Kapitel IV.

Algebraische Gleichungen.

Von *Alfred Loewy* in Freiburg i. Br.

§ 1. Historisches. Literatur.

Aufgabe der Algebra ist das Studium der ganzen rationalen Funktionen oder Polynome in einer oder mehreren Variablen (vgl. S. 31). Der Name „Algebra" stammt von dem Titel des mathematischen Lehrbuches *Aldschebr walmukâbala* des Arabers Muhammed ibn Mûsâ Alchwarizmî (Anfang des 9. Jahrh.). Ihren Ausgangspunkt hat die Algebra in der Theorie der Gleichungen, und diese bilden auch ihren vornehmsten Gegenstand. Mit *Gleichungen des ersten Grades* beschäftigt sich bereits das altägyptische Rechenbuch des *Ahmes* (etwa 1700 v. Chr.). Die Auflösung der *Gleichungen zweiten Grades* war den griechischen Mathematikern bekannt. In geometrischer Form findet man sie in Euklids Elementen (um 300 v. Chr.) (Buch II, Satz 11, Buch VI, Satz 28 u. 29); zahlreichen quadratischen Gleichungen begegnet man in dem ältesten Denkmal griechischer algebraischer Wissenschaft, in Diophantus' Arithmetica (3. bis 4. Jahrh. n. Chr.). Die Auflösung der *Gleichungen dritten und vierten Grades* verdankt man italienischen Mathematikern des 16. Jahrhunderts: Scipione del Ferro, Tartaglia, Cardano und Ferrari (vgl. § 8).

Zu einem Herausgehen über ihre ersten Anfänge konnte die Algebra erst durch Schöpfung der *Buchstabenrechnung* gelangen. Vieta (*In artem analyticam isagoge* (1591)) hat zuerst die Buchstaben nicht nur wie bisher für die Unbekannten verwendet, sondern auch für Größen, die bestimmte gegebene Zahlenwerte besitzen. Vieta (*De aequationum recognitione et emendatione,* aus dem Nachlaß 1615 erschienen) hat auch den Zusammenhang zwischen den Wurzeln und Koeffizienten einer

Gleichung entdeckt; er beschränkte sich hierbei auf die positiven Lösungen, die er allein als Auflösungen zuließ. Girard (*Invention nouvelle en l'algèbre* (1629)) hat zuerst ausgesprochen: Jede Gleichung besitzt soviel Wurzeln, wie ihr Grad angibt; den Satz von Vieta hat er ohne Einschränkung, sogar beim Auftreten imaginärer oder mehrfacher Wurzeln. Er berechnet auch die Summen der vier ersten Potenzen der Gleichungswurzeln aus den Gleichungskoeffizienten. Descartes hat im dritten Buch seiner *Géométrie* (1637) (deutsche Ausgabe von Ludw. Schlesinger, Berlin 1894), welche seine berühmte Zeichenregel enthält und auch sonst reich an algebraischen Theoremen ist, den Satz: Wenn eine Gleichung mit der Unbekannten z die Wurzel α_1 besitzt, so ist ihre auf Null gebrachte linke Seite durch $z - \alpha_1$ ohne Rest teilbar. Auf Grund dieses Satzes erfordert der sogenannte *Fundamentalsatz oder Wurzelexistenzsatz* der Algebra nur den Nachweis, daß jede algebraische Gleichung wenigstens eine Wurzel besitzt; hieraus folgt, daß die auf Null gebrachte linke Seite jeder Gleichung n^{ten} Grades in n Faktoren ersten Grades zerfällt und daher, wenn man den Begriff der mehrfachen Wurzeln einführt, bei richtiger Zählung der Wurzeln genau n Wurzeln besitzt. Eine Regel zur Erkennung mehrfacher Wurzeln stammt von Hudde (*Huddenii epistolae* in Schootens Ausgabe von Cartesius' *Geometria* aus dem Jahre 1659, p. 433 u. 507). D'Alembert (*Recherches sur le calcul intégral, Histoire de l'acad. de Berlin, année 1746*) versuchte zuerst, einen Beweis für den Fundamentalsatz der Algebra zu liefern und hierdurch der Algebra eine einwandfreie Grundlage zu geben; daher bezeichnet man den Wurzelexistenzsatz auch als d'Alembert'sches Theorem. Den ersten auf strengerer Grundlage beruhenden Beweis des Fundamentalsatzes gab Gauß (*Ges. Werke* **3**, 1) in seiner Doktordissertation (1799) und hob hierbei die Mängel in den Beweisen seiner Vorgänger d'Alembert, Euler, de Foncenex und Lagrange hervor. In den Jahren 1815, 1816 und 1849 publizierte Gauß noch drei weitere Beweise für den Fundamentalsatz der Algebra (Gauß, *Ges. Werke* **3**, 31, 57, 71). Vgl. die vier Gaußschen Beweise für die Zerlegung ganzer algebraischer Funktionen in reelle Faktoren ersten oder zweiten Grades, herausgegeben von E. Netto, *Ostwalds Klassiker der exakten Wiss.,* Nr. 14.

Die Tatsache, daß sich die Wurzeln der Gleichungen der vier ersten Grade durch Radikale aus den Koeffizienten bilden lassen, veranlaßte die Mathematiker des 17. und 18. Jahrhunderts, auch bei den Gleichungen höheren Grades nach einer *algebraischen Auflösung* zu suchen. Unter einer solchen versteht man eine Darstellung der Wurzeln aus den Koeffizienten mittelst einer endlichen Anzahl von Radikalen oder Wurzelzeichen, anders ausgedrückt: eine Rückführung der gegebenen Gleichung auf eine Kette reiner Gleichungen der Form $z^n = a$. Bei diesen Bemühungen gelangte Tschirnhaus, *Methodus auferendi omnes terminos intermedios ex data aequatione, Acta eruditorum* (1683) zu der heute nach seinem Namen sogenannten Tschirnhausentransformation. Lagranges *Réflexions sur la résolution algébrique des équations* (1770), *Œuvres* **3**, 205 (vgl. S. 168) verfolgen, wie es in der Einleitung heißt, den Zweck, a priori zu zeigen, warum die bei den Gleichungen der vier ersten Grade angewendeten Methoden bei den höheren Gleichungen versagen. Hierbei untersucht Lagrange die rationalen Funktionen der Gleichungswurzeln und ihre Werteänderungen bei Permutationen. Gleichzeitig und unabhängig von ihm haben sich auch Waring (*Miscellanea analytica* (1762), *Meditationes algebraicae* (1770), 3. ed. (1782)) und Vandermonde (vgl. unten, sowie Lagrange, *Œuvres* **8**, 324) mit diesen Fragen beschäftigt. Von Lagrange entnahmen Ruffini und Abel die leitenden Ideen für den von ihnen erbrachten Beweis, daß die *allgemeine Gleichung von höherem als viertem Grade algebraisch nicht lösbar ist,* d. h. ihre Wurzeln sich nicht aus den Koeffizienten mit Hilfe von Radikalen ableiten lassen. Ruffini, *Teoria generale delle equazioni in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto, Bologna* (1799), vgl. Burkhardt, *Ztschr. für Math. u. Phys.* **37**, Suppl. S. 119 (1892), Abel, *Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen, Journ. f. Math.* **1**, 65 (1826), *Œuvres par Sylow et Lie* (1881), **1**, 66, vgl. Pierpont, *Monatsh. f. Math.* **6**, 15 (1895).

Während die allgemeinen Gleichungen von höherem als viertem Grade nach dem Abel-Ruffinischen Theorem nicht algebraisch auflösbar sind, gibt es *spezielle Gleichungsgruppen,* deren Wurzeln sich *algebraisch* finden lassen. Vandermonde, *Mém. sur la résolution des équations, Histoire de l'acad. des sciences* (1771), deutsche Ausgabe, Berlin 1888, S. 63, hat als erster in der Gleichung $z^{11} = 1$ eine algebraisch auflösbare Gleichung kennen gelehrt und ihre Wurzeln mit Hilfe von Radikalen dargestellt. In Sectio 7 seiner *Disquitiones arithmeticae* (1801) (*Ges. Werke* **1**, 412) hat Gauß allgemein für die bei der *Kreis-*

teilung auftretenden Gleichungen, d. h. für die Gleichungen $z^n = 1$, die algebraische Auflösbarkeit nachgewiesen. (Vgl. § 12.) Eine große und zwar die einfachste und fundamentalste Klasse algebraisch auflösbarer Gleichungen lehrte Abel (*Journ. f. Math.* **4**, 131 (1829), *Œuvres par Sylow et Lie* **1**, 478, deutsche Ausg. mit Anm. von Loewy in *Ostwalds Klassikern der exakt. Wiss.*, Nr. 111) kennen. Diese Gleichungen werden nach Kronecker (*Monatsb. d. Berl. Akad.* (1853), 368, ebenda (1877), 846 und C. Jordan (*Traité*, p. 287)) als Abelsche Gleichungen bezeichnet. (Vgl. § 11.) Den größten Fortschritt in der Behandlung beliebiger algebraischer Gleichungen bedeuten die Arbeiten von Galois durch die Entdeckung der nach seinem Namen genannten Gruppe (vgl. S. 169). (Vgl. § 10.) Diese schreibt die für die Behandlung der betreffenden Gleichung einzuschlagenden Wege vor und sagt auch im besonderen aus, ob die Gleichung algebraisch auflösbar oder nicht auflösbar ist. C. Jordan nennt in höchster Bescheidenheit seinen fundamentalen *Traité des substitutions et des équations algébriques*, Paris 1870, einen bloßen Kommentar zu Galois' Werken.

Während die allgemeinen Gleichungen von höherem als viertem Grade nicht algebraisch lösbar sind, haben sie nach dem Fundamentalsatz der Algebra natürlich Lösungen. Der historische Weg, der dazu führte, die Wurzeln der *Gleichung fünften Grades* in ihrer Abhängigkeit von den Gleichungskoeffizienten darzustellen, war folgender: Die Transformation p^{ter} Ordnung (p ungerade Primzahl) der elliptischen Funktionen führte bereits Abel und Jacobi auf besondere algebraische Gleichungen $(p+1)^{\text{ten}}$ Grades, deren Wurzeln sich mittelst der Theorie der elliptischen Funktionen darstellen lassen. Die Galoissche Gruppe dieser Transformationsgleichungen ist nach Adjunktion einer Quadratwurzel die Modulargruppe der Ordnung $\frac{1}{2}p(p^2-1)$, also für $p \geqq 5$ eine einfache Gruppe. Die fraglichen Gleichungen sind daher infolge der Natur ihrer Galoisschen Gruppe nicht durch Radikale lösbar (vgl. die Darstellung bei H. Weber, *Algebra* **3**, 284, sowie bei Hölder, *Enzykl. d. math. Wiss.* **1**, 509). Für $p = 5$ besitzt die Modulargruppe eine Untergruppe des Index 5, daher muß sich für die fragliche Gleichung sechsten Grades eine rationale Resolvente (Hilfsgleichung) fünften Grades bilden lassen. Zu diesem gruppentheoretischen Ergebnis war bereits Galois (vgl. oben S. 215 letzte Zeile) gelangt, und Betti (1853) (*Opere mat.* **1**, 95) hat es bewiesen. Für die $p = 5$

entsprechende „Modulargleichung" sechsten Grades, die zwischen der vierten Wurzel $\sqrt[4]{k}$ des Legendreschen Moduls und seinem transformierten Wert besteht, und deren Wurzeln sich explizit als elliptische Modulfunktionen darstellen lassen, hat Hermite (*C. R.* **46**, 508 (1858), *Œuvres* **2**, 5) wirklich eine Resolvente fünften Grades aufgestellt und ihre Wurzeln, die rationale Funktionen der Wurzeln der Modulargleichung sechsten Grades sind, angegeben. Diese Gleichung fünften Grades hat dieselbe Galoissche Gruppe wie die allgemeine Gleichung fünften Grades nach Adjunktion der Quadratwurzel ihrer Diskriminante, nämlich die alternierende Gruppe von fünf Symbolen. Mit der Bemerkung, daß sich nach den Untersuchungen des englischen Mathematikers Ierrard (1834) (die älteren des schwedischen Mathematikers Bring (1786) wurden erst im Jahre 1861 durch Hills Mitteilung an die schwedische Akademie der Vergessenheit entrissen) jede Gleichung fünften Grades ohne Verwendung anderer Irrationalitäten als Quadrat- und Kubikwurzeln in die obige Resolvente der Form $u^5 - u - A = 0$ mit nur einem Parameter A überführen läßt, hatte Hermite die erste Auflösung der Gleichung fünften Grades gewonnen. (Über die Methode von Bring und Hermite vgl. Klein, *Ikosaeder*, S 143 u. 244, über Bring vgl. Eneström, *Bibl. math.* (3) **8**, 417 (1908)). Die bei Hermites oder ähnlichen Formeln stattfindende Benutzung elliptischer Modulfunktionen ist, wie F. Klein, *Ikosaeder*, S. 131, besonders *Journ. f. Math.* **129**, 154 (1905) hervorgehoben hat, ein Umweg, ebenso wie die Lösung der reinen Gleichung $z^n = a$ durch Logarithmen in der Form $z = e^{\frac{1}{n} l a}$.

Im gleichen Jahre 1858 wie Hermite publizierte auch Kronecker, *C. R.* **46**, 1150 (1858), *Monatsb. d. Berl. Akad.* (1861), 609 eine Auflösung der Gleichung fünften Grades. Er geht direkt von der allgemeinen Gleichung fünften Grades aus und macht ihre Auflösung von einer Gleichung zwölften Grades abhängig, deren Koeffizienten rationale Funktionen der Koeffizienten der Gleichung fünften Grades und der Quadratwurzel aus der Diskriminante sind. Die Resolvente ist zwar höheren Grades als die Ausgangsgleichung, aber insofern einfacher, weil zwischen ihren Wurzeln lineare Relationen bestehen, die für sie charakteristisch sind. Aus ihnen folgt, daß sich die Wurzeln der Gleichung zwölften Grades linear und homogen durch drei Parameter darstellen (Kiepert, *Journ. f. Math.* **87**, 115 (1879), Cayley, *Math. Ann.* **30**, 78 (1887), *Journ. f. Math.* **113**, 42 (1894), *Coll. math. papers* **12**, 493, **13**, 473). Führt man in der Gleichung zwölften Grades, welche die Unbekannte nur quadratisch enthält, das Quadrat der Unbekannten als neue Unbekannte ein, so hat man eine Gleichung sechsten Grades. Auf solche Gleichungen ist zuerst Jacobi (*Journ. f. Math.* **3**, 308 (1828), *Ges. Werke* **1**, 261) in der Theorie der elliptischen Funktionen gekommen. Er hat nämlich gezeigt, daß, wenn p eine ungerade Primzahl und M der Multiplikator für eine Transformation p^{ter} Ordnung der elliptischen Funktionen ist, M Wurzel einer Gleichung $(p+1)^{\text{ten}}$ Grades ist, deren Koeffizienten rationale Funktionen des Moduls k sind. Die Quadratwurzeln der Lösungen einer solchen Gleichung $(p+1)^{\text{ten}}$ Grades lassen sich linear und homogen durch $\frac{p+1}{2}$ Parameter ausdrücken. Die eingehende Untersuchung und Verwertung der $p=5$ entsprechenden allgemeinen Jacobischen Gleichungen sechsten Grades für die Auflösung der Gleichung fünften Grades ist das Verdienst von Brioschi, dessen Arbeiten über diesen Gegenstand ebenfalls 1858 beginnen. Vgl. die Würdigung Brioschis durch Noether, *Math. Ann.* **50**, 483 (1898), sowie die zusammenfassende Darstellung von Brioschi, *Math. Ann.* **13**, 109 (1878). Über die Geschichte der Gleichung fünften Grades bis 1858 vgl. Pierpont, *Monatsh. f. Math.* **6**, 15 (1895).

Ein wesentlich neues Moment brachte Klein (vgl. seine zusammenfassende Darstellung in *Vorlesungen über das Ikosaeder,* Leipzig 1884) in die Theorie der Gleichung fünften Grades durch die Einführung der *Ikosaederirrationalität* (vgl. S. 240). Sie stellt sich neben die Radikale als neue und zwar ihrer Natur nach einfachste Transzendente; sie ist die Lösung einer Gleichung sechzigsten Grades mit nur einem Parameter, der Ikosaedergleichung, die in dem durch Adjunktion der fünften Einheitswurzeln erweiterten Körper[1]) ihre eigene Galoissche oder Normalgleichung ist, deren Galoissche Gruppe demnach die niedrigste einfachste Gruppe ist, die nicht Primzahlordnung besitzt. Die Auflösung der Gleichung fünften Grades besteht in zwei Schritten: der erste ist die Überführung einer beliebigen Gleichung fünften Grades in die Ikosaedergleichung und die Bestimmung der hierzu notwendigen Operationen, der zweite, transzendente Teil ist die Berechnung der Ikosaederirrationalität; diese wird durch die Verwendung hypergeometrischer Reihen ausgeführt, ähnlich wie sich die reinen

1) Die Erweiterung des Körpers ist deswegen erforderlich, weil die fünften Einheitswurzeln bei den Ikosaedersubstitutionen auftreten (vgl. S. 237).

Gleichungen $z^n = a$ durch binomische Reihen lösen lassen. Die Verwandschaft der Ikosaedergleichung mit Gleichungen sechsten Grades und deren Kenntnis aus der Theorie der elliptischen Funktionen erklärt, daß der historische Weg der Lösung der Gleichung fünften Grades über die Gleichungen sechsten Grades und die elliptischen Modulfunktionen führte. (Über die Behandlung der Gleichungen fünften und höheren Grades vgl. § 14.)

Den praktischen Rechner wird die *näherungsweise Berechnung der Wurzeln numerischer Gleichungen* besonders interessieren. Eine Vorläuferin der in Newtons *Analysis per aequationes* (1669) (M. Cantor, *Geschichte der Math.* **3**, 105) gelehrten „Newtonschen Näherungsmethode" findet man schon bei Vieta (1600) (Cantor **2**, 640). Rolles *Traité d'algèbre* (1690) und Newtons *Arithmetica universalis* (1707) geben Grenzen, zwischen denen die reellen Wurzeln einer algebraischen Gleichung liegen. Den größten Fortschritt in der Behandlung numerischer Gleichungen bedeuten die klassischen Arbeiten von Lagrange, Fourier und Sturm. Lagrange, *Traité de la résolution des équations numériques* (1798, nouv. éd. 1808), *Œuvres de Lagrange* **8**. Fourier, *Analyse des équations déterminées* (1831), deutsche Ausg. mit Anm. von A. Loewy in *Ostwalds Klassikern der exakt. Wiss.* Nr. 127. Ch. Sturm, *Mémoire sur la résolution des équations numériques, Mém. prés. par div. sav. à l'acad. des sc. de France* (1835), deutsche Ausg. mit Anm. von A. Loewy in *Ostwalds Klassikern der exakt. Wiss.* Nr. 143. Sturms Aufsatz hat zum erstenmal die genaue Anzahl reeller Wurzeln einer numerischen Gleichung mit reellen Koeffizienten zwischen zwei gegebenen reellen Zahlen bestimmen gelehrt, während die früheren Kriterien nur Grenzen für jene Zahl lieferten.

Die voraufgegangenen Zeilen bezwecken nicht, eine Geschichte der Algebra zu geben; sie wollen nur einige orientierende Bemerkungen machen. Über die ältere Geschichte der Algebra vgl. man M. Cantor, *Vorl. über Geschichte der Math.* Bd. 1—4, die systematische Darstellung bei Tropfke, *Geschichte der Elementarmathematik,* Leipzig 1902, **1**, 123, L. Matthiessen, *Grundzüge der antiken und modernen Algebra der litteralen Gleichungen*, Leipzig 1878 (am Schluß reichhaltiges Literaturverzeichnis).

Von Lehrbüchern nennen wir:

H. Weber, *Lehrbuch der Algebra,* Bd. **1**, **2** und **3**, Braunschweig, 2. Aufl., 1898, 1899 u. 1908. E. Netto, *Vorlesungen über Algebra,* Bd. **1** u. **2**, Leipzig 1896 u. 1900. J. A. Serret, *Handbuch der höheren Algebra*, deutsch von Wertheim, Bd. **1** u. **2**, Leipzig, 2. Aufl., 1878 u. 1879. G. Bauer, *Vorlesungen über Algebra*, Leipzig 1903. J. Petersen, *Theorie der algebraischen Gleichungen*, Kopenhagen 1878. Runge, *Praxis der Gleichungen*, Samml. Schubert **14**, Leipzig 1900. Cesàro, *Elementares Lehrbuch der algebraischen Analysis und der Infinitesimalrechnung*, deutsch herausg. von Kowalewski, Leipzig 1904, S. 368—485. A. Loewy, *Kurzgefaßtes Lehrbuch der Algebra*, erscheint bei Veit & Co., Leipzig 1910. W. S. Burnside and A. Panton, *Theory of equations*, 4. Aufl., London 1900. M. Bôcher, *Introduction to higher algebra*, New York 1908, deutsche Ausg. erscheint 1909 bei Teubner, Leipzig. F. Cajori, *Introduction to the modern theory of equations*, New York 1904. L. E. Dickson, *Introduction to the theory of algebraic equations*, New York 1903. Borel et Drach, *Introduction à l'étude de la théorie des nombres et de l'algèbre supérieure*, Paris 1895. J. Tannery, *Leçons d'algèbre et d'analyse*, Paris 1906, 2 vol. Vogt, *Leçons sur la résolution algébrique des équations*, Paris 1895. Bianchi, *Lezioni sulla teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois*, Pisa 1900. Capelli, *Istituzioni di analisi algebrica*, 3. ed., Napoli 1902.

Wir verweisen noch auf die Artikel in der *Encyklopädie der math. Wiss.*, Bd. I, „Rationale Funktionen einer Veränderlichen; ihre Nullstellen" von Netto, S. 227, „Rationale Funktionen mehrerer Veränderlichen" von Netto, S. 255, „Separation und Approximation der Wurzeln" von Runge, S. 404, „Rationale Funktionen der Wurzeln; symmetrische und Affektfunktionen" von Vahlen, S. 449, „Galoissche Theorie mit Anwendungen" von Hölder, S. 480. In der *Encyclopédie des sciences math.* liegen in französischer Bearbeitung nach den Artikeln von Netto vor: *Les fonctions rationelles* von Le Vavasseur.

§ 2. Rationale Funktionen. Teilbarkeitsgesetze.

Bedeuten $a_0, a_1, a_2, \ldots, a_n$ beliebig gegebene reelle oder komplexe Größen und z eine Veränderliche, so heißt, wenn $a_0 \neq 0$ ist, der Ausdruck $a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n$ eine *ganze rationale Funktion n^{ten} Grades* oder *ein Polynom n^{ten} Grades* in z. Eine solche ganze rationale Funktion von z bezeichnet man abgekürzt mit $f(z)$ oder $g(z)$ oder $P(z)$ oder $\varphi(z)$; hat man mehrere ganze Funktionen von z, so fügt man auch Indices bei und schreibt $f_1(z)$, $f_2(z)$ usw. *Das Produkt*

$f(z) \cdot g(z)$ zweier ganzer Funktionen $f(z)$ vom m^{ten} und $g(z)$ vom n^{ten} Grade ist ein Polynom vom Grade $m + n$.

Der Quotient $\frac{f(z)}{g(z)}$ zweier ganzer Funktionen heißt eine *gebrochene rationale Funktion.* Ist $f(z)$ von niedrigerem Grade als $g(z)$, so heißt $\frac{f(z)}{g(z)}$ *echt gebrochen. Ist $f(z)$ eine ganze Funktion vom m^{ten} Grad und $g(z)$ eine solche vom n^{ten} Grad und $m \geqq n$,* so gibt es zwei eindeutig bestimmte ganze Funktionen $G_1(z)$ vom Grad $m - n$[1]) und $R_1(z)$ vom $n - 1^{\text{ten}}$ oder niedrigeren Grade, daß $f(z) = g(z) G_1(z) + R_1(z)$ wird. Mithin ist $\frac{f(z)}{g(z)} = G_1(z) + \frac{R_1(z)}{g(z)}$; $G_1(z)$ heißt der Quotient, $R_1(z)$ der Rest der Division. Ist der Rest $R_1(z)$ gleich Null, so heißt $f(z)$ durch $g(z)$ ohne Rest teilbar; $\frac{f(z)}{g(z)}$ ist in diesem Falle, wie man sagt, nur scheinbar gebrochen. $g(z)$ heißt ein *Teiler* oder *Divisor* von $f(z)$. *Jede ganze Funktion ist durch jede Konstante und durch sich selbst teilbar.*

Ist α irgendeine Konstante, so ist $f(z) - f(\alpha)$ stets durch $z - \alpha$ ohne Rest teilbar.

Ist $f(z)$ eine ganze Funktion m^{ten} Grades und $g(z)$ vom n^{ten} Grade $m \geqq n$, so kann man durch fortgesetzte Division folgende Gleichungskette aufstellen:

$$\begin{aligned}
f(z) &= g(z) G_1(z) + R_1(z), \\
g(z) &= R_1(z) G_2(z) + R_2(z), \\
&\vdots \qquad\qquad \vdots \\
R_{\lambda-2}(z) &= R_{\lambda-1}(z) G_\lambda(z) + R_\lambda.
\end{aligned}$$

Die sukzessiv auftretenden Reste $R_1, R_2, \ldots, R_\lambda$ sind ganze Funktionen, deren Grade abnehmen. *Das Verfahren, unter dem Namen „Euclidscher Algorithmus" bekannt, läßt sich so weit treiben, bis man zu einem Rest R_λ kommt, der eine Konstante ist.* Ist R_λ eine von Null verschiedene Konstante, so sind die zwei Funktionen $f(z)$ und $g(z)$ *teilerfremd* oder *relativ prim,* d. h. es gibt außer Konstanten keine ganze Funktion, die sowohl $f(z)$ als auch $g(z)$ ohne Rest teilt. Man sagt auch: $f(z)$ und $g(z)$ haben keinen gemeinsamen Divisor. Ist R_λ gleich Null, so haben $f(z)$ und $g(z)$ die ganze Funktion $R_{\lambda-1}(z)$ zum gemeinsamen Teiler. *$R_{\lambda-1}(z)$ ist der größte gemeinsame Teiler von*

1) Eine Konstante ist eine ganze Funktion vom Grad Null.

