein besonderes Zeichen bezeichnet haben. Daraus aber, dass sie dieses Zeichen ebenso wie die Rechenzeichen für Addition, Subtraktion, Multiplikation, Division und Potenzierung unter dem Namen *analytische Ausdrücke* zusammengefasst haben, folgt keineswegs, dass sich eine Wurzel jeder Gleichung durch sie darstellen lässt. Oder, um die Worte beiseitezulassen: Ohne hinreichenden Grund wird vorausgesetzt, dass sich die Auflösung jeder Gleichung auf die Auflösung reiner Gleichungen zurückführen lässt. Vielleicht wäre es nicht so schwierig, diese Unmöglichkeit schon für den fünften Grad mit aller Strenge zu beweisen; meine Untersuchungen darüber werde ich an anderer Stelle ausführlicher vorlegen. Hier genügt es, dass die allgemeine Lösbarkeit der Gleichungen, in jenem Sinn verstanden, noch sehr zweifelhaft ist und daher ein Beweis, dessen ganze Beweiskraft von jener Voraussetzung abhängt, beim gegenwärtigen Stand der Sache kein Gewicht hat.

10.

Später versuchte auch der berühmte DE FONCENEX, nachdem er in EULERS erstem Beweis einen Mangel bemerkt hatte (oben Artikel 8, Einwand 4), den er nicht beheben konnte, noch einen anderen Weg und legte ihn in der genannten Abhandlung auf S. 120 vor^{*)}. Er besteht in Folgendem.

Es sei die Gleichung $Z = 0$ vorgelegt, wobei Z eine Funktion vom Grad m der Unbekannten z bezeichnet. Ist m eine ungerade Zahl, so steht bereits fest, dass diese Gleichung eine reelle Wurzel hat. Ist aber m gerade, so versucht der berühmte Foncenex auf folgende Weise zu beweisen, dass die Gleichung wenigstens eine Wurzel der Form $p + q\sqrt{-1}$ hat. Es sei $m = 2^n i$, wobei i eine ungerade Zahl bezeichnet, und es werde vorausgesetzt, dass $zz + uz + M$ ein Teiler der Funktion Z ist. Dann sind die einzelnen Werte von u die Summen von je zwei Wurzeln der Gleichung $Z = 0$ mit umgekehrtem Vorzeichen; daher hat u insgesamt $\frac{m \cdot m - 1}{1 \cdot 2} = m'$ Werte. Wird vorausgesetzt, dass u durch eine Gleichung $U = 0$ bestimmt wird (wobei U ein Polynom in u und den bekannten Koeffizienten in Z bezeichnet), so hat diese den Grad m' . Man sieht aber leicht, dass m' eine Zahl der Form $2^{n-1} i'$ sein wird, wobei i' eine ungerade Zahl bezeichnet. Ist nun m' nicht ungerade, so werde wiederum $uu + u'u + M'$ als Teiler von U vorausgesetzt. Durch ähnliche Überlegungen wird klar, dass u' durch eine Gleichung $U' = 0$ bestimmt wird, wobei U' eine Funktion vom Grad $\frac{m' \cdot m' - 1}{1 \cdot 2}$ in u' ist. Setzt man $\frac{m' \cdot m' - 1}{1 \cdot 2} = m''$, so ist m'' eine Zahl der Form $2^{n-2} i''$, wobei i'' eine ungerade Zahl bezeichnet. Ist nun m'' nicht ungerade, so werde $u'u' + u''u' + M''$ als Teiler der Funktion U' angenommen. Dann wird u'' durch eine Gleichung $U'' = 0$ bestimmt, die, wenn man ihren Grad gleich m''' setzt, für m''' eine Zahl der Form $2^{n-3} i'''$ ergibt. Offenbar ist in der Folge der Gleichungen $U = 0$, $U' = 0$, $U'' = 0$ usw. die Gleichung an der Stelle n von ungeradem Grad und hat daher eine reelle Wurzel. Wir setzen der Kürze halber $n = 3$, sodass die Gleichung $U'' = 0$ eine reelle Wurzel u'' hat; denn man sieht ohne Mühe, dass dieselbe Schlussweise für jeden anderen Wert von n gilt. Dann behauptet der berühmte de Foncenex, dass sich der Koeffizient M'' durch u'' und die Koeffizienten in U' (die, wie man leicht erkennt, Polynome in den Koeffizienten in Z sind), also durch u'' und die Koeffizienten in Z rational bestimmen lässt und daher reell ist. Hieraus folgt, dass die Wurzeln der Gleichung $u'u' + u''u' + M'' = 0$ in der Form $p + q\sqrt{-1}$ enthalten sein werden; sie werden aber offenbar zugleich die Gleichung $U' = 0$ erfüllen. Es gibt daher einen Wert von u' , der in der Form $p + q\sqrt{-1}$ enthalten ist. Nun lässt sich der Koeffizient M' auf dieselbe Weise wie zuvor rational durch u' und die Koeffizienten in Z bestimmen und wird daher ebenfalls in der Form $p + q\sqrt{-1}$ enthalten sein. Somit werden die

^{*)}Im zweiten Band derselben *Miscellanea*, S. 337, sind Erläuterungen zu dieser Abhandlung enthalten. Diese betreffen jedoch nicht die vorliegende Untersuchung, sondern die Logarithmen negativer Größen, von denen in derselben Abhandlung die Rede war.

Wurzeln der Gleichung $uu + u'u + M'$ in derselben Form enthalten sein und zugleich die Gleichung $U = 0$ erfüllen; das heißt, diese Gleichung wird eine Wurzel in der Form $p + q\sqrt{-1}$ haben. Schließlich folgt hieraus auf ähnliche Weise, dass auch M in derselben Form enthalten ist, ebenso eine Wurzel der Gleichung $zz + uz + M = 0$, die offenbar auch die vorgelegte Gleichung $Z = 0$ erfüllen wird. Daher wird jede Gleichung wenigstens eine Wurzel der Form $p + q\sqrt{-1}$ haben.

11.

Die Einwände 1, 2 und 3, die ich gegen EULERS ersten Beweis erhoben habe (Artikel 8), haben gegen diese Methode dieselbe Beweiskraft, jedoch mit dem Unterschied, dass der zweite Einwand, dem EULERS Beweis nur in einigen besonderen Fällen ausgesetzt war, den vorliegenden in allen Fällen treffen muss. Man kann nämlich a priori beweisen: Selbst wenn eine Formel gegeben ist, die den Koeffizienten M' rational durch u' und die Koeffizienten in Z ausdrückt, muss diese für mehrere Werte von u' notwendig unbestimmt werden. Ebenso wird die Formel, die den Koeffizienten M'' durch u'' darstellt, für gewisse Werte von u'' unbestimmt usw. Dies erkennt man am deutlichsten, wenn man eine Gleichung vierten Grades als Beispiel nimmt. Wir setzen also $m = 4$, und die Wurzeln der Gleichung $Z = 0$ seien $\alpha, \beta, \gamma, \delta$. Dann ist klar, dass die Gleichung $U = 0$ sechsten Grades sein wird und ihre Wurzeln $-(\alpha + \beta), -(\alpha + \gamma), -(\alpha + \delta), -(\beta + \gamma), -(\beta + \delta), -(\gamma + \delta)$ sind. Die Gleichung $U' = 0$ ist dagegen fünfzehnten Grades, und die Werte von u' sind

$$\begin{array}{lll} 2\alpha + \beta + \gamma, & 2\alpha + \beta + \delta, & 2\alpha + \gamma + \delta, \\ 2\beta + \alpha + \gamma, & 2\beta + \alpha + \delta, & 2\beta + \gamma + \delta, \\ 2\gamma + \alpha + \beta, & 2\gamma + \alpha + \delta, & 2\gamma + \beta + \delta, \\ 2\delta + \alpha + \beta, & 2\delta + \alpha + \gamma, & 2\delta + \beta + \gamma, \\ \alpha + \beta + \gamma + \delta, & \alpha + \beta + \gamma + \delta, & \alpha + \beta + \gamma + \delta \end{array}$$

Bei dieser Gleichung muss man nun stehen bleiben, da ihr Grad ungerade ist. Sie wird tatsächlich die reelle Wurzel $\alpha + \beta + \gamma + \delta$ haben (die dem ersten Koeffizienten in Z mit umgekehrtem Vorzeichen gleich und daher nicht nur reell, sondern auch rational sein wird, wenn die Koeffizienten in Z rational sind). Man kann aber ohne Mühe erkennen: Ist eine Formel gegeben, die den Wert von M' rational durch den zugehörigen Wert von u' ausdrückt, so wird sie notwendig für $u' = \alpha + \beta + \gamma + \delta$ unbestimmt. Denn dieser Wert ist *dreimal* eine Wurzel der Gleichung $U' = 0$, und ihm entsprechen drei Werte von M' , nämlich $(\alpha + \beta)(\gamma + \delta)$, $(\alpha + \gamma)(\beta + \delta)$ und $(\alpha + \delta)(\beta + \gamma)$, die alle irrational sein können. Offenbar könnte aber eine rationale Formel in diesem Fall weder einen irrationalen Wert von M' noch drei verschiedene Werte liefern. Aus diesem Beispiel lässt sich hinreichend entnehmen, dass die Methode des berühmten DE FONCENEX keineswegs befriedigt. Soll sie aber in

jeder Hinsicht vollständig werden, so muss die Eliminationstheorie weit tiefer untersucht werden.

12.

Schließlich hat der ausgezeichnete LA GRANGE unseren Satz in der Abhandlung *Sur la forme des racines imaginaires des équations*, *Nouv. Mém. de l'Acad. de Berlin* 1772, S. 222 ff., behandelt. Dieser große Mathematiker hat sich besonders bemüht, die Mängel in EULERS erstem Beweis zu ergänzen, und tatsächlich vor allem das, was oben (Artikel 8) den zweiten und vierten Einwand ausmacht, so tief untersucht, dass nichts weiter zu wünschen bleibt, außer dass vielleicht in der früheren Untersuchung über die Eliminationstheorie, auf der diese ganze Untersuchung beruht, einige Zweifel übrig zu sein scheinen. — Den dritten Einwand hat er jedoch überhaupt nicht berührt; vielmehr baut die ganze Untersuchung auf der Voraussetzung auf, jede Gleichung vom Grad m habe tatsächlich m Wurzeln.

Nach sorgfältiger Erwägung dessen, was bisher dargelegt wurde, hoffe ich daher, dass den Sachkundigen ein neuer, aus ganz anderen Grundsätzen abgeleiteter Beweis dieses höchst wichtigen Satzes nicht unwillkommen sein wird. Diesen darzustellen, gehe ich nun sogleich an.

13.

LEMMA. *Bezeichnet m eine beliebige positive ganze Zahl, so ist die Funktion $\sin \varphi \cdot x^m - \sin m\varphi \cdot r^{m-1}x + \sin(m-1)\varphi \cdot r^m$ durch $xx - 2\cos \varphi \cdot rx + rr$ teilbar.*

Beweis. Für $m = 1$ wird jene Funktion $= 0$ und ist daher durch jeden Faktor teilbar; für $m = 2$ wird der Quotient gleich $\sin \varphi$, und für jeden größeren Wert ist der Quotient $\sin \varphi \cdot x^{m-2} + \sin 2\varphi \cdot rx^{m-3} + \sin 3\varphi \cdot rrx^{m-4} + \text{usw.} + \sin(m-1)\varphi \cdot r^{m-2}$. Denn man bestätigt leicht, dass nach Multiplikation dieser Funktion mit $xx - 2\cos \varphi \cdot rx + rr$ das Produkt der vorgelegten Funktion gleich wird.

14.

LEMMA. *Sind die Größe r und der Winkel φ so bestimmt, dass die Gleichungen*

$$\begin{aligned} r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + Br^{m-2} \cos(m-2)\varphi + \text{usw.} \\ + Krr \cos 2\varphi + Lr \cos \varphi + M = 0 \quad . \quad . \quad [1] \\ r^m \sin m\varphi + Ar^{m-1} \sin(m-1)\varphi + Br^{m-2} \sin(m-2)\varphi + \text{usw.} \\ + Krr \sin 2\varphi + Lr \sin \varphi = 0 \quad . \quad . \quad [2] \end{aligned}$$

gelten, so ist das Polynom $x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + Kxx + Lx + M = X$ durch den quadratischen Faktor $xx - 2\cos \varphi \cdot rx + rr$ teilbar, sofern nicht $r \sin \varphi = 0$ gilt; ist dagegen $r \sin \varphi = 0$, so ist dasselbe Polynom durch den linearen Faktor $x - r \cos \varphi$ teilbar.

Beweis. I. Nach dem vorigen Artikel sind alle folgenden Größen durch $xx - 2 \cos \varphi \cdot rx + rr$ teilbar:

$$\begin{array}{lll}
 \sin \varphi \cdot rx^m - \sin m\varphi \cdot r^m x & & + \sin(m-1)\varphi \cdot r^{m+1} \\
 A \sin \varphi \cdot rx^{m-1} - A \sin(m-1)\varphi \cdot r^{m-1} x & + & A \sin(m-2)\varphi \cdot r^m \\
 B \sin \varphi \cdot rx^{m-2} - B \sin(m-2)\varphi \cdot r^{m-2} x & + & B \sin(m-3)\varphi \cdot r^{m-1} \\
 & \text{usw.} & \text{usw.} \\
 K \sin \varphi \cdot rxx - K \sin 2\varphi \cdot rrx & & + K \sin \varphi \cdot r^3 \\
 L \sin \varphi \cdot rx - L \sin \varphi \cdot rx & & * \\
 M \sin \varphi \cdot r & & * \\
 & & + M \sin(-\varphi) \cdot r
 \end{array}$$

Daher ist auch ihre Summe durch $xx - 2 \cos \varphi \cdot rx + rr$ teilbar. Die ersten Teile dieser Größen bilden aber die Summe $\sin \varphi \cdot rX$; die zweiten ergeben zusammen nach [2] den Wert 0. Dass auch die Summe der dritten Teile verschwindet, erkennt man leicht, wenn man [1] mit $\sin \varphi$ und [2] mit $\cos \varphi$ multipliziert und das erste Produkt vom zweiten abzieht. Daraus folgt, dass das Polynom $\sin \varphi \cdot rX$ durch $xx - 2 \cos \varphi \cdot rx + rr$ teilbar ist, und damit auch das Polynom X , sofern nicht $r \sin \varphi = 0$ gilt. Q. E. P.

II. Ist dagegen $r \sin \varphi = 0$, so ist entweder $r = 0$ oder $\sin \varphi = 0$. Im ersten Fall ist nach [1] auch $M = 0$, und daher ist X durch x oder durch $x - r \cos \varphi$ teilbar; im zweiten Fall ist $\cos \varphi = \pm 1$, $\cos 2\varphi = +1$, $\cos 3\varphi = \pm 1$ und allgemein $\cos n\varphi = \cos \varphi^n$. Wegen [1] ergibt sich also $X = 0$, wenn man $x = r \cos \varphi$ setzt, und folglich ist das Polynom X durch $x - r \cos \varphi$ teilbar. Q. E. S.

15.

Der vorige Satz wird gewöhnlich mit Hilfe imaginärer Größen bewiesen; siehe EULER, *Introd. in Anal. Inf.*, Bd. I, S. 110. Ich hielt es für der Mühe wert zu zeigen, wie er sich ebenso leicht ohne ihre Hilfe herleiten lässt. Es ist nun klar, dass zum Beweis unseres Satzes nur noch Folgendes zu zeigen ist: *Für jedes vorgegebene Polynom X der Form $x^m + Ax^{m-1} + Bx^{m-2} + \text{usw.} + Lx + M$ lassen sich r und φ so bestimmen, dass die Gleichungen [1] und [2] gelten.* Daraus folgt nämlich, dass X einen reellen Faktor ersten oder zweiten Grades besitzt. Die Division ergibt notwendig einen reellen Quotienten niedrigeren Grades, der aus demselben Grund ebenfalls einen Faktor ersten oder zweiten Grades besitzt. Setzt man dieses Verfahren fort, so wird X schließlich in reelle lineare oder quadratische Faktoren zerlegt. Diesen Satz zu beweisen ist also das Ziel der folgenden Untersuchungen.

16.

Man denke sich eine feste unendliche Ebene (die Ebene der Tafel, Fig. 1) und darin eine feste unendliche Gerade GC , die durch einen festen Punkt C geht. Man wähle eine Länge als Einheit, sodass sich alle Geradenlängen durch Zahlen ausdrücken lassen. In jedem Punkt P der Ebene, dessen Abstand vom Mittelpunkt C gleich r ist und dessen Winkel $GCP = \varphi$ beträgt, errichte man eine Senkrechte gleich dem Wert des Ausdrucks

$$r^m \sin m\varphi + Ar^{m-1} \sin(m-1)\varphi + \text{usw.} + Lr \sin \varphi$$

den ich im Folgenden der Kürze halber stets mit T bezeichnen werde. Den Abstand r betrachte ich stets als positiv. Für Punkte auf der anderen Seite der Achse muss der Winkel φ entweder als größer als zwei rechte Winkel oder als negativ angesehen werden (was hier auf dasselbe hinausläuft). Die Endpunkte dieser Senkrechten (die für einen positiven Wert von T oberhalb der Ebene, für einen negativen unterhalb und bei verschwindendem Wert in der Ebene selbst zu nehmen sind) liegen auf einer stetigen gekrümmten Fläche, die sich nach allen Richtungen ins Unendliche erstreckt. Ich werde sie im Folgenden der Kürze halber die *erste Fläche* nennen. Ganz ebenso beziehe man auf dieselbe Ebene, denselben Mittelpunkt und dieselbe Achse eine andere Fläche, deren Höhe über jedem Punkt der Ebene gleich

$$r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + \text{usw.} + Lr \cos \varphi + M$$

ist; diesen Ausdruck werde ich der Kürze halber stets mit U bezeichnen. Diese Fläche, die ebenfalls stetig ist und sich nach allen Richtungen ins Unendliche erstreckt, werde ich von der vorigen durch die Bezeichnung *zweite Fläche* unterscheiden. Damit ist klar, dass die ganze Aufgabe darin besteht zu zeigen, dass es mindestens einen Punkt gibt, der zugleich in der Ebene, auf der ersten Fläche und auf der zweiten Fläche liegt.

17.

Man erkennt leicht, dass die erste Fläche teils oberhalb, teils unterhalb der Ebene liegt. Denn offenbar lässt sich der Abstand r vom Mittelpunkt so groß wählen, dass die übrigen Glieder in T gegenüber dem ersten Glied $r^m \sin m\varphi$ verschwinden; dieses kann aber durch geeignete Wahl des Winkels φ sowohl positiv als auch negativ werden. Die feste Ebene wird daher notwendig von der ersten Fläche geschnitten. Diese Schnittlinie der Ebene mit der ersten Fläche werde ich die *erste Linie* nennen; sie wird also durch die Gleichung $T = 0$ bestimmt. Aus demselben Grund wird die Ebene von der zweiten Fläche geschnitten; der Schnitt bildet eine durch die Gleichung $U = 0$ bestimmte Kurve, die ich die *zweite Linie* nennen werde. Eigentlich besteht jede der beiden Kurven aus mehreren Zweigen, die vollständig voneinander getrennt sein können, während jeder für sich eine stetige Linie ist. Die erste Linie ist

sogar stets eine sogenannte zusammengesetzte Kurve, und die Achse GC ist als Teil dieser Kurve anzusehen: Welchen Wert man r auch gibt, es gilt stets $T = 0$, wenn $\varphi = 0$ oder $= 180^\circ$ ist. Doch ist es besser, die Gesamtheit aller Zweige, die durch sämtliche Punkte mit $T = 0$ gehen, als eine einzige Kurve zu betrachten (entsprechend dem in der höheren Geometrie allgemein üblichen Gebrauch), und ebenso sämtliche Zweige durch alle Punkte mit $U = 0$. Es ist nun klar, dass die Aufgabe darauf zurückgeführt ist zu zeigen, dass es mindestens einen Punkt in der Ebene gibt, in dem irgendein Zweig der ersten Linie von einem Zweig der zweiten Linie geschnitten wird. Dazu müssen wir die Beschaffenheit dieser Linien näher betrachten.

18.

Zunächst bemerke ich, dass beide Kurven algebraisch sind, und zwar bei Darstellung durch rechtwinklige Koordinaten vom Grad m . Wählt man nämlich den Anfangspunkt der Abszissen in C , die Abszissen x in Richtung G und die Ordinaten y in Richtung P , so gilt $x = r \cos \varphi$, $y = r \sin \varphi$ und daher allgemein, welchen Wert n auch haben mag,

$$\begin{aligned} r^n \sin n\varphi &= nx^{n-1}y - \frac{n \cdot n - 1 \cdot n - 2}{1 \cdot 2 \cdot 3}x^{n-3}y^3 \\ &\quad + \frac{n \dots n - 4}{1 \dots 5}x^{n-5}y^5 - \text{usw.}, \\ r^n \cos n\varphi &= x^n - \frac{n \cdot n - 1}{1 \cdot 2}x^{n-2}yy \\ &\quad + \frac{n \cdot n - 1 \cdot n - 2 \cdot n - 3}{1 \cdot 2 \cdot 3 \cdot 4}x^{n-4}y^4 - \text{usw.} \end{aligned}$$

Also bestehen sowohl T als auch U aus mehreren Gliedern der Form $ax^\alpha y^\beta$, wobei α und β positive ganze Zahlen bezeichnen, deren Summe im größten Fall $= m$ ist. Ferner lässt sich leicht voraussehen, dass alle Glieder von T den Faktor y enthalten und die erste Linie somit eigentlich aus einer Geraden (mit der Gleichung $y = 0$) und einer Kurve vom Grad $m - 1$ zusammengesetzt ist; doch brauchen wir auf diese Unterscheidung hier nicht einzugehen.

Wichtiger wird die Untersuchung sein, ob die erste und die zweite Linie ins Unendliche verlaufende Arme besitzen und wie viele und welcher Art diese sind. In unendlicher Entfernung vom Punkt C fällt die erste Linie, deren Gleichung $\sin m\varphi + \frac{A}{r} \sin(m-1)\varphi + \frac{B}{rr} \sin(m-2)\varphi$ usw. $= 0$ lautet, mit der Linie zusammen, deren Gleichung $\sin m\varphi = 0$ ist. Diese stellt m Geraden dar, die sich im Punkt C schneiden. Die erste ist die Achse GCG' ; die übrigen sind gegen sie unter den Winkeln $\frac{1}{m}180$, $\frac{2}{m}180$, $\frac{3}{m}180$ usw. Grad geneigt. Die erste Linie besitzt daher $2m$ unendliche Zweige, welche den Umfang eines mit unendlichem Radius beschriebenen Kreises in $2m$ gleiche Teile zerlegen: Der erste Zweig schneidet den Umfang im Schnittpunkt von Kreis und Achse, der zweite im Abstand $\frac{1}{m}180^\circ$, der dritte im Abstand $\frac{2}{m}180^\circ$ usw. Ebenso besitzt

die zweite Linie in unendlicher Entfernung vom Mittelpunkt eine durch die Gleichung $\cos m\varphi = 0$ ausgedrückte Asymptote. Diese ist eine Gesamtheit von m Geraden, die sich ebenfalls im Punkt C unter gleichen Winkeln schneiden, jedoch so, dass die erste mit der Achse CG den Winkel $\frac{1}{m}90^\circ$ bildet, die zweite den Winkel $\frac{3}{m}90^\circ$, die dritte den Winkel $\frac{5}{m}90^\circ$ usw. Daher besitzt auch die zweite Linie $2m$ unendliche Zweige, von denen jeder die Mitte zwischen zwei benachbarten Zweigen der ersten Linie einnimmt. Sie schneiden also den Umfang eines mit unendlich großem Radius beschriebenen Kreises in Punkten, deren Winkelabstände von der Achse $\frac{1}{m}90^\circ$, $\frac{3}{m}90^\circ$, $\frac{5}{m}90^\circ$ usw. betragen. Ferner ist klar, dass die Achse selbst stets zwei unendliche Zweige der ersten Linie bildet, nämlich den ersten und den an der Stelle $m + 1$. Sehr deutlich zeigt sich diese Lage der Zweige in Fig. 2, die für den Fall $m = 4$ gezeichnet ist. Die Zweige der zweiten Linie sind dort zur Unterscheidung von denen der ersten punktiert dargestellt; dasselbe gilt auch für die vierte Figur^{*)}. — Da diese Folgerungen aber von größter Bedeutung sind und unendlich große Größen bei manchen Lesern Anstoß erregen könnten, werde ich im nächsten Artikel zeigen, wie man sie auch ohne die Hilfe von Unendlichkeiten herleiten kann.

19.

SATZ. Bleibt alles wie oben, so lässt sich um den Mittelpunkt C ein Kreis beschreiben, auf dessen Umfang $2m$ Punkte mit $T = 0$ und ebenso viele mit $U = 0$ liegen, und zwar so, dass jeder der letzteren zwischen zweien der ersteren liegt.

Die Summe aller positiv genommenen Koeffizienten A, B usw. K, L, M sei $= S$, und man wähle R zugleich $> S\sqrt{2}$ und $> 1^*)$. Dann behaupte ich, dass für den mit dem Radius R beschriebenen Kreis notwendig gilt, was der Satz ausspricht. Der Kürze halber bezeichne man den Punkt dieses Umfangs, der $\frac{1}{m}45$ Grad von dessen Schnitt mit dem linken Teil der Achse entfernt ist, oder für den $\varphi = \frac{1}{m}45^\circ$ gilt, mit (1); ebenso den Punkt im Abstand $\frac{3}{m}45^\circ$ von diesem Schnitt, oder für den $\varphi = \frac{3}{m}45^\circ$ gilt, mit (3); ferner den Punkt mit $\varphi = \frac{5}{m}45^\circ$ mit (5) usw. bis zu $(8m - 1)$. Dieser liegt $\frac{8m-1}{m}45$ Grad von jenem Schnitt entfernt, wenn man stets in derselben Richtung fortschreitet (oder $\frac{1}{m}45^\circ$ in der entgegengesetzten Richtung). So erhält man insgesamt $4m$ Punkte auf dem Umfang in gleichen Abständen. Zwischen $(8m - 1)$ und (1) liegt ein Punkt mit $T = 0$; ebenso liegt je ein solcher Punkt zwischen (3) und (5), zwischen (7) und (9), zwischen (11) und (13) usw., sodass ihre Anzahl

^{*)}Die vierte Figur wurde unter der Annahme $X = x^4 - 2xx + 3x + 10$ gezeichnet, sodass Leser, die mit allgemeinen und abstrakten Untersuchungen weniger vertraut sind, die gegenseitige Lage beider Kurven an einem konkreten Fall betrachten können. Die Länge der Linie CG wurde als $= 10$ angenommen ($CN = 1,26255$.)