$f(z)$ und $g(z)$, d. h. jeder gemeinsame Teiler von $f(z)$ und $g(z)$ ist Teiler von $R_{\lambda-1}$. Der größte gemeinsame Teiler zweier ganzer Funktionen ist eine bis auf eine multiplikative Konstante eindeutig bestimmte ganze Funktion. Der Euclidsche Algorithmus und die Bestimmung des größten gemeinsamen Teilers zweier ganzer rationaler Funktionen läßt sich mittelst ausschließlich rationaler Rechenoperationen ausführen.

Die charakteristische Bedingung dafür, daß zwei ganze Funktionen $f(z)$ und $g(z)$ teilerfremd sind, besteht in der Existenz zweier ganzer Funktionen $P(z)$ und $Q(z)$ von der Beschaffenheit, daß $Pf + Qg = 1$ ist. Ist $f(z)$ eine ganze Funktion vom m^{ten} Grad und $g(z)$ vom n^{ten} Grad, so lassen sich, wenn die zwei Funktionen f und g teilerfremd sind, auf eine einzige Art zwei Funktionen P_0 höchstens vom Grad $n-1$ und Q_0 höchstens vom Grad $m-1$ bestimmen, daß $P_0 f + Q_0 g = 1$ ist. Mittelst P_0 und Q_0 drücken sich P und Q in der Form $P_0 + gS$ und $Q_0 - fS$ aus, wobei S irgendeine ganze Funktion von z bedeutet.

Sind $f(z)$ und $g(z)$ teilerfremde ganze Funktionen und $U(z)$ eine derartige ganze Funktion von z, daß das Produkt $U(z)f(z)$ durch $g(z)$ ohne Rest teilbar ist, so ist $U(z)$ durch $g(z)$ teilbar.

Die charakteristische Bedingung dafür, daß zwei ganze Funktionen $f(z)$ vom Grad m und $g(z)$ vom Grad n einen gemeinsamen Teiler haben, besteht in der Existenz zweier ganzer Funktionen $G(z)$ höchstens $n-1^{ten}$ Grades und $F(z)$ höchstens $m-1^{ten}$ Grades von der Beschaffenheit, daß $fG + gF = 0$ ist. Ist G vom Grad $n-k$ und F demnach vom Grad $m-k$, so haben f und g einen gemeinsamen Teiler, der mindestens vom Grad k ist.

Sind $f_1(z), f_2(z), \ldots, f_r(z)$ irgendwelche ganze Funktionen von z, so heißt die ganze Funktion niedrigsten Grades, welche durch jede der Funktionen $f_1, f_2, \ldots, f_r$ ohne Rest teilbar ist, *das kleinste gemeinsame Vielfache von $f_1, f_2, \ldots, f_r$.*

Man kann auch *ganze rationale Funktionen* oder *Polynome mehrerer Veränderlichen* betrachten. Hierunter versteht man, wenn $z_1, z_2, \ldots, z_r$ Variable bedeuten, einen Ausdruck, der aus einer endlichen Anzahl von Summanden der Form

$$a_{\alpha_1 \alpha_2 \ldots \alpha_r} z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_r^{\alpha_r}$$

besteht; $\alpha_1, \alpha_2, \ldots, \alpha_r$ bedeuten ganze positive *Zahlen* einschließlich der Null, $a_{\alpha_1 \alpha_2 \ldots \alpha_r}$ beliebige Konstanten. Unter dem *Grad der ganzen Funktion* der r Variablen versteht man den Maximalwert, den $\alpha_1 + \alpha_2 + \cdots + \alpha_r$ bei allen Gliedern mit

17*

$a_{\alpha_1 \alpha_2 \ldots \alpha_r} \neq 0$ annimmt. *Die Anzahl der Glieder einer ganzen rationalen Funktion n^{ten} Grades in r Variablen ist* $\leqq \binom{n+r}{r}$. *Das Produkt zweier ganzer Funktionen ist wieder eine ganze Funktion, deren Grad gleich der Summe der Grade der Faktoren ist.*

Eine ganze rationale Funktion von einer oder mehreren Veränderlichen heißt *unzerlegbar* oder *absolut irreduzibel*, wenn sie nicht als das Produkt zweier ganzer rationaler Funktionen dargestellt werden kann, von denen jede von niedrigerem Grad als die ursprüngliche Funktion ist. *Die einzigen unzerlegbaren ganzen Funktionen in einer Veränderlichen sind die Funktionen ersten Grades, hingegen gibt es unzerlegbare Funktionen mehrerer Variablen von höherem als erstem Grad,* z. B. ist $z_1^2 - z_2^3$ eine unzerlegbare Funktion.

Wenn eine ganze rationale Funktion der r Variablen $z_1, z_2, \ldots, z_r$ in zwei Faktoren zerlegbar ist, die in bezug auf die eine Variable, etwa z_1, ganz, in bezug auf die anderen Variablen $z_2, z_3, \ldots, z_r$ wenigstens rational sind, so ist sie auch als Produkt zweier Funktionen darstellbar, die in allen r Variablen ganz und rational sind.

Eine ganze rationale Funktion kann, wenn man von konstanten Faktoren absieht, nur auf eine Art in ein Produkt unzerlegbarer Faktoren zerlegt werden.

Über ganze rationale Funktionen mehrerer Variablen vgl. Weber, *Algebra* **1**, 71, Netto, *Algebra* **2**, 1, Méray, *Nouv. Ann. de math.* (4) **7**, 193 (1907). Über Teilbarkeitsgesetze der ganzen rationalen Funktionen bei Zugrundelegung eines Körpers vgl. § 9, wo man auch weitere Literatur findet.

§ 3. Fundamentalsatz der Algebra. Einfache und mehrfache Wurzeln.

Hat man eine ganze rationale Funktion $g(z)$ einer Veränderlichen z, so kann man jene besonderen Werte von z aufsuchen, die, an die Stelle von z gesetzt, das Polynom $g(z)$ identisch zu Null machen. Sie heißen die *Wurzeln* oder *Lösungen der Gleichung* $g(z) = 0$. Der Grad des Polynoms $g(z)$ heißt der *Grad der Gleichung*.

Als notwendig und hinreichend, damit eine Größe α_1 Wurzel der Gleichung $g(z) = 0$ ist, erweist sich die Teilbarkeit von $g(z)$ durch $z - \alpha_1$ (Descartes, *Géométrie* (1637), vgl. oben S. 251).

Fundamentalsatz der Algebra: Jede algebraische Gleichung mit beliebigen Koeffizienten hat wenigstens eine Wurzel. Über den Fundamentalsatz vgl. oben S. 251, ferner die historisch-kritische Studie von G. Loria, *Rivista di mat.*, Bd. 1, *Bibl. math.*, N. F. **5**, 99 (1891), **7**, 47 (1893), sowie die eingehende Besprechung der verschiedenen Beweise in dem Artikel „Les fonctions rationelles" (Netto-Le Vavasseur) der *Encycl. des sc. math.* **1**, vol. 2, 189.

Aus dem Fundamentalsatz der Algebra folgt: *Jede ganze rationale Funktion* $g(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n$ $(a_0 \neq 0)$ *läßt sich in ein Produkt* $a_0(z-\alpha_1)(z-\alpha_2)\ldots(z-\alpha_n)$ *zerlegen. Die Größen* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *und auch nur sie allein sind die Wurzeln der Gleichung* $g(z) = 0$.

Die Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$ brauchen nicht sämtlich voneinander verschieden zu sein; um den Satz aussprechen zu können, daß eine jede Gleichung n^{ten} Grades soviel Wurzeln besitzt, wie ihr Grad angibt, ist der *Begriff der mehrfachen Wurzeln* einzuführen. Tritt unter den Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Größe α_1 genau r_1-fach, α_2 genau r_2-fach usw., α_k genau r_k-fach auf und ist $r_1 + r_2 + \cdots + r_k = n$, so heißt α_1 eine *r_1-fache*, α_2 eine *r_2-fache*, ..., α_k eine *r_k-fache Wurzel der Gleichung* $g(z) = 0$.

Ist die Größe α *eine r-fache Wurzel der Gleichung* $g(z) = 0$, *so ist* $g(z)$ *durch* $(z-\alpha)^r$ *und keine höhere Potenz von* $z - \alpha$ *als die r-te ohne Rest teilbar.*

Die Größe α *ist dann und nur dann eine r-fache Wurzel von* $g(z) = 0$, *wenn* α *die ganze rationale Funktion* $g(z)$ *samt ihren ersten* $r - 1$ *Abgeleiteten, hingegen nicht mehr* $g^{(r)}(z)$ *annulliert* (Huddesche Regel vgl. oben S. 251).

Die *erste Abgeleitete der ganzen Funktion*

$$g(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n$$

lautet

$$g'(z) = n a_0 z^{n-1} + (n-1) a_1 z^{n-2} + (n-2) a_2 z^{n-3} + \cdots + \\ + 2 a_{n-2} z + a_{n-1}.$$

(Vgl. Differentialrechnung.) Die k^{te} Abgeleitete einer Funktion $g(z)$ ist die erste Abgeleitete der $(k-1)^{\text{ten}}$ Abgeleiteten.

Eine Gleichung $g(z) = 0$ *hat dann und nur dann keine mehrfachen Wurzeln, wenn die Funktion* $g(z)$ *und ihre erste Abgeleitete* $g'(z)$ *teilerfremd sind. Ist* $D_1(z)$ *der größte gemeinsame Teiler von* $g(z)$ *und* $g'(z)$, *so ist* $\frac{g(z)}{D_1(z)} = G_1(z)$ *eine ganze Funktion. Die Gleichung* $G_1(z) = 0$ *hat nur einfache Wurzeln und wird durch sämtliche Wurzeln von* $g(z) = 0$ *befriedigt.*

Der größte gemeinsame Teiler der ganzen Funktion $D_i(z)$ und ihrer ersten Abgeleiteten $D_i'(z)$ sei mit $D_{i+1}(z)$ bezeichnet. Man bilde aus $D_1(z)$ die Funktion $D_2(z)$, dann $D_3(z)$ usw. *Die Gleichung $g(z) = 0$ hat dann und nur dann i-fache, aber keine $(i+1)$-fachen Wurzeln, wenn D_i eine Konstante wird und zwar die erste auftretende Konstante ist.* Die Gleichung $D_i(z) = 0$ wird nämlich nur durch mindestens $(i+1)$-fache Wurzeln der Gleichung $g(z) = 0$ befriedigt, und jede tritt in einer um i niedrigeren Multiplizität als bei der Gleichung $g(z) = 0$ auf.

Bildet man die ganzen, nur scheinbar gebrochenen Funktionen

$$\frac{g(z)}{D_1(z)} = G_1(z), \quad \frac{D_1(z)}{D_2(z)} = G_2(z), \quad \frac{D_2(z)}{D_3(z)} = G_3(z), \ldots,$$

so haben sämtliche Gleichungen $G_1(z) = 0$, $G_2(z) = 0$, $G_3(z) = 0, \ldots$ nur einfache Wurzeln und keine anderen Wurzeln als solche der Gleichung $g(z) = 0$, und zwar wird $G_1(z) = 0$ durch alle Wurzeln der Gleichung $g(z) = 0$ erfüllt, $G_2(z) = 0$ durch alle mindestens zweifachen, $G_3(z) = 0$ durch alle mindestens dreifachen usw.

Hat eine Gleichung $g(z) = 0$ mit reellen Koeffizienten die imaginäre Größe $\alpha + i\beta$ zur r-fachen Wurzel, so ist auch die konjugiert imaginäre Größe $\alpha - i\beta$ eine r-fache Wurzel der Gleichung $g(z) = 0$.

§ 4. Partialbruchzerlegung einer gebrochenen rationalen Funktion.

Jede nicht echt gebrochene Funktion $\frac{f(z)}{g(z)}$ läßt sich als Summe einer ganzen Funktion $G_1(z)$ und einer echt gebrochenen Funktion $\frac{R(z)}{g(z)}$ darstellen (vgl. S. 258).

Ist $\frac{R(z)}{g(z)}$ echt gebrochen, also $R(z)$ eine ganze Funktion niedrigeren Grades als $g(z)$, und hat $g(z)$ die Form

$$g(z) = (z-\alpha_1)^{r_1}(z-\alpha_2)^{r_2}\ldots(z-\alpha_k)^{r_k},$$

so daß $\alpha_1, \alpha_2, \ldots, \alpha_k$ bezw. r_1-, r_2-, $\ldots$, r_k-fache Wurzeln von $g(z) = 0$ bedeuten, so wird

$$\begin{aligned}\frac{R(z)}{g(z)} = {} & \frac{A_1}{(z-\alpha_1)^{r_1}} + \frac{A_2}{(z-\alpha_1)^{r_1-1}} + \cdots + \frac{A_{r_1}}{z-\alpha_1} + \\ & \frac{B_1}{(z-\alpha_2)^{r_2}} + \frac{B_2}{(z-\alpha_2)^{r_2-1}} + \cdots + \frac{B_{r_2}}{z-\alpha_2} + \\ & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ & \frac{K_1}{(z-\alpha_k)^{r_k}} + \frac{K_2}{(z-\alpha_k)^{r_k-1}} + \cdots + \frac{K_{r_k}}{z-\alpha_k};\end{aligned}$$

hierbei sind $A_1, A_2, \ldots, A_{r_1}, B_1, B_2, \ldots, B_{r_2}, K_1, K_2, \ldots, K_{r_k}$ *eindeutig bestimmte Konstanten. Die Größen A werden durch die folgenden Rekursionsformeln gefunden, bei denen die in Klammern stehenden oberen Indices Abgeleitete bedeuten* (vgl. Differentialrechnung):

$$A_1 \frac{g^{(r_1)}(\alpha_1)}{r_1!} = R(\alpha_1),$$

$$A_2 \frac{g^{(r_1)}(\alpha_1)}{r_1!} + A_1 \frac{g^{(r_1+1)}(\alpha_1)}{(r_1+1)!} = \frac{R'(\alpha_1)}{1},$$

$$A_3 \frac{g^{(r_1)}(\alpha_1)}{r_1!} + A_2 \frac{g^{(r_1+1)}(\alpha_1)}{(r_1+1)!} + A_1 \frac{g^{(r_1+2)}(\alpha_1)}{(r_1+2)!} = \frac{R''(\alpha_1)}{1 \cdot 2},$$

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

Da α_1 *eine* r_1*-fache Wurzel von* $g(z) = 0$ *ist, wird* $g^{(r_1)}(\alpha_1) \neq 0$. *Analoge Formeln gelten für die Größen* $B_1, B_2, \ldots, B_{r_2}$ *usw.* Eine derartige Zerlegung bezeichnet man als eine Zerlegung einer *gebrochenen rationalen Funktion in Partialbrüche;* sie ist für die Integralrechnung besonders wichtig. Leibniz und Johann Bernoulli haben sich bereits 1702 und 1703 mit ihr zuerst für $r_1 = r_2 = \cdots = r_k = 1$, dann für beliebige $r_1, r_2, \ldots, r_k$ beschäftigt (vgl. M. Cantors *Vorl. über Geschichte der Math.* **3**, 272).

Für $r_1 = r_2 = \cdots = r_k = 1$ erhält man die einfachen Formeln $A_1 = \frac{R(\alpha_1)}{g'(\alpha_1)}$, $B_1 = \frac{R(\alpha_2)}{g'(\alpha_2)}, \ldots, K_1 = \frac{R(\alpha_k)}{g'(\alpha_k)}$. Hieraus ergibt sich die sogenannte *Lagrangesche Interpolationsformel* (Lagrange, *Leçons élémentaires* (1795), *Œuvres* **7**, 285, früher bei Waring, *Phil. Trans.* **69** (1779), vgl. Braunmühl, *Bibl. math.* (3) **2**, 95 (1901)): *Eine ganze rationale Funktion* $R(z)$, *die höchstens vom Grad* $k-1$ *ist und für die* k *untereinander verschiedenen Werte* $\alpha_1, \alpha_2, \ldots, \alpha_k$ *die* k *vorgegebenen Werte* $u_1 = R(\alpha_1)$, $u_2 = R(\alpha_2), \ldots, u_k = R(\alpha_k)$ *annimmt, hat den Wert:*

$$R(z) = u_1 \frac{g(z)}{(z-\alpha_1)\, g'(\alpha_1)} + u_2 \frac{g(z)}{(z-\alpha_2)\, g'(\alpha_2)} + \cdots + u_k \frac{g(z)}{(z-\alpha_k)\, g'(\alpha_k)};$$

hierbei ist

$$g(z) = (z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_k),$$

$$g'(\alpha_i) = (\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_k)$$
$$(i = 1, 2, \ldots, k).$$

Es gibt nur eine solche Funktion $R(z)$.

In innigstem Zusammenhang mit der Lagrangeschen Interpolationsformel stehen die Eulerschen Formeln (Euler, *Institutiones calculi integralis* (1769) vol. 2, § 1169 und 1170): *Hat die Gleichung* $g(z)=0$ *lauter verschiedene Wurzeln* α_1, $\alpha_2, \ldots, \alpha_n$, *so ist:*

$$\frac{\alpha_1^{\,m}}{g'(\alpha_1)} + \frac{\alpha_2^{\,m}}{g'(\alpha_2)} + \cdots + \frac{\alpha_n^{\,m}}{g'(\alpha_n)} = 0 \qquad (m = 0, 1, 2, \ldots, n-2),$$

$$\frac{\alpha_1^{\,n-1}}{g'(\alpha_1)} + \frac{\alpha_2^{\,n-1}}{g'(\alpha_2)} + \cdots + \frac{\alpha_n^{\,n-1}}{g'(\alpha_n)} = \frac{1}{g_0},$$

wenn g_0 *der Koeffizient der höchsten Potenz von* z *in* $g(z)$ *ist.* Hieraus folgt: *Für jede ganze rationale Funktion* $R(z)$, *deren Grad um wenigstens zwei Einheiten niedriger als der von* $g(z)$ *ist, besteht, wenn* $g(z)=0$ *lauter verschiedene Wurzeln* α_1, $\alpha_2, \ldots, \alpha_n$ *besitzt, die Gleichung:*

$$\frac{R(\alpha_1)}{g'(\alpha_1)} + \frac{R(\alpha_2)}{g'(\alpha_2)} + \cdots + \frac{R(\alpha_n)}{g'(\alpha_n)} = 0.$$

Sind $g_1(z), g_2(z), \ldots, g_k(z)$ *ganze Funktionen von* z, *von denen je zwei relativ prim sind, ist* $\frac{R(z)}{g(z)}$ *eine echt gebrochene Funktion und* $g(z) = g_1(z)^{r_1} g_2(z)^{r_2} \ldots g_k(z)^{r_k}$, *so besteht die Gleichung:*

$$\begin{aligned}\frac{R(z)}{g(z)} = {} & \frac{A_1}{g_1(z)^{r_1}} + \frac{A_2}{g_1(z)^{r_1-1}} + \cdots + \frac{A_{r_1}}{g_1(z)} + \\ & + \frac{B_1}{g_2(z)^{r_2}} + \frac{B_2}{g_2(z)^{r_2-1}} + \cdots + \frac{B_{r_2}}{g_2(z)} + \\ & \qquad \vdots \\ & + \frac{K_1}{g_k(z)^{r_k}} + \frac{K_2}{g_k(z)^{r_k-1}} + \cdots + \frac{K_{r_k}}{g_k(z)};\end{aligned}$$

hierbei sind $A_1, A_2, \ldots, A_{r_1}$ *eindeutig bestimmte ganze Funktionen von* z, *deren Grad niedriger als* $g_1(z)$ *ist,* $B_1, B_2, \ldots, B_{r_2}$ *eindeutig bestimmte ganze Funktionen von* z, *deren Grad niedriger als* $g_2(z)$ *ist, usw., schließlich* $K_1, K_2, \ldots, K_{r_k}$ *eindeutig bestimmte ganze Funktionen, deren Grad niedriger als* $g_r(z)$ *ist.*

Der erste Satz dieses Paragraphen ist nur ein Spezialfall der zuletzt angegebenen Formel. Ferner ergibt sich aus ihr: *Ist* $g(z) = (az^2 + bz + c)^{r_1} g_2(z)$ *und sind* $g_2(z)$ *und* $az^2 + bz + c$ *relativ prim, so hat man, wenn* $R(z)$ *von niedrigerem Grad als* $g(z)$ *ist, die Zerlegung:*

$$\frac{R(z)}{g(z)} = \frac{A_1 z + B_1}{(a z^2 + b z + c)^{r_1}} + \frac{A_2 z + B_2}{(a z^2 + b z + c)^{r_1 - 1}} + \cdots +$$
$$+ \frac{A_{r_1} z + B_{r_1}}{a z^2 + b z + c} + \frac{F(z)}{g_2(z)};$$

hierbei ist $F(z)$ von niedrigerem Grad als $g_2(z)$, die Größen A und B bedeuten Konstante.

Jede ganze Funktion $g(z)$ mit reellen Koeffizienten läßt sich in ein Produkt von reellen Faktoren ersten Grades $z - \alpha$ und zweiten Grades $az^2 + bz + c$ zerlegen. Hieraus folgt auf Grund des voraufgegangenen Satzes: *Haben in der echt gebrochenen Funktion $\frac{R(z)}{g(z)}$ die ganzen Funktionen $R(z)$ und $g(z)$ reelle Koeffizienten, so läßt sich $\frac{R(z)}{g(z)}$ als eine Summe elementarer Brüche der Form $\frac{A}{(z-\alpha)^{\lambda}}$ und $\frac{Bz + C}{(az^2 + bc + c)^{\mu}}$ darstellen, wobei A, B, C, α, a, b, c lauter reelle Größen sind.* Diese Zerlegung ist für die Integralrechnung wichtig.

§ 5. Symmetrische Funktionen der Gleichungswurzeln.

Hat man die Gleichung $a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$ mit den n Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$, so drücken sich die symmetrischen Grundfunktionen der Wurzeln durch die Gleichungskoeffizienten in der Form aus (vgl. für das Folgende S. 219):

$$S_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n = -\frac{a_1}{a_0},$$
$$S_2 = \sum \alpha_1 \alpha_2 = \qquad + \frac{a_2}{a_0},$$
$$S_3 = \sum \alpha_1 \alpha_2 \alpha_3 = \qquad - \frac{a_3}{a_0},$$
$$\vdots$$
$$S_n = \alpha_1 \cdot \alpha_2 \ldots \alpha_n = \quad (-1)^n \frac{a_n}{a_0}.$$

(Vieta (1615), Girard (1629), vgl. S. 250.)

Jede ganze symmetrische Funktion der Gleichungswurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit ganzzahligen Koeffizienten ist auf eine und auch nur auf eine Weise als ganze ganzzahlige Funktion der Quotienten $\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, \frac{a_n}{a_0}$ darstellbar. Jede typische symmetrische Funktion $(\nu_1, \nu_2, \ldots, \nu_n)$ (vgl. S. 218) *der Gleichungswurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ wird durch Multiplikation mit $a_0^{\nu_1}$, je-*

doch keiner niedrigeren als der ν_1^{ten} Potenz von a_0, eine ganze homogene Funktion der Größen $a_0, a_1, \ldots, a_n$, also eine Summe von Gliedern der Form $a_0^{\lambda_0} a_1^{\lambda_1} a_2^{\lambda_2} \ldots a_n^{\lambda_n}$, mit ganzzahligen Zahlenkoeffizienten vom Grad ν_1; es ist also $\lambda_0 + \lambda_1 + \cdots + \lambda_n = \nu_1$ (Folge des Waringschen Resultates auf S. 219, vgl. Sylvester, *Coll. math. papers* **1**, 595).

Hat man ein Glied $Z_{\lambda_0 \lambda_1 \ldots \lambda_n} a_0^{\lambda_0} a_1^{\lambda_1} a_2^{\lambda_2} \ldots a_n^{\lambda_n}$, wobei $Z_{\lambda_0 \lambda_1 \ldots \lambda_n}$ einen bloßen Zahlenkoeffizienten bedeutet, so bezeichnet man $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots + n\lambda_n$ als das *Gewicht des Gliedes*. Hat man eine Funktion, die aus einer Summe von Gliedern der Form $Z_{\lambda_0 \lambda_1 \ldots \lambda_n} a_0^{\lambda_0} a_1^{\lambda_1} a_2^{\lambda_2} \ldots a_n^{\lambda_n}$ besteht, und haben alle Glieder das nämliche Gewicht $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots + n\lambda_n$, so heißt der Ausdruck *isobar*.

Jede typische symmetrische Funktion $(\nu_1, \nu_2, \ldots, \nu_n)$ *der Gleichungswurzeln ist nach Multiplikation mit $a_0^{\nu_1}$ als ganze homogene isobare Funktion der Gleichungskoeffizienten $a_0, a_1, a_2, \ldots, a_n$ vom Gewicht $\nu_1 + \nu_2 + \cdots + \nu_n$ ausdrückbar* (Cayley, *Coll. math. papers* **2**, 418).

Die ganzen Potenzen $s_\nu = (\nu, 0, 0, \ldots, 0) = \alpha_1^\nu + \alpha_2^\nu + \cdots + \alpha_n^\nu$ der Gleichungswurzeln lassen sich in rekurrenter Weise durch die Gleichungskoeffizienten mittelst der Newtonschen Formeln (Newton, *Arithmetica universalis* (1707)) *bestimmen:*

$$\begin{aligned} a_0 s_1 + a_1 &= 0, \\ a_0 s_2 + a_1 s_1 + 2a_2 &= 0, \\ a_0 s_3 + a_1 s_2 + a_2 s_1 + 3a_3 &= 0, \\ \cdots\cdots\cdots\cdots & \\ a_0 s_n + a_1 s_{n-1} + a_2 s_{n-2} + \cdots + n a_n &= 0, \\ a_0 s_{n+k} + a_1 s_{n+k-1} + a_2 s_{n+k-2} + \cdots + a_n s_k &= 0 \quad (k = 0, 1, 2 \ldots). \end{aligned}$$

Eine explizite Darstellung der Potenzsummen s_ν geben die *Waringschen Formeln* (vgl. S. 219, vorletzte Zeile):

$$s_\nu = \nu \sum \frac{(\lambda_1 + \lambda_2 + \cdots + \lambda_n - 1)!}{\lambda_1!\, \lambda_2! \ldots \lambda_n!} \left(-\frac{a_1}{a_0}\right)^{\lambda_1} \cdot \left(-\frac{a_2}{a_0}\right)^{\lambda_2} \cdots \left(-\frac{a_n}{a_0}\right)^{\lambda_n};$$

das Summenzeichen ist über alle ganzen positiven Zahlen einschließlich 0 zu erstrecken, die der Gleichung $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots + n\lambda_n = \nu$ genügen.

Die Gleichungskoeffizienten drücken sich durch die Potenzsummen s in der Form:

$$a_\nu = a_0 \sum \frac{(-1)^{\lambda_1 + \lambda_2 + \cdots + \lambda_\nu}}{\lambda_1!\, \lambda_2! \ldots \lambda_\nu!} \left(\frac{s_1}{1}\right)^{\lambda_1} \cdot \left(\frac{s_2}{2}\right)^{\lambda_2} \cdots \left(\frac{s_\nu}{\nu}\right)^{\lambda_\nu}$$

aus; hierbei ist das Summenzeichen über alle ganzen positiven Zahlen einschließlich 0 zu erstrecken, die der Gleichung

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots + \nu\lambda_\nu = \nu$$

genügen.

In Determinantenform erhält man:

$$(-1)^\nu \cdot (\nu!)\, a_\nu = a_0 \begin{vmatrix} s_1 & 1 & 0 & \dots 0 & 0 \\ s_2 & s_1 & 2 & \dots 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{\nu-1} & s_{\nu-2} & s_{\nu-3} & \dots s_1 & \nu-1 \\ s_\nu & s_{\nu-1} & s_{\nu-2} & \dots s_2 & s_1 \end{vmatrix}.$$

In Verallgemeinerung der Potenzsummen s_ν kann man die symmetrische Funktion

$$\sum \varphi(\alpha_1) = \varphi(\alpha_1) + \varphi(\alpha_2) + \cdots + \varphi(\alpha_n)$$

betrachten, wobei $\varphi(z)$ irgendeine ganze rationale Funktion von z bedeutet und $\alpha_1, \alpha_2, \dots, \alpha_n$ die Wurzeln der vorgelegten Gleichung $f(z) = 0$ des n^{ten} Grades sind. $\sum \varphi(\alpha_1)$ ist der Koeffizient von z^{-1} bei der Entwicklung $\frac{f'(z)}{f(z)}\varphi(z)$ nach fallenden Potenzen von z, wobei $f'(z)$ die erste Abgeleitete von $f(z)$ ist. (Cauchy, *Exercices de math.* **1** (1826), *Œuvres* (2) **6**, 401.) Wie $\frac{f'(z)}{f(z)}\varphi(z)$ eine erzeugende Funktion für die symmetrische Funktion $\sum\varphi(\alpha_1)$ ist, haben Borchardt, *Monatsb. d. Berl. Akad.* (1855), 165, *Ges. Werke*, Berlin 1888, S. 99 und Kronecker, *Monatsb. d. Berl. Akad.* (1880), 936 die typischen symmetrischen Funktionen der Gleichungswurzeln als Entwicklungskoeffizienten einer erzeugenden Funktion dargestellt.

Die symmetrischen Funktionen genügen gewissen partiellen Differentialgleichungen; vgl. Faà di Bruno, *Binäre Formen*, Leipzig 1881, S. 18, Netto, *Algebra* **1**, 133.

Tabellen, welche alle symmetrischen Funktionen der Wurzeln bis zum zehnten Grade für eine beliebige algebraische Gleichung enthalten, findet man bereits in Meyer Hirschs *Sammlung von Beispielen, Formeln u. Aufgaben aus der Buchstabenrechnung u. Algebra* (1804), des weiteren bei Cayley, *Coll. math. papers* **2**, 417 (ebenda in den Notes, S. 602 zahlreiche Literatur), Faà di Bruno, *Binäre Formen*, S. 302, Kostka, *Math.-Ver.* **16**, 429 (1907).

§ 6. Resultante und Diskriminante.

Zwei Gleichungen:

$$f(z) \equiv a_0 z^m + a_1 z^{m-1} + a_2 z^{m-2} + \cdots + a_m = 0,$$
$$g(z) \equiv b_0 z^n + b_1 z^{n-1} + b_2 z^{n-2} + \cdots + b_n = 0$$

haben dann und nur dann wenigstens eine gemeinsame Wurzel, wenn eine gewisse ganze rationale Funktion der Koeffizienten, welche die *Resultante der zwei Gleichungen* heißt, verschwindet. Da die charakteristische Bedingung für das Vorhandensein einer gemeinsamen Wurzel von $f(z) = 0$ und $g(z) = 0$ die Existenz eines gemeinsamen Teilers von $f(z)$ und $g(z)$ ist, kann man auch sagen: *Das Verschwinden der Resultante ist die notwendige und hinreichende Bedingung dafür, daß $f(z)$ und $g(z)$ einen gemeinsamen Teiler besitzen.* Auf Grund der letzten Aussage kann man die Resultante auch ohne Voraussetzung der Wurzelexistenz definieren und beim Beweise des Fundamentalsatzes der Algebra verwerten. Vgl. den Gauß-Gordanschen Beweis des Fundamentalsatzes der Algebra (Gauß, *Zweiter Beweis des Fundamentalsatzes*, Gordan, *Math. Ann.* **10**, 572 (1876), *Vorl. über Invariantentheorie*, **1**, 166).

Die Resultante R_{fg} läßt sich aus einem System von $m+n$ linearen homogenen Gleichungen als Determinante $(m+n)^{\text{ten}}$ Grades finden, nämlich

$$R_{fg} = \left|\begin{array}{ccccc}
a_0 & a_1 & a_2 \dots a_m & 0 & 0 \dots\dots 0 \\
0 & a_0 & a_1 \dots a_{m-1} & a_m & 0 \dots\dots 0 \\
0 & 0 & a_0 \dots a_{m-2} & a_{m-1} & a_m \dots 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \dots\dots\dots & \dots\dots & \dots\dots a_m \\
b_0 & b_1 & b_2 \dots b_n & 0 & 0 \dots\dots 0 \\
0 & b_0 & b_1 \dots b_{n-1} & b_n & 0 \dots\dots 0 \\
\vdots & & & & \\
0 & 0 & 0 \dots\dots\dots & \dots\dots & \dots\dots b_n
\end{array}\right|
\begin{array}{l}
\left.\vphantom{\begin{array}{c}1\\1\\1\\1\\1\end{array}}\right\} n \text{ Zeilen} \\
\left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} m \text{ Zeilen}
\end{array}$$

Die fraglichen linearen Gleichungen ergeben sich

a) durch das Verfahren von Euler (*Introductio in analysin infinitorum,* Lausanne 1748, t. **2**, Cap. 19, p. 265), das übrigens schon auf Leibniz (*Ges. Werke,* herausg. von Pertz, 3. Folge: *Math.*, herausg. von Gerhardt, Halle 1863, Bd. 7, S. 6) zurückgeht. Man stellt die Bedingung dafür auf, daß zwei ganze Funktionen $F(z)$ und $G(z)$ vom Grade $\leqq m-1$ bezw. $\leqq n-1$ existieren und $fG+gF$ identisch verschwindet (vgl. S. 259). Eine Transposition der sich ergebenden linearen homogenen Gleichungen führt zu dem linearen homogenen System mit der Determinante R_{fg};

b) durch die von Sylvester sogenannte *dialytische* Methode. Diese eliminiert $1, z, z^2, \ldots, z^{n+m-1}$ aus den Gleichungen $f(z)=0$, $zf(z)=0$, $z^2f(z)=0, \ldots, z^{n-1}f(z)=0$, $g(z)=0$, $zg(z)=0, \ldots, z^{m-1}g(z)=0$ (Sylvester, *Phil. Mag.* **16**, (1840), *Cambr. Math. Journ.* **2** (1841), *Coll. math. papers* **1**, 54, 61, vgl. die Würdigung Sylvesters durch Noether, *Math. Ann.* **50**, 136 (1898)).

Die Resultante R_{fg} ist eine ganze rationale Funktion n^{ten} Grades der Koeffizienten $a_0, a_1, \ldots, a_m$ und m^{ten} Grades von $b_0, b_1, b_2, \ldots, b_n$; sie ist als Funktion der sämtlichen Größen $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n$ unzerlegbar und ferner isobar vom Gewicht mn. R_{fg} ist linear und homogen aus f und g komponierbar, *also $R_{fg}=fP+gQ$, wobei P und Q ganze Funktionen sind.*

Die Unzerlegbarkeit und die Fähigkeit der linearen homogenen Komposition aus f und g sind charakteristische Eigenschaften der Resultante (vgl. S. 273).

Für die Vertauschung von f und g gilt:

$$R_{fg}=(-1)^{mn}R_{gf}.$$

Die Resultante läßt sich auch als *symmetrische Funktion der Gleichungswurzeln* auffassen (sogenannte erste Eulersche Methode, Euler, *Histoire de l'acad. de Berlin*, année 1748, 234, Cramer, *Introduction à l'analyse des lignes courbes*, Genf 1750, 660). Es ist:

$$\begin{aligned}
R_{fg} &= a_0^n g(\alpha_1)g(\alpha_2)\ldots g(\alpha_m),\\
R_{fg} &= (-1)^{mn}\cdot b_0^m f(\beta_1)f(\beta_2)\ldots f(\beta_n),\\
R_{fg} &= a_0^n b_0^m(\alpha_1-\beta_1)(\alpha_1-\beta_2)\ldots(\alpha_1-\beta_n).\\
&\qquad\qquad (\alpha_2-\beta_1)(\alpha_2-\beta_2)\ldots(\alpha_2-\beta_n).\\
&\qquad\qquad\quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots\\
&\qquad\qquad (\alpha_m-\beta_1)(\alpha_m-\beta_2)\ldots(\alpha_m-\beta_n);
\end{aligned}$$

hierbei sind $\alpha_1, \alpha_2, \ldots, \alpha_m$ die Wurzeln der Gleichung $f(z)=0$ und $\beta_1, \beta_2, \ldots, \beta_n$ diejenigen von $g(z)=0$.

Die zwei ganzen Funktionen $f(z)$ und $g(z)$ haben dann und nur dann einen größten gemeinsamen Teiler, der genau vom k^{ten} Grade ist, wenn R_{fg}, R_1, $R_2, \ldots, R_{k-1}$ verschwinden, hingegen R_k von Null verschieden ist. R_j entsteht aus R_{fg}, indem man die j letzten Zeilen der a, die j letzten Zeilen der b und die $2j$ letzten Kolonnen streicht (vgl. Faà di Bruno, *Binäre Formen,* Leipzig 1881, S. 57, Scheibner, *Leipz. Ber.* (1888), 3, Noether, Lüroth in den *Sitzungsb. d. physik.-med. Societät in Erlangen* (1895), Lüroth, *Ztschr. f. Math. u. Phys.* **40**, 247 (1895), Heffter, *Math. Ann.* **54**, 541 (1901)).

Für $m = n$ kann R_{fg} in eine Determinante m^{ten} Grades zusammengezogen werden, nämlich:

$$R_{fg} = (-1)^{\frac{m(m+1)}{2}} \, | c_{ik} | \qquad (i, k = 0, 1, 2, \ldots, m-1).$$

Zu dieser sogen. *Bézoutschen Determinante* $| c_{ik} |$ gelangt man durch das abgekürzte Verfahren von Bézout (*Mém. Acad. de Paris* (1764), Jacobi, *Journ. f. Math.* **15**, 101 (1836), *Ges. Werke* **3**, 295, Cauchy, *Exercices d'analyse* (1840), abgedruckt *Nouvelles Annales* (2) **15**, 385 (1876)). Aus $f = a_0 z^m + a_1 z^{m-1} + \cdots + a_m$ und $g = b_0 z^m + b_1 z^{m-1} + \cdots + b_m$ bilde man sich

$$\begin{gathered}
b_0 f - a_0 g = 0, \\
(b_0 z + b_1) f - (a_0 z + a_1) g = 0, \\
(b_0 z^2 + b_1 z + b_2) f - (a_0 z^2 + a_1 z + a_2) g = 0, \\
\vdots \\
(b_0 z^{m-1} + b_1 z^{m-2} + \cdots + b_{m-1}) f - (a_0 z^{m-1} + a_1 z^{m-2} + \cdots + a_{m-1}) g = 0.
\end{gathered}$$

Die erhaltenen Gleichungen:

$$c_{i0} z^{m-1} + c_{i1} z^{m-2} + \cdots + c_{im-1} = 0 \qquad (i = 0, 1, 2, \ldots, m-1)$$

sind sämtlich vom Grade $m - 1$; durch Elimination von 1, z, $z^2, \ldots, z^{m-1}$ erhält man die Determinante $| c_{ik} |$ $(i, k = 0, 1, 2, \ldots, m-1)$. Sie ist *symmetrisch,* und es ist

$$\begin{gathered}
c_{i0} = d_{i+1,0}, \quad c_{i1} = d_{i+2,0} + d_{i+1,1}, \\
c_{i2} = d_{i+3,0} + d_{i+2,1} + d_{i+1,2}, \ldots, c_{im-1} = d_{mi},
\end{gathered}$$

wobei $d_{ik} = a_i b_k - a_k b_i$ ist.

Die Größen c_{ik} ergeben sich nach Cayley (*Journ. f. Math.* **53**, 366 (1857), *Coll. math. papers* **4**, 38) als *Entwicklungs-*

koeffizienten der scheinbar gebrochenen Funktion $\frac{f(x)g(y)-g(x)f(y)}{y-x}$ nach ganzen positiven Potenzen von x und y. Es ist

$$\frac{f(x)g(y)-f(y)g(x)}{y-x}=\sum_{i=0}^{i=m-1}\sum_{k=0}^{k=m-1} c_{ik}x^{m-k-1}y^{m-i-1}.$$

Der gefundenen ganzen rationalen Funktion kann man mit Sylvester (*Phil. Transact.* (1853), *Coll. math. papers* **1**, 430 u. 545) die quadratische Form $\sum_{i=0}^{i=m-1}\sum_{k=0}^{k=m-1} c_{ik}t_i t_k$ der m Variablen $t_0, t_1, \ldots, t_{m-1}$ zuordnen; diese heißt die *Bézoutiante von f und g.*

Notwendig und hinreichend, damit f und g einen größten gemeinsamen Divisor genau vom k^{ten} Grade haben, ist das Verschwinden der Determinanten

$$\sum \pm c_{00}c_{11}\cdots c_{m-1\,m-1}, \quad \sum \pm c_{00}c_{11}\cdots c_{m-2\,m-2}, \ldots$$
$$\sum \pm c_{00}c_{11}\cdots c_{m-k\,m-k},$$

hingegen muß $\sum \pm c_{00}c_{11}\cdots c_{m-k-1,\,m-k-1}$ von Null verschieden sein. *Die Bézoutiante von f und g hat dann genau den Rang* $m-k$.

Die voraufgehenden Betrachtungen lassen sich auch auf $m>n$ ausdehnen. Ist

$f(z)=a_0z^m+a_1z^{m-1}+\cdots+a_m$, $g(z)=b_0z^n+b_1z^{n-1}+\cdots+b_n$,

so gehe man zunächst von $f(z)$ und

$g(z)=B_0z^m+B_1z^{m-1}+\cdots+B_{m-n-1}z^{n+1}+b_0z^n+b_1z^{n-1}+\cdots+b_n$

aus und setze dann $B_0=B_1=\cdots=B_{m-n-1}=0$. Man erhält $R_{fg}=(-1)^{\frac{m(m+1)}{2}}\cdot\frac{1}{a_0^{m-n}}\left|c_{ik}\right|$ $(i, k=0, 1, \ldots, m-1)$.

Der Fall, daß f und g verschiedene Grade haben, läßt sich auch durch Betrachtung von $f(z)=0$ und $z^{m-n}g(z)=0$ auf den Fall gleichen Grades zurückführen. Die erhaltene Resultante ist durch a_m^{m-n} zu dividieren, um die wahre Resultante R_{fg} zu finden.

Will man im Fall $m>n$ bei der Resultantenbildung *keine fremden Faktoren* einführen, sondern die wahre Resultante R_{fg} erhalten, so hat man aus den zwei Funktionen

$$f(z)=a_0z^m+a_1z^{m-1}+\cdots+a_m$$

und

$$g(z)=b_0z^n+b_1z^{n-1}+\cdots+b_n$$

die n Gleichungen zu bilden: $fg_{n-s} - gf_{m-s} = 0$ $(s = n, n-1, \ldots, 1)$,

wobei $f_t = a_0 z^t + a_1 z^{t-1} + \cdots + a_t$ $(t = m - n, m - n + 1, \ldots, m-1)$,

$$g_t = b_0 z^t + b_1 z^{t-1} + \cdots + b_t \qquad (t = 0, 1, 2, \ldots, n-1)$$

ist. Für $m = n$ gehen sie in die früheren über. Für $m > n$ füge man noch $g(z) = 0$, $zg(z) = 0, \ldots, z^{m-n-1}g(z) = 0$ hinzu. Man hat dann im ganzen m Gleichungen, von denen jede höchstens vom Grade $m - 1$ ist und aus denen man $1, z, z^2, \ldots, z^{m-1}$ eliminieren kann. Diese Behandlung des Falles $m > n$ nach der Methode von Bézout, bei der die Determinante jedoch *nicht* wie im Fall $m = n$ symmetrisch ausfällt, geht auf Rosenhain, *Journ. f. Math.* **28**, 269 (1844) (Gleichungen 81 a. a. O.) zurück. Eine eingehende Darstellung bei H. Weber, *Algebra* **1**, 179.

Sowohl die Resultante als auch die im folgenden zu besprechende Diskriminante genügen gewissen *partiellen Differentialgleichungen*, die Brioschi (*Journ. f. Math.* **53**, 372 (1857)) aufgestellt hat. Vgl. die eingehende Behandlung von Noether in Faà di Bruno, *Binäre Formen*, Leipzig 1881, S. 275. Die Literatur über Resultanten findet man bei Pascal, *Determinanten,* Leipzig 1900, S. 206, sowie bei E. Netto, *Enzyklopädie d. math. Wiss.* **1**, 245 (französische Bearbeitung von Le Vavasseur, *Encycl. des sc. math.* **1**, vol. 2, p. 73 ff.). Vgl. auch das Kapitel über Invariantentheorie.

Die Untersuchung der Resultante zweier ganzer Funktionen $f(z)$ und $g(z)$ je einer Variablen ist für das folgende *allgemeinste Problem aus der Theorie der algebraischen Gleichungen* grundlegend:

Gegeben seien r ganze Funktionen $f_1(z_1, z_2, \ldots, z_p)$, $f_2(z_1, z_2, \ldots, z_p), \ldots, f_r(z_1, z_2, \ldots, z_p)$ der p Variablen $z_1, z_2, \ldots, z_p$. Man soll entscheiden, ob es Werte $z_1, z_2, \ldots, z_p$ gibt, die gleichzeitig alle Gleichungen $f_1(z_1, z_2, \ldots, z_p) = 0$, $f_2(z_1, z_2, \ldots, z_p) = 0, \ldots, f_r(z_1, z_2, \ldots, z_p) = 0$ befriedigen, und man soll, wenn es solche Werte gibt, diese bestimmen. Die Erledigung dieses Problems erfordert außer rationalen Operationen bloß die Behandlung von Gleichungen mit nur einer Unbekannten; es ist also auf den Fall $p = 1$ reduzierbar.

Sind die r Gleichungen $f_1 = 0$, $f_2 = 0, \ldots, f_r = 0$ miteinander verträglich, so heißt ein Wertsystem, das allen Gleichungen gleichzeitig genügt, eine *Wurzel* oder eine *Lösung des Gleichungssystems*.

Satz von Kronecker (*Festschrift, Journ. f. Math.* **92**, 30 (1882), *Ges. Werke* **2**, 280): *Der Gesamtinhalt eines beliebigen Systems von Gleichungen* $f_1(z_1, z_2, \ldots, z_p) = 0$, $f_2(z_1, z_2, \ldots, z_p) = 0$, $\ldots$, $f_r(z_1, z_2, \ldots, z_p) = 0$ *kann vollständig durch ein System von höchstens* $p+1$ *Gleichungen* $\varphi_1(z_1, z_2, \ldots, z_p) = 0$, $\varphi_2(z_1, z_2, \ldots, z_p) = 0, \ldots, \varphi_{p+1}(z_1, z_2, \ldots, z_p) = 0$ *ersetzt werden, so daß jede Lösung des f-Systems eine solche des φ-Systems ist und umgekehrt.* Für das Resultat, daß unter Umständen tatsächlich $p+1$ Gleichungen erforderlich sind, vgl. das von Vahlen, *Journ. f. Math.* **108**, 346 (1891) gegebene Beispiel einer algebraischen Raumkurve unseres R_3, die nur als Durchschnitt von vier Flächen darstellbar ist.

Hat man $p+1$ allgemeine Gleichungen

$$\varphi_1(z_1, z_2, \ldots, z_p) = 0,\ \varphi_2(z_1, z_2, \ldots, z_p) = 0, \ldots, \\ \varphi_{p+1}(z_1, z_2, \ldots, z_p) = 0$$

von den Graden $m_1, m_2, \ldots, m_{p+1}$ mit Koeffizienten a, so gibt es eine ganze rationale Funktion der Koeffizienten a, die *sog. Resultante* $R(a)$ *des Gleichungssystems, die bis auf einen numerischen Faktor durch folgende zwei Eigenschaften eindeutig bestimmt ist: erstens* $R(a)$ *ist eine ganze rationale unzerlegbare Form der* a, *zweitens* $R(a)$ *komponiert sich linear und homogen aus* $\varphi_1, \varphi_2, \ldots, \varphi_{p+1}$, also $R(a) = P_1\varphi_1 + P_2\varphi_2 + \cdots + P_{p+1}\varphi_{p+1}$, wobei $P_1, P_2, \ldots, P_{p+1}$ ganze Funktionen von $z_1, z_2, \ldots, z_p$ sind. Die Resultante $R(a)$ enthält das Glied $a_{11}^{M_1} a_{22}^{M_2} \ldots a_{p+1,p+1}^{M_{p+1}}$, wobei $M_i = \frac{M}{m_i}$ $(i = 1, 2, \ldots, p+1)$, $M = m_1 m_2 \ldots m_{p+1}$ und a_{ii} $(i = 1, 2, \ldots, p)$ der Koeffizient von $z_i^{m_i}$ in $\varphi_i(z_1, z_2, \ldots, z_p)$, $a_{p+1,p+1}$ das konstante Glied in $\varphi_{p+1}(z_1, z_2, \ldots, z_p)$ ist; legt man dem Glied $a_{11}^{M_1} a_{22}^{M_2} \ldots a_{p+1,p+1}^{M_{p+1}}$ den Koeffizienten $+1$ bei, so ist die Resultante $R(a)$ eindeutig bestimmt.

Die Resultante $R(a)$ *ist eine homogene Funktion* M_i^{ten} *Grades der Koeffizientenreihe* a *von* φ_i, also eine homogene Funktion $\left(\sum_{i=1}^{i=p+1} M_i\right)^{\text{ten}}$ Grades aller Koeffizienten a. Die Resultante $R(a)$ ist eine *isobare Funktion des Gewichtes* M, dabei ist als Gewicht eines jeden Koeffizienten a aus φ_i die Zahl $m_i - s$ zu nehmen, wobei s die Summe aller Exponenten von $z_1, z_2, \ldots, z_p$ bedeutet, mit denen das betreffende a in der Funktion φ_i multipliziert ist.

Aus dem Theorem über das Gewicht ergibt sich der *Satz von Bézout* (*Théorie des équations algébriques*, Paris 1779): *Sind* $p+1$ *allgemeine Gleichungen* $\varphi_1(z_1, z_2, \ldots, z_{p+1}) = 0$, $\varphi_2(z_1, z_2, \ldots, z_{p+1}) = 0, \ldots, \varphi_{p+1}(z_1, z_2, \ldots, z_{p+1}) = 0$ *mit* $p+1$ *Unbekannten von den Graden* m_1 *bezw.* $m_2, \ldots, m_{p+1}$ *gegeben, so haben sie* $m_1 \cdot m_2 \cdots m_{p+1}$ *Lösungen.*

Als Literatur über die hier nur kurz angeschnittenen Fragen vgl.: Kronecker, *Festschrift, Journ. f. Math.* **92**, 1 (1882), *Ges. Werke* **2**, 237, Mertens, *Sitzungsb. der Wiener Akad.* **93**, Abt. 2, 527 (1886), **108**, Abt. 2a, 1173 u. 1344 (1899), Macaulay, *Proc. Lond. M. S.* **35**, 3 (1903), Netto, *Algebra* **2**, 1—203, sowie besonders Julius König, *Einleitung in die allgemeine Theorie der algebraischen Größen*, Leipzig 1903.

Bildet man von einer ganzen Funktion

$$f(z) = a_0 z^m + a_1 z^{m-1} + \cdots + a_m$$

und ihrer ersten Abgeleiteten

$$f'(z) = m a_0 z^{m-1} + (m-1) a_1 z^{m-2} + \cdots + a_{m-1}$$

die Resultante

$$R_{ff'} = \begin{vmatrix} a_0 & a_1 & a_2 & \ldots a_m & 0 & \ldots 0 \\ 0 & a_0 & a_1 & \ldots a_{m-1} & a_m & \ldots 0 \\ \vdots & & & & & \\ 0 & 0 & 0 \ldots & \ldots & \ldots & a_m \\ m a_0 & (m-1) a_1 & (m-2) a_2 & \ldots a_{m-1} & 0 & \ldots 0 \\ 0 & m a_0 & (m-1) a_1 & \ldots 2 a_{m-2} & a_{m-1} & \ldots 0 \\ \vdots & & & & & \\ 0 & 0 & 0 \ldots & \ldots & \ldots & a_{m-1} \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} m-1 \text{ Ze} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} m \text{ Zeilen} \end{matrix}$$

so ist diese offenbar durch a_0 teilbar. $D = \frac{1}{a_0} (-1)^{\frac{m(m-1)}{2}} R_{ff'}$ heißt nach Sylvester (*Phil. Mag.* **2** (1851), 406, *Coll. math. papers* **1**, 280) die *Diskriminante* der algebraischen Gleichung $f(z) = 0$. Gauß (*Ges. Werke* **3**, 38) wendet hierfür die Bezeichnung „Determinante von $f(z)$“ an.

Hat $f(z) = 0$ die m Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_m$, so ist:

$$D = (-1)^{\frac{m(m-1)}{2}} a_0^{m-2} f'(\alpha_1) f'(\alpha_2) \ldots f'(\alpha_m),$$

$$D = a_0^{2m-2} \begin{vmatrix} 1 & 1 & \ldots 1 \\ \alpha_1 & \alpha_2 & \ldots \alpha_m \\ \alpha_1^2 & \alpha_2^2 & \ldots \alpha_m^2 \\ \vdots & \vdots & \vdots \\ \alpha_1^{m-1} & \alpha_2^{m-1} & \ldots \alpha_m^{m-1} \end{vmatrix}^2$$

$$= a_0^{2m-2} \Delta(\alpha_1, \alpha_2, \ldots, \alpha_m)^2,$$

wobei $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_m)$ das Differenzenprodukt der Gleichungswurzeln bedeutet (vgl. S. 68 unten und 69 oben).