^{*)}Ist $S > \sqrt{\frac{1}{2}}$, so folgt die zweite Bedingung aus der ersten; ist dagegen $S < \sqrt{\frac{1}{2}}$, so folgt die erste aus der zweiten.

$2m$ beträgt. Auf dieselbe Weise liegen je einzelne Punkte mit $U = 0$ zwischen (1) und (3), zwischen (5) und (7), zwischen (9) und (11); ihre Anzahl ist also ebenfalls $= 2m$. Außer diesen $4m$ Punkten gibt es schließlich auf dem ganzen Umfang keine weiteren, in denen entweder T oder U den Wert $= 0$ hat.

Beweis. I. Im Punkt (1) ist $m\varphi = 45^\circ$ und daher

$$T = R^{m-1}(R\sqrt{\frac{1}{2}} + A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi + \text{usw.} + \frac{L}{R^{m-2}}\sin\varphi)$$

Die Summe $A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi$ usw. kann aber gewiss nicht größer als S sein und ist daher notwendig kleiner als $R\sqrt{\frac{1}{2}}$. Daraus folgt, dass der Wert von T in diesem Punkt gewiss positiv ist. Umso mehr hat also T einen positiven Wert, wenn $m\varphi$ zwischen 45° und 135° liegt, d. h. der Wert von T ist vom Punkt (1) bis (3) stets positiv. Aus demselben Grund hat T vom Punkt (9) bis (11) überall einen positiven Wert und allgemein von jedem Punkt $(8k+1)$ bis $(8k+3)$, wobei k eine beliebige ganze Zahl bezeichnet. Ebenso hat T überall zwischen (5) und (7), zwischen (13) und (15) usw. und allgemein zwischen $(8k+5)$ und $(8k+7)$ einen negativen Wert; in allen diesen Intervallen kann es also nirgends $= 0$ sein. Da dieser Wert aber in (3) positiv und in (5) negativ ist, muss er irgendwo zwischen (3) und (5) $= 0$ sein; ebenso irgendwo zwischen (7) und (9), zwischen (11) und (13) usw. bis einschließlich des Intervalls zwischen $(8m-1)$ und (1), sodass insgesamt in $2m$ Punkten $T = 0$ gilt. Q. E. P.

II. Dass es außer diesen $2m$ Punkten keine weiteren mit dieser Eigenschaft gibt, erkennt man folgendermaßen. Da zwischen (1) und (3), zwischen (5) und (7) usw. keine solchen Punkte liegen, könnte es mehr davon nur geben, wenn in irgendeinem Intervall zwischen (3) und (5) oder zwischen (7) und (9) usw. mindestens zwei lägen. Dann müsste aber T irgendwo in demselben Intervall ein *Maximum* oder *Minimum* sein, und daher wäre $\frac{dT}{d\varphi} = 0$. Es ist jedoch $\frac{dT}{d\varphi} = mR^{m-2}(R\cos m\varphi + \frac{m-1}{m}A\cos(m-1)\varphi + \text{usw.})$, und $\cos m\varphi$ ist zwischen (3) und (5) stets negativ und $> \sqrt{\frac{1}{2}}$. Daraus erkennt man leicht, dass $\frac{dT}{d\varphi}$ in diesem ganzen Intervall eine negative Größe ist; ebenso ist es zwischen (7) und (9) überall positiv, zwischen (11) und (13) negativ usw. Es kann also in keinem dieser Intervalle 0 sein, und die Annahme kann nicht bestehen. Folglich usw. Q. E. S.

III. Ganz ebenso beweist man, dass U überall zwischen (3) und (5), zwischen (11) und (13) usw. und allgemein zwischen $(8k+3)$ und $(8k+5)$ einen negativen Wert hat, dagegen zwischen (7) und (9), zwischen (15) und (17) usw. und allgemein zwischen $(8k+7)$ und $(8k+9)$ einen positiven. Daraus folgt sofort, dass irgendwo zwischen (1) und (3), zwischen (5) und (7) usw., also in $2m$ Punkten, $U = 0$ gelten muss. In keinem dieser Intervalle kann aber $\frac{dU}{d\varphi} = 0$ sein (was man leicht ebenso wie oben beweist). Daher gibt es auf dem Kreisumfang nicht mehr als jene $2m$ Punkte, in denen $U = 0$ gilt. Q. E. T. und Q.

Der Teil des Satzes, wonach es nicht mehr als $2m$ Punkte mit $T = 0$ und nicht mehr als $2m$ Punkte mit $U = 0$ gibt, lässt sich übrigens auch daraus beweisen, dass die Gleichungen $T = 0$, $U = 0$ Kurven vom Grad m darstellen. Aus der höheren Geometrie ist bekannt, dass solche Kurven von einem Kreis als Kurve zweiten Grades nicht in mehr als $2m$ Punkten geschnitten werden können.

20.

Beschreibt man um denselben Mittelpunkt einen anderen Kreis mit einem größeren Radius als R und teilt ihn auf dieselbe Weise, so liegt auch auf ihm zwischen den Punkten (3) und (5) ein Punkt mit $T = 0$, ebenso zwischen (7) und (9) usw. Man erkennt leicht, dass solche zwischen (3) und (5) auf den beiden Umfängen liegenden Punkte einander umso näher sein müssen, je weniger sich der Radius dieses Kreises vom Radius R unterscheidet. Dasselbe gilt, wenn man einen Kreis mit einem etwas kleineren Radius als R beschreibt, der jedoch größer als $S\sqrt{2}$ und 1 bleibt. Daraus versteht man ohne Mühe, dass der Umfang des mit dem Radius R beschriebenen Kreises in dem Punkt zwischen (3) und (5), in dem $T = 0$ gilt, tatsächlich von irgendeinem Zweig der ersten Linie *geschnitten* wird; dasselbe gilt für die übrigen Punkte mit $T = 0$. Ebenso ist klar, dass der Umfang dieses Kreises in allen $2m$ Punkten mit $U = 0$ von irgendeinem Zweig der zweiten Linie geschnitten wird. Diese Folgerungen lassen sich auch so ausdrücken: Beschreibt man um den Mittelpunkt C einen Kreis von der erforderlichen Größe, so treten $2m$ Zweige der ersten Linie und ebenso viele der zweiten in ihn ein, und zwar so, dass je zwei benachbarte Zweige der ersten Linie durch irgendeinen Zweig der zweiten voneinander getrennt werden. Siehe Fig. 2, in der der Kreis nun eine endliche statt einer unendlichen Größe hat. Die den einzelnen Zweigen beige-schriebenen Zahlen dürfen nicht mit den Zahlen verwechselt werden, mit denen ich im vorigen und in diesem Artikel der Kürze halber bestimmte Grenzen auf dem Umfang bezeichnet habe.

21.

Aus dieser gegenseitigen Lage der in den Kreis eintretenden Zweige lässt sich die Notwendigkeit eines Schnittes irgendeines Zweiges der ersten Linie mit einem Zweig der zweiten innerhalb des Kreises auf so viele verschiedene Arten herleiten, dass ich beinahe nicht weiß, welche Methode vor den übrigen zu wählen ist. Am deutlichsten scheint mir die folgende. Bezeichnen wir (Fig. 2) den Punkt des Kreisumfangs, in dem er vom linken Teil der Achse geschnitten wird (der selbst einer der $2m$ Zweige der ersten Linie ist), mit 0; den nächsten Punkt, in dem ein Zweig der zweiten Linie eintritt, mit 1; den darauf folgenden, in dem der zweite Zweig der ersten Linie eintritt, mit 2; und so fort bis $4m - 1$. Damit tritt in jedem mit einer geraden Zahl bezeichneten Punkt ein Zweig der zweiten Linie in den Kreis ein, dagegen ein Zweig der zweiten

Linie in allen mit ungeraden Zahlen bezeichneten Punkten. Aus der höheren Geometrie ist nun bekannt, dass jede algebraische Kurve (oder jeder einzelne Teil einer algebraischen Kurve, falls sie aus mehreren zusammengesetzt ist) entweder in sich zurückkehrt oder nach beiden Seiten ins Unendliche verläuft. Tritt also irgendein Zweig einer algebraischen Kurve in ein begrenztes Gebiet ein, so muss er es notwendig irgendwo wieder verlassen^{*)}. Daraus schließt man leicht, dass jeder mit einer geraden Zahl bezeichnete Punkt (oder der Kürze halber *jeder gerade Punkt*) innerhalb des Kreises durch einen Zweig der ersten Linie mit einem anderen geraden Punkt verbunden sein muss; ebenso jeder mit einer ungeraden Zahl bezeichnete Punkt durch einen Zweig der zweiten Linie mit einem anderen solchen Punkt. Obwohl diese Verbindung von je zwei Punkten je nach der Beschaffenheit des Polynoms X sehr verschieden sein und daher nicht allgemein bestimmt werden kann, lässt sich doch leicht beweisen, dass *sie, wie sie auch beschaffen sein mag, stets einen Schnitt der ersten mit der zweiten Linie hervorbringt.*

22.

Der Beweis dieser Notwendigkeit lässt sich wohl am bequemsten durch Widerspruch führen. Nehmen wir also an, die Verbindung je zweier gerader und je zweier ungerader Punkte könne so eingerichtet werden, dass daraus kein Schnitt eines Zweiges der ersten Linie mit einem Zweig der zweiten entsteht. Da die Achse ein Teil der ersten Linie ist, ist offenbar der Punkt 0 mit dem Punkt $2m$ verbunden. Der Punkt 1 kann daher mit keinem jenseits der Achse liegenden Punkt verbunden sein, d. h. mit keinem Punkt, der durch eine größere Zahl als $2m$ bezeichnet wird; sonst würde die Verbindungslinie notwendig die Achse schneiden. Nimmt man also

^{*)}Es scheint gewiss hinreichend gut bewiesen zu sein, dass eine algebraische Kurve weder irgendwo plötzlich abbrechen kann (wie es etwa bei der transzendenten Kurve mit der Gleichung $y = \frac{1}{\log x}$ geschieht), noch sich nach unendlich vielen Windungen gleichsam in irgendeinem Punkt verlieren kann (wie die logarithmische Spirale); und meines Wissens hat niemand dagegen einen Zweifel erhoben. Sollte dennoch jemand einen Beweis verlangen, der keinerlei Zweifeln ausgesetzt ist, so werde ich es übernehmen, ihn bei einer anderen Gelegenheit zu geben. Im vorliegenden Fall ist aber klar: Verließe irgendein Zweig, etwa 2, den Kreis nirgends wieder (Fig. 3), so könnte man zwischen 0 und 2 in den Kreis eintreten, dann um diesen ganzen Zweig herumgehen (der sich im Kreisgebiet verlieren müsste) und schließlich zwischen 2 und 4 wieder aus dem Kreis austreten, ohne auf dem ganzen Weg irgendwo die erste Linie zu treffen. Dass dies widersinnig ist, erkennt man daran, dass man beim Eintritt in den Kreis die erste Fläche über sich hatte, beim Austritt aber unter sich. Man müsste daher notwendig irgendwo auf die erste Fläche selbst, also auf einen Punkt der ersten Linie getroffen sein. — Aus dieser Überlegung, die sich auf Grundsätze der Geometrie der Lage stützt, die nicht weniger gültig sind als die der Geometrie der Größe, folgt übrigens nur, dass man, wenn man auf irgendeinem Zweig der ersten Linie in den Kreis eintritt, an einer anderen Stelle wieder austreten kann, wobei man stets auf der ersten Linie bleibt; nicht aber, dass der Weg eine stetige Linie in dem Sinne ist, wie man es in der höheren Geometrie versteht. Hier genügt jedoch, dass der Weg im gewöhnlichen Sinne eine stetige Linie ist, d. h. nirgends unterbrochen, sondern überall zusammenhängend.

an, 1 sei mit dem Punkt n verbunden, so ist $n < 2m$. Aus einem ähnlichen Grund gilt $n' < n$, wenn man annimmt, 2 sei mit n' verbunden; sonst würde nämlich der Zweig $2 \dots n'$ notwendig den Zweig $1 \dots n$ schneiden. Aus demselben Grund ist der Punkt 3 mit einem der zwischen 4 und n' liegenden Punkte verbunden. Nimmt man an, 3, 4, 5 usw. seien mit n'' , n''' , n'''' usw. verbunden, so liegt offenbar n''' zwischen 5 und n'' , n'''' zwischen 6 und n''' usw. Es ist also klar, dass man schließlich zu irgendeinem Punkt h gelangt, der mit dem Punkt $h + 2$ verbunden ist. Dann schneidet der Zweig, der im Punkt $h + 1$ in den Kreis eintritt, notwendig den Zweig, der die Punkte h und $h + 2$ verbindet. Da aber der eine dieser beiden Zweige zur ersten Linie und der andere zur zweiten gehört, ist nun klar, dass die Annahme widersprüchlich ist und daher notwendig irgendwo ein Schnitt der ersten mit der zweiten Linie stattfindet. Verbindet man dies mit dem Vorhergehenden, so ergibt sich aus allen dargelegten Untersuchungen, dass der Satz, *jedes Polynom in einer Variablen lasse sich in reelle Faktoren ersten oder zweiten Grades zerlegen*, mit voller Strenge bewiesen ist.