Setzt man $s_\nu = \alpha_1^\nu + \alpha_2^\nu + \cdots + \alpha_m^\nu$, ist also s_ν die Summe der ν^{ten} Potenzen der Gleichungswurzeln, so wird D durch eine rekurrierende Determinante (vgl. S. 67) gegeben:

$$D = a_0^{2m-2} \begin{vmatrix} s_0 & s_1 & \ldots s_{m-1} \\ s_1 & s_2 & \ldots s_m \\ s_2 & s_3 & \ldots s_{m+1} \\ \vdots & \vdots & \vdots \\ s_{m-1} & s_m & \ldots s_{2m-2} \end{vmatrix}.$$

Die Diskriminamte D ist eine ganze homogene Funktion der Gleichungskoeffizientem $a_0, a_1, \ldots, a_m$ vom Grade $2m-2$; sie ist eine unzerlegbare Funktion der Koeffizienten, und ferner ist sie in ihnen isobar vom Gewicht $m(m-1)$. Das Verschwinden der Diskriminante ist die notwendige und hinreichende Bedingung dafür, daß die Gleichung $f(z) = 0$ wenigstens zwei gleiche Wurzeln besitzt.

Sei D_ν die rekurrierende Determinante:

$$\begin{vmatrix} s_0 & s_1 & \ldots s_{\nu-1} \\ s_1 & s_2 & \ldots s_\nu \\ \vdots & \vdots & \vdots \\ s_{\nu-1} & s_\nu & \ldots s_{2\nu-2} \end{vmatrix},$$

so gilt folgender Satz: *Die Gleichung $f(z) = 0$ hat dann und* *nur dann genau k untereinander verschiedene Wurzeln, wenn die Determinanten* $D_{k+1}, D_{k+2}, \ldots, D_m = \frac{D}{a_0^{2m-2}}$ *verschwinden, hingegen* D_k *von Null verschieden ist.* (Borchardt, *Journ. de math.* **12** (1847), *Ges. Werke*, Berlin 1888, S. 24, L. Baur, *Math. Ann.* **50**, 241 (1898).)

Bei einer Gleichung mit reellen Koeffizienten ohne mehrfache Wurzeln besitzt die Diskriminante positives oder negatives Vorzeichen, je nachdem die Gleichung eine gerade oder ungerade Anzahl von Paaren konjugiert imaginärer Wurzeln hat. (A. Brill, *Math. Ann.* **12**, 87 (1877).)

Deutet man bei einer Gleichung mit reellen Koeffizienten $a_0, a_1, \ldots, a_m$ diese als homogene Koordinaten im R_m, so heißt $D(a_0, a_1, \ldots, a_m) = 0$ die *Diskriminantenfläche.* Der Name stammt von Kronecker, *Monatsb. d. Berl. Akad.* (1878), 120, *Ges. Werke* **2**, 68. Vgl. ferner Hilbert, *Math. Ann.* **30**, 437 (1887).

Ebenso wie die Resultante ist auch die Diskriminante auf Gleichungssysteme erweitert worden. Vgl. die bei der Resultante von Gleichungssystemen zitierte Literatur auf S. 274.

§ 7. Transformation einer Gleichung. Tschirnhausentransformation. Mit der Tschirnhausentransformation zusammenhängende Normalformen. Funktionen mehrerer Wurzeln. Gleichung der quadrierten Wurzeldifferenzen.

Ersetzt man in der Gleichung

$$f(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n = 0$$

mit den Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Größe z durch $t + h$, so hat die neue Gleichung n^{ten} Grades in t:

$$\frac{t^n f^{(n)}(h)}{n!} + \frac{t^{n-1} f^{(n-1)}(h)}{(n-1)!} + \cdots + f(h) = 0$$

die n Wurzeln $\alpha_1 - h, \alpha_2 - h, \ldots, \alpha_n - h$. Hierbei bedeutet $f^{(i)}(h)$ die i^{te} Abgeleitete von $f(h) = a_0 h^n + a_1 h^{n-1} + \cdots + a_n$.

Wählt man für h einen derartigen Wert, daß

$$\frac{f^{(n-1)}(h)}{(n-1)!} = n a_0 h + a_1$$

verschwindet, also $h = \frac{-a_1}{n a_0}$, *so fehlt der Gleichung in t ihr zweites Glied.*

Die Transformation $t = z - h$ ist nur ein Spezialfall der sog. *Tschirnhausentransformation* (vgl. S. 252). Unter dieser versteht man folgendes: t sei eine ganze rationale Funktion von z:

$$t = \varphi(z) = p_0 + p_1 z + p_2 z^2 + \cdots + p_{n-1} z^{n-1}.$$

Man soll die Gleichung in t aufstellen, welche die Wurzeln $t_1 = \varphi(\alpha_1)$, $t_2 = \varphi(\alpha_2), \ldots, t_n = \varphi(\alpha_n)$ besitzt, wenn $f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$ die Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ hat.[1]) Die Größen $t_i = \varphi(\alpha_i)$ $(i = 1, 2, \ldots, n)$ genügen der Gleichung

$$\begin{aligned}\Phi(t) &= (t - t_1)(t - t_2) \ldots (t - t_n) = \\ &= t^n + q_1 t^{n-1} + q_2 t^{n-2} + \cdots + q_n = 0.\end{aligned}$$

Die Größen q_i $(i = 1, 2, \ldots, n)$ sind ganze homogene Funktionen i^{ten} Grades von $p_0, p_1, \ldots, p_{n-1}$, deren Koeffizienten ganze Funktionen von $\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, \frac{a_n}{a_0}$ sind. Die Gleichung $\Phi(t) = 0$ heißt eine *Tschirnhausenresolvente von* $f(z) = 0$. Man kann $q_1, q_2, \ldots, q_n$ auf folgende Weise finden: Man bilde sich durch sukzessive Potenzierung die Gleichungskette:

$$\begin{aligned}t &= p_0 + p_1 z + p_2 z^2 + \cdots + p_{n-1} z^{n-1}, \\ t^2 &= p_0' + p_1' z + p_2' z^2 + \cdots + p_{n-1}' z^{n-1}, \\ t^3 &= p_0'' + p_1'' z + p_2'' z^2 + \cdots + p_{n-1}'' z^{n-1}, \\ &\vdots \\ t^n &= p_0^{(n-1)} + p_1^{(n-1)} z + p_2^{(n-1)} z^2 + \cdots + p_{n-1}^{(n-1)} z^{n-1},\end{aligned}$$

wobei die höheren als n^{ten} Potenzen von z mit Hilfe der Gleichung $f(z) = 0$ beseitigt sind. Setzt man $\sigma_i = t_1^i + t_2^i + \cdots + t_n^i$ und $s_i = \alpha_1^i + \alpha_2^i + \cdots + \alpha_n^i$, so ist:

$$\sigma_i = n p_0^{(i-1)} + p_1^{(i-1)} s_1 + p_2^{(i-1)} s_2 + \cdots + p_{n-1}^{(i-1)} s_{n-1}$$
$$(i = 1, 2, \ldots, n).$$

Aus den Potenzsummen $\sigma_1, \sigma_2, \ldots, \sigma_n$ lassen sich die Koeffizienten $q_1, q_2, \ldots, q_n$ der Gleichung $\Phi(t) = 0$ bestimmen. (Vgl. S. 266.) Die Gleichung $\Phi(t) = 0$ ist das Eliminationsresultat von z aus $f(z) = 0$ und $t - \varphi(z) = 0$. Sind $t_1, t_2, \ldots, t_n$

1) Die Aufstellung einer Gleichung für $\varphi(\alpha_1)$, wobei $\varphi(\alpha_1)$ voraussetzungsgemäß eine ganze rationale Funktion von α_1, die höchstens vom Grade $n - 1$ ist, bedeutet, involviert keine Beschränkung; denn man kann jede ganze oder gebrochene rationale Funktion einer Wurzel α_1 der Gleichung $f(z) = 0$ in eine ganze rationale Funktion von α_1 verwandeln, die höchstens vom Grade $n - 1$ ist.

untereinander verschieden, so ergeben sich die zugehörigen $\alpha_1, \alpha_2, \ldots, \alpha_n$ aus linearen Gleichungen. Ist $t_1 = \varphi(\alpha_1) = \varphi(\alpha_2) = \cdots = \varphi(\alpha_e)$, also t_1 eine e-fache Wurzel von $\Phi(t) = 0$, so haben die zwei Gleichungen $f(z) = 0$ und $t_1 - \varphi(z) = 0$ die e Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_e$ gemeinsam, die man demnach aus einer Gleichung e^{ten} Grades finden kann. Hat $f(z) = 0$ lauter verschiedene Wurzeln, so muß $e < n$ sein. Hieraus folgt: *Kann man eine Tschirnhausenresolvente $\Phi(t) = 0$ von $f(z) = 0$ auflösen, so ist $f(z) = 0$ hierdurch entweder vollständig gelöst oder seine Behandlung auf Gleichungen niedrigeren Grades zurückgeführt.*

Durch geeignete Wahl der Größen $p_0, p_1, \ldots, p_{n-1}$ kann man aus $f(z) = 0$ eine *Tschirnhausenresolvente $\Phi(t) = 0$ von einfacherer Struktur als* $f(z) = 0$ ableiten.

Setzt man bei der *Gleichung dritten Grades*

$$a_0 z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

$t = p_0 + p_1 z + p_2 z^2$ und wählt das Verhältnis $p_0 : p_1 : p_2$ aus den zwei Gleichungen $q_1 = 0$, $q_2 = 0$, von denen die erste linear, die zweite quadratisch ist, so erhält man als Tschirnhausenresolvente die reine Gleichung $t^3 + q_3 = 0$.

Die *Gleichung vierten Grades*

$$a_0 z^4 + a_1 z^3 + a_2 z^2 + a_3 z + a_4 = 0$$

wird durch die Tschirnhausentransformation: $t = p_0 + p_1 z + p_2 z^2 + p_3 z^3$ gelöst, indem man p_0, p_1, p_2, p_3 derartig bestimmt, daß die zwei Gleichungen $q_1 = 0$ und $q_3 = 0$ vom ersten und dritten Grade bestehen. Die Tschirnhausenresolvente $t^4 + q_2 t^2 + q_4 = 0$ ist dann durch Quadratwurzeln lösbar.

Für die allgemeinen Gleichungen höheren als vierten Grades kann die Tschirnhausentransformation keine Auflösungsmethoden, sondern nur *Normalformen* liefern. Bestimmt man in $t = p_0 + p_1 z + p_2 z^2 + \cdots + p_{n-1} z^{n-1}$ die Größen p so, daß die Gleichungen $q_1 = 0$ und $q_2 = 0$ vom ersten und zweiten Grade bestehen, so erfordert dies außer rationalen Operationen nur das Ziehen einer Quadratwurzel. Die alsdann aus

$$a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

hervorgehende Gleichung

$$t^n + q_3 t^{n-3} + q_4 t^{n-4} + \cdots + q_n = 0$$

heißt eine *Hauptgleichung.* Als *Hauptgleichung* bezeichnet man jede Gleichung n^{ten} Grades, in der keine Glieder mit der $(n-1)^{\text{ten}}$ und $(n-2)^{\text{ten}}$ Potenz der Unbekannten auftreten. (Klein, *Ikosaeder,* S. 142.)

Wählt man die Größen p derartig, daß gleichzeitig die drei Gleichungen ersten, zweiten und dritten Grades $q_1 = 0$, $q_2 = 0$, $q_3 = 0$ bestehen, so führt dies auf eine Gleichung sechsten Grades. Durch geeignete Verfügung über die p kann diese Gleichung sechsten Grades mit Hilfe von Quadratwurzeln auf eine kubische Gleichung zurückgeführt werden. Im besonderen läßt sich jede *Gleichung fünften Grades durch Ziehen von Quadratwurzeln und Auflösung einer kubischen Gleichung in die sog. Bring-Jerrardsche Normalform* $t^5 + q_4 t + q_5 = 0$ bringen. Setzt man $t = u\sqrt[4]{q_4}$, so erhält man eine Normalform $u^5 - u - A = 0$ mit nur einem Parameter. (Vgl. S. 254, sowie die Darstellung bei Weber, *Algebra* **1**, 260, ferner Rahts, *Math. Ann.* **28**, 34 (1887).)

Hat man eine Gleichung n^{ten} Grades

$$a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

und wählt:

$$\begin{aligned}
p_0 &= a_0 u_1 + a_1 u_2 + a_2 u_3 + \cdots + a_{n-1} u_n,\\
p_1 &= \qquad\quad a_0 u_2 + a_1 u_3 + \cdots + a_{n-2} u_n,\\
p_2 &= \qquad\qquad\qquad a_0 u_3 + \cdots + a_{n-3} u_n,\\
&\vdots\\
p_{n-1} &= \qquad\qquad\qquad\qquad\qquad\quad a_0 u_n,
\end{aligned}$$

wobei $u_1, u_2, \ldots, u_n$ Unbestimmte sind, so geht

$$t = p_0 + p_1 z + p_2 z^2 + \cdots + p_{n-1} z^{n-1}$$

über in

$$\begin{aligned}
t = a_0 u_1 + (a_0 z + a_1) u_2 + (a_0 z^2 + a_1 z + a_2) u_3 + \cdots +\\
+ (a_0 z^{n-1} + a_1 z^{n-2} + \cdots + a_{n-1}) u_n
\end{aligned}$$

und stellt, da $a_0 \neq 0$ ist, die allgemeinste ganze Funktion $(n-1)^{\text{ten}}$ Grades von z dar. Der Koeffizient von u_i ist der Faktor von u^{n-i} in der Entwicklung von $\frac{f(u) - f(z)}{u - z}$ nach ganzen positiven Potenzen von u. Bildet man sich die ganze Funktion von u:

$$\frac{f(u) - f(z)}{u - z} - \frac{1}{n} f'(u) = u^{n-2} F_0(z) + u^{n-3} F_1(z) + \cdots + F_{n-2}(z),$$

wobei $f'(u)$ die erste Abgeleitete von $f(u)$ ist, und wählt $t = u_2 F_0(z) + u_3 F_1(z) + \cdots + u_n F_{n-2}(z)$, so sind die Koeffizienten der Tschirnhausenresolvente $\Phi(t) = 0$ simultane Invarianten der zwei Funktionen $f(z)$ und

$$G(z) = u_2 - (n-2) u_3 z + \binom{n-2}{2} u_4 z^2 - \cdots \pm u_n z^{n-2}.$$

(Hermite, *C. R.* **46**, 961 (1858), *Œuvres* **2**, 30, vgl. Weber, *Algebra* **1**, 240.)

Die sich nur auf eine einzige Gleichungswurzel beziehende Tschirnhausentransformation läßt sich auf *Funktionen mehrerer Gleichungswurzeln* ausdehnen: $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ sei irgendeine ganze rationale Funktion der Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ der Gleichung $f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$. *Ist* $\varphi(x_1, x_2, \ldots, x_n)$ *eine* ϱ*-wertige Funktion* (vgl. S. 217) *der Größen* $x_1, x_2, \ldots, x_n$ *und sind* $\varphi_1 = \varphi(x_1, x_2, \ldots, x_n)$, $\varphi_2(x_1, x_2, \ldots, x_n), \ldots, \varphi_\varrho(x_1, x_2, \ldots, x_n)$ *die* ϱ *mit* φ *konjugierten Funktionen, so sind* $\varphi_1(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\varphi_2(\alpha_1, \alpha_2, \ldots, \alpha_n), \ldots, \varphi_\varrho(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *die* ϱ *Wurzeln der Gleichung:*

$$\Phi(t) = (t - \varphi_1)(t - \varphi_2) \ldots (t - \varphi_\varrho) =$$
$$= t^\varrho + q_1 t^{\varrho-1} + q_2 t^{\varrho-2} + \cdots + q_\varrho = 0.$$

Die Größen $q_1, q_2, \ldots, q_\varrho$ *sind als symmetrische Funktionen der Gleichungswurzeln von* $f(z) = 0$ *ganze rationale Funktionen von* $\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, \frac{a_n}{a_0}$. Die Gleichung $\Phi(t) = 0$ heißt eine *transformierte Gleichung,* auch *Resolvente von* $f(z) = 0$. *Eine auf die angegebene Weise abgeleitete transformierte Gleichung kann bei einer Gleichung* $f(z) = 0$ *von höherem als vierten Grade, außer wenn* φ_1 *symmetrisch oder zweiwertig ist, nicht niedriger als* n^{ten} *Grades sein.* (Für die Gleichung vierten Grades vgl. § 8, vgl. ferner den Schluß des § 10.)

Von den Resolventen $\Phi(t) = 0$ sei hier noch die Gleichung für die *Quadrate der Wurzeldifferenzen einer Gleichung* $f(z) = 0$ angeführt. Mit ihr haben sich Waring (*Miscellanea analytica* (1762), *Meditationes algebraicae,* 3. ed., p. 30 (1782)) und Lagrange (1798), *Œuvres* **8**, 24 u. 140 beschäftigt. Wählt man für φ_1 die $\frac{n(n-1)}{2}$ wertige Funktion $\varphi_1 = (x_1 - x_2)^2$, so genügen die $\frac{n(n-1)}{2}$ Größen $(\alpha_i - \alpha_k)^2$ der Gleichung:

$$\Phi(t) = t^\varrho + q_1 t^{\varrho-1} + q_2 t^{\varrho-2} + \cdots + q_\varrho = 0.$$

$\left(\varrho = \frac{n(n-1)}{2}\cdot\right)$ Ist σ_i die Summe der i^{ten} Potenzen der Wurzeln dieser Gleichung und $s_i = \alpha_1^i + \alpha_2^i + \cdots + \alpha_n^i$, so ist

$$\sigma_i = n s_{2i} - (2i) s_1 s_{2i-1} + \binom{2i}{2} s_2 s_{2i-2} + \cdots + (-1)^i \binom{2i}{i} \frac{s_i s_i}{2},$$

und aus σ_i $(i=1,2,\ldots,\varrho)$ kann man $q_1, q_2, \ldots, q_\varrho$ finden (vgl. S. 266). Die Größe q_ϱ ist gleich $(-1)^\varrho \Delta^2$, wobei Δ das Differenzenprodukt der n Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ von $f(z) = 0$ ist (vgl. S. 68). Die Gleichung der quadrierten Wurzeldifferenzen hatte früher vornehmlich den Zweck, eine untere Grenze für den absoluten Betrag der Wurzeldifferenzen der Ausgangsgleichung zu finden; doch kann man dies nach Cauchy (*Analyse algébrique* (1821), Note III, *Œuvres* (2) **3**, 398), ohne die Gleichung selbst aufzustellen. Ist nämlich g eine obere Grenze für die Wurzeln von $f(z) = 0$, d. h. sind alle Wurzeln von $f(z) = 0$ absolut genommen kleiner als eine positive Größe g, so ist der absolute Betrag

$$|\alpha_i - \alpha_k| > \frac{|\Delta|}{(2g)^{\frac{n(n-1)}{2} - 1}},$$

wobei $|\Delta|$ der absolute Betrag des Differenzenproduktes der n Wurzeln von $f(z) = 0$ ist.

§ 8. Die kubische und die biquadratische Gleichung. Reziproke Gleichungen.

Die *kubische Gleichung:*

(1) $$a_0 z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

transformiert sich durch $z = t - \frac{a_1}{3a_0}$ in

$$a_0 t^3 + b_2 t + b_3 = 0.$$

Setzt man

$$p = \frac{b_2}{a_0} = \frac{3a_2 a_0 - a_1^2}{3a_0^2},$$

$$q = \frac{b_3}{a_0} = \frac{-9a_0 a_1 a_2 + 2a_1^3 + 27a_0^2 a_3}{27a_0^3},$$

so wird die Auflösung jeder kubischen Gleichung (1) auf die von (2): $t^3 + pt + q = 0$ zurückgeführt. Ist ε eine beliebige der zwei primitiven dritten Einheitswurzeln $-\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$, so lauten die drei Wurzeln der Gleichung (2):

$$t_1 = u + v,$$
$$t_2 = u\varepsilon + v\varepsilon^2,$$
$$t_3 = u\varepsilon^2 + v\varepsilon;$$

hierbei bedeutet u einen beliebigen der drei Werte von

$$\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$

die Größe v ist gleich $\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$, jedoch darf für v nicht willkürlich einer der drei Werte der dritten Wurzel gewählt werden, sondern es ist derjenige zu nehmen, der durch $v = -\frac{p}{3u}$ bestimmt ist. Die Lösung

$$t_1 = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

heißt die *Cardanische Formel.*

Die erste Auflösung der kubischen Gleichung stammt von Scipione del Ferro. Nach Cardanos *Artis magnae sive de regulis algebraicis liber unus* (1545) fand er sie im Jahre 1515 und teilte sie dem Floridus mit. In einem wissenschaftlichen Wettstreit stellte letzterer dem Nicolo Tartaglia im Jahre 1535 dreißig Aufgaben, die sämtlich auf kubische Gleichungen hinausliefen und die diesen zu einer erneuten Auffindung der Lösung der kubischen Gleichung führten. Von Tartaglia erfuhr Cardano die Lösung und machte sie gegen den Willen des Tartaglia in seiner *Ars magna* öffentlich bekannt. Cardano lehrte auch die Beseitigung des zweiten Gliedes aus einer allgemeinen kubischen Gleichung (vgl. Cantor, *Geschichte der Math.* **2**, 484, Zeuthen, *Geschichte der Math. im 16. und 17. Jahrhundert, Abh. zur Geschichte der Math.* **17**, Leipzig 1903, S. 81, Eneström, *Bibl. math.* (3) **7**, 38 (1906)).

Ist $\frac{q^2}{4}+\frac{p^3}{27} = 0$, so hat die Gleichung die drei Wurzeln

$$t_1 = 2\sqrt[3]{-\frac{q}{2}}, \quad t_2 = t_3 = -\sqrt[3]{-\frac{q}{2}}.$$

Sind *p und q reelle Größen,* so hat die Gleichung $t^3 + pt + q = 0$, falls

a) $\frac{q^2}{4} + \frac{p^3}{27} > 0$ ist, eine reelle und zwei konjugiert imaginäre Wurzeln. Wählt man für u die reelle Wurzel und demnach auch $v = -\frac{p}{3u}$ reell, so ist t_1 die reelle Wurzel.

b) Ist $\frac{q^2}{4} + \frac{p^3}{27} = 0$, so sind sowohl die einfache Wurzel t_1 als auch die Doppelwurzel t_2 reell.

c) Ist $\frac{q^2}{4} + \frac{p^3}{27} < 0$, so sind alle drei Wurzeln reell. Die obigen Formeln haben dann den Übelstand, die reellen Wurzeln auf imaginäre Weise zu liefern. Man bezeichnet den Fall c) von alters her als *casus irreducibilis,* ohne daß die Bezeichnung etwas mit irreduzibler Gleichung (§ 9) zu tun hätte. Der Fall c) erwies sich insofern nicht reduzibel, als der Satz gilt: *Für die allgemeine Gleichung dritten Grades mit reellen Koeffizienten und drei reellen Wurzeln kann es keine Lösungsform geben, welche die Wurzeln nur mittels reeller Radikale liefert* (Mollame, *Nap. Rendiconti* (2) **4**, 167 (1890), Hölder, *Math. Ann.* **38**, 307 (1891), Kneser, ebenda **41**, 344 (1893)).

Der Fall c) läßt sich ohne Durchgang durch das Imaginäre mit Hilfe der *trigonometrischen Funktionen* erledigen. Ist $\frac{q^2}{4} + \frac{p^3}{27} < 0$, so muß $p = -P$ sein, wobei P eine positive Größe ist. Definiert man: $\cos\varphi = -\frac{q}{2 \cdot \frac{P}{3} \cdot \sqrt{\frac{P}{3}}}$, wobei φ durch passende Wahl des Vorzeichens von $\sqrt{\frac{P}{3}}$ im ersten Quadranten genommen werden kann, so sind:

$$t_1 = 2\sqrt{\frac{P}{3}} \cos\frac{\varphi}{3}, \quad t_2 = 2\sqrt{\frac{P}{3}} \cos\frac{\varphi + 2\pi}{3},$$

$$t_3 = 2\sqrt{\frac{P}{3}} \cos\frac{\varphi + 4\pi}{3}$$

die drei reellen Wurzeln der Gleichung $t^3 - Pt + q = 0$. Der Kern dieser von Vieta (*Supplementum geometriae* (1593), *De aequationum recognitione et emendatione* (1615)) stammenden Methode basiert auf der trigonometrischen Relation

$$\cos^3\left(\frac{\varphi}{3}\right) - \frac{3}{4}\cos\left(\frac{\varphi}{3}\right) - \frac{\cos\varphi}{4} = 0.$$

Besonders interessant ist Lagranges (*Réflexions sur la ré-*

solution algébrique des équations (1770), *Œuvres* **3**, 217) Lösung der kubischen Gleichung. Sie beruht auf gruppentheoretischer Grundlage. Sei:

$$z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

die gegebene Gleichung mit den Wurzeln α_1, α_2, α_3, so ist $(\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3)^3$ eine zweiwertige Funktion der Wurzeln, wenn ε eine beliebige der zwei dritten Einheitswurzeln $-\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$ ist. Die angegebene zweiwertige Funktion genügt der *quadratischen Resolvente:*

$$T^2 - (9a_1a_2 - 2a_1^3 - 27a_3)T + (a_1^2 - 3a_2)^3 = 0$$

mit den zwei Wurzeln:

$$(\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3)^3 = \frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) + \frac{3i}{2}\sqrt{3D},$$

$$(\alpha_1 + \varepsilon^2\alpha_2 + \varepsilon\alpha_3)^3 = \frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) - \frac{3i}{2}\sqrt{3D}.$$

Beachtet man, daß $\alpha_1 + \alpha_2 + \alpha_3 = -a_1$ ist, so findet man:

$$3\alpha_1 = -a_1 + \sqrt[3]{\frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) + \frac{3i}{2}\sqrt{3D}} + \sqrt[3]{\frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) - \frac{3i}{2}\sqrt{3D}},$$

$$3\alpha_2 = -a_1 + \varepsilon^2\sqrt[3]{\frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) + \frac{3i}{2}\sqrt{3D}} + \varepsilon\sqrt[3]{\frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) - \frac{3i}{2}\sqrt{3D}},$$

$$3\alpha_3 = -a_1 + \varepsilon\sqrt[3]{\frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) + \frac{3i}{2}\sqrt{3D}} + \varepsilon^2\sqrt[3]{\frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) - \frac{3i}{2}\sqrt{3D}}.$$

D hat den Wert $a_1^2a_2^2 - 27a_3^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3$ und ist die *Diskriminante* von $z^3 + a_1z^2 + a_2z + a_3 = 0$ oder die durch -27 dividierte Diskriminante der quadratischen Resolvente. Von den bei der Lösung der kubischen Gleichung auftretenden zwei dritten Wurzeln ist nur eine willkürlich, weil ihr Produkt $(\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3)(\alpha_1 + \varepsilon^2\alpha_2 + \varepsilon\alpha_3) = a_1^2 - 3a_2$ ist.