23.

Aus denselben Grundsätzen lässt sich übrigens ohne große Schwierigkeit herleiten, dass es nicht nur einen, sondern mindestens m Schnitte der ersten mit der zweiten Linie gibt. Allerdings kann die erste Linie auch von mehreren Zweigen der zweiten im selben Punkt geschnitten werden; in diesem Fall besitzt das Polynom X mehrere gleiche Faktoren. Da es hier jedoch genügt, die Notwendigkeit eines einzigen Schnittes bewiesen zu haben, halte ich mich der Kürze halber nicht länger dabei auf. Aus demselben Grund gehe ich hier auch auf andere Eigenschaften dieser Linien nicht näher ein, etwa darauf, dass die Schnitte stets unter rechten Winkeln erfolgen; oder dass, wenn mehrere Arme beider Kurven in demselben Punkt zusammenkommen, ebenso viele Arme der ersten wie der zweiten Linie vorhanden sind, die abwechselnd liegen und sich unter gleichen Winkeln schneiden usw.

Schließlich bemerke ich, dass es keineswegs unmöglich ist, den vorigen Beweis, den ich hier auf geometrische Grundsätze gestützt habe, auch in rein analytischer Form darzustellen. Doch glaubte ich, die hier entwickelte Darstellung werde weniger abstrakt ausfallen und die eigentliche Kraft des Beweises werde hier viel deutlicher vor Augen geführt, als von einem analytischen Beweis zu erwarten wäre.

Zum Abschluss werde ich noch eine andere Methode zum Beweis unseres Satzes andeuten. Auf den ersten Blick wird sie nicht nur von dem vorigen Beweis, sondern auch von allen übrigen oben angeführten Beweisen sehr verschieden erscheinen; ihrem Wesen nach ist sie dennoch eigentlich dieselbe wie die von D'ALEMBERT. Den Vergleich mit dieser und die Untersuchung der Parallele zwischen beiden überlasse ich den Sachkundigen, allein für die sie hinzugefügt ist.

24.

Über der Ebene von Fig. 4 denke ich mir die erste und die zweite Fläche in Bezug auf die Achse CG und den festen Punkt C auf dieselbe Weise wie oben beschrieben. Man nehme irgendeinen Punkt auf irgendeinem Zweig der ersten Linie, also einen Punkt mit $T = 0$ (etwa einen beliebigen Punkt M auf der Achse). Gilt in ihm nicht auch $U = 0$, so gehe man von diesem Punkt auf der ersten Linie in der Richtung weiter, in der der absolute Betrag von U abnimmt. Nimmt im Punkt M der absolute Betrag von U nach beiden Seiten ab, so ist es gleichgültig, in welcher Richtung man weitergeht; was zu tun ist, wenn U nach beiden Seiten wächst, werde ich sogleich zeigen. Es ist also klar, dass man, wenn man stets auf der ersten Linie weitergeht, notwendig schließlich zu einem Punkt gelangt, in dem $U = 0$ gilt, oder zu einem solchen, in dem der Wert von U ein Minimum wird, etwa zum Punkt N . Im ersten Fall ist das Gesuchte gefunden. Im zweiten lässt sich beweisen, dass sich in diesem Punkt mehrere Zweige der ersten Linie schneiden (und zwar eine gerade Anzahl von Zweigen), von denen die Hälfte so beschaffen ist, dass beim Abbiegen in einen von ihnen (nach dieser oder jener Seite) der Wert von U weiterhin abnimmt. (Den Beweis dieses Satzes, der eher lang als schwierig ist, muss ich der Kürze halber weglassen.) Auf diesem Zweig kann man also wieder weitergehen, bis U entweder $= 0$ wird (wie es in Fig. 4 in P geschieht) oder wiederum ein Minimum. Dann biegt man erneut ab und gelangt notwendig schließlich zu einem Punkt, in dem $U = 0$ gilt.

Gegen diesen Beweis könnte man den Zweifel vorbringen, ob es nicht möglich sei, dass, wie weit man auch fortschreitet und obwohl der Wert von U stets abnimmt, diese Abnahmen doch immer langsamer werden und jener Wert irgendeine Grenze nirgends erreicht. Dieser Einwand entspräche dem vierten in Artikel 6. Es wäre aber nicht schwer, eine Grenze anzugeben, jenseits deren sich der Wert von U notwendig nicht nur immer schneller ändern muss, sondern auch nicht mehr *abnehmen* kann. Der Wert 0 muss also notwendig schon vor dem Erreichen dieser Grenze vorgekommen sein. Dies und das Übrige, was ich in diesem Beweis nur andeuten konnte, behalte ich mir für eine andere Gelegenheit zu einer ausführlicheren Behandlung vor.

Die Grundsätze, auf denen dieser Beweis beruht, haben wir Anfang Oktober 1797 entdeckt.

Fig 1.

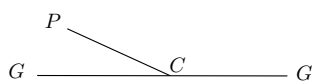


Fig.2.

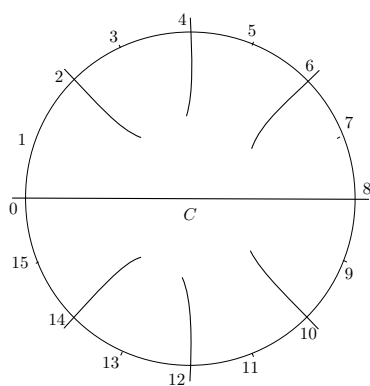


Fig 4

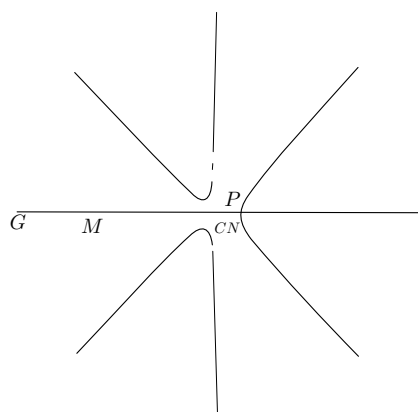
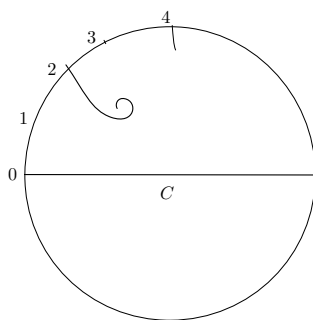


Fig 3



EIN WEITERER NEUER BEWEIS

DES SATZES

DASS JEDES POLYNOM

IN EINER VARIABLEN

IN REELLE FAKTOREN ERSTEN ODER ZWEITEN GRADES

ZERLEGT WERDEN KANN

V O N

CARL FRIEDRICH GAUSS

DER KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
VORGELEGT, 1815, DEZEMBER 7.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. III.

Göttingen MDCCCXVI.

**EIN WEITERER NEUER BEWEIS DES SATZES,
DASS JEDES POLYNOM
IN EINER VARIABLEN
IN REELLE FAKTOREN ERSTEN ODER ZWEITEN
GRADES
ZERLEGT WERDEN KANN.**

1.

Obwohl der Beweis des Satzes über die Zerlegung von Polynomen in Faktoren, den ich in einer vor sechzehn Jahren veröffentlichten Abhandlung gegeben habe, sowohl an Strenge als auch an Einfachheit nichts zu wünschen übrig zu lassen scheint, hoffe ich doch, dass es den Mathematikern nicht unwillkommen sein wird, wenn ich auf dieselbe höchst wichtige Frage zurückkomme und versuche, einen anderen, nicht weniger strengen Beweis aus ganz anderen Grundsätzen zu begründen. Jener frühere Beweis hängt nämlich wenigstens zum Teil von geometrischen Betrachtungen ab; der Beweis, den ich hier darzustellen beginne, wird dagegen auf rein analytischen Grundsätzen beruhen. In der angeführten Abhandlung habe ich die bedeutenderen analytischen Methoden besprochen, mit denen andere Mathematiker bis dahin unseren Satz zu beweisen versucht hatten, und ihre Mängel ausführlich dargelegt. Der schwerwiegendste und tatsächlich grundlegende dieser Mängel ist allen jenen Versuchen ebenso wie den neueren, die mir bekannt geworden sind, gemeinsam. Doch habe ich schon damals erklärt, dass er bei einem analytischen Beweis keineswegs unvermeidlich zu sein scheint. Die Sachkundigen mögen nun beurteilen, ob die damals gegebene Zusage durch diese neuen Bemühungen vollständig eingelöst ist.

2.

Der Hauptuntersuchung werden einige Voruntersuchungen vorausgeschickt, sowohl damit nicht der Eindruck entsteht, etwas fehle, als auch weil ihre Behandlung vielleicht selbst auf Dinge, die andere bereits berührt haben, noch etwas neues Licht werfen kann. Zunächst werden wir den größten gemeinsamen Teiler zweier Polynome in einer Unbestimmten behandeln. Dabei sei vorweg bemerkt, dass hier stets nur von Polynomen die Rede ist: Bildet man aus zweien von ihnen ein Produkt, so heißt jedes ein *Teiler* dieses Produkts. Der *Grad* eines Teilers bestimmt sich nach dem Exponenten der höchsten darin vorkommenden Potenz der Unbestimmten, ohne jede Rücksicht auf die Zahlenkoeffizienten. Im Übrigen können wir die Eigenschaften gemeinsamer

Teiler von Polynomen umso kürzer behandeln, als sie denen der gemeinsamen Teiler von Zahlen vollkommen entsprechen.

Sind zwei Polynome Y, Y' in der Unbestimmten x gegeben, von denen das erste einen höheren oder wenigstens keinen niedrigeren Grad als das zweite hat, so bilden wir die folgenden Gleichungen:

$$\begin{aligned} Y &= qY' + Y'' \\ Y' &= q'Y'' + Y''' \\ Y'' &= q''Y''' + Y'''' \\ &\text{usw. bis} \\ Y^{(\mu-1)} &= q^{(\mu-1)}Y^{(\mu)} \end{aligned}$$

Dabei gilt folgende Regel: Zuerst wird Y auf die übliche Weise durch Y' dividiert; dann Y' durch den Rest Y'' der ersten Division, der einen niedrigeren Grad als Y' hat; dann wieder der erste Rest durch den zweiten, Y''' , und so fort, bis man zu einer Division ohne Rest gelangt. Dass dies schließlich notwendig eintreten muss, folgt daraus, dass der Grad der Polynome Y', Y'', Y''' usw. fortwährend abnimmt. Dass diese Funktionen ebenso wie die Quotienten q, q', q'' usw. *Polynome* in x sind, braucht kaum erwähnt zu werden. Danach ist klar:

I. Geht man von der letzten dieser Gleichungen zur ersten zurück, so erkennt man, dass das Polynom $Y^{(\mu)}$ jedes der vorhergehenden teilt und daher gewiss ein gemeinsamer Teiler der vorgegebenen Polynome Y, Y' ist.

II. Geht man von der ersten Gleichung zur letzten weiter, so zeigt sich, dass jeder gemeinsame Teiler der Polynome Y, Y' auch jedes der folgenden und damit auch das letzte, $Y^{(\mu)}$, teilt. Die Polynome Y, Y' können daher keinen gemeinsamen Teiler höheren Grades als $Y^{(\mu)}$ haben. Jeder gemeinsame Teiler desselben Grades wie $Y^{(\mu)}$ steht zu diesem im Verhältnis einer Zahl zu einer Zahl; daher ist dieser selbst als größter gemeinsamer Teiler anzusehen.

III. Hat $Y^{(\mu)}$ den Grad 0, ist es also eine Zahl, so kann keine Funktion der Unbestimmten x im eigentlichen Sinne die Polynome Y, Y' teilen. In diesem Fall sagt man daher, diese Polynome hätten keinen gemeinsamen Teiler.

IV. Man nehme die vorletzte unserer Gleichungen und eliminiere daraus $Y^{(\mu-1)}$ mit Hilfe der drittletzten Gleichung; dann eliminiere man wiederum $Y^{(\mu-2)}$ mit Hilfe der vorhergehenden Gleichung und so fort. Auf diese Weise erhält man

$$\begin{aligned} Y^{(\mu)} &= +kY^{(\mu-2)} - k'Y^{(\mu-1)} \\ &= -k'Y^{(\mu-3)} + k''Y^{(\mu-2)} \\ &= +k''Y^{(\mu-4)} - k'''Y^{(\mu-3)} \\ &= -k'''Y^{(\mu-5)} + k''''Y^{(\mu-4)} \\ &\quad \text{usw.} \end{aligned}$$

wenn man annimmt, die Polynome k, k', k'' usw. seien nach der folgenden Regel gebildet:

$$\begin{aligned} k &= 1 \\ k' &= q^{(\mu-2)} \\ k'' &= q^{(\mu-3)}k' + k \\ k''' &= q^{(\mu-4)}k'' + k' \\ k'''' &= q^{(\mu-5)}k''' + k'' \\ &\quad \text{usw.} \end{aligned}$$

Damit gilt

$$\pm k^{(\mu-2)}Y \mp k^{(\mu-1)}Y' = Y^{(\mu)}$$

wobei die oberen Zeichen für gerades μ und die unteren für ungerades gelten. Haben also Y und Y' keinen gemeinsamen Teiler, so kann man auf diese Weise zwei Polynome Z, Z' in der Unbestimmten x finden, sodass

$$ZY + Z'Y' = 1$$

V. Diese Aussage gilt offenbar auch umgekehrt: Kann die Gleichung

$$ZY + Z'Y' = 1$$

so erfüllt werden, dass Z, Z' Polynome in der Unbestimmten x sind, dann können Y und Y' gewiss keinen gemeinsamen Teiler haben.

3.

Die zweite Voruntersuchung betrifft die Umformung symmetrischer Funktionen. Es seien a, b, c usw. unbestimmte Größen, und ihre Anzahl sei m . Mit λ' bezeichnen wir ihre Summe, mit λ'' die Summe ihrer Produkte aus je zweien, mit λ''' die Summe ihrer Produkte aus je dreien usw., sodass die Entwicklung des Produkts

$$(x - a)(x - b)(x - c) \dots$$

den Ausdruck

$$x^m - \lambda' x^{m-1} + \lambda'' x^{m-2} - \lambda''' x^{m-3} + \text{usw.}$$

ergibt. Somit sind $\lambda', \lambda'', \lambda'''$ usw. symmetrische Funktionen der Unbestimmten a, b, c usw., d. h. solche, in denen diese Unbestimmten auf dieselbe Weise vorkommen, oder deutlicher: solche, die bei jeder Vertauschung dieser Unbestimmten untereinander unverändert bleiben. Allgemeiner ist offenbar jedes Polynom in $\lambda', \lambda'', \lambda'''$ usw. (ob es nur diese Unbestimmten oder noch andere, von a, b, c usw. unabhängige enthält) ein symmetrisches Polynom in den Unbestimmten a, b, c usw.

4.

Der umgekehrte Satz liegt etwas weniger nahe. Es sei ρ eine symmetrische Funktion der Unbestimmten a, b, c usw.; sie besteht also aus einer bestimmten Anzahl von Gliedern der Form

$$M a^\alpha b^\beta c^\gamma \dots$$

wobei α, β, γ usw. nichtnegative ganze Zahlen bezeichnen und M ein bestimmter oder wenigstens von a, b, c usw. unabhängiger Koeffizient ist (falls außer a, b, c usw. noch andere Unbestimmte in die Funktion ρ eingehen). Zunächst legen wir für diese einzelnen Glieder eine bestimmte Ordnung fest. Dazu ordnen wir zuerst die Unbestimmten a, b, c usw. in einer bestimmten, an sich völlig beliebigen Reihenfolge an, etwa so, dass a die erste Stelle einnimmt, b die zweite, c die dritte usw. Von den beiden Gliedern

$$M a^\alpha b^\beta c^\gamma \dots \quad \text{und} \quad M a^{\alpha'} b^{\beta'} c^{\gamma'} \dots$$

weisen wir dann dem ersten eine höhere Stelle in der Ordnung zu als dem zweiten, wenn

$$\begin{aligned} &\text{oder } \alpha > \alpha', \quad \text{oder } \alpha = \alpha' \text{ und } \beta > \beta', \\ &\text{oder } \alpha = \alpha', \quad \beta = \beta' \text{ und } \gamma > \gamma', \quad \text{oder usw.} \end{aligned}$$

also wenn die erste nicht verschwindende unter den Differenzen $\alpha - \alpha', \beta - \beta', \gamma - \gamma'$ usw. positiv ist. Da Glieder derselben Stelle in der Ordnung sich nur im Koeffizienten M unterscheiden und daher zu einem Glied zusammengefasst werden können, nehmen wir an, dass die einzelnen Glieder der Funktion ρ verschiedene Stellen in der Ordnung einnehmen.

Nun bemerken wir: Ist $Ma^\alpha b^\beta c^\gamma \dots$ unter allen Gliedern der Funktion ρ das höchste in dieser Ordnung, so muss α größer oder wenigstens nicht kleiner als β sein. Wäre nämlich $\beta > \alpha$, so hätte das Glied $Ma^\beta b^\alpha c^\gamma \dots$, das die Funktion ρ wegen ihrer Symmetrie ebenfalls enthalten muss, eine höhere Stelle als $Ma^\alpha b^\beta c^\gamma \dots$, gegen die Voraussetzung. Ebenso ist β größer oder wenigstens nicht kleiner als γ ; ferner ist γ nicht kleiner als der nächste Exponent δ usw. Daher sind die einzelnen Differenzen $\alpha - \beta, \beta - \gamma, \gamma - \delta$ usw. nichtnegative ganze Zahlen.

Zweitens betrachten wir ein Produkt aus beliebig vielen Polynomen in den Unbestimmten a, b, c usw. Sein höchstes Glied muss das Produkt der höchsten Glieder dieser Faktoren sein. Ebenso ist klar, dass die höchsten Glieder der Funktionen $\lambda', \lambda'', \lambda'''$ usw. jeweils a, ab, abc usw. sind. Daraus folgt, dass das höchste aus dem Produkt

$$p = M\lambda'^{\alpha-\beta}\lambda''^{\beta-\gamma}\lambda'''^{\gamma-\delta} \dots$$

hervorgehende Glied $Ma^\alpha b^\beta c^\gamma \dots$ ist. Setzt man also $\rho - p = \rho'$, so liegt das höchste Glied der Funktion ρ' in der Ordnung gewiss niedriger als das höchste Glied der Funktion ρ . Offenbar sind aber p und daher auch ρ' symmetrische Polynome in a, b, c usw. Behandelt man daher ρ' ebenso wie vorher ρ , so zerfällt es in $p' + p''$, wobei p' ein Produkt aus Potenzen von $\lambda', \lambda'', \lambda'''$ usw., multipliziert mit einem bestimmten oder wenigstens von a, b, c usw. unabhängigen Koeffizienten, ist, während p'' ein symmetrisches Polynom in a, b, c usw. ist, dessen höchstes Glied in der Ordnung niedriger liegt als das höchste Glied von ρ' . Führt man auf dieselbe Weise fort, so wird ρ offenbar schließlich auf die Form $p + p' + p'' + p'''$ usw. gebracht, also in ein Polynom in $\lambda', \lambda'', \lambda'''$ usw. umgeformt.

5.

Den im vorigen Artikel bewiesenen Satz können wir auch so aussprechen: Ist irgendein symmetrisches Polynom ρ in den Unbestimmten a, b, c usw. gegeben, so lässt sich ein Polynom in ebenso vielen anderen Unbestimmten l', l'', l''' usw. angeben, das durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in ρ übergeht. Außerdem zeigt man leicht, dass *dies nur auf eine einzige Weise möglich ist*. Nehmen wir nämlich an, zwei verschiedene Funktionen der Unbestimmten l', l'', l''' usw., etwa r und r' , ergäben nach den Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. dieselbe Funktion von a, b, c usw. Dann wäre $r - r'$ eine Funktion von l', l'', l''' usw., die für sich nicht verschwindet,

nach jenen Substitutionen aber identisch verschwindet. Dass dies widersinnig ist, erkennen wir leicht, wenn wir bedenken, dass $r - r'$ notwendig aus einer bestimmten Anzahl von Teilen der Form

$$Ml'^{\alpha}l''^{\beta}l'''^{\gamma} \dots$$

besteht, deren Koeffizienten M nicht verschwinden und die sich jeweils in ihren Exponenten unterscheiden.

Die aus diesen einzelnen Teilen hervorgehenden höchsten Glieder werden daher durch

$$Ma^{\alpha+\beta+\gamma+\text{usw.}}b^{\beta+\gamma+\text{usw.}}c^{\gamma+\text{usw.}} \dots$$

dargestellt und gehören somit verschiedenen Stellen in der Ordnung an, sodass das höchste Glied überhaupt auf keine Weise wegfallen kann.

Die eigentliche Rechnung bei solchen Umformungen ließe sich durch mehrere Abkürzungen erheblich verkürzen. Dabei halten wir uns hier jedoch nicht auf, da für unseren Zweck schon die bloße Möglichkeit der Umformung genügt.

6.

Wir betrachten das Produkt aus $m(m-1)$ Faktoren

$$\begin{aligned} &(a-b)(a-c)(a-d) \dots \\ &\times (b-a)(b-c)(b-d) \dots \\ &\times (c-a)(c-b)(c-d) \dots \\ &\times (d-a)(d-b)(d-c) \dots \\ &\text{usw.} \end{aligned}$$

das wir mit π bezeichnen. Da es die Unbestimmten a, b, c usw. symmetrisch enthält, nehmen wir an, es sei auf die Form eines Polynoms in $\lambda', \lambda'', \lambda'''$ usw. gebracht. Dieses Polynom gehe in p über, wenn anstelle von $\lambda', \lambda'', \lambda'''$ usw. jeweils l', l'', l''' usw. eingesetzt werden. Danach nennen wir p die *Determinante* des Polynoms

$$y = x^m - l'x^{m-1} + l''x^{m-2} - l'''x^{m-3} + \text{usw.}$$

So haben wir zum Beispiel für $m = 2$

$$p = -l'^2 + 4l''$$

Ebenso findet man für $m = 3$

$$p = -l'^2l''^2 + 4l'^3l''' + 4l''^3 - 18l'l''l''' + 27l'''^2$$

Die Determinante des Polynoms y ist also ein Polynom in den Koeffizienten l', l'', l''' usw., das durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in

das Produkt aus allen Differenzen zwischen je zweien der Größen a, b, c usw. übergeht. Im Fall $m = 1$, wenn also nur eine einzige Unbestimmte a und daher überhaupt keine Differenz vorhanden ist, empfiehlt es sich, die Zahl 1 selbst als Determinante des Polynoms y anzunehmen.

Bei der Festlegung des Begriffs der Determinante mussten die Koeffizienten des Polynoms y als unbestimmte Größen betrachtet werden. Die Determinante eines Polynoms mit bestimmten Koeffizienten,

$$Y = x^m - L'x^{m-1} + L''x^{m-2} - L'''x^{m-3} + \text{usw.}$$

ist eine bestimmte Zahl P , nämlich der Wert des Polynoms p für $l' = L', l'' = L'', l''' = L'''$ usw. Nehmen wir also an, Y lasse sich in lineare Faktoren zerlegen,

$$Y = (x - A)(x - B)(x - C) \dots$$

oder Y entstehe aus

$$v = (x - a)(x - b)(x - c) \dots$$

indem man $a = A, b = B, c = C$ usw. setzt, sodass dieselben Substitutionen $\lambda', \lambda'', \lambda'''$ usw. jeweils in L', L'', L''' usw. überführen, so ist P offenbar gleich dem Produkt aus den Faktoren

$$\begin{aligned} & (A - B)(A - C)(A - D) \dots \\ & \times (B - A)(B - C)(B - D) \dots \\ & \times (C - A)(C - B)(C - D) \dots \\ & \times (D - A)(D - B)(D - C) \dots \\ & \text{usw.} \end{aligned}$$

Ist also $P = 0$, so müssen sich unter den Größen A, B, C usw. wenigstens zwei gleiche befinden; ist dagegen nicht $P = 0$, so sind sämtliche Größen A, B, C usw. notwendig ungleich. Nun bemerken wir: Setzt man $\frac{dY}{dx} = Y'$, oder

$$\begin{aligned} Y' &= mx^{m-1} - (m-1)L'x^{m-2} + (m-2)L''x^{m-3} \\ &\quad - (m-3)L'''x^{m-4} + \text{usw.} \end{aligned}$$

so gilt

$$\begin{aligned} Y' &= (x - B)(x - C)(x - D) \dots \\ &\quad + (x - A)(x - C)(x - D) \dots \\ &\quad + (x - A)(x - B)(x - D) \dots \\ &\quad + (x - A)(x - B)(x - C) \dots \\ &\quad + \text{usw.} \end{aligned}$$

Sind also zwei der Größen A, B, C usw. gleich, etwa $A = B$, so ist Y' durch $x - A$ teilbar; mit anderen Worten, Y und Y' enthalten den gemeinsamen Teiler $x - A$. Nimmt man umgekehrt an, Y' habe mit Y irgendeinen gemeinsamen Teiler, so muss Y' einen der linearen Faktoren $x - A, x - B, x - C$ usw. enthalten, etwa den ersten, $x - A$. Dies kann offenbar nur geschehen, wenn A einer der übrigen Größen B, C, D usw. gleich ist. Aus alledem erhalten wir also zwei SÄTZE:

I. *Ist die Determinante des Polynoms $Y = 0$, so hat Y gewiss mit Y' einen gemeinsamen Teiler; haben also Y und Y' keinen gemeinsamen Teiler, so kann die Determinante des Polynoms Y nicht $= 0$ sein.*

II. *Ist die Determinante des Polynoms Y nicht $= 0$, so können Y und Y' gewiss keinen gemeinsamen Teiler haben; oder, wenn Y und Y' einen gemeinsamen Teiler haben, muss die Determinante des Polynoms Y notwendig $= 0$ sein.*

7.

Doch ist sorgfältig zu beachten, dass die ganze Kraft dieses sehr einfachen Beweises auf der Annahme beruht, das Polynom Y lasse sich in lineare Faktoren zerlegen. Gerade hier, wo die allgemeine Möglichkeit dieser Zerlegung bewiesen werden soll, wäre diese Annahme nichts anderes als eine Vorwegnahme des zu Beweisenden. Dennoch haben sich nicht alle, die analytische Beweise des Hauptsatzes versucht haben, vor genau solchen Fehlschlüssen gehütet. Den Ursprung dieses täuschenden Anscheins haben wir schon in der Formulierung der Untersuchung selbst bemerkt: Alle haben nur nach der *Form* der Wurzeln von Gleichungen gefragt, während sie deren voreilig angenommene *Existenz* hätten beweisen müssen. Doch ist über dieses Vorgehen, das sich allzu weit von Strenge und Klarheit entfernt, schon in der oben angeführten Abhandlung genug gesagt worden. Wir werden daher nun die Sätze des vorigen Artikels, von denen wir für unseren Zweck wenigstens einen nicht entbehren können, auf eine festere Grundlage stellen. Wir beginnen mit dem zweiten als dem leichteren.