Vom Standpunkt der Galoisschen Theorie kann man sagen: Die Galoissche Gruppe der allgemeinen Gleichung dritten

Grades ist die symmetrische Gruppe dritten Grades, also eine Gruppe der Ordnung 6. Nach Adjunktion von $\sqrt{D}$, also der Quadratwurzel aus der Diskriminante, wird sie die alternierende Gruppe dritten Grades von der Ordnung 3, und die Gleichung wird in dem durch Adjunktion von $\sqrt{D}$ erweiterten Körper eine einfache Abelsche Gleichung. Mithin ist alsdann zur vollständigen Lösung einer kubischen Gleichung nach der allgemeinen Theorie der Abelschen Gleichungen außer der Kenntnis der dritten Einheitswurzeln nur noch das Ziehen einer einzigen dritten Wurzel erforderlich. Dies zeigt auch die oben für die Gleichung dritten Grades gegebene Lösung, wenn man die Relation

$$\frac{3i}{2}\sqrt{3D} = +\frac{3}{2}(\varepsilon - \varepsilon^2)\sqrt{D}$$

beachtet und bedenkt, daß nach Kenntnis der dritten Wurzel

$$\sqrt[3]{\frac{1}{2}(9a_1a_2 - 2a_1^3 - 27a_3) + \frac{3}{2}(\varepsilon - \varepsilon^2)\sqrt{D}}$$

die andere dritte Wurzel sich als Produkt des reziproken Wertes in $a_1^2 - 3a_2$ ergibt.

Für die Lösung der kubischen Gleichung mittels invariantentheoretischer Methoden vgl. Cayley, *Coll. math. papers* **2**, 542, Faà di Bruno, *Binäre Formen*, Leipzig 1881, S. 211, Gordan, *Invariantentheorie* **2**, 175. Für die Auflösung durch Tschirnhausentransformation vgl. § 7. Für andere Methoden vgl. Matthießen, *Antike u. moderne Algebra*, Leipzig 1878, S. 362, ferner J. Lüroth, *Vorles. über numerisches Rechnen*, Leipzig 1900, S. 166, Klein in *Dycks Katalog math. Modelle*, München 1892, S. 3.

Die Gleichung *vierten Grades*, auch *biquadratische Gleichung* genannt,

$$(1) \qquad a_0z^4 + a_1z^3 + a_2z^2 + a_3z + a_4 = 0$$

transformiert sich durch $z = t - \frac{a_1}{4a_0}$ in

$$a_0t^4 + b_2t^2 + b_3t + b_4 = 0.$$

Setzt man $p = \frac{b_2}{a_0}$, $q = \frac{b_3}{a_0}$, $r = \frac{b_4}{a_0}$, so wird die Auflösung jeder Gleichung vierten Grades (1) reduziert auf

$$(2) \qquad t^4 + pt^2 + qt + r = 0.$$

Zur Lösung von (2) bedient man sich der *kubischen Resolvente*

$$(3) \qquad u^3 + \frac{p}{2} u^2 + \frac{p^2 - 4r}{16} u - \frac{q^2}{64} = 0.$$

Die Gleichung (3) habe die Wurzeln u_1, u_2, u_3, dann lauten die Wurzeln der Gleichung (2):

$$t_1 = \sqrt{u_1} + \sqrt{u_2} + \sqrt{u_3},$$
$$t_2 = \sqrt{u_1} - \sqrt{u_2} - \sqrt{u_3},$$
$$t_3 = -\sqrt{u_1} + \sqrt{u_2} - \sqrt{u_3},$$
$$t_4 = -\sqrt{u_1} - \sqrt{u_2} + \sqrt{u_3}.$$

Unter $\sqrt{u_1}$ und $\sqrt{u_2}$ sind beliebige Werte der zweideutigen Quadratwurzeln zu verstehen, hingegen ist für $\sqrt{u_3}$ derjenige Wert der Quadratwurzel zu wählen, der durch

$$\sqrt{u_3} = -\frac{q}{8\sqrt{u_1}\sqrt{u_2}}$$

bestimmt ist. Die Diskriminante D der biquadratischen Gleichung (2) ist

$$D = 16p^4 r - 4p^3 q^2 - 128 p^2 r^2 + 144 p q^2 r + 256 r^3 - 27 q^4,$$

sie ist gleich der mit 16^3 multiplizierten Diskriminante der kubischen Resolvente (3). Das Verschwinden von D bedeutet, daß die biquadratische Gleichung und ihre kubische Resolvente mehrfache Wurzeln besitzen.

Die erste Auflösung der biquadratischen Gleichung stammt von Luigi Ferrari und ist zugleich mit der Lösung der Gleichung dritten Grades von Cardano, dem Lehrer des Ferrari, in der *Ars magna* (1545) publiziert worden.

Hat die Gleichung (2) *reelle Koeffizienten* p, q, r, so ist $u_1 u_2 u_3 = \frac{q^2}{64}$ nicht negativ. Falls $q \neq 0$ ist, sind demnach drei Fälle zu unterscheiden:

a) u_1, u_2, u_3 sind positiv, die biquadratische Gleichung hat vier reelle Wurzeln.

b) u_1 ist positiv, u_2 und u_3 sind negativ, t_1 und t_2 werden konjugiert imaginär, ebenso t_3 und t_4.

c) u_1 ist positiv, u_2 und u_3 sind konjugiert imaginär, mithin werden $\sqrt{u_2}$ und $\sqrt{u_3}$ konjugiert imaginär, also t_1 und t_2 reell, t_3 und t_4 konjugiert imaginär.

Ist $q=0$, so hat die kubische Resolvente eine verschwindende Wurzel, daher die biquadratische Gleichung zwei entgegengesetzt gleiche Wurzelpaare.

Ist $D<0$, so hat die kubische Resolvente zwei konjugiert imaginäre Wurzeln, und die biquadratische Gleichung hat zwei reelle und zwei konjugiert imaginäre Wurzeln.

Ist $D>0$, so hat die kubische Resolvente drei reelle Wurzeln, und die biquadratische Gleichung hat vier reelle oder zwei Paare konjugiert imaginärer Wurzeln. Die charakteristische Bedingung dafür, daß die Gleichung $z^4+pz^2+qz+r=0$ vier reelle Wurzeln besitzt, von denen auch zwei (aber nicht mehr) untereinander gleich sein können, ist $D \geqq 0$, $p<0$, $q^2-4r>0$. Vgl. hierzu Klein, *Elementarmathematik von höherem Standpunkte aus*, Teil I, ausg. von Hellinger, Leipzig 1908, S. 220.

Lagrange (*Réflexions sur la résolution algébrique des équations, Œuvres* **3**, 266, vgl. oben S. 218) verwendet zur Auflösung der biquadratischen Gleichung:

$$z^4+a_1z^3+a_2z^2+a_3z+a_4=0$$

mit den Wurzeln α_1, α_2, α_3, α_4 die dreiwertige Funktion $(\alpha_1+\alpha_2-(\alpha_3+\alpha_4))^2$. Sie und ihre zwei konjugierten Werte $(\alpha_1+\alpha_3-(\alpha_2+\alpha_4))^2$ und $(\alpha_1+\alpha_4-(\alpha_3+\alpha_2))^2$ genügen der kubischen Resolvente:

$$(3') \qquad \begin{aligned} U^3-(3a_1^2-8a_2)U^2+(3a_1^4-16a_1^2a_2+16a_2^2+\\ +16a_1a_3-64a_4)U-(a_1^3-4a_1a_2+8a_3)^2=0. \end{aligned}$$

Bezeichnet man die Wurzeln der Gleichung (3′) mit U_1, U_2, U_3, so ist:

$$\begin{aligned} 4\alpha_1 &= -a_1+\sqrt{U_1}+\sqrt{U_2}+\sqrt{U_3}, \\ 4\alpha_2 &= -a_1+\sqrt{U_1}-\sqrt{U_2}-\sqrt{U_3}, \\ 4\alpha_3 &= -a_1-\sqrt{U_1}+\sqrt{U_2}-\sqrt{U_3}, \\ 4\alpha_4 &= -a_1-\sqrt{U_1}-\sqrt{U_2}+\sqrt{U_3}. \end{aligned}$$

Unter $\sqrt{U_1}$ und $\sqrt{U_2}$ sind beliebige Werte der zweideutigen Quadratwurzeln zu verstehen; hingegen ist für $\sqrt{U_3}$ derjenige Wert der Quadratwurzel zu wählen, der durch

$$\sqrt{U_3}=\frac{4a_1a_2-a_1^3-8a_3}{\sqrt{U_1}\sqrt{U_2}}$$

bestimmt ist; denn

$$(\alpha_1+\alpha_2-(\alpha_3+\alpha_4))\cdot(\alpha_1+\alpha_3-(\alpha_2+\alpha_4))\cdot(\alpha_1+\alpha_4-(\alpha_3+\alpha_2))$$

ist eine symmetrische Funktion der Wurzeln, die gleich $4a_1a_2 - a_1^3 - 8a_3$ ist.

Für $a_1 = 0$, $a_2 = p$, $a_3 = q$, $a_4 = r$, $U = 16u$ geht die Gleichung (3′) in (3) über.

Dasselbe wie die obige dreiwertige Funktion leistet auch die ebenfalls dreiwertige Funktion $\alpha_1\alpha_2 + \alpha_3\alpha_4$ (Lagrange, *Œuvres* **3**, 263). Verwendet man an ihrer Stelle die ebenfalls dreiwertige Funktion $\frac{a_2}{3} - \alpha_1\alpha_2 - \alpha_3\alpha_4$, so gelangt man zu der kubischen Resolvente

$$T^3 - \frac{A}{3}T + \frac{B}{27} = 0 \tag{3''}$$

mit den Wurzeln $\frac{a_2}{3} - \alpha_1\alpha_2 - \alpha_3\alpha_4$, $\frac{a_2}{3} - \alpha_1\alpha_3 - \alpha_2\alpha_4$ und $\frac{a_2}{3} - \alpha_1\alpha_4 - \alpha_2\alpha_3$. Hierbei sind

$$A = a_2^2 + 12a_4 - 3a_1a_3,$$
$$B = 27a_1^2a_4 + 27a_3^2 + 2a_2^3 - 72a_2a_4 - 9a_1a_2a_3$$

die erste und zweite Invariante der biquadratischen Gleichung:

$$z^4 + a_1z^3 + a_2z^2 + a_3z + a_4 = 0;$$

ihre Diskriminante, die gleich derjenigen der Resolventen (3′) und (3″) ist, hat den Wert $D = \frac{1}{27}(4A^3 - B^2)$. Diese Methode beruht auf invariantentheoretischer Grundlage, vgl. Cayley, *Coll. math. papers* **2**, 545, Faà di Bruno, *Binäre Formen,* S. 214, Gordan, *Invariantentheorie* **2**, 191.

Vom Standpunkt der Galoisschen Theorie kann man sagen: Die Galoissche Gruppe der allgemeinen Gleichung vierten Grades ist die symmetrische Gruppe vierten Grades, also eine Gruppe der Ordnung 24. Nach Adjunktion von $\sqrt{D}$, also der Quadratwurzel aus der Diskriminante, wird sie die alternierende Gruppe vierten Grades von der Ordnung 12. Diese hat eine invariante Untergruppe $\mathfrak{G}_4$ des Index 3 (vgl. S. 209). Eine Funktion der Wurzeln, die bei dieser Gruppe ungeändert bleibt, ist $(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$. In dem durch $\sqrt{D}$ erweiterten Körper genügt diese Funktion mit ihren in bezug auf die alternierende Gruppe konjugierten Werten $(\alpha_1 - \alpha_3)(\alpha_4 - \alpha_2)$ und $(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$ der Resolvente:

$$T^3 - AT + \sqrt{D} = 0,$$

die eine einfache Abelsche Gleichung ist und die Diskriminante B^2 besitzt. Zur Lösung dieser kubischen Normalgleichung ist die Kenntnis der dritten Einheitswurzeln und das Ziehen einer einzigen dritten Wurzel erforderlich. Ist dies geschehen, so hat die vorgelegte biquadratische Gleichung in dem erweiterten Körper die $\mathfrak{G}_4$ zur Galoisschen Gruppe. Da die $\mathfrak{G}_4$ eine invariante Untergruppe der Ordnung 2 besitzt, so hat man, um die Wurzeln der biquadratischen Gleichung zu finden, schließlich noch zwei Quadratwurzeln zu ziehen. Diese Operationen kommen auch in den anderen Lösungen zum Ausdruck; denn die kubischen Resolventen (3), (3′) und (3″) sind nach Adjunktion von $\sqrt{D}$ einfache Abelsche Gleichungen, und außer ihrer Lösung ist stets noch das Ziehen zweier Quadratwurzeln erforderlich, um die Wurzeln der vorgelegten biquadratischen Gleichung zu erhalten. — Die Auflösung der Gleichung vierten Grades läßt sich auch mit der Irrationalität des Oktaeders oder nach Adjunktion der Quadratwurzel der Diskriminante mit der Irrationalität des Tetraeders in Verbindung bringen. $\mathfrak{O}_{24}$ und $\mathfrak{T}_{12}$ sind ja mit der symmetrischen bezw. alternierenden Gruppe von vier Symbolen isomorph. (Vgl. S. 238 u. 240, sowie Klein, *Ikosaeder*, S. 126 u. Gordan, *Invariantentheorie* **2**, 213.)

Wie sich die Gleichung dritten Grades mittelst trigonometrischer Funktionen, so läßt sich die Gleichung vierten Grades mittelst elliptischer Funktionen behandeln. Hermite, *C. R.* **46**, 715, 961 (1858), *Œuvres* 2, 22 und 30; vgl. auch C. Jordan, *Traité des substitutions*, p. 370. Für andere Methoden der Auflösung der Gleichung vierten Grades vgl. Matthießen, *Antike u. moderne Algebra*, S. 540, Tortolini, *Annali di mat.* **1**, 310 (1858). Für die Auflösung durch Tschirnhausentransformation vgl. § 7.

Auf Gleichungen niedrigeren Grades lassen sich auch die von Moivre (Miscellanea analytica (1730)) zuerst untersuchten und von Euler (1732) sogenannten *reziproken Gleichungen* zurückführen. (Historisches bei Tropfke, *Geschichte der Elementarmathematik* **1**, 265). *Als reziproke Gleichungen bezeichnet man solche, welche die Eigenschaft haben, neben jeder Größe λ auch den reziproken Wert $\frac{1}{\lambda}$ zur Wurzel zu haben. Eine Gleichung $a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$ ist dann und nur dann reziprok, wenn ihre Koeffizienten so beschaffen sind, daß*

$a_i = a_{n-i}\,(i = 0, 1, 2, \ldots, \frac{n}{2} \text{ bezw. } \frac{n-1}{2})$ *oder* $a_i = -a_{n-i}\,(i = 0, 1, 2, \ldots, \frac{n}{2} \text{ bezw. } \frac{n-1}{2})$ *ist.*

Befreit man die vorgelegte reziproke Gleichung durch Division mit $z-1$ bezw. $z+1$ von den möglicherweise vorhandenen Wurzeln ± 1, so hat sie stets die Form:

$$(1)\quad b_0 z^{2\varrho} + b_1 z^{2\varrho-1} + \cdots + b_{\varrho-1} z^{\varrho+1} + b_\varrho z^\varrho + b_{\varrho-1} z^{\varrho-1} + b_{\varrho-2} z^{\varrho-2} + \cdots + b_0 =$$

Dividiert man diese reziproke Gleichung geraden Grades durch z^ϱ und setzt $z + \frac{1}{z} = Z_1$, so erhält man eine Gleichung ϱ^{ten} Grades in Z_1, nämlich:

$$(2)\qquad c_0 Z_1^\varrho + c_1 Z_1^{\varrho-1} + \cdots + c_\varrho = 0.$$

Zur Umformung dient hierbei die Rekursionsformel

$$Z_{i+1} = Z_1 Z_i - Z_{i-1} \qquad (i = 1, 2, \ldots),$$

wobei $Z_i = z^i + \frac{1}{z^i}$ $(i = 1, 2, \ldots)$ und $Z_0 = 2$ ist. Aus jeder der ϱ Wurzeln von (2) gehen zwei Wurzeln von (1) hervor; sie ergeben sich aus der quadratischen Gleichung $z^2 - z Z_1 + 1 = 0$.

§ 9. Körper. Reduzibilität und Irreduzibilität. Algebraischer Körper. Primitive und imprimitive Größen. Normalgleichung.

Unter einem *Körper, Rationalitätsbereich* oder *Feld* wird im folgenden jedes *unendliche* System von Größen verstanden, das von der Vollständigkeit ist, daß die Summe, die Differenz, das Produkt und der Quotient irgend zweier Größen des Systems immer wieder zu Größen desselben Systems führt (vgl. S. 176, wo auch endliche Körper betrachtet wurden). Jeder auf diese Weise definierte Körper enthält alle rationalen Zahlen. *Der Körper aller rationalen Zahlen ist der kleinste mögliche Körper;* er heißt der *absolute Rationalitätsbereich.* Ein Körper kann mit den rationalen Zahlen erschöpft sein oder außer ihnen noch andere Größen $R, R', \ldots$ enthalten; in letzterem Fall umfaßt der Körper seiner Definition entsprechend auch alle Größen, die aus $R, R', \ldots$ durch die vier Grundoperationen hervorgehen. Erweitert man einen Körper durch Hinzufügung einer neuen, ihm bisher nicht angehörigen Größe, so spricht man von einer *Adjunktion.*

Der Begriff des Körpers findet sich bereits bei Abel, *Œuvres* **1**, 479, **2**, 220 und Galois, *Œuvres*, p. 34. Die Bezeichnung „Körper" ist von Dedekind eingeführt worden, vgl. Dirichlet-Dedekind, *Vorlesungen über Zahlentheorie,* 4. Aufl., Braunschweig 1894, S. 452. Von Kronecker (*Fest-*

schrift, Journ. f. Math. **92**, 3 (1882), *Ges. Werke* **2**, 248) stammt die Bezeichnung „Rationalitätsbereich". Hierunter versteht er jedoch in engerer Weise als oben nur solche Körper, die aus dem absoluten Rationalitätsbereich durch Adjunktion einer endlichen Anzahl von Konstanten und Unbestimmten hervorgehen (vgl. Koenig, *Algebraische Größen,* S. 183).

Hat man eine beliebige ganze Funktion von einer oder mehreren Variablen, so ist durch ihre Koeffizienten stets ein gewisser Körper P_1 mitgegeben, nämlich der kleinste Körper, der alle Koeffizienten der Funktion enthält.

Eine ganze Funktion mit Koeffizienten aus irgendeinem Körper P[1]) heißt *in diesem Körper reduzibel,* wenn sie sich in das Produkt zweier ganzer Funktionen zerlegen läßt, von denen jede von niedrigerem Grade als die ursprüngliche Funktion ist und ebenso wie diese nur Koeffizienten aus P besitzt. Kann eine ganze Funktion mit Koeffizienten aus P nicht derartig zerlegt werden, so heißt sie *in* P *irreduzibel.* Die Reduzibilität bezw. Irreduzibilität einer ganzen Funktion hängt wesentlich von P ab. Eine im *Körper aller Zahlen* irreduzible Funktion heißt *absolut irreduzibel* (vgl. S. 260). Eine ganze Funktion einer *einzigen* Variablen von höherem als erstem Grade ist im Körper aller Zahlen stets reduzibel. Hat eine ganze Funktion $f(z)$ einer *einzigen* Variablen von höherem als zweitem Grade *reelle Koeffizienten,* so ist $f(z)$ im Körper *aller reellen* Zahlen stets reduzibel; denn jede ganze Funktion $f(z)$ mit reellen Koeffizienten läßt sich in ein Produkt von Polynomen ersten und zweiten Grades mit reellen Koeffizienten zerlegen.

Eine im Körper P *reduzible ganze Funktion von beliebig vielen Veränderlichen kann nur auf eine Art als ein Produkt von im Körper* P *irreduziblen ganzen Funktionen dargestellt werden. Hierbei gelten im Körper* P *irreduzible Funktionen, deren Quotienten konstant sind, als nicht verschieden.* Für Methoden, welche die Zerlegung einer gegebenen ganzen Funktion in irreduzible Faktoren für einen beliebigen algebraischen Körper (über die Wortbedeutung vgl. unten) durch eine endliche Anzahl von Schritten ausführen, vgl. *Kronecker, Festschrift, Journ. f. Math.* **92**, 11 (1882), *Ges. Werke* **2**, 256, Runge, *Journ. f. Math.* **99**, 89 (1886), Molk, *Acta math.* **6**, 10 (1885), Mandl, *Journ. f. Math.* **113**, 252 (1894), Hancock, *Ann. de l'éc. norm.* (3) **17**, 89 (1900), Weber, *Algebra* **2**, 563, Koenig, *Algebraische Größen*, S. 127.

1) Der Körper P muß entweder mit dem Körper P_1 zusammenfallen oder ihn umfassen.

Eine Gleichung $f(z) = 0$ heißt in einem Körper P irreduzibel, wenn es die ganze Funktion $f(z)$ ist.

Satz von Abel (*Œuvres* **1**, 480, *Ostwalds Klassiker* Nr. 111, S. 5): *Hat eine in einem Körper* P *irreduzible Gleichung* $f(z) = 0$ *mit irgendeiner anderen Gleichung* $\varphi(z) = 0$, *die ebenso wie* $f(z)$ *auch nur Koeffizienten aus* P *besitzt, eine Wurzel gemeinsam, so genügen alle Wurzeln von* $f(z) = 0$ *auch der Gleichung* $\varphi(z) = 0$; *alsdann ist* $\varphi(z)$ *durch* $f(z)$ *teilbar.*

Hieraus folgt: *Eine irreduzible Gleichung kann mit keiner Gleichung niedrigeren Grades, die Koeffizienten aus dem gleichen Körper besitzt, eine Wurzel gemeinsam haben. Eine irreduzible Gleichung kann keine mehrfachen Wurzeln besitzen. Die linken Seiten zweier irreduziblen Gleichungen mit einer gemeinsamen Wurzel können sich nur um einen konstanten Faktor unterscheiden.*

Über die Irreduzibilität gibt aus der Natur der Gleichungskoeffizienten folgendes Schoenemann-Eisensteinsches Theorem, gewöhnlich Eisensteinscher Satz genannt, Aufschluß (Schoenemann, *Journ. f. Math.* **32**, 100 (1846), Eisenstein ebenda **39**, 166 (1850), Schoenemann, Reklamation ebenda **40**, 188 (1850)): *Ist in einer Gleichung mit ganzzahligen Koeffizienten der Koeffizient der höchsten Potenz gleich* 1 *(oder allgemeiner eine zu der Primzahl p relativ prime ganze Zahl) und sind alle übrigen Koeffizienten durch die nämliche Primzahl p teilbar, der letzte aber nicht durch* p^2, *so ist die Gleichung im Körper der rationalen Zahlen irreduzibel.*

Der Beweis des Schoenemann-Eisensteinschen Satzes läßt sich mit Hilfe des Satzes von Gauß (*Disquisitiones arithmeticae,* Art. 42) erbringen: *Eine jede im Körper der rationalen Zahlen reduzible ganze Funktion*

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n$$

mit ganzzahligen Koeffizienten $a_1, a_2, \ldots, a_n$ *kann nie anders in zwei Faktoren*

$$f_1(z) = z^{n_1} + b_1 z^{n_1-1} + b_2 z^{n_1-2} + \cdots + b_{n_1} \quad (n_1 > 0)$$
$$f_2(z) = z^{n_2} + c_1 z^{n_2-1} + c_2 z^{n_2-2} + \cdots + c_{n_2} \quad (n_2 > 0)$$

mit rationalen Zahlen zerlegt werden, als daß sämtliche Größen $b_1, b_2, \ldots, b_{n_1}, c_1, c_2, \ldots, c_{n_2}$ *ganzzahlig sind.*

An den Schoenemann-Eisensteinschen Satz anknüpfende Untersuchungen, die aus der *Teilbarkeit der Gleichungskoeffizienten* auf die Reduzibilität bezw. Irreduzibilität der Gleichung schließen, stammen von Koenigsberger, *Journ. f. Math.* **115**, 53 (1895), Netto, *Math. Ann.* **48**, 81 (1897), M. Bauer, *Journ. f. Math.* **128**, 298 (1905), **132**, 21 (1907), **134**, 15 (1908), Dumas, *Journ. de math.* (6) **2**, 191 (1908), Perron, *Math. Ann.* **60**, 448 (1905); Irreduzibilitätskriterien auf Grund von *Größenbeziehungen zwischen den Gleichungskoeffizienten* bei Perron, *Journ. f. Math.* **132**, 288 (1907).

Irgendeine Größe ζ heißt *in bezug auf einen Körper* P *algebraisch* oder eine *aus* P *stammende algebraische Zahl,* wenn ζ einer algebraischen Gleichung mit Koeffizienten aus P genügt. *Zu jeder aus* P *stammenden algebraischen Zahl* ζ *gehört eine in* P *irreduzible Gleichung* $J(z) = 0$ *mit Koeffizienten aus* P; *ihre linke Seite ist bis auf eine beliebige,* P *angehörige Konstante eindeutig bestimmt.* $J(z) = 0$ *ist die Gleichung niedrigsten Grades mit Koeffizienten aus* P, *die* ζ *zur Wurzel hat.* Ist n der Grad von $J(z) = 0$, so heißt ζ eine *aus* P *stammende algebraische Größe* n^{ten} *Grades.* Jede rationale Funktion $\frac{g(\zeta)}{h(\zeta)}$ von ζ mit Koeffizienten aus P kann mit Hilfe der irreduziblen Gleichung $J(z) = 0$ vom Grade n in eine ganze rationale Funktion

$$c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_{n-1}\zeta^{n-1}$$

mit Koeffizienten aus P umgewandelt werden. Durchlaufen $c_0, c_1, c_2, \ldots, c_{n-1}$ alle Größen aus P, so stellt

$$c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_{n-1}\zeta^{n-1}$$

alle Größen des aus P durch Adjunktion von ζ hervorgehenden Körpers dar, und zwar eine jede nur einmal. Der aus P durch Adjunktion von ζ hervorgehende Körper heißt ein *algebraischer Körper über* P (Weber, *Algebra* **1**, 492), ein *algebraischer Oberkörper von* P oder ein *Relativkörper in bezug auf* P (Hilbert, *Math.-Ver.* **4**, *die Theorie der algebraischen Zahlkörper*, S. 203 (1897)) oder ein dem *Bereich* P *entstammender Gattungsbereich* (Kronecker, *Festschrift,* S. 7, jedoch benützt Kronecker diese Bezeichnung nur bei dem von ihm verwendeten engeren Begriff des Rationalitätsbereiches). P heißt der *Stammbereich.* Genügt ζ einer in P irreduziblen Gleichung n^{ten} Grades, so heißt *der Körper* (P, ζ) *vom Grade n.* Ein *aus dem absoluten Rationalitätsbereich* hervorgehender algebraischer Körper heißt kurzweg ein *algebraischer Körper.* Dieser läßt sich auch so definieren: Er geht aus dem absoluten Rationalitätsbereich durch Adjunktion einer Wurzel einer irreduziblen Gleichung mit ganzzahligen Koeffizienten hervor.

Hat man eine beliebige endliche Anzahl $\eta_1, \eta_2, \ldots, \eta_r$ aus einem Körper P stammender algebraischer Zahlen, so kann man stets eine und sogar unendlich viele aus P stammende algebraische Zahlen ζ finden, so daß ζ eine ganze rationale Funktion von $\eta_1, \eta_2, \ldots, \eta_r$ mit Koeffizienten aus P wird und $\eta_1, \eta_2, \ldots, \eta_r$ ganze rationale Funktionen von ζ mit Koeffizienten aus P sind. *Jeder durch Adjunktion einer endlichen Anzahl aus* P *stammender algebraischer Größen aus* P *hervorgehende Körper über* P *kann daher entstanden gedacht werden durch Adjunktion einer einzigen Wurzel einer in* P *irreduziblen algebraischen Gleichung mit Koeffizienten aus* P (Satz von Abel, *Œuvres* **1**, 547, vgl. auch Galois, *Œuvres*, p. 37). Man kann ζ einfach in der Form $\mu_1\eta_1 + \mu_2\eta_2 + \cdots + \mu_r\eta_r$ wählen, wobei für $\mu_1, \mu_2, \ldots, \mu_r$ gewöhnliche rationale Zahlen genommen werden können (vgl. G. Cantor, *Math. Ann.* **5**, 133 (1872), Weber, *Algebra* **1**, 500).

Hat die im Körper P irreduzible Gleichung $J(z) = 0$ vom Grade n die Wurzeln $\zeta_1, \zeta_2, \ldots, \zeta_n$ und ist $\varphi(\zeta_1)$ eine ganze rationale Funktion von ζ_1 mit Koeffizienten aus P, so genügt $t_1 = \varphi(\zeta_1)$ einer Gleichung

$$\Phi(t) = (t - t_1)(t - t_2) \cdots (t - t_n) = 0$$

mit den Wurzeln $t_i = \varphi(\zeta_i)$ $(i = 1, 2, \ldots, n)$.

Die aus der irreduziblen Gleichung $J(z) = 0$ *hervorgehende Tschirnhausenresolvente* $\Phi(t) = 0$ (vgl. S. 277) *hat Koeffizienten aus* P *und ist entweder eine in* P *irreduzible Gleichung oder ihre linke Seite ist die* e^{te} *Potenz einer in* P *irreduziblen ganzen Funktion* $\Phi_1(t)$ *vom Grade* n_1. Hieraus folgt: *Die Größen*

$$\varphi(\zeta_1), \varphi(\zeta_2), \ldots, \varphi(\zeta_n)$$

sind entweder sämtlich untereinander verschieden oder sie zerfallen in n_1 *Systeme von je* e *gleichen:*

$$\varphi(\zeta_1) = \varphi(\zeta_2) \cdots = \varphi(\zeta_e), \varphi(\zeta_{e+1}) = \varphi(\zeta_{e+2}) = \cdots = \varphi(\zeta_{2e}), \ldots,$$
$$\varphi(\zeta_{n-e+1}) = \varphi(\zeta_{n-e+2}) = \cdots = \varphi(\zeta_n).$$

Die Größen $t_1 = \varphi(\zeta_1)$, $t_2 = \varphi(\zeta_2), \ldots, t_n = \varphi(\zeta_n)$ *heißen in bezug auf den Körper* P *konjugierte Größen. Sind sie sämtlich voneinander verschieden, dann und auch nur dann ist nicht bloß* $t_i = \varphi(\zeta_i)$ *eine rationale Funktion von* ζ_i, *sondern auch umgekehrt* ζ_i *eine rationale Funktion von* t_i *mit Koeffizienten aus* P.

Adjungiert man einem Körper P die algebraische aus P stammende Größe ζ_1, so erhält man einen Körper (P, ζ_1) über P.

Adjungiert man statt ζ_1 eine rationale Funktion $t_1 = \varphi(\zeta_1)$ von ζ_1 mit Koeffizienten aus P, so erhält man einen Körper (P, t_1), der nur Größen aus dem Körper (P, ζ_1) enthält. Ist t_1 von allen seinen konjugierten Größen verschieden, dann und nur dann sind die Körper (P, t_1) und (P, ζ_1) identisch. In diesem Fall heißt $t_1 = \varphi(\zeta_1)$ eine *primitive Größe des Körpers* (P, ζ_1).

Ein Körper, der sämtliche Größen des Körpers P umfaßt und dessen Größen ausnahmslos dem algebraischen Körper (P, ζ_1) über P angehören, ohne jedoch den Körper (P, ζ_1) zu erschöpfen, heißt ein *Divisor*, echter *Teiler* oder *Unterkörper von* (P, ζ_1). Jeder Divisor von (P, ζ_1) wird aus P erhalten, indem man dem Körper P eine gewisse ganze Funktion $t_1 = \varphi(\zeta_1)$ mit Koeffizienten aus P adjungiert. Charakteristisch dafür, daß (P, t_1) ein Divisor von (P, ζ_1) ist, erweist sich, daß t_1 eine *imprimitive Größe des Körpers* (P, ζ_1) ist, d. h. $t_1 = \varphi(\zeta_1)$ nicht von allen seinen konjugierten Größen verschieden ist. *Ein Körper* (P, ζ_1), *der nur primitive Größen enthält, also keine Divisoren besitzt, heißt ein primitiver Körper.*

Ist $J(z) = 0$ die irreduzible Gleichung mit Koeffizienten aus P, der ζ_1 genügt, so ist der Körper (P, ζ_1) dann und nur dann ein primitiver Körper, wenn alle Tschirnhausenresolventen von $J(z) = 0$ mit Koeffizienten aus P ausnahmslos in P irreduzibel sind. Alsdann heißt die irreduzible Gleichung $J(z) = 0$ selbst eine *in* P *irreduzible primitive Gleichung.* Jede in P irreduzible, nicht primitive Gleichung heißt *imprimitiv. Jede in* P *irreduzible Gleichung von Primzahlgrad ist notwendig primitiv.*

Ist $J(z) = 0$ *eine im* P *imprimitive Gleichung* n^{ten} *Grades mit der Wurzel* ζ_1 *und bedeutet* $t_1 = \varphi(\zeta_1)$ *irgendeine imprimitive Größe des Körpers* (P, ζ_1), *die einer in* P *irreduziblen Gleichung* n_1^{ten} *Grades genügt, so wird die in* P *irreduzible Gleichung* $J(z) = 0$ *im Körper* (P, t_1) *reduzibel, und* ζ_1 *genügt in ihm einer irreduziblen Gleichung* e^{ten} *Grades, wobei* $n = n_1 e$ *ist.*

Anders ausgedrückt: *Jede im Körper* P *imprimitive Gleichung* $J(z) = 0$ *läßt sich durch Elimination von* t *aus zwei Gleichungen:*

$$t^{n_1} + c_1 t^{n_1 - 1} + c_2 t^{n_1 - 2} + \cdots + c_{n_1} = 0$$

und

$$z^e + \alpha_1(t) z^{e-1} + \alpha_2(t) z^{e-2} + \cdots + \alpha_e(t) = 0$$

finden; *die erste Gleichung ist im Körper* P, *die zweite im Körper* (P, t) *irreduzibel* (vgl. Jordan, *Traité*, p. 260, H. Weber, *Algebra* **1**, 501ff. u. 524ff.).

Der obige Satz, daß der Grad n_1 jedes Unterkörpers (P, t_1) eines imprimitiven Körpers (P, ζ_1) vom Grad n — nur solche Körper können ja Unterkörper haben — ein Divisor von n ist, ergibt sich als Korollar aus dem Kronecker-Kneserschen Satz (Hölder, *Math. Ann.* **38**, 309 (1891), Kneser, *Math. Ann.* **30**, 195 (1887), *Journ. f. Math.* **106**, 51 (1890), Landsberg, ebenda, **132**, 8 (1907)): *Sind ξ und ζ die Wurzeln zweier im Körper* P *irreduzibler Gleichungen vom Grade n_1 bezw. n und sind die Grade der irreduziblen Gleichungen, denen ξ nach Adjunktion von ζ und ζ nach Adjunktion von ξ genügen, e_1 bezw. e, so ist $n_1 e = n e_1$. Ist also $e < n$, so muß $e_1 < n_1$ sein, d. h. die zwei Gleichungen wirken aufeinander reduzierend.* (In dem obigen speziellen Satz ist ξ die im Körper (P, ζ) liegende Größe $t_1 = \varphi(\zeta)$ und daher $e_1 = 1$).

Ist $J(z) = 0$ eine im Körper P irreduzible Gleichung n^{ten} Grades mit den Wurzeln $\zeta_1, \zeta_2, \ldots, \zeta_n$, so heißen die Körper $(\mathsf{P}, \zeta_1), (\mathsf{P}, \zeta_2), \ldots (\mathsf{P}, \zeta_n)$ *in bezug auf* P *konjugierte Körper.* Ein Körper, der mit allen seinen konjugierten übereinstimmt, heißt ein Galoisscher oder Normalkörper. Eine im Körper P irreduzible Gleichung $J(z) = 0$ heißt eine *Normalgleichung* oder Galoissche *Gleichung*, wenn ihre sämtlichen Wurzeln rationale Funktionen einer einzigen mit Koeffizienten aus P sind. *Bei einer Normalgleichung sind alle Wurzeln nicht nur rationale Funktionen einer bestimmten Wurzel mit Koeffizienten aus* P, *sondern jeder beliebigen. Die Normalgleichungen und auch nur sie allein erzeugen Normalkörper.*

Hat eine beliebige reduzible oder irreduzible Gleichung $f(z) = 0$ mit Koeffizienten aus einem Körper P *lauter verschiedene Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$, so kann man stets eine Größe ζ_1 von folgender Beschaffenheit finden: ζ_1 ist eine ganze rationale Funktion von $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit Koeffizienten aus* P, *und jede der Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$ läßt sich als ganze rationale Funktion von ζ_1 mit Koeffizienten aus* P *ausdrücken.* (Vgl. oben S. 294.) *Die in* P *irreduzible Gleichung, der ζ_1 genügt, ist eine Normalgleichung.* Jede in P irreduzible Gleichung, die eine solche Funktion ζ_1 zur Wurzel hat, heißt eine Galoissche *Resolvente von $f(z) = 0$. Alle* Galoisschen *Resolventen von $f(z) = 0$ sind von gleichem Grade und jede eine Tschirnhausenresolvente einer jeden anderen.* Die Rückführung jeder beliebigen Gleichung $f(z) = 0$ mit Koeffizienten aus dem Körper P auf eine Galoissche Resolvente ist das Fundament der im § 10 behandelten Galoisschen Theorie. (Galois, *Œuvres*, p. 36.)

Hat man eine Gleichung $f(z) = 0$ ohne mehrfache Wurzeln, so kann man sich die Koeffizienten einer Funktion ζ_1 der eben definierten Beschaffenheit und eine Galoissche Resolvente, der ζ_1 genügt, auf folgende Art ohne Kenntnis der Wurzeln von $f(z) = 0$ verschaffen:

$$\tau_1 = \mu_1\alpha_1 + \mu_2\alpha_2 + \cdots + \mu_n\alpha_n$$

sei eine lineare homogene Funktion der Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit zunächst unbestimmten Koeffizienten $\mu_1, \mu_2, \ldots, \mu_n$. Die Funktion τ_1 nehme bei den $\nu = n!$ Permutationen der Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$ die ν Werte $\tau_1, \tau_2, \ldots, \tau_\nu$ an. Man bilde sich die transformierte Gleichung

$$g(\tau) = (\tau - \tau_1)(\tau - \tau_2)\cdots(\tau - \tau_\nu) = 0$$

von $f(z) = 0$. Die Koeffizienten von $g(\tau) = 0$ sind als symmetrische Funktionen der Wurzeln von $f(z) = 0$ von diesen unabhängig, die Diskriminante von $g(\tau) = 0$ wird eine ganze rationale Funktion von $\mu_1, \mu_2, \ldots, \mu_n$, die nicht identisch verschwindet, da die Wurzeln von $f(z) = 0$ untereinander verschieden sind. Alsdann wähle man, was auf unendlich viele Arten möglich ist, für

$$\mu_1, \mu_2, \ldots, \mu_n$$

solche rationale Zahlen, daß die Diskriminante einen von Null verschiedenen Wert besitzt, also $g(\tau) = 0$ keine mehrfachen Wurzeln hat, d. h. die Größen $\tau_1, \tau_2, \ldots, \tau_\nu$ sämtlich voneinander verschieden sind (vgl. Weber, *Algebra* **1**, 147, Bachmann, *Math. Ann.* **18**, 452 (1881)). Sind $\mu_1, \mu_2, \ldots, \mu_n$ derartig bestimmt, so zerlege man $g(\tau)$ in seine in P irreduziblen Faktoren. Ist $G(\tau)$ ein *beliebiger* irreduzibler Faktor von $g(\tau)$, so ist $G(\tau) = 0$ eine Galoissche Resolvente von $f(z) = 0$ und *jede* Wurzel von $G(\tau) = 0$ eine Funktion ζ_1 der verlangten Beschaffenheit.

Wir führen zum Schluß noch einen Satz von Hilbert (*Journ. f. Math.* **110**, 122 (1892)) über die Irreduzibilität einer ganzen Funktion mehrerer Veränderlicher an:

Ist eine ganze rationale $F(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$ *von* $m + n$ *Variablen* $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m$ *in irgendeinem algebraischen Körper irreduzibel, so ist es stets auf unendlich viele Weisen möglich, in dieser Funktion für* $y_1, y_2, \ldots, y_m$ *ganze rationale Zahlen einzusetzen, so daß hierdurch die vorgelegte Funktion in eine Funktion der* n *Variablen* $x_1, x_2, \ldots, x_n$ *übergeht, die in eben diesem Körper irreduzibel ist.*

§ 10. Die Galoissche Gruppe einer Gleichung. Natürliche und akzessorische Irrationalitäten. Rationale Resolventen. Reduktion der Gruppe und Rückführung einer Gleichung auf eine Kette von Hilfsgleichungen. Allgemeine Gleichungen. Affektlose Gleichungen.

P sei ein beliebiger Körper und $f(z) = 0$ irgendeine Gleichung n^{ten} Grades mit Koeffizienten aus P. Von der Gleichung $f(z) = 0$ wird nur, und zwar im folgenden ausnahmslos, vorausgesetzt, daß ihre sämtlichen Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ voneinander verschieden sind. Wir betrachten die Gesamtheit aller Gleichungen mit Koeffizienten aus P, die $\alpha_1, \alpha_2, \ldots, \alpha_n$ ganz und rational enthalten und die richtige Relationen sind, falls für $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Wurzeln der vorgelegten Gleichung $f(z) = 0$ gesetzt werden. *Die Gesamtheit aller Permutationen unter den Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$, die jede zwischen diesen bestehende richtige Gleichung mit Koeffizienten aus P wieder in eine richtige Gleichung überführen, bildet eine Permutationsgruppe $\mathfrak{G}$ n^{ten} Grades; diese heißt die Galoissche Gruppe der Gleichung $f(z) = 0$.* Die Galoissche Gruppe $\mathfrak{G}$ hängt von der Gleichung $f(z) = 0$ und dem der Betrachtung zugrunde liegenden Körper P ab.

Von irgendeiner rationalen Funktion $R(\alpha_1, \alpha_2, \ldots, \alpha_n)$ der Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit Koeffizienten aus P sagt man: sie bleibt bei einer Permutation $\begin{pmatrix} \alpha_1, \alpha_2 \ldots \alpha_n \\ \alpha_{i_1}, \alpha_{i_2} \ldots \alpha_{i_n} \end{pmatrix}$ *numerisch ungeändert,* wenn $R(\alpha_1, \alpha_2, \ldots, \alpha_n)$ und $R(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n})$ für die Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ von $f(z) = 0$ den gleichen Wert annehmen. Bei numerischer Unveränderlichkeit brauchen $R(\alpha_1, \alpha_2, \ldots, \alpha_n)$ und $R(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n})$ nicht formal übereinzustimmen.

Aus der Definition der Galoisschen Gruppe folgt:

Besitzt eine rationale Funktion von $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit Koeffizienten aus P eine dem Körper P angehörige Zahl als Wert, wenn man für $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Wurzeln von $f(z) = 0$ setzt, so bleibt die betreffende Funktion bei allen Permutationen der Galoisschen Gruppe $\mathfrak{G}$ numerisch ungeändert.

Dieser Satz ist umkehrbar: *Bleibt eine rationale Funktion der Gleichungswurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit Koeffizienten aus P bei allen Permutationen der Galoisschen Gruppe $\mathfrak{G}$ numerisch ungeändert, so ist ihr Wert eine dem Körper P angehörige Zahl.*

Bleiben alle richtigen Gleichungen mit Koeffizienten aus P, die $\alpha_1, \alpha_2, \ldots, \alpha_n$ ganz und rational enthalten, bei allen Permu-

tationen einer Permutationsgruppe $\mathfrak{H}$ n^{ten} *Grades unter den Größen* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *richtig, und hat ferner jede rationale Funktion von* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *mit Koeffizienten aus* P, *die bei allen Permutationen von* $\mathfrak{H}$ *numerisch ungeändert bleibt, einen Wert aus* P, *so enthält* $\mathfrak{H}$ *alle Permutationen der Galoisschen Gruppe* $\mathfrak{G}$ *der Gleichung* $f(z) = 0$, *und* $\mathfrak{H}$ *ist mit* $\mathfrak{G}$ *identisch.*

$\zeta_1 = V(\alpha_1, \alpha_2, \ldots, \alpha_n)$ sei eine beliebige rationale Funktion von $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit Koeffizienten aus P von der Beschaffenheit, daß sich die Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$ als ganze rationale Funktionen von ζ_1 mit Koeffizienten aus P in der Form

$$\alpha_k = \chi_k(\zeta_1) \qquad (k = 1, 2, \ldots, n)$$

ausdrücken lassen. Die in P irreduzible Gleichung, die ζ_1 zur Wurzel hat, sei die Gleichung $G(\zeta) = 0$ vom Grade g; $G(\zeta) = 0$ ist also eine Galoissche Resolvente (vgl. S. 297) von $f(z) = 0$. Bedeutet ζ_i eine beliebige der g Wurzeln von $G(\zeta) = 0$, so sind $\chi_1(\zeta_i), \chi_2(\zeta_i), \ldots, \chi_n(\zeta_i)$, abgesehen von der Reihenfolge, die n Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ von $f(z) = 0$. Es gilt folgender Satz:

Man erhält sämtliche Permutationen der Galoisschen Gruppe $\mathfrak{G}$ *der Gleichung* $f(z) = 0$ *und auch nur diese, sowie eine jede nur einmal, wenn man in der Permutation:*

$$\begin{pmatrix} \chi_1(\zeta_1)\, \chi_2(\zeta_1) \cdots \chi_n(\zeta_1) \\ \chi_1(\zeta_i)\, \chi_2(\zeta_i) \cdots \chi_n(\zeta_i) \end{pmatrix}$$

die Größe ζ_i *sämtliche* g *Wurzeln der Galoisschen Resolvente* $G(\zeta) = 0$ *durchlaufen läßt.*

Wählt man für $G(\zeta)$ eine andere Galoissche Resolvente von $f(z) = 0$, so erscheinen die Permutationen der Galoisschen Gruppe $\mathfrak{G}$ von $f(z) = 0$ eventuell in anderer Reihenfolge.

Die Natur der Galoisschen Gruppe gibt über die Eigenschaften einer Gleichung folgende Aufschlüsse:

Eine Gleichung ist in dem der Betrachtung zugrunde liegenden Körper irreduzibel oder reduzibel, je nachdem ihre Galoissche Gruppe eine transitive oder intransitive Permutationsgruppe ist.

Eine irreduzible Gleichung ist in dem der Untersuchung zugrunde liegenden Körper P *dann und nur dann primitiv* (vgl. S. 210), *wenn ihre Galoissche Gruppe eine primitive Permutationsgruppe ist. Die Galoissche Gruppe jeder im Körper* P *irreduziblen imprimitiven Gleichung ist eine imprimitive Permutationsgruppe*

Die Galoissche Gruppe einer Normalgleichung und auch nur einer solchen Gleichung ist eine reguläre Permutationsgruppe, d. h. eine transitive Permutationsgruppe von derselben Ordnung wie Grad (vgl. S. 212).

Hat man eine Gleichung $f(z) = 0$ mit Koeffizienten aus einem Körper P und den Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$, so heißt eine ganze rationale Funktion $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ von $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit Koeffizienten aus P, deren Wert dem Körper P nicht angehört, *eine der Gleichung $f(z) = 0$ natürliche Irrationalität.* Eine solche natürliche Irrationalität kann auch als eine in dem durch die Galoissche Resolvente $G(\zeta) = 0$ bestimmten Galoisschen Körper (P, ζ_1) gelegene Größe definiert werden.

Eine natürliche Irrationalität φ bleibt nicht bei allen Permutationen der Galoisschen Gruppe $\mathfrak{G}$ der Gleichung $f(z) = 0$ numerisch ungeändert; denn sonst wäre sie bereits im Körper P gelegen.

Die Gesamtheit aller Permutationen der Galoisschen Gruppe $\mathfrak{G}$, bei denen $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ numerisch ungeändert bleibt, bildet eine Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$. Die Gruppe $\mathfrak{H}$ heißt die zu der natürlichen Irrationalität φ zugehörige Gruppe. Umgekehrt gehören zu jeder Untergruppe $\mathfrak{H}$ der Galoisschen Gruppe $\mathfrak{G}$ eine und sogar unendlich viele natürliche Irrationalitäten $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$, die nur bei den Permutationen von $\mathfrak{H}$ numerisch ungeändert bleiben, bei allen $\mathfrak{H}$ nicht angehörigen Permutationen von $\mathfrak{G}$ ihren numerischen Wert ändern.

Gehört die natürliche Irrationalität φ_1 zu der Untergruppe $\mathfrak{H}$ der Galoisschen Gruppe $\mathfrak{G}$ und ist $\mathfrak{G} = \mathfrak{H} G_1 + \mathfrak{H} G_2 + \cdots \mathfrak{H} G_\varrho$ die Zerlegung der Gruppe $\mathfrak{G}$ nach dem Modul $\mathfrak{H}$, so nimmt φ_1 den ϱ Nebengruppen entsprechend bei allen Permutationen von $\mathfrak{G}$ die ϱ numerisch verschiedenen Werte $\varphi_1, \varphi_2, \ldots, \varphi_\varrho$ an. *Diese genügen der im Körper P irreduziblen Gleichung*

$$\Phi(t) = (t - \varphi_1)(t - \varphi_2) \ldots (t - \varphi_\varrho) = 0.$$

Sie heißt eine *Resolvente von $f(z) = 0$* und präziser, da alle ihre Wurzeln rationale Funktionen der Wurzeln von $f(z) = 0$ mit Koeffizienten aus P sind, eine *rationale Resolvente von $f(z) = 0$. Ist $\mathfrak{J}$ die invariante Untergruppe von $\mathfrak{G}$, welche die konjugierten Gruppen $G_i^{-1} \mathfrak{H} G_i$ $(i = 1, 2, \ldots, \varrho)$ gemein haben, so ist die Galoissche Gruppe von $\Phi(t) = 0$ mit der Faktorgruppe $\mathfrak{G}/\mathfrak{J}$ isomorph.* Die ϱ konjugierten Größen φ_i $(i = 1, 2, \ldots, \varrho)$ haben die Gruppen $G_i^{-1} \mathfrak{H} G_i$ $(i = 1, 2, \ldots, \varrho)$ als zugehörige Gruppen. Die Erweiterung des Körpers P durch eine Größe φ_i reduziert die

Galoissche Gruppe $\mathfrak{G}$ von $f(z) = 0$ auf die zu φ_i zugehörige Gruppe $G_i^{-1}\mathfrak{H}G_i$; die Adjunktion aller Wurzeln von $\Phi(t) = 0$ zum Körper P reduziert demnach die Galoissche Gruppe von $f(z) = 0$ auf die Gruppe $\mathfrak{J}$, den Durchschnitt aller konjugierten Gruppen.