8.

Wir bezeichnen mit ρ die Funktion

$$\begin{aligned} & \frac{\pi(x-b)(x-c)(x-d) \dots}{(a-b)^2(a-c)^2(a-d)^2 \dots} \\ & + \frac{\pi(x-a)(x-c)(x-d) \dots}{(b-a)^2(b-c)^2(b-d)^2 \dots} \\ & + \frac{\pi(x-a)(x-b)(x-d) \dots}{(c-a)^2(c-b)^2(c-d)^2 \dots} \\ & + \frac{\pi(x-a)(x-b)(x-c) \dots}{(d-a)^2(d-b)^2(d-c)^2 \dots} \\ & + \text{usw.} \end{aligned}$$

die, weil π durch jeden einzelnen Nenner teilbar ist, ein Polynom in den Unbestimmten x, a, b, c usw. ist. Ferner setzen wir $\frac{dv}{dx} = v'$, sodass gilt

$$\begin{aligned} v' &= (x-b)(x-c)(x-d) \dots \\ &+ (x-a)(x-c)(x-d) \dots \\ &+ (x-a)(x-b)(x-d) \dots \\ &+ (x-a)(x-b)(x-c) \dots \\ &+ \text{usw.} \end{aligned}$$

Für $x = a$ gilt offenbar $\rho v' = \pi$. Daraus schließen wir, dass das Polynom $\pi - \rho v'$ identisch durch $x - a$ und ebenso durch $x - b, x - c$ usw. sowie durch ihr Produkt v teilbar ist. Setzen wir also

$$\frac{\pi - \rho v'}{v} = \sigma$$

so ist σ ein Polynom in den Unbestimmten x, a, b, c usw., das wie ρ hinsichtlich der Unbestimmten a, b, c usw. symmetrisch ist. Es lassen sich daher zwei Polynome r, s in den Unbestimmten x, l', l'', l''' usw. finden, die durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. jeweils in ρ, σ übergehen. Bezeichnen wir nun entsprechend das Polynom

$$\begin{aligned} & mx^{m-1} - (m-1)l'x^{m-2} + (m-2)l''x^{m-3} \\ & - (m-3)l'''x^{m-4} + \text{usw.} \end{aligned}$$

also die Ableitung $\frac{dy}{dx}$, mit y' , sodass y' durch dieselben Substitutionen in v' übergeht, so geht offenbar $p - sy - ry'$ durch dieselben Substitutionen in $\pi - \sigma v - \rho v'$, also in 0 über und muss daher schon für sich identisch verschwinden (Artikel 5). Wir haben somit die identische Gleichung

$$p = sy + ry'$$

Nehmen wir nun an, durch die Substitution $l' = L', l'' = L'', l''' = L'''$ usw. ergebe sich $r = R, s = S$, so gilt ebenfalls identisch

$$P = SY + RY'$$

Da hier S, R Polynome in x sind, P dagegen eine bestimmte Größe oder Zahl ist, folgt von selbst, dass Y und Y' keinen gemeinsamen Teiler haben können, wenn nicht $P = 0$ ist. Dies ist genau der zweite Satz von Artikel 6.

9.

Den Beweis des ersten Satzes werden wir so abschließen, dass wir zeigen: Haben Y und Y' keinen gemeinsamen Teiler, so kann gewiss nicht $P = 0$ gelten. Dazu nehmen wir zunächst an, nach den Vorschriften von Artikel 2 seien zwei Polynome in der Unbestimmten x , nämlich fx und φx , gefunden worden, sodass die identische Gleichung

$$fx \cdot Y + \varphi x \cdot Y' = 1$$

gilt. Wir schreiben sie hier in der Form

$$fx \cdot v + \varphi x \cdot v' = 1 + fx \cdot (v - Y) + \varphi x \cdot \frac{d(v - Y)}{dx}$$

oder, da

$$\begin{aligned} v' &= (x - b)(x - c)(x - d) \dots \\ &+ (x - a) \cdot \frac{d[(x - b)(x - c)(x - d) \dots]}{dx} \end{aligned}$$

gilt, in der folgenden Form:

$$\begin{aligned} &\varphi x \cdot (x - b)(x - c)(x - d) \dots \\ &+ \varphi x \cdot (x - a) \cdot \frac{d[(x - b)(x - c)(x - d) \dots]}{dx} \\ &+ fx \cdot (x - a)(x - b)(x - c)(x - d) \dots \\ &= 1 + fx \cdot (v - Y) + \varphi x \cdot \frac{d(v - Y)}{dx} \end{aligned}$$

Der Kürze halber bezeichnen wir das Polynom

$$fx \cdot (y - Y) + \varphi x \cdot \frac{d(y - Y)}{dx}$$

in den Unbestimmten x, l', l'', l''' usw.

$$\text{mit } F(x, l', l'', l''' \text{ usw.})$$

Damit gilt identisch

$$\begin{aligned} 1 + fx \cdot (v - Y) + \varphi x \cdot \frac{d(v - Y)}{dx} \\ = 1 + F(x, \lambda', \lambda'', \lambda''' \text{ usw.}) \end{aligned}$$

Wir erhalten also die identischen Gleichungen [1]

$$\begin{aligned} \varphi a \cdot (a - b)(a - c)(a - d) \dots \\ = 1 + F(a, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ \varphi b \cdot (b - a)(b - c)(b - d) \dots \\ = 1 + F(b, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ \varphi c \cdot (c - a)(c - b)(c - d) \dots \\ = 1 + F(c, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ \text{usw.} \end{aligned}$$

Nehmen wir nun an, das Produkt aus allen Ausdrücken

$$\begin{aligned} 1 + F(a, l', l'', l''' \text{ usw.}) \\ 1 + F(b, l', l'', l''' \text{ usw.}) \\ 1 + F(c, l', l'', l''' \text{ usw.}) \\ \text{usw.} \end{aligned}$$

das ein Polynom in den Unbestimmten a, b, c usw., l', l'', l''' usw. und hinsichtlich a, b, c usw. symmetrisch ist, werde durch

$$\psi(\lambda', \lambda'', \lambda''' \text{ usw.}, l', l'', l''' \text{ usw.})$$

dargestellt. Dann ergibt die Multiplikation sämtlicher Gleichungen [1] die neue identische Gleichung [2]

$$\pi \varphi a \cdot \varphi b \cdot \varphi c \dots = \psi(\lambda', \lambda'', \lambda''' \text{ usw.}, \lambda', \lambda'', \lambda''' \text{ usw.})$$

Da ferner das Produkt $\varphi a \cdot \varphi b \cdot \varphi c \dots$ die Unbestimmten a, b, c usw. symmetrisch enthält, lässt sich offenbar ein Polynom in den Unbestimmten

l', l'', l''' usw. finden, das durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in $\varphi a . \varphi b . \varphi c \dots$ übergeht. Dieses Polynom sei t . Dann gilt ebenfalls identisch [3]

$$pt = \psi(l', l'', l''' \text{ usw.}, l', l'', l''')$$

denn die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. führen diese Gleichung in die identische Gleichung [2] über.

Aus der Definition der Funktion F selbst folgt nun identisch

$$F(x, L', L'', L''' \text{ usw.}) = 0$$

Daher gilt auch identisch

$$1 + F(a, L', L'', L''' \text{ usw.}) = 1$$

$$1 + F(b, L', L'', L''' \text{ usw.}) = 1$$

$$1 + F(c, L', L'', L''' \text{ usw.}) = 1$$

usw.

und somit ebenfalls identisch

$$\psi(\lambda', \lambda'', \lambda''' \text{ usw.}, L', L'', L''' \text{ usw.}) = 1$$

also auch identisch [4]

$$\psi(l', l'', l''' \text{ usw.}, L' . L'', L''' \text{ usw.}) = 1$$

Verbinden wir die Gleichungen [3] und [4] und setzen $l' = L', l'' = L'', l''' = L'''$ usw., so erhalten wir daher [5]

$$PT = 1$$

wobei T den Wert des Polynoms t bei diesen Substitutionen bezeichnet. Da dieser Wert notwendig eine endliche Größe ist, kann P gewiss nicht $= 0$ sein.
Q. E. D.

10.

Aus dem Vorhergehenden ist nun klar, dass sich jedes Polynom Y in einer Unbestimmten x , dessen Determinante $= 0$ ist, in Faktoren zerlegen lässt, von denen keiner die Determinante 0 hat. Bestimmt man nämlich den größten gemeinsamen Teiler der Polynome Y und $\frac{dY}{dx}$, so ist das erste damit in zwei Faktoren zerlegt. Hat einer dieser Faktoren^{*)} wiederum die Determinante 0, so wird er auf dieselbe Weise in zwei Faktoren zerlegt. So fahren wir fort, bis Y schließlich in Faktoren zerlegt ist, von denen keiner die Determinante 0 hat.

Ferner sieht man leicht, dass sich unter diesen Faktoren, in die Y zerlegt wird, wenigstens einer befinden muss, der folgende Eigenschaft hat: Unter den Faktoren der Zahl, die seinen Grad angibt, kommt die Zahl zwei nicht öfter vor als unter den Faktoren der Zahl m , die den Grad des Polynoms Y angibt. Setzt man also $m = k \cdot 2^\mu$, wobei k eine ungerade Zahl bezeichnet, so findet sich unter den Faktoren des Polynoms Y wenigstens einer vom Grad $k' \cdot 2^\nu$, wobei auch k' ungerade ist und entweder $\nu = \mu$ oder $\nu < \mu$ gilt. Die Richtigkeit dieser Behauptung folgt von selbst daraus, dass m die Summe der Zahlen ist, welche die Grade der einzelnen Faktoren von Y angeben.

11.

Bevor wir weitergehen, erläutern wir einen Ausdruck, dessen Einführung bei allen Untersuchungen über symmetrische Funktionen sehr nützlich ist und der auch uns sehr gelegen kommt. Es sei M eine Funktion einiger der Unbestimmten a, b, c usw.; μ sei dabei die Anzahl derjenigen, die in den Ausdruck M eingehen, ohne Rücksicht auf andere Unbestimmte, die M etwa noch enthält. Vertauscht man diese μ Unbestimmten auf alle möglichen Arten sowohl untereinander als auch mit den übrigen $m - \mu$ aus a, b, c usw., so entstehen aus M andere, M ähnliche Ausdrücke. Insgesamt erhält man

$$m(m-1)(m-2)(m-3)\dots(m-\mu+1)$$

Ausdrücke einschließlich M selbst. Ihre Gesamtheit nennen wir kurz die *Gesamtheit aller M* . Damit ist von selbst klar, was die Summe aller M , das Produkt aus allen M usw. bedeutet. So heißt zum Beispiel π das Produkt aus allen $a - b$, v das Produkt aus allen $x - a$ und v' die Summe aller $\frac{v}{x-a}$ usw.

Ist M hinsichtlich einiger der μ darin enthaltenen Unbestimmten symmetrisch, so ändern deren Vertauschungen untereinander die Funktion M nicht. In der Gesamtheit aller M kommt daher jedes Glied mehrfach vor, und zwar $1 \cdot 2 \cdot 3 \dots \nu$ Mal, wenn ν die Anzahl der Unbestimmten ist, hinsichtlich deren M symmetrisch ist. Ist aber M nicht nur hinsichtlich ν Unbestimmter

^{*)}Tatsächlich kann nur derjenige Faktor, der jener gemeinsame Teiler ist, die Determinante 0 haben. Doch würde der Beweis dieses Satzes hier zu einigen Umwegen führen; er ist hier auch nicht nötig, da man den anderen Faktor, selbst wenn auch dessen Determinante verschwinden könnte, auf dieselbe Weise behandeln und in Faktoren zerlegen dürfte.

symmetrisch, sondern außerdem hinsichtlich ν' anderer und ferner hinsichtlich ν'' anderer usw., so bleibt M unverändert, ob nun zwei der ersten ν Unbestimmten untereinander vertauscht werden oder zwei der zweiten ν' oder zwei der dritten ν'' usw. Es entsprechen somit stets

$$1.2.3\dots\nu. \quad 1.2.3\dots\nu'. \quad 1.2.3\dots\nu'' \text{ usw.}$$

Vertauschungen identischen Gliedern. Behalten wir von diesen identischen Gliedern jeweils nur eines, so erhalten wir insgesamt

$$\frac{m(m-1)(m-2)(m-3)\dots(m-\mu+1)}{1.2.3\dots\nu.1.2.3\dots\nu'.1.2.3\dots\nu'' \text{ usw.}}$$

Glieder. Ihre Gesamtheit nennen wir die *Gesamtheit aller M mit ausgeschlossenen Wiederholungen*, um sie von der *Gesamtheit aller M mit zugelassenen Wiederholungen* zu unterscheiden. Wird nichts ausdrücklich bemerkt, so verstehen wir stets, dass die Wiederholungen zugelassen sind.