Lagrangescher, von Galois erweiterter Satz (vgl. S. 221): *Ist φ_1 eine zur Untergruppe $\mathfrak{H}$ der Galoisschen Gruppe $\mathfrak{G}$ gehörige natürliche Irrationalität und bleibt eine zweite natürliche Irrationalität $\psi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ bei allen Permutationen von $\mathfrak{H}$ numerisch ungeändert, so ist ψ eine rationale Funktion von φ_1 mit Koeffizienten aus* P. *Ist $\mathfrak{H}'$ die zu ψ zugehörige Untergruppe der Galoisschen Gruppe $\mathfrak{G}$ und $\sigma = \frac{h'}{h}$ der Index der Untergruppe $\mathfrak{H}$ von $\mathfrak{H}'$, so genügt φ_1 einer Gleichung σ^{ten} Grades, deren Koeffizienten dem durch Adjunktion von ψ erweiterten Körper* P *angehören; die Gleichung σ^{ten} Grades, der φ_1 genügt, ist in diesem erweiterten Körper irreduzibel.*

Korollar: Hat man zwei natürliche Irrationalitäten, die zu derselben Untergruppe der Galoisschen Gruppe gehören, so ist jede eine rationale Funktion der anderen mit Koeffizienten aus P. *Die rationalen Resolventen mit Koeffizienten aus* P, *denen sie genügen, gehen daher durch Tschirnhausentransformation auseinander hervor.*

Im Gegensatz zu den natürlichen Irrationalitäten spricht man von den *für die Gleichung $f(z) = 0$ akzessorischen Irrationalitäten. Hierunter versteht man jede dem Körper* P *nicht angehörige Größe, die sich nicht in die Form $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ mit Koeffizienten aus* P *bringen läßt.* Die Adjunktion einer akzessorischen Irrationalität η zum Körper P ändert die Galoissche Gruppe $\mathfrak{G}$ von $f(z) = 0$ entweder überhaupt nicht oder reduziert sie auf eine ihrer Untergruppen $\mathfrak{H}$. *Reduziert die Adjunktion einer akzessorischen Irrationalität η die Galoissche Gruppe $\mathfrak{G}$ von $f(z) = 0$ auf eine Untergruppe $\mathfrak{H}$ und wählt man eine zu $\mathfrak{H}$ zugehörige natürliche Irrationalität φ, so ist φ eine rationale Funktion von η mit Koeffizienten aus* P. *Jede Größe η, deren Adjunktion die Galoissche Gruppe $\mathfrak{G}_g$ von $f(z) = 0$ auf $\mathfrak{H}_h$ reduziert, genügt einer in* P *irreduziblen Gleichung, deren Grad ein Vielfaches des Index $\frac{g}{h}$ der Gruppe $\mathfrak{H}_h$ von $\mathfrak{G}_g$ ist und nur dann gleich $\frac{g}{h}$ wird, wenn η keine akzessorische, sondern eine natürliche Irrationalität ist. In letzterem Fall ist auch η eine rationale Funktion von φ mit Koeffizienten aus* P.

Alle Wurzeln einer im Körper P *irreduziblen Gleichung, deren Adjunktion die Galoissche Gruppe der gegebenen Gleichung reduziert, sind entweder ausnahmslos natürliche oder ausnahmslos akzessorische Irrationalitäten.* Reduziert die Adjunktion einer Wurzel einer irreduziblen Gleichung die Galoissche Gruppe $\mathfrak{G}$ einer gegebenen Gleichung $f(z) = 0$, so reduziert sie auch die Adjunktion jeder anderen Wurzel der irreduziblen Gleichung, und zwar auf dieselbe oder eine innerhalb $\mathfrak{G}$ ähnliche Untergruppe.

Satz von C. Jordan (*Traité*, p. 269) und Hölder (*Math. Ann.* **34**, 47 (1889)): *Reduziert sich die Galoissche Gruppe* $\mathfrak{G}$ *einer Gleichung* $f(z) = 0$ *mit Koeffizienten aus* P *durch Adjunktion sämtlicher Wurzeln einer beliebigen (reduziblen oder irreduziblen) Gleichung* $F(t) = 0$ *mit Koeffizienten aus* P *auf eine Untergruppe* $\mathfrak{J}$, *so reduziert sich die Galoissche Gruppe* $\mathfrak{G}_1$ *von* $F(t) = 0$ *durch Adjunktion aller Wurzeln von* $f(z) = 0$ *auf eine Untergruppe* $\mathfrak{J}_1$. *Die Gruppen* $\mathfrak{J}$ *und* $\mathfrak{J}_1$ *sind invariante Untergruppen von* $\mathfrak{G}$ *bezw.* $\mathfrak{G}_1$, *ferner sind die Faktorgruppen* $\mathfrak{G}/\mathfrak{J}$ *und* $\mathfrak{G}_1/\mathfrak{J}_1$ *holoedrisch isormorph.*

Korollare: a) *Die Adjunktion einer einzigen Wurzel einer irreduziblen Hilfsgleichung* $F(t) = 0$ *reduziert die Galoissche Gruppe* $\mathfrak{G}$ *der Gleichung* $f(z) = 0$ *dann und nur dann auf eine invariante Untergruppe, wenn* $F(t) = 0$ *eine Normalgleichung im Körper* P *ist.*

b) Erniedrigt die Adjunktion aller Wurzeln einer Gleichung $F(t) = 0$ *mit einfacher Galoisscher Gruppe die Galoissche Gruppe von* $f(z) = 0$, *so zerfällt die Hilfsgleichung* $F(t) = 0$ *durch Adjunktion aller Wurzeln von* $f(z) = 0$ *in lauter Faktoren ersten Grades, d. h. die Wurzeln von* $F(t) = 0$ *sind rationale Funktionen derjenigen von* $f(z) = 0$ *mit Koeffizienten aus dem Körper* P *oder anders ausgedrückt: sie sind natürliche Irrationalitäten der Gleichung* $f(z) = 0$.

Da jede invariante Untergruppe einer primitiven Permutationsgruppe transitiv ist (vgl. S. 210), so folgt aus dem Jordan-Hölderschen Hauptsatz auch: *Eine in einem Körper* P *irreduzible primitive Gleichung, die durch Adjunktion aller Wurzeln einer Hilfsgleichung reduzibel wird, zerfällt in lauter Faktoren ersten Grades.*

Wird eine in einem Körper P *irreduzible imprimitive Gleichung durch Adjunktion aller Wurzeln einer Hilfsgleichung reduzibel, so zerfällt sie in lauter Faktoren des nämlichen Grades; diese haben in dem durch Adjunktion aller Wurzeln der Hilfsgleichung erweiterten Körper isomorphe Galoissche Gruppen* (vgl. die für imprimitive Gruppen geltenden Sätze auf S. 210, ferner Weber, *Algebra* **1**, 563).

Ist $f(z) = 0$ *eine beliebige Gleichung mit Koeffizienten aus einem Körper* P *und der Galoisschen Gruppe* $\mathfrak{G}$ *und besitzt diese die Kompositionsreihe* $\mathfrak{G}, \mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_{\nu-1}, 1$ (vgl. S. 197), *so läßt sich die Behandlung der vorgelegten Gleichung auf eine Gleichungskette* $f_1(z) = 0,\ f_2(z) = 0, \ldots, f_\nu(z) = 0$ *von folgender Beschaffenheit zurückführen: Jede dieser Gleichungen ist in dem Körper* P, *nachdem man ihm sämtliche Wurzeln der voraufgehenden Gleichungen adjungiert hat, irreduzibel und besitzt eine einfache Gruppe, die mit den sukzessiven Faktorgruppen* $\mathfrak{G}/\mathfrak{G}_1$, $\mathfrak{G}_1/\mathfrak{G}_2, \ldots, \mathfrak{G}_{\nu-2}/\mathfrak{G}_{\nu-1}, \mathfrak{G}_{\nu-1}$ *holoedrisch isomorph ist. Die Galoissche Gruppe der vorgelegten Gleichung reduziert sich nach Adjunktion der Wurzeln der Hilfsgleichungen sukzessiv auf* $\mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_{\nu-1}, 1$. *Infolge des voraufgehenden Korollars b) sind die Hilfsgleichungen in dem Körper, dem ihre Koeffizienten angehören, rationale Resolventen von* $f(z) = 0$. *Man kann die Hilfsgleichungen im besonderen stets so wählen, daß sie sämtlich Normalgleichungen sind, infolgedessen ihre Grade gleich den Ordnungen ihrer Galoisschen Gruppen werden und die Adjunktion je einer einzigen ihrer Wurzeln genügt.*

Für eine *veränderte Wahl der Hilfsgleichungen* gilt folgendes Theorem: Es seien $f_1(z) = 0, f_2(z) = 0, \ldots, f_\lambda(z) = 0$ irgendwelche Gleichungen ohne mehrfache Wurzeln von folgender Beschaffenheit: $f_1(z) = 0$ habe Koeffizienten aus P und eine einfache Galoissche Gruppe Γ_1. Die Gleichung $f_i(z) = 0$ habe Koeffizienten aus dem durch Adjunktion aller Wurzeln von $f_1(z) = 0,\ f_2(z) = 0, \ldots, f_{i-1}(z) = 0$ erweiterten Körper P und in diesem Oberkörper, dem ihre Koeffizienten angehören, eine einfache Galoissche Gruppe Γ_i. Reduziert sich die Galoissche Gruppe $\mathfrak{G}$ von $f(z) = 0$ durch Adjunktion aller Wurzeln von

$$f_1(z) = 0, f_2(z) = 0, \ldots, f_\lambda(z) = 0$$

auf die Einheit, d. h. drücken sich die Wurzeln von $f(z) = 0$ rational durch die von $f_1(z) = 0, f_2(z) = 0, \ldots, f_\lambda(z) = 0$ mit Koeffizienten aus P aus, so kommen unter den λ Gruppen Γ_1, $\Gamma_2, \ldots, \Gamma_\lambda$ ν Gruppen vor, die mit den Faktorgruppen

$$\mathfrak{G}/\mathfrak{G}_1, \mathfrak{G}_1/\mathfrak{G}_2, \ldots, \mathfrak{G}_{\nu-2}/\mathfrak{G}_{\nu-1}, \mathfrak{G}_{\nu-1},$$

vielleicht nur in anderer Reihenfolge, holoedrisch isomorph sind. *Durch Herbeiziehen beliebiger Hilfsgleichungen, deren Wurzeln akzessorische Irrationalitäten* sind, *wird niemals das Auftreten der mit den Faktorgruppen* $\mathfrak{G}/\mathfrak{G}_1, \mathfrak{G}_1/\mathfrak{G}_2, \ldots, \mathfrak{G}_{\nu-2}/\mathfrak{G}_{\nu-1}, \mathfrak{G}_{\nu-1}$ *isomorphen Gruppen vermieden: diese müssen stets, nur möglicher-*

weise in verschiedener Reihenfolge, auftreten. Ist $\nu = \lambda$, *so sind alle irreduziblen Faktoren von* $f_1(z) = 0, f_2(z) = 0, \ldots, f_\nu(z) = 0$ *rationale Resolventen von* $f(z) = 0$ (Hölder, *Math. Ann.* **34**, 49 (1889)).

Unter einer *allgemeinen Gleichung*

$$a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

vom n^{ten} Grade versteht man eine solche, bei der die Koeffizienten $a_0, a_1, \ldots, a_n$ willkürliche Variablen sind. Der Körper P, in dem die allgemeine Gleichung n^{ten} Grades betrachtet wird, muß alle rationalen Funktionen von $a_0, a_1, a_2, \ldots, a_n$ enthalten. Die Koeffizienten dieser Funktionen können entweder ausschließlich als gewöhnliche rationale Zahlen angenommen oder als Zahlen eines beliebigen Zahlkörpers oder noch allgemeiner als irgendwelche Zahlen vorausgesetzt werden. Im letzteren Fall enthält der Körper P außer den Unbestimmten $a_0, a_1, a_2, \ldots, a_n$ alle numerischen Größen. *Die Galoissche Gruppe der allgemeinen Gleichung* n^{ten} *Grades ist die symmetrische Gruppe* n^{ten} *Grades der Ordnung* $n!$. *In dem durch Adjunktion der Quadratwurzel aus der Diskriminante erweiterten Körper reduziert sich die Galoissche Gruppe auf die alternierende Gruppe* n^{ten} *Grades der Ordnung* $\frac{n!}{2}$, *die für* $n > 4$ *einfach ist. Für* $n > 4$ *ist die allgemeine Gleichung* n^{ten} *Grades nicht mehr algebraisch auflösbar.* (Vgl. S. 252.) Für die Fälle $n = 4$ und $n = 3$ vgl. § 8.

Ist $f(z) = 0$ die *allgemeine* Gleichung n^{ten} Grades, so sind ihre Wurzeln ebenso wie die Koeffizienten als willkürliche Variablen anzusehen. Eine zu einer Untergruppe $\mathfrak{H}_h$ der Galoisschen Gruppe der Ordnung $n!$ zugehörige natürliche Irrationalität $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ ist alsdann nichts anderes als eine zu der Gruppe $\mathfrak{H}_h$ zugehörige rationale Funktion $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ der n Variablen $\alpha_1, \alpha_2, \ldots, \alpha_n$, die bei allen Permutationen von $\mathfrak{H}_h$ und keinen weiteren formal ungeändert bleibt. Nimmt die Funktion φ bei den Permutationen der symmetrischen Gruppe die ϱ Werte $\varphi_1 = \varphi, \varphi_2, \ldots, \varphi_\varrho$ an, so ist die Resolvente

$$\Phi(t) = (t - \varphi_1)(t - \varphi_2) \ldots (t - \varphi_\varrho) = 0$$

mit der auf S. 280 definierten transformierten Gleichung identisch. Auf diese Weise ordnen sich die Betrachtungen auf S. 217 und S. 221 der allgemeinen Galoisschen Theorie unter. Im besondern geht aus dem von Galois verallgemeinerten Lagrangeschen Satz (vgl. S. 301) der Lagrangesche Satz (vgl. S. 221) hervor.

Eine Gleichung n^{ten} Grades, deren Galoissche Gruppe die symmetrische Gruppe n^{ten} Grades ist, heißt nach Kronecker (*Festschrift*, § 12, *Journ. f. Math.* **92** (1882), *Ges. Werke* **2**, 287) *eine Gleichung ohne Affekt.* Daß nicht nur die allgemeine Gleichung n^{ten} Grades affektlos ist, sondern auch spezielle Gleichungen mit numerischen Koeffizienten existieren, die ebenfalls affektlos sind, besagt der Satz von Hilbert (*Journ. f. Math.* **110**, 128 (1892), Weber, *Algebra* **1**, 652, E. Maillet, *Journ. de math.* (5) **5**, 205 (1899), M. Bauer, *Journ. f. Math.* **132**, 33 (1907)): *In jedem beliebigen, durch eine algebraische Zahl bestimmten Körper kann man stets Gleichungen von gegebenem Grade n konstruieren, deren Koeffizienten gewöhnliche rationale Zahlen sind und deren Galoissche Gruppe in eben jenem Körper (also a fortiori im absoluten Rationalitätsbereich) die symmetrische Gruppe n^{ten} Grades ist, und ebenso solche, deren Galoissche Gruppe in jenem Körper die alternierende Gruppe n^{ten} Grades ist.*

Ist $n > 4$, so gibt es für eine Gleichung n^{ten} Grades, deren Galoissche Gruppe die symmetrische Gruppe ist, abgesehen von Resolventen zweiten Grades, keine rationalen Resolventen von niedrigerem als n^{tem} Grade. Diese sind, abgesehen von $n = 6$, Tschirnhausenresolventen der ursprünglichen Gleichung. (Vgl. das Bertrandsche Problem auf S. 216.) Für $n = 4$ gibt es rationale Resolventen dritten Grades, vgl. die Gleichungen (3′) und (3″) auf S. 287 und 288.

Außer den im § 1 genannten Lehrbüchern, dem Enzyklopädieartikel von Hölder und den in diesem Paragraphen zitierten Schriften vgl. man für die Galoissche Theorie noch die Darstellungen von Bachmann, *Math. Ann.* **18**, 449 (1881), Bolza, *Am. J. math.* **13**, 59 (1891), *Math. Ann.* **42**, 253 (1893), Pierpont, *Annals of math.* (2) **1**, 113 u. **2**, 22 (1900), Mertens, *Sitzungsb. d. Wiener Akad.* **111**, Abt. IIa, 17 (1902).

§ 11. Abelsche Gleichungen.

Eine Gleichung $f(z) = 0$ mit lauter verschiedenen Wurzeln und mit Koeffizienten aus einem Körper P heißt eine *Abelsche Gleichung* (präziser eine im Körper P Abelsche Gleichung), wenn sich alle ihre Wurzeln als rationale Funktionen einer einzigen, z. B. α_1 mit Koeffizienten aus P ausdrücken lassen und außerdem stets

$$\Theta_i(\Theta_k(\alpha_1)) = \Theta_k(\Theta_i(\alpha_1))$$

ist, wenn $\Theta_i(\alpha_1)$ und $\Theta_k(\alpha_1)$ zwei beliebige Wurzeln von $f(z) = 0$ sind. $\Theta_i(\alpha_1)$ und $\Theta_k(\alpha_1)$ bedeuten rationale Funktionen von α_1 mit Koeffizienten aus P.

Die Galoissche Gruppe einer Abelschen Gleichung ist eine Abelsche Gruppe (vgl. S. 202). *Jede irreduzible Gleichung, deren Galoissche Gruppe eine Abelsche Gruppe ist, ist eine Abelsche Gleichung.* Läßt man den Zusatz irreduzibel fort, so gilt nur das Theorem: Jeder irreduzible Faktor der linken Seite einer Gleichung mit kommutativer Galoisscher Gruppe ist eine Abelsche Gleichung. Eine reduzible Gleichung mit kommutativer Galoisscher Gruppe braucht nämlich nicht so beschaffen zu sein, daß sich alle ihre Wurzeln rational durch eine von ihnen ausdrücken lassen. C. Jordan,* *Traité*, p. 287 bezeichnet jede Gleichung mit kommutativer Galoisscher Gruppe als eine Abelsche Gleichung. Die oben gegebene engere Definition ist die ursprüngliche Abels (§ 4 seiner fundamentalen Arbeit, vgl. oben S. 253).

Eine Gleichung n^{ten} Grades mit n verschiedenen Wurzeln und mit Koeffizienten aus einem Körper P heißt eine *einfache Abelsche Gleichung,* wenn sich ihre Wurzeln in der Form

$$\alpha_1, \quad \alpha_2 = \Theta(\alpha_1), \quad \alpha_3 = \Theta(\alpha_2) = \Theta^2(\alpha_1), \ldots$$
$$\alpha_n = \Theta(\alpha_{n-1}) = \Theta^{n-1}(\alpha_1), \Theta(\alpha_n) = \Theta^n(\alpha_1) = \alpha_1$$

ausdrücken lassen, wobei $\Theta(\alpha_1)$ eine rationale Funktion von α_1 mit Koeffizienten aus P bedeutet. *Die Galoissche Gruppe einer einfachen Abelschen Gleichung n^{ten} Grades mit den n Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ besteht entweder aus einer zyklischen Permutation $C = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ und ihren Potenzen oder aus den Permutationen $1, C^e, C^{2e}, \ldots, C^{(f-1)e}$, wobei $n = ef$ ist. Im ersten Fall ist die Gleichung irreduzibel, im zweiten Fall zerfällt ihre linke Seite in e irreduzible einfache Abelsche Gleichungen des Grades f.*

Umgekehrt: *Eine Gleichung n^{ten} Grades, deren Galoissche Gruppe aus der durch die zyklische Permutation $C = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ und ihren Potenzen erzeugten Gruppe oder einer ihrer Untergruppen besteht, ist eine einfache Abelsche Gruppe.*

Eine rationale Funktion von n beliebigen Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$, die bei Anwendung der zyklischen Permutation $C = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ formal ungeändert bleibt, heißt eine *zyklische Funktion der n Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$.*

Aus den beiden letzten Sätzen folgt: *Eine Gleichung n^{ten} Grades mit n verschiedenen Wurzeln und Koeffizienten aus einem Körper P ist dann und nur dann eine einfache Abelsche Glei-*

chung, wenn sich ihre Wurzeln in eine solche Reihenfolge bringen lassen, daß ihre zyklischen Funktionen mit Koeffizienten aus P *dem Körper* P *angehören.* Die einfachen Abelschen Gleichungen werden daher auch als *zyklische Gleichungen* bezeichnet.

Ist ε eine beliebige n^{te} Einheitswurzel (vgl. § 12), so ist

$$(\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3 + \cdots + \varepsilon^{n-1}\alpha_n)^n$$

im Körper der n^{ten} Einheitswurzeln eine zyklische Funktion der n Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$. Für eine einfache Abelsche Gleichung mit Koeffizienten aus P und Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ ist demnach diese Größe eine in dem durch Adjunktion der n^{ten} Einheitswurzeln erweiterten Körper P gelegene bekannte Zahl b. Die für den erweiterten Körper natürliche Irrationalität

$$\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3 + \cdots + \varepsilon^{n-1}\alpha_n$$

der Gleichung $f(z) = 0$ wird als ihre *Lagrangesche Resolvente*[1]) (Lagrange, *Œuvres* **3**, 331) bezeichnet. Man findet sie durch Ziehen der n^{ten} Wurzel aus b. Wählt man für ε eine *primitive n^{te} Einheitswurzel* von der Beschaffenheit, daß b nicht verschwindet, so lassen sich die Wurzeln einer einfachen Abelschen Gleichung in dem durch Adjunktion der n^{ten} Einheitswurzeln erweiterten Körper durch Ausziehen einer einzigen n^{ten} Wurzel, nämlich derjenigen aus der Größe b, finden (Abel, a. a. O., § 3). Ist $n = p^\lambda$ eine Primzahlpotenz, so kann man stets eine derartige primitive $p^{\lambda\,\text{te}}$ Einheitswurzel angeben, daß b von Null verschieden ist. Wegen der für $b = 0$ vorzunehmenden Modifikation vgl. Weber, *Algebra* **1**, 589. Stets gilt der Satz: *Alle Wurzeln einer im Körper* P *einfachen Abelschen Gleichung lassen sich bestimmen, indem man dem Körper* P *eine primitive n^{te} Einheitswurzel adjungiert und außerdem eine n^{te} Wurzel aus einer einzigen Größe zieht.*

Sind zwei Wurzeln einer irreduziblen Gleichung vom Primzahlgrad in einem derartigen Verhältnis, daß man die eine rational durch die andere ausdrücken kann, so ist die Gleichung eine irreduzible einfache Abelsche Gleichung. Normalgleichung vom Primzahlgrad und irreduzible einfache Abelsche Gleichung sind identische Begriffe (Abel, a. a. O., § 3).

1) Unter Umständen nennt man auch eine Wurzel einer Resolventengleichung eine Resolvente, daher der Name „Lagrangesche Resolvente". Diese genügt der Gleichung $z^n = b$, die in dem durch Adjunktion von ε erweiterten Körper (P, ε) eine rationale Resolvente der vorgelegten einfachen Abelschen Gleichung im Sinne der Bezeichnung auf S. 300 ist.

Eine einfache Abelsche Gleichung mit *reellen Koeffizienten*, bei welcher der zugrunde liegende *Körper* P *nur aus lauter reellen Zahlen* besteht, hat entweder nur reelle oder nur imaginäre Wurzeln. Der erste Fall tritt stets ein, wenn die Gleichung ungeraden Grades ist. Zur Lösung einer einfachen Abelschen Gleichung n^{ten} Grades mit zugrunde liegendem *reellem* Körper P ist die Adjunktion einer primitiven n^{ten} Einheitswurzel, das Ausziehen einer Quadratwurzel aus einer positiven Zahl und die Teilung eines Winkels in n gleiche Teile erforderlich (Abel, a. a. O. § 3). Die Vereinfachung gegenüber den einfachen Abelschen Gleichungen, bei denen der Körper P auch imaginäre Zahlen enthalten kann, liegt darin, daß bei jenen außer der Kenntnis einer primitiven n^{ten} Einheitswurzel noch eine n^{te} Wurzel aus einer Größe der Form $\varrho(\cos\varphi + i \sin\varphi)$ zu ziehen ist und dies das Ausziehen einer n^{ten} Wurzel aus der positiven Größe ϱ und die Teilung eines Winkels in n gleiche Teile erfordert.

Da jeder irreduzible Faktor einer Abelschen Gleichung wiederum eine Abelsche Gleichung ist, kann man sich auf die Betrachtung der irreduziblen Abelschen Gleichungen beschränken. Jede irreduzible (auch nicht einfache) Abelsche Gleichung ist eine Normalgleichung; daher ist die Ordnung ihrer Galoisschen Gruppe gleich dem Grade n der Gleichung. Ist $\mathfrak{G}$ die Galoissche Gruppe einer irreduziblen Abelschen Gleichung des Grades n, so kann man für die Abelsche Gruppe $\mathfrak{G}$ ein System von σ erzeugenden Basiselementen $A_1, A_2, \ldots, A_\sigma$ der Ordnungen $g_1, g_2, \ldots, g_\sigma$ derartig auswählen, daß das Produkt $g_1 g_2 \cdots g_\sigma = n$ wird (vgl. S. 202). Wählt man alsdann σ zu den durch

$$(A_2, A_3, \ldots, A_\sigma), \quad (A_1, A_3, \ldots, A_\sigma), \ldots, (A_1, A_2, \ldots, A_{\sigma-1})$$

erzeugten Gruppen zugehörige natürliche Irrationalitäten, so genügt jede von ihnen einer irreduziblen *einfachen* Abelschen Gleichung des Grades g_1 bzw. $g_2, \ldots, g_\sigma$, wie aus den Ergebnissen auf S. 300 folgt. Hieraus ergibt sich der Satz: *Die Wurzeln jeder beliebigen irreduziblen Abelschen Gleichung n^{ten} Grades mit Koeffizienten aus* P *lassen sich als rationale Funktionen mit Koeffizienten aus* P *von Wurzeln irreduzibler einfacher Abelscher Gleichungen mit Koeffizienten aus* P *darstellen, bei denen das Produkt der Grade gleich n ist.*

Da man die Basis einer Abelschen Gruppe (vgl. S. 203) verschieden wählen kann, so ergeben sich folgende Sätze:

I. Die Auflösung einer irreduziblen Abelschen Gleichung des Grades n mit der Galoisschen Gruppe $\mathfrak{G}$ kann auf die Auflösung einer Reihe nebeneinander zu lösender irreduzibler einfacher Abelscher Gleichungen der Grade $p_1^{\tau_1}, p_2^{\tau_2}, \ldots, p_\sigma^{\tau_\sigma}$ mit Koeffizienten aus dem der Betrachtung zugrunde liegenden Körper reduziert werden; hierbei ist $n = p_1^{\tau_1} p_2^{\tau_2} \ldots p_\sigma^{\tau_\sigma}$, und $p_1, p_2, \ldots, p_\sigma$ bedeuten Primzahlen, die unter Umständen nicht alle voneinander verschieden sind und deren Anzahl alsdann größer als die Zahl der in n enthaltenen verschiedenen Primzahlen ist.

II. Die Auflösung einer irreduziblen Abelschen Gleichung des Grades n läßt sich auf die Auflösung einer Reihe nebeneinander zu lösender, irreduzibler einfacher Abelscher Gleichungen mit Koeffizienten aus dem der Betrachtung zugrunde liegenden Körper reduzieren, so daß der Grad einer jeden Gleichung dieser Reihe teilbar durch den Grad der folgenden Gleichung oder ihm gleich wird und das Produkt der Grade aller Gleichungen gleich der Zahl n ist. Die Anzahl der Gleichungen ist gleich dem Range der Gruppe (vgl. S. 203).

Die Behandlung einer beliebigen Abelschen Gleichung ist demnach auf diejenige einfacher Abelscher Gleichungen zurückführbar. Da diese zur Lösung nur eine Wurzelausziehung und Kenntnis der Einheitswurzeln erfordern, die sich ebenfalls durch Radikale darstellen lassen, so folgt: *Jede Abelsche Gleichung ist algebraisch auflösbar* (Abel, a. a. O. § 4).