Ferner sieht man leicht, dass die Summe aller M oder das Produkt aus allen M oder allgemein irgendeine symmetrische Funktion aller M stets eine symmetrische Funktion der Unbestimmten a, b, c usw. ist, ob Wiederholungen zugelassen oder ausgeschlossen werden.

12.

Nun betrachten wir, mit u, x als Unbestimmten, das Produkt aus allen $u - (a + b)x + ab$ mit ausgeschlossenen Wiederholungen und bezeichnen es mit ζ . Somit ist ζ das Produkt aus den folgenden $\frac{1}{2}m(m-1)$ Faktoren:

$$\begin{aligned} &u - (a + b)x + ab \\ &u - (a + c)x + ac \\ &u - (a + d)x + ad \\ &\text{usw.} \\ &u - (b + c)x + bc \\ &u - (b + d)x + bd \\ &\text{usw.} \\ &u - (c + d)x + cd \\ &\text{usw. usw.} \end{aligned}$$

Da diese Funktion die Unbestimmten a, b, c usw. symmetrisch enthält, lässt sich ein Polynom in den Unbestimmten u, x, l', l'', l''' usw. angeben, das wir mit z bezeichnen und das in ζ übergeht, wenn anstelle der Unbestimmten l', l'', l''' usw. $\lambda', \lambda'', \lambda'''$ usw. eingesetzt werden. Schließlich bezeichnen wir mit Z die Funktion allein der Unbestimmten u, x , in die z übergeht, wenn den

Unbestimmten l', l'', l''' usw. die bestimmten Werte L', L'', L''' usw. gegeben werden.

Diese drei Funktionen ζ, z, Z lassen sich als Polynome vom Grad $\frac{1}{2}m(m-1)$ in der Unbestimmten u mit unbestimmten Koeffizienten auffassen. Diese Koeffizienten sind

für ζ , Funktionen der Unbestimmten x, a, b, c usw.

für z , Funktionen der Unbestimmten x, l', l'', l''' usw.

für Z , Funktionen allein der Unbestimmten x .

Die einzelnen Koeffizienten von z gehen durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in die Koeffizienten von ζ und durch die Substitutionen $l' = L', l'' = L'', l''' = L'''$ usw. in die Koeffizienten von Z über. Was wir eben über die Koeffizienten gesagt haben, gilt ebenso für die Determinanten der Funktionen ζ, z, Z . Diese wollen wir nun näher untersuchen, und zwar mit dem Ziel, den folgenden Satz zu beweisen.

SATZ. Gilt nicht $P = 0$, so kann die Determinante der Funktion Z gewiss nicht identisch $= 0$ sein.

13.

Der Beweis dieses Satzes wäre allerdings sehr leicht, wenn man annehmen dürfte, Y lasse sich in lineare Faktoren zerlegen:

$$(x - A)(x - B)(x - C)(x - D) \dots$$

Dann wäre nämlich auch gewiss, dass Z das Produkt aus allen $u - (A + B)x + AB$ und die Determinante der Funktion Z das Produkt aus den Differenzen zwischen je zweien der Größen

$$(A + B)x - AB$$

$$(A + C)x - AC$$

$$(A + D)x - AD$$

usw.

$$(B + C)x - BC$$

$$(B + D)x - BD$$

usw.

$$(C + D)x - CD$$

usw. usw.

ist. Dieses Produkt kann aber nicht identisch verschwinden, wenn nicht einer seiner Faktoren selbst identisch $= 0$ wird. Daraus würde folgen, dass zwei der Größen A, B, C usw. gleich sind und somit die Determinante P des Polynoms $Y = 0$ wird, gegen die Voraussetzung.

Doch lassen wir diese Argumentation beiseite, die offenbar wie in Artikel 6 von einer Vorwegnahme des zu Beweisenden ausgeht, und gehen sogleich zu einem sicheren Beweis des Satzes von Artikel 12 über.

14.

Die Determinante der Funktion ζ ist das Produkt aus allen Differenzen zwischen je zweien der Ausdrücke $(a+b)x - ab$. Die Anzahl dieser Differenzen ist

$$\frac{1}{2}m(m-1)(\frac{1}{2}m(m-1)-1) = \frac{1}{4}(m+1)m(m-1)(m-2)$$

Diese Zahl gibt also den Grad der Determinante der Funktion ζ hinsichtlich der Unbestimmten x an. Die Determinante der Funktion z hat denselben Grad. Dagegen kann die Determinante der Funktion Z durchaus einen niedrigeren Grad haben, wenn einige Koeffizienten, von der höchsten Potenz von x an, verschwinden. Wir haben nun zu beweisen, dass in der Determinante der Funktion Z gewiss nicht *alle* Koeffizienten verschwinden können.

Betrachten wir die Differenzen, deren Produkt die Determinante der Funktion ζ ist, näher, so finden wir: Ein Teil von ihnen, nämlich die Differenzen zwischen je zweien der Ausdrücke $(a+b)x - ab$ mit einem gemeinsamen Element, liefert

$$\text{das Produkt aus allen } (a-b)(x-c)$$

Aus den übrigen, nämlich den Differenzen zwischen je zweien der Ausdrücke $(a+b)x - ab$ mit verschiedenen Elementen, entsteht dagegen

$$\begin{aligned} &\text{das Produkt aus allen } (a+b-c-d)x - ab + cd, \\ &\text{mit ausgeschlossenen Wiederholungen.} \end{aligned}$$

Das erste Produkt enthält offenbar jeden Faktor $a-b$ genau $m-2$ Mal und jeden Faktor $x-c$ genau $(m-1)(m-2)$ Mal. Daraus schließen wir leicht, dass dieses Produkt

$$= \pi^{m-2} \nu^{(m-1)(m-2)}$$

ist. Bezeichnen wir also das zweite Produkt mit ρ , so ist die Determinante der Funktion ζ

$$= \pi^{m-2} \nu^{(m-1)(m-2)} \rho$$

Bezeichnen wir ferner mit r diejenige Funktion der Unbestimmten x, l', l'', l''' usw., die durch die Substitutionen $l' = \lambda', l'' = \lambda'', l''' = \lambda'''$ usw. in ρ übergeht, und mit R die Funktion allein von x , in die r durch die Substitutionen $l' = L', l'' = L'', l''' = L'''$ usw. übergeht, so ist offenbar die Determinante der Funktion z

$$= p^{m-2} y^{(m-1)(m-2)} r$$

die Determinante der Funktion Z dagegen

$$= P^{m-2} Y^{(m-1)(m-2)} R$$

Da nach Voraussetzung P nicht $= 0$ ist, kommt es nun darauf an, zu beweisen, dass R gewiss nicht identisch verschwinden kann.

15.

Dazu führen wir noch eine weitere Unbestimmte w ein und betrachten das Produkt aus allen

$$(a + b - c - d)w + (a - c)(a - d)$$

mit ausgeschlossenen Wiederholungen. Da es a, b, c usw. symmetrisch enthält, lässt es sich als Polynom in den Unbestimmten $w, \lambda', \lambda'', \lambda'''$ usw. darstellen. Wir bezeichnen diese Funktion mit $f(w, \lambda', \lambda'', \lambda''' \text{ usw.})$. Die Anzahl jener Faktoren $(a + b - c - d)w + (a - c)(a - d)$ ist

$$= \frac{1}{2}m(m-1)(m-2)(m-3)$$

woraus wir leicht schließen, dass

$$f(0, \lambda', \lambda'', \lambda''' \text{ usw.}) = \pi^{(m-2)(m-3)}$$

und daher auch

$$f(0, l', l'', l''' \text{ usw.}) = p^{(m-2)(m-3)}$$

sowie

$$f(0, L', L'', L''' \text{ usw.}) = P^{(m-2)(m-3)}$$

gilt. Das Polynom $f(w, L', L'', L''' \text{ usw.})$ hat im Allgemeinen den Grad

$$\frac{1}{2}m(m-1)(m-2)(m-3)$$

in besonderen Fällen kann es aber durchaus einen niedrigeren Grad haben, wenn etwa einige Koeffizienten, von der höchsten Potenz von w an, verschwinden. Unmöglich ist dagegen, dass die ganze Funktion identisch $= 0$ ist, denn die eben gefundene Gleichung zeigt, dass wenigstens ihr letztes Glied nicht verschwindet. Wir nehmen an, das höchste Glied des Polynoms $f(w, L', L'', L''' \text{ usw.})$ mit nicht verschwindendem Koeffizienten sei Nw^ν . Setzen wir nun $w = x - a$, so ist $f(x - a, L', L'', L''' \text{ usw.})$ offenbar ein Polynom in den Unbestimmten x, a oder, was dasselbe ist, ein Polynom in x mit Koeffizienten, die von der Unbestimmten a abhängen. Sein höchstes Glied ist dabei jedoch Nx^ν und hat somit einen bestimmten, von a unabhängigen Koeffizienten, der nicht $= 0$ ist. Ebenso sind $f(x - b, L', L'', L''' \text{ usw.})$, $f(x - c, L', L'', L''' \text{ usw.})$

Polynome in der Unbestimmten x , deren höchstes Glied jeweils Nx^ν ist, während die Koeffizienten der folgenden Glieder jeweils von b, c usw. abhängen. Das Produkt aus den m Faktoren

$$\begin{aligned} &f(x - a, L', L'', L''' \text{ usw.}) \\ &f(x - b, L', L'', L''' \text{ usw.}) \\ &f(x - c, L', L'', L''' \text{ usw.}) \\ &\text{usw.} \end{aligned}$$

ist daher ein Polynom in x , dessen höchstes Glied $N^m x^{m\nu}$ ist, während die Koeffizienten der folgenden Glieder von den Unbestimmten a, b, c usw. abhängen.

Wir betrachten nun weiter das Produkt aus den folgenden m Faktoren:

$$\begin{aligned} &f(x - a, l', l'', l''' \text{ usw.}) \\ &f(x - b, l', l'', l''' \text{ usw.}) \\ &f(x - c, l', l'', l''' \text{ usw.}) \\ &\text{usw.} \end{aligned}$$

Da es eine Funktion der Unbestimmten x, a, b, c usw., l', l'', l''' usw. ist, und zwar hinsichtlich a, b, c usw. symmetrisch, lässt es sich als Funktion der Unbestimmten $x, \lambda', \lambda'', \lambda'''$ usw., l', l'', l''' usw. darstellen, die wir mit

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.}, l', l'', l''' \text{ usw.})$$

bezeichnen. Somit ist

$$\varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.}, \lambda', \lambda'', \lambda''' \text{ usw.})$$

das Produkt aus den Faktoren

$$\begin{aligned} &f(x - a, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ &f(x - b, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ &f(x - c, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ &\text{usw.} \end{aligned}$$

und daher identisch durch ρ teilbar, da man leicht sieht, dass jeder Faktor von ρ in einem jener Faktoren enthalten ist. Wir setzen also

$$\begin{aligned} &\varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.}, \lambda', \lambda'', \lambda''' \text{ usw.}) \\ &= \rho \psi(x, \lambda', \lambda'', \lambda''' \text{ usw.}) \end{aligned}$$

wobei das Zeichen ψ ein Polynom bezeichnet. Daraus folgt aber leicht, dass auch identisch

$$\begin{aligned} &\varphi(x, L', L'', L''' \text{ usw.}, L', L'', L''' \text{ usw.}) \\ &= R\psi(x, L', L'', L''' \text{ usw.}) \end{aligned}$$

gilt. Oben haben wir jedoch bewiesen, dass das Produkt aus den Faktoren

$$\begin{aligned} & f(x - a, L', L'', L''' \text{ usw.}) \\ & f(x - b, L', L'', L''' \text{ usw.}) \\ & f(x - c, L', L'', L''' \text{ usw.}) \\ & \text{usw.} \end{aligned}$$

das $= \varphi(x, \lambda', \lambda'', \lambda''' \text{ usw.}, L', L'', L''' \text{ usw.})$ ist, das höchste Glied $N^m x^{m\nu}$ hat. Dasselbe höchste Glied hat daher auch die Funktion $\varphi(x, L', L'', L''' \text{ usw.}, L', L'', L''' \text{ usw.})$, und sie ist somit gewiss nicht identisch $= 0$. Folglich kann auch R nicht identisch $= 0$ sein und daher ebenso wenig die Determinante der Funktion Z . Q. E. D.

16.

SATZ. *Es bezeichne $\varphi(u, x)^{*)}$ ein Produkt aus beliebig vielen Faktoren, in welche die Unbestimmten u, x nur linear eingehen, die also die Form*

$$\begin{aligned} & \alpha + \beta u + \gamma x \\ & \alpha' + \beta' u + \gamma' x \\ & \alpha'' + \beta'' u + \gamma'' x \\ & \text{usw.} \end{aligned}$$

haben; ferner sei w eine weitere Unbestimmte. Dann ist die Funktion

$$\varphi(u + w \cdot \frac{d\varphi(u, x)}{dx}, x - w \cdot \frac{d\varphi(u, x)}{du}) = \Omega$$

identisch durch $\varphi(u, x)$ teilbar.

Beweis. Setzen wir

$$\begin{aligned} \varphi(u, x) &= (\alpha + \beta u + \gamma x)Q \\ &= (\alpha' + \beta' u + \gamma' x)Q' \\ &= (\alpha'' + \beta'' u + \gamma'' x)Q'' \\ & \text{usw.} \end{aligned}$$

so sind Q, Q', Q'' usw. Polynome in den Unbestimmten $u, x, \alpha, \beta, \gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ usw., und es gilt

$$\begin{aligned} \frac{d\varphi(u, x)}{dx} &= \gamma Q + (\alpha + \beta u + \gamma x) \cdot \frac{dQ}{dx} \\ &= \gamma' Q' + (\alpha' + \beta' u + \gamma' x) \cdot \frac{dQ'}{dx} \\ &= \gamma'' Q'' + (\alpha'' + \beta'' u + \gamma'' x) \cdot \frac{dQ''}{dx} \\ & \text{usw.} \end{aligned}$$

^{*)}Jeder wird auch ohne unseren Hinweis sehen, dass die im vorigen Artikel eingeführten Zeichen auf diesen Artikel allein beschränkt sind und daher die jetzige Bedeutung der Zeichen φ, w nicht mit der früheren verwechselt werden darf.

$$\begin{aligned}
 \frac{d\varphi(u, x)}{du} &= \beta Q + (\alpha + \beta u + \gamma x) \cdot \frac{dQ}{du} \\
 &= \beta' Q' + (\alpha' + \beta' u + \gamma' x) \cdot \frac{dQ'}{du} \\
 &= \beta'' Q'' + (\alpha'' + \beta'' u + \gamma'' x) \cdot \frac{dQ''}{du} \\
 &\text{usw.}
 \end{aligned}$$

Setzt man diese Werte in die Faktoren ein, deren Produkt Ω ist, nämlich in

$$\begin{aligned}
 &\alpha + \beta u + \gamma x + \beta w \cdot \frac{d\varphi(u, x)}{dx} - \gamma w \cdot \frac{d\varphi(u, x)}{du} \\
 &\alpha' + \beta' u + \gamma' x + \beta' w \cdot \frac{d\varphi(u, x)}{dx} - \gamma' w \cdot \frac{d\varphi(u, x)}{du} \\
 &\alpha'' + \beta'' u + \gamma'' x + \beta'' w \cdot \frac{d\varphi(u, x)}{dx} - \gamma'' w \cdot \frac{d\varphi(u, x)}{du} \\
 &\text{usw., jeweils}
 \end{aligned}$$

so erhalten diese die folgenden Werte:

$$\begin{aligned}
 &(\alpha + \beta u + \gamma x)(1 + \beta w \cdot \frac{dQ}{dx} - \gamma w \cdot \frac{dQ}{du}) \\
 &(\alpha' + \beta' u + \gamma' x)(1 + \beta' w \cdot \frac{dQ'}{dx} - \gamma' w \cdot \frac{dQ'}{du}) \\
 &(\alpha'' + \beta'' u + \gamma'' x)(1 + \beta'' w \cdot \frac{dQ''}{dx} - \gamma'' w \cdot \frac{dQ''}{du}) \\
 &\text{usw.}
 \end{aligned}$$

Daher ist Ω das Produkt aus $\varphi(u, x)$ und den Faktoren

$$\begin{aligned}
 &1 + \beta w \cdot \frac{dQ}{dx} - \gamma w \cdot \frac{dQ}{du} \\
 &1 + \beta' w \cdot \frac{dQ'}{dx} - \gamma' w \cdot \frac{dQ'}{du} \\
 &1 + \beta'' w \cdot \frac{dQ''}{dx} - \gamma'' w \cdot \frac{dQ''}{du} \\
 &\text{usw., also aus } \varphi(u, x) \text{ und einem Polynom in den Unbestimmten } u, x, w, \alpha, \beta, \\
 &\gamma, \alpha', \beta', \gamma', \alpha'', \beta'', \gamma'' \text{ usw. Q. E. D.}
 \end{aligned}$$

17.

Der Satz des vorigen Artikels ist offenbar auf die Funktion ζ anwendbar, die wir von nun an durch

$$f(u, x, \lambda', \lambda'', \lambda''' \text{ usw.})$$

darstellen. Dann ist

$$f(u + w \cdot \frac{d\zeta}{dx}, x - w \cdot \frac{d\zeta}{du}, \lambda', \lambda'', \lambda''' \text{ usw.})$$

identisch durch ζ teilbar. Den Quotienten, ein Polynom in den Unbestimmten u, x, w, a, b, c usw., das hinsichtlich a, b, c usw. symmetrisch ist, stellen wir durch

$$\psi(u, x, w, \lambda', \lambda'', \lambda''' \text{ usw.})$$

dar. Daraus schließen wir, dass auch identisch

$$\begin{aligned} f(u + w \cdot \frac{dz}{dx}, x - w \cdot \frac{dz}{du}, l', l'', l''' \text{ usw.}) \\ = z\psi(u, x, w, l', l'', l''' \text{ usw.}) \end{aligned}$$

sowie

$$\begin{aligned} f(u + w \cdot \frac{dZ}{dx}, x - w \cdot \frac{dZ}{du}, L', L'', L''' \text{ usw.}) \\ = Z\psi(u, x, w, L', L'', L''' \text{ usw.}) \end{aligned}$$

gilt. Stellen wir also die Funktion Z einfach durch $F(u, x)$ dar, sodass

$$f(u, x, L', L'', L''' \text{ usw.}) = F(u, x)$$

gilt, so haben wir identisch

$$\begin{aligned} F(u + w \cdot \frac{dZ}{dx}, x - w \cdot \frac{dZ}{du}) \\ = Z\psi(u, x, w, L', L'', L''' \text{ usw.}) \end{aligned}$$

18.

Nehmen wir nun an, aus bestimmten Werten von u, x , nämlich aus $u = U, x = X$, ergebe sich

$$\frac{dZ}{dx} = X', \quad \frac{dZ}{du} = U'$$

Dann gilt identisch

$$\begin{aligned} F(U + wX', X - wU') \\ = F(U, X) \cdot \psi(U, X, w, L', L'', L''' \text{ usw.}) \end{aligned}$$

Sooft U' nicht verschwindet, dürfen wir

$$w = \frac{X - x}{U'}$$

setzen. Daraus ergibt sich

$$\begin{aligned} F(U + \frac{XX'}{U'} - \frac{X'x}{U'}, x) \\ = F(U, X) \cdot \psi(U, X, \frac{X-x}{U'}, L', L'', L''' \text{ usw.}) \end{aligned}$$

Dies lässt sich auch so aussprechen:

Setzt man in der Funktion Z den Wert $u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$, so geht sie in

$$F(U, X) \cdot \psi(U, X, \frac{X-x}{U'}, L', L'', L''' \text{ usw.})$$

über.

19.

Da im Fall, dass nicht $P = 0$ gilt, die Determinante der Funktion Z eine für sich nicht verschwindende Funktion der Unbestimmten x ist, ist die Anzahl der bestimmten Werte von x , bei denen diese Determinante den Wert 0 annehmen kann, offenbar endlich. Es lassen sich daher unendlich viele bestimmte Werte von x angeben, die jener Determinante einen von 0 verschiedenen Wert geben. Es sei X ein solcher Wert von x , den man außerdem als *reell* annehmen darf. Die Determinante der Funktion $F(u, X)$ ist dann nicht $= 0$. Nach Satz II von Artikel 6 können also die Funktionen

$$F(u, X) \quad \text{und} \quad \frac{dF(u, X)}{du}$$

keinen gemeinsamen Teiler haben. Wir nehmen ferner an, es gebe einen bestimmten Wert von u , etwa U , der entweder reell oder imaginär, also von der Form $g + h\sqrt{-1}$ ist und $F(u, X) = 0$ bewirkt, sodass $F(U, X) = 0$ gilt. Dann ist $u - U$ ein Faktor des Polynoms $F(u, X)$, und die Funktion $\frac{dF(u, X)}{du}$ ist daher gewiss nicht durch $u - U$ teilbar. Nehmen wir also an, diese Funktion, $\frac{dF(u, X)}{du}$, erhalte den Wert U' , wenn $u = U$ gesetzt wird. Dann kann gewiss nicht $U' = 0$ sein. Offenbar ist aber U' der Wert der partiellen Ableitung $\frac{dZ}{du}$ für $u = U, x = X$. Bezeichnen wir ferner den Wert der partiellen Ableitung $\frac{dZ}{dx}$ bei denselben Werten von u, x mit X' , so ist nach dem im vorigen Artikel Bewiesenen klar, dass die Funktion Z durch die Substitution

$$u = U + \frac{XX'}{U'} - \frac{X'x}{U'}$$

identisch verschwindet und daher identisch durch den Faktor

$$u + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

teilbar ist. Setzen wir nun $u = xx$, so ist offenbar $F(xx, x)$ durch

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'})$$

teilbar und nimmt daher den Wert 0 an, wenn für x eine Wurzel der Gleichung

$$xx + \frac{X'}{U'}x - (U + \frac{XX'}{U'}) = 0$$

genommen wird, also wenn man

$$x = \frac{-X' \pm \sqrt{(4UU'U' + 4XX'U' + X'X')}}{2U'}$$

setzt. Diese Werte sind bekanntlich entweder reell oder von der Form $g + h\sqrt{-1}$.

Nun lässt sich leicht beweisen, dass bei denselben Werten von x auch die Funktion Y verschwinden muss. Denn $f(xx, x, \lambda', \lambda'', \lambda''' \text{ usw.})$ ist offenbar das Produkt aus allen $(x - a)(x - b)$ mit ausgeschlossenen Wiederholungen und somit $= v^{m-1}$. Daraus folgt von selbst

$$\begin{aligned} f(xx, x, l', l'', l''' \text{ usw.}) &= y^{m-1} \\ f(xx, x, L', L'', L''' \text{ usw.}) &= Y^{m-1} \end{aligned}$$

oder $F(xx, x) = Y^{m-1}$, dessen bestimmter Wert also nur verschwinden kann, wenn zugleich der Wert von Y verschwindet.

20.

Mithilfe der vorangehenden Untersuchungen ist die *Lösung* der Gleichung $Y = 0$, also das Auffinden eines bestimmten Wertes von x , der entweder reell oder von der Form $g + h\sqrt{-1}$ ist und ihr genügt, auf die Lösung der Gleichung $F(u, X) = 0$ zurückgeführt, sofern die Determinante der Funktion Y nicht $= 0$ ist. Zu bemerken ist: Sind alle Koeffizienten in Y , also die Zahlen L', L'', L''' usw., reelle Größen, so sind auch alle Koeffizienten in $F(u, X)$ reell, sofern für X eine reelle Größe genommen wird, was zulässig ist. Der Grad der zweiten Gleichung $F(u, X) = 0$ wird durch die Zahl $\frac{1}{2}m(m-1)$ ausgedrückt. Ist also m eine gerade Zahl von der Form $2^\mu k$, wobei k eine unbestimmte ungerade Zahl bezeichnet, so hat die zweite Gleichung einen Grad von der Form $2^{\mu-1}k$.

Ist die Determinante der Funktion $Y = 0$, so lässt sich nach Artikel 10 ein anderes, sie teilendes Polynom $\mathfrak{Y}$ angeben, dessen Determinante nicht $= 0$ ist und dessen Grad durch eine Zahl von der Form $2^\nu k$ ausgedrückt wird, wobei entweder $\nu < \mu$ oder $\nu = \mu$ gilt. Jede Lösung der Gleichung $\mathfrak{Y} = 0$ genügt auch der Gleichung $Y = 0$. Die Lösung der Gleichung $\mathfrak{Y} = 0$ wird wiederum auf die Lösung einer anderen Gleichung zurückgeführt, deren Grad durch eine Zahl von der Form $2^{\nu-1}k$ ausgedrückt wird.

Daraus schließen wir also, dass sich allgemein die Lösung jeder Gleichung, deren Grad eine gerade Zahl von der Form $2^\mu k$ ist, auf die Lösung einer anderen Gleichung zurückführen lässt, deren Grad die Form $2^{\mu'} k$ hat, wobei

$\mu' < \mu$ gilt. Ist diese Zahl noch immer gerade, also μ' nicht $= 0$, so wird dieselbe Methode erneut angewandt. So fahren wir fort, bis wir zu einer Gleichung gelangen, deren Grad ungerade ist. Alle ihre Koeffizienten sind reell, sofern sämtliche Koeffizienten der ursprünglichen Gleichung reell waren. Eine solche Gleichung ungeraden Grades ist bekanntlich gewiss lösbar, und zwar durch eine reelle Wurzel. Daher sind auch alle vorhergehenden Gleichungen lösbar, entweder durch reelle Wurzeln oder durch Wurzeln von der Form $g + h\sqrt{-1}$.

Damit ist erwiesen, dass jedes Polynom Y von der Form $x^m - L'x^{m-1} + L''x^{m-2} - \text{usw.}$, wobei L', L'' usw. bestimmte reelle Größen sind, einen Faktor $x - A$ enthält, wobei A eine entweder reelle Größe oder eine Größe von der Form $g + h\sqrt{-1}$ ist. Im letzteren Fall sieht man leicht, dass Y auch durch die Substitution $x = g - h\sqrt{-1}$ den Wert 0 erhält, also durch $x - (g - h\sqrt{-1})$ und daher auch durch das Produkt $xx - 2gx + gg + hh$ teilbar ist. Jedes Polynom Y enthält also gewiss einen reellen Faktor ersten oder zweiten Grades. Da dasselbe wiederum für den Quotienten gilt, ist klar, dass sich Y in reelle Faktoren ersten oder zweiten Grades zerlegen lässt. Dies zu beweisen war das Ziel dieser Abhandlung.