Die Wurzeln jeder im Körper P irreduziblen Abelschen Gleichung n^{ten} Grades lassen sich mit Hilfe einer Wurzel α der Gleichung in die Form

$$(A) \qquad \Theta_1^{h_1} \Theta_2^{h_2} \ldots \Theta_\sigma^{h_\sigma}(\alpha)$$

bringen, so daß in dieser Form jede Wurzel der Gleichung einmal und auch nur einmal erscheint, falls h_i die Zahlen $0, 1, 2, \ldots, g_i - 1$ durchläuft. Die mit einander vertauschbaren Θ_i bedeuten die Operationen einer rationalen Funktion mit Koeffizienten aus P und die Zahl h_i die h_i-fache Wiederholung $(i = 1, 2, \ldots, \sigma)$; g_i ist die kleinste Zahl, für die $\Theta_i^{g_i}(\alpha) = 1$ ist. Nennt man $g_1, g_2, \ldots, g_\sigma$ *die Wiederholungszahlen,* so gilt folgender Satz: *Jeder Basis der Galoisschen Gruppe $\mathfrak{G}$ einer irreduziblen Abelschen Gleichung entspricht eine Darstellung der Gleichungswurzeln in der Form (A), so daß die Wiederholungszahlen mit den Ordnungszahlen der Basiselemente übereinstimmen.*

Jede irreduzible Abelsche Gleichung, deren Grad keine

Primzahl ist, ist als Normalgleichung imprimitiv, da ihre Galoissche Gruppe als reguläre Gruppe imprimitiv ist (vgl. S. 212). *Die Auflösung einer irreduziblen Abelschen Gleichung vom Primzahlpotenzgrad p^τ kann auf die von τ nacheinander zu lösenden irreduziblen Abelschen Gleichungen vom Primzahlgrad p reduziert werden.*

Satz von Kronecker (*Monatsb. d. Berl. Akad.* (1853), 373, ebenda (1877), 849, Weber, *Algebra* **2**, 762, Hilbert, *Math.-Ver.* **4**, *Die Theorie der algebraischen Zahlkörper*, Kap. 23, Mertens, *Journ. f. Math.* **131**, 87 (1906), Weber, ebenda **132**, 167 (1907), *Math. Ann.* **67**, 32 (1909)): *Alle Wurzeln Abelscher Gleichungen mit ganzzahligen Koeffizienten sind rationale Funktionen von Einheitswurzeln mit rationalen Zahlenkoeffizienten, und alle rationalen Funktionen von Einheitswurzeln mit rationalen Zahlenkoeffizienten sind Wurzeln ganzzahliger Abelscher Gleichungen.* Anders ausgedrückt: *Jeder durch eine irreduzible Abelsche Gleichung aus dem natürlichen Rationalitätsbereich hervorgehende Zahlkörper ist ein Kreisteilungskörper, d. h. ein durch eine Einheitswurzel $e^{\frac{2\pi i}{m}}$ erzeugter Körper oder ein in diesem Körper enthaltener Unterkörper, und jeder Kreisteilungskörper ist ein Abelscher Körper.*

Ebenso wie nach dem voraufgehenden Satz die Exponentialfunktion $e^{2\pi i\omega}$ für rationale Werte des Arguments ω mit den Abelschen Gleichungen mit ganzzahligen Koeffizienten verknüpft ist, trifft dies auch für die *elliptische Modulfunktion, z. B. die Invariante $j(\omega)$, zu, wenn ω Wurzel einer ganzzahligen quadratischen Gleichung mit negativer Diskriminante ist.* Eine derartige Modulfunktion heißt nach Kronecker *singulär. Eine singuläre Invariante $j(\omega)$ genügt einer irreduziblen Gleichung mit ganzzahligen Koeffizienten, der sogenannten Klassengleichung, die auch noch in dem durch Adjunktion der Quadratwurzel aus der Diskriminante der quadratischen Gleichung erweiterten Körper irreduzibel bleibt und dann eine irreduzible Abelsche Gleichung ist.* Daß die singulären elliptischen Modulfunktionen durch Wurzelzeichen ausdrückbar sind, was aus der Natur der Klassengleichung, eine „relativ Abelsche“ Gleichung zu sein, folgt, ahnte bereits Abel, vgl. die Bemerkungen von Sylow in Abels *Œuvres* **2**, 316; den ersten Beweis gab Kronecker, *Monatsb. d. Berl. Akad.* (1857), 455, (1862), 363 und (1877), 851. Eine zusammenfassende Darstellung mit zahlreichen Literaturnachweisen findet man in Webers Artikel *„Komplexe*

Multiplikation", Enzyklopädie der math. Wiss. **1**, 716 und in dem dritten Buche des dritten Bandes seiner Algebra. Vgl. auch F. Klein, *Ausgewählte Kapitel der Zahlentheorie, Autographierte Vorlesungen*, Göttingen 1896. Es gilt auch umgekehrt folgender Satz, Kroneckers „liebster Jugendtraum" (Brief von Kronecker an Dedekind, veröff. von Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 115): *Alle in einem imaginären quadratischen Körper Abelschen Gleichungen lassen sich durch die Körper der singulären Moduln und durch die Kreisteilungskörper lösen.* Einen Beweis hat zuerst Fueter, *Journ. f. Math.* **132**, 255 (1907) geliefert; vgl. auch Fueter, *Göttinger Diss.* (1903). Eine Ausdehnung dieser Untersuchungen ist der von Hilbert, (*Gött. Nachr.* (1898), abgedr. *Acta math.* **26**, 99 (1902)) und Furtwängler (*Math. Ann.* **63**, 1 (1907)) stammende Nachweis der Existenz eines Klassenkörpers für einen beliebigen algebraischen Grundkörper P, der im einfachsten Fall der obige imaginäre quadratische Körper ist. Dieser allgemeine Klassenkörper wird durch eine im Körper P Abelsche Gleichung mit Koeffizienten aus P oder aus einem in diesem Körper enthaltenen Unterkörper definiert.

§ 12. Die Einheitswurzeln. Die Kreisteilungsgleichung. Gaußsche Summen. Reine Gleichung.

Alle Wurzeln der Gleichung $z^n = 1$ *heißen* n^{te} *Einheitswurzeln; sie sind sämtlich voneinander verschieden und werden, wenn* k *die Werte* $0, 1, 2, \ldots, n-1$ *durchläuft, in der Form* $\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ *gegeben.*

Die Bilder der Größen ε_k in der sog. Gaußschen Ebene der komplexen Zahlen liegen auf einem Kreise mit dem Radius Eins und bilden ein reguläres n-Eck, dessen erster Eckpunkt sich auf der Achse der reellen Zahlen befindet; die Teilung des Kreises in n gleiche Teile hängt demnach von der Lösung der Gleichung $z^n = 1$ ab.

Befriedigt ε *die Gleichung* $z^n = 1$, *so ist auch* ε^m *eine* n^{te} *Einheitswurzel, wenn* m *irgendeine ganze positive oder negative Zahl einschließlich der Null ist. Das Produkt zweier beliebiger* n^{ter} *Einheitswurzeln ist wiederum eine* n^{te} *Einheitswurzel.*

Ist ε *zugleich* n^{te} *und* m^{te} *Einheitswurzel, so ist es auch* d^{te} *Einheitswurzel, wenn* d *der größte gemeinsame Teiler von* n *und* m *ist.*

Die Summe s_k *der* k^{ten} *Potenzen aller* n^{ten} *Einheitswurzeln ist*

Null, außer wenn k durch n teilbar ist. Ist k durch n teilbar, so ist $s_k = n$.

*Eine n^{te} Einheitswurzel heißt eine **primitive** n^{te} Einheitswurzel, wenn ε keiner Gleichung $z^m = 1$ genügt, wobei $m < n$ ist.* Eine nicht primitive n^{te} Einheitswurzel heißt eine *imprimitive n^{te} Einheitswurzel.*

Eine charakteristische Eigenschaft einer primitiven n^{ten} Einheitswurzel ε ist, daß ihre Potenzen $\varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^n$ sämtliche verschiedene n^{te} Einheitswurzeln ergeben. Durch Potenzieren einer imprimitiven n^{ten} Einheitswurzel erhält man niemals sämtliche n^{te} Einheitswurzeln.

Jede imprimitive n^{te} Einheitswurzel genügt einer Gleichung $z^m = 1$, wobei m ein Divisor von n ist. Umgekehrt ist jede Wurzel von $z^m = 1$, wenn m ein Teiler von n ist, eine imprimitive n^{te} Einheitswurzel. Jede imprimitive n^{te} Einheitswurzel ist primitive m^{te} Einheitswurzel, wobei m ein gewisser Divisor von n ist.

Die Gleichung $z^n = 1$ hat soviel primitive n^{te} Einheitswurzeln, wie die Anzahl $\varphi(n)$ derjenigen ganzen positiven Zahlen beträgt, die kleiner als n und relativ prim zu n sind. Ist p eine Primzahl, so ist jede Wurzel der Gleichung $z^p = 1$, abgesehen von der Zahl 1, primitive p^{te} Einheitswurzel. Es ist $\varphi(p) = p - 1$.

Ist p^k die k^{te} Potenz der Primzahl p, so findet man alle Wurzeln der Gleichung $z^{p^k} = 1$, indem man je eine Wurzel $\omega_1, \omega_2, \ldots, \omega_k$ der k Gleichungen $z^p = 1, z^p = \omega_1, z^p = \omega_2, \ldots, z^p = \omega_{k-1}$ wählt und das Produkt $\omega_1 . \omega_2 \ldots \omega_k$ bildet. Dann und nur dann, wenn ω_1 eine primitive p^{te} Einheitswurzel ist, d. h. $\omega_1 \neq 1$, ist das Produkt $\omega_1 . \omega_2 \ldots \omega_k$ eine primitive $p^{k\,te}$ Einheitswurzel. Es ist $\varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$.

Ist $n = p_1^{k_1} \cdot p_2^{k_2} \ldots p_l^{k_l}$, wobei $p_1, p_2, \ldots, p_l$ lauter untereinander verschiedene Primzahlen sind, so findet man alle Wurzeln der Gleichung $z^n = 1$, indem man je eine Wurzel $\lambda_1, \lambda_2, \ldots, \lambda_l$ der Gleichungen $z^{p_1^{k_1}} = 1, z^{p_2^{k_2}} = 1, \ldots, z^{p_l^{k_l}} = 1$ wählt und ihr Produkt $\lambda_1 . \lambda_2 \ldots \lambda_l$ bildet. Dieses Produkt stellt dann und nur dann eine primitive n^{te} Einheitswurzel dar, wenn alle Größen $\lambda_1, \lambda_2, \ldots, \lambda_l$ primitive $p_1^{k_1}$ bzw. $p_2^{k_2}, \ldots, p_l^{k_l\,te}$ Einheitswurzeln sind. Es ist $\varphi(n) = \varphi(p_1^{k_1})\,\varphi(p_2^{k_2}) \ldots \varphi(p_l^{k_l}) =$

$$= p_1^{k_1} \cdot p_2^{k_2} \ldots p_l^{k_l}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_l}\right).$$

Ist ε eine primitive n^{te} Einheitswurzel, so sind, wenn k zu n

relativ prim ist, alle k^{ten} Potenzen von ε und auch nur diese Potenzen primitive n^{te} Einheitswurzeln.

Die Summe aller primitiven n^{ten} Einheitswurzeln wird mit $\mu(n)$ bezeichnet. Ist n durch das Quadrat einer Primzahl teilbar, so hat die zahlentheoretische Funktion $\mu(n)$ den Wert 0, ist n das Produkt von t verschiedenen Primzahlen, so hat $\mu(n)$ den Wert $(-1)^t$; $\mu(1)$ ist gleich $+1$. (Moebius, *Journ. f. Math.* **9**, 109 (1832), *Ges. Werke* **4**, 595, Mertens, *Journ. f. Math.* **77**, 289 (1874)).

Die $\varphi(n)$ primitiven n^{ten} Einheitswurzeln genügen der Gleichung $\varphi(n)^{ten}$ Grades:

$$Z_n = \prod \left(z^{\frac{n}{t}} - 1\right)^{\mu(t)} = 0;$$

hierbei ist das Produkt über alle Teiler t von n, einschließlich n und 1, zu erstrecken, und $\mu(t)$ bedeutet die oben definierte zahlentheoretische Funktion. Die Gleichung $Z_n = 0$ hat ganzzahlige Koeffizienten; sie ist im absoluten Rationalitätsbereiche irreduzibel, und bleibt es auch noch bei Adjunktion einer primitiven q^{ten} Einheitswurzel, falls n und q relativ prime Zahlen sind. (Kronecker, *Journ. de math.* **19**, 192 (1854), *Ges. Werke* **1**, 92, *Journ. f. Math.* **100**, 79 (1887)).

Da die sukzessiven Potenzen jeder Wurzel der Gleichung $Z_n = 0$ alle n Wurzeln der Gleichung $z^n = 1$ liefern, von der die Teilung des Kreises in n gleiche Teile abhängt, heißt die Gleichung $Z_n = 0$ die *Kreisteilungsgleichung.*

Für eine Primzahl $n = p$ lautet die Kreisteilungsgleichung:

$$\frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \cdots + 1 = 0.$$

Für eine Primzahlpotenz $n = p^k$ lautet die Kreisteilungsgleichung

$$\frac{z^{p^k} - 1}{z^{p^{k-1}} - 1} = z^{(p-1)p^{k-1}} + z^{(p-2)p^{k-1}} + z^{(p-3)p^{k-1}} + \cdots + z^{p^{k-1}} + 1 = 0.$$

Ist $n = p_1^{k_1} \cdot p_2^{k_2} \ldots p_l^{k_l}$ ($p_1, p_2, \ldots, p_l$ verschiedene Primzahlen), so ist

$$Z_n = \prod \left(z^{\frac{n}{t}} - 1\right)^{\mu(t)} = \frac{\left(z^n - 1\right)\left(z^{\frac{n}{p_1 p_2}} - 1\right)\left(z^{\frac{n}{p_1 p_3}} - 1\right)\ldots}{\left(z^{\frac{n}{p_1}} - 1\right)\left(z^{\frac{n}{p_2}} - 1\right)\left(z^{\frac{n}{p_3}} - 1\right)\ldots} = 0.$$

Die Diskriminante der Gleichung $Z_n = 0$ hat den Wert $\dfrac{(-1)^{\frac{\varphi(n)}{2}} \cdot n^{\varphi(n)}}{p_1^{\frac{\varphi(n)}{\varphi(p_1)}} \cdot p_2^{\frac{\varphi(n)}{\varphi(p_2)}} \cdots p_l^{\frac{\varphi(n)}{\varphi(p_l)}}}$, wobei φ die oben eingeführte zahlentheoretische Funktion bedeutet. (Vgl. die elementare Ableitung von Rados, *Journ. f. Math.* **131**, 49 (1906)).

Die Irreduzibilität der Gleichung $Z_p = 0$ im absoluten Rationalitätsbereich hat zuerst Gauß (*Disquisitiones arithmeticae* (1801), Art. 341) bewiesen. Andere Beweise stammen von Kronecker, *Journ. f. Math.* **29**, 280 (1845), *Journ. de math.* (2) **1**, 399 (1856), *Ges. Werke* **1**, 1 und 99, Schoenemann und Eisenstein (Schoenemann, *Journ. f. Math.* **32**, 100 (1846), Eisenstein, ebenda **39**, 166 (1850), Schoenemanns Reklamation, ebenda **40**, 188 (1850), a. a. O. Zeile 8 v. u. ist **32**, § 61 zu lesen). Die Irreduzibilität von $Z_{p^k} = 0$ im absoluten Rationalitätsbereich bei Serret, *Journ. de math.* **15**, 296 (1850). Daß die Gleichung $Z_n = 0$ für *beliebiges n* im absoluten Rationalitätsbereich irreduzibel ist, und es auch sogar bleibt, wenn eine Wurzel einer ganzzahligen irreduziblen Gleichung adjungiert wird, deren Diskriminante zu n relativ prim ist, hat Kronecker (*Journ. de math.* **19**, 177 (1854), *Ges. Werke* **1**, 75, *Journ. f. Math.* **100**, 79 (1887)) zuerst bewiesen. Andere Beweise der Irreduzibilität von $Z_n = 0$ für beliebiges n stammen von Dedekind, *Journ. f. Math.* **54**, 27 (1857), Arndt, *Journ. f. Math.* **56**, 178 (1859), Lebesgue, *Journ. de math.* (2) **4**, 105 (1859).

Die Kreisteilungsgleichung $Z_n = 0$ ist eine irreduzible Abelsche Gleichung. Ihre Galoissche Gruppe ist eine transitive Abelsche Gruppe des Grades und der Ordnung $\varphi(n)$, die holoedrisch isomorph ist mit der Gruppe der Zahlklassen der zu n relativ primen Zahlen (vgl. S. 203, Z. 10 v. u.). *Die Gruppe ist dann und nur dann zyklisch, wenn n die Potenz einer ungeraden Primzahl, das Doppelte hiervon oder 2 oder 4 ist. Für diese und nur für diese Werte der Zahl n ist die Kreisteilungsgleichung eine irreduzible einfache Abelsche Gleichung.*

Aus dem Satz: „Eine Normalgleichung ist dann und nur dann durch *Quadratwurzeln* lösbar, wenn ihr Grad eine Potenz von 2 ist", folgt: *Die Wurzeln der Kreisteilungsgleichung $Z_n = 0$ sind dann und nur dann durch Quadratwurzeln darstellbar, wenn der Grad $\varphi(n)$ von $Z_n = 0$ eine Potenz von 2 ist.* Da sich alle Wurzeln von $z^n = 1$ durch Potenzieren einer beliebigen primitiven n^{ten} Einheitswurzel ergeben, folgt *das Theorem von* Gauß (*Disquisitiones arithmeticae*, Art. 365, 366): *Damit die Gleichung $z^n = 1$ durch Quadratwurzeln lösbar sein soll, ist notwendig und hinreichend, daß n entweder gleich einer Primzahl der Form $2^h + 1$ oder gleich 2^m oder gleich einem Produkt mehrerer verschiedener Zahlen dieser Formen ist. Dann und nur dann, wenn sich die Gleichung $z^n = 1$ durch Quadratwurzeln auflösen läßt, kann der Kreisumfang mit Zirkel und Lineal in n gleiche Teile geteilt werden.* Für dieselben Werte von n kann auch der *Umfang der Lemniskate* mit Hilfe von Zirkel und Lineal in n gleiche Teile geteilt werden (Gauß, *Disquisitiones arithmeticae,* Art. 335, Abel, *Recherches sur les fonctions elliptiques, Œuvres* **1**, p. 361, Eisenstein, *Journ. f. Math.* **39**, 160, 224, 275 (1850), Schwering, *Journ. f. Math.* **107**, 196 (1890)). Eine Zahl der Form $2^h + 1$ kann nur dann Primzahl sein, wenn $h = 2^k$ ist; jedoch sind nicht alle Zahlen der Form $2^{2^k} + 1$ Primzahlen. $k = 0, 1, 2, 3, 4$ liefert die Primzahlen 3, 5, 17, 257, 65537; hingegen erhält man für $k = 5$ die Zahl $2^{2^5} + 1 = 4294967297$, die durch 641 teilbar ist. Vermutlich existiert nur eine endliche Anzahl von Primzahlen der Form $2^{2^k} + 1$. Die Gleichung $z^3 = 1$ hat die Wurzeln

$$1, -\frac{1}{2} \pm \frac{i}{2}\sqrt{3},$$

die Gleichung $z^5 = 1$ besitzt die primitive Wurzel

$$\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} = \frac{1}{4}\left(-1 + \sqrt{5} + i\sqrt{10 + 2\sqrt{5}}\right),$$

die Wurzeln der Gleichung $z^{17} = 1$ findet man in Gauß, *Disquisitiones arithmeticae,* Art. 354. Die Gleichung $z^{257} = 1$ hat Richelot, *Journ. f. Math.* **9**, 1 (1832) behandelt. Für die Gleichung $z^{65537} = 1$ vgl. Hermes, *Gött. Nachr.* (1894), 170. Unterhalb 100 gibt es im ganzen 25 Zahlen, für die $z^n = 1$ durch Quadratwurzeln lösbar ist, nämlich $n = 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96$.

Die geometrische Konstruktion des regulären Siebzehnecks mittelst des Lineals und eines festen Kreises geben v. Staudt, *Journ. f. Math.* **24**, 251 (1842) und Schroeter, ebenda **75**, 13 (1873), nach Mascheroni unter alleiniger Anwendung des Zirkels Gérard, *Math. Ann.* **48**, 390 (1897). Die Konstruktion des regulären 257-Ecks bei Pascal, *Rend. Accad. di Na-*

poli (1887). Für nicht mittelst Zirkels und Lineals durchführbare Fälle der Kreisteilung, nämlich 7, 13 und 97 vgl. Pascal, *Giorn. di mat.* **25**, 82 (1887), für 19 und 37 Amaldi, ebenda **30**, 141 (1892). Für die hier behandelten Fragen vgl. besonders Klein, *Vorträge über ausgewählte Fragen der Elementargeometrie*, ausg. von Taegert, Leipzig 1895, und Enriques, *Fragen der Elementargeometrie*, Teil II, deutsch von Fleischer, Leipzig 1907.

Wir beschränken uns darauf, von den Fällen, in denen die Kreisteilungsgleichung eine irreduzible einfache Abelsche Gleichung ist ($n = 2, 4, p^\lambda, 2p^\lambda$, vgl. oben), denjenigen näher zu betrachten, für den n eine Primzahl ist.

Ist p eine Primzahl, so lassen sich die Wurzeln der Gleichung

$$\frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \cdots + 1 = 0$$

in der Form $\alpha, \Theta(\alpha), \Theta^2(\alpha), \ldots, \Theta^{p-2}(\alpha)$ anordnen, hierbei ist α eine beliebige Wurzel, $\Theta^i(\alpha) = \alpha^{g^i}$, und g bedeutet eine primitive Wurzel für die Primzahl p.[1]

Da die Gleichung $\frac{z^p - 1}{z - 1} = 0$ eine im Körper der reellen Zahlen einfache Abelsche Gleichung ist, kann ihre Lösung bewerkstelligt werden (vgl. S. 308) *mittelst einer primitiven $(p-1)^{ten}$ Einheitswurzel, Teilung eines Winkels in $p - 1$ gleiche Teile und Ausziehung einer Quadratwurzel aus einer positiven Zahl, die hier die Zahl p ist* (Gauß, *Disquisitiones arithmeticae,* Art. 360).

Zur weiteren Behandlung von $\frac{z^p - 1}{z - 1} = 0$ hat Gauß, *Disquisitiones arithmeticae,* Art. 343, die *f-gliedrigen Perioden* eingeführt. Sei $p - 1$ irgendwie in zwei ganzzahlige positive Faktoren e und f zerlegt. Ist α eine beliebige Wurzel der Gleichung $\frac{z^p - 1}{z - 1} = 0$, so heißen die e Funktionen:

$$\eta_\lambda = \alpha^{g^\lambda} + \alpha^{g^{e+\lambda}} + \alpha^{g^{2e+\lambda}} + \cdots \alpha^{g^{(f-1)e+\lambda}} \qquad (\lambda = 0, 1, 2, \ldots, e-1)$$

die e Gaußschen f-gliedrigen Perioden. Die e Perioden sind Wurzeln der Gleichung e^{ten} Grades:

$$\Phi = (\eta - \eta_0)(\eta - \eta_1)(\eta - \eta_2) \cdots (\eta - \eta_{e-1}) = 0.$$

1) g heißt eine primitive Wurzel für die Primzahl p, wenn die Zahlen $g, g^2, g^3, \ldots, g^{p-1}$ bei ihrer Division durch p, von der Reihenfolge abgesehen, die Zahlen $1, 2, \ldots, p-1$ ergeben.

Diese hat ganzzahlige Koeffizienten und ist eine im absoluten Rationalitätsbereich irreduzible einfache Abelsche Gleichung. Jede der Perioden ist also eine ganze rationale Funktion jeder anderen mit rationalen Zahlenkoeffizienten. Nach Adjunktion irgendeiner Wurzel dieser Normalgleichung zerfällt die Gleichung $\frac{z^p - 1}{z - 1} = 0$ in das Produkt der e Gleichungen:

$$\chi_\lambda = \left(z - \alpha^{g^\lambda}\right)\left(z - \alpha^{g^{e+\lambda}}\right)\left(z - \alpha^{g^{2e+\lambda}}\right)\ldots\left(z - \alpha^{g^{(f-1)e+\lambda}}\right) = 0.$$
$$(\lambda = 0, 1, 2, \ldots, e-1)$$

Die Koeffizienten jeder dieser e Gleichungen $\chi_\lambda = 0$ *sind lineare ganze Funktionen der e Perioden* $\eta_0, \eta_1, \ldots, \eta_{e-1}$ *mit ganzzahligen Koeffizienten, und jede dieser Gleichungen ist in dem durch Adjunktion der e Perioden erweiterten Körper eine irreduzible einfache Abelsche Gleichung.* Läßt sich die Zahl f irgendwie in zwei ganzzahlige Faktoren e' und f' spalten, so bilde man die sog. f'-gliedrigen Perioden:

$$\eta'_\lambda = \alpha^{g^{\lambda e}} + \alpha^{g^{(e'+\lambda)e}} + \alpha^{g^{(2e'+\lambda)e}} + \cdots + \alpha^{g^{((f'-1)e'+\lambda)e}}$$
$$(\lambda = 0, 1, 2, \ldots, e'-1).$$

Die Größen $\eta_0', \eta_1', \ldots, \eta'_{e'-1}$ genügen einer Gleichung, deren Koeffizienten lineare ganze Funktionen von $\eta_0, \eta_1, \ldots, \eta_{e-1}$ mit ganzzahligen Koeffizienten sind. Diese Gleichung ist in dem durch die Perioden $\eta_0, \eta_1, \ldots, \eta_{e-1}$ erweiterten Körper eine irreduzible Abelsche Gleichung. Nach Adjunktion einer Wurzel dieser Normalgleichung zerfällt jede der e Gleichungen χ_λ in e' Gleichungen vom Grade f'. Jede dieser Gleichungen ist in dem durch $\eta_0', \eta_1', \ldots, \eta'_{e'-1}$ erweiterten Körper eine irreduzible einfache Abelsche Gleichung. Dieses Verfahren läßt sich fortsetzen, indem man f' in Faktoren spaltet. Vgl. Gauß, *Disquisitiones arithmeticae,* Art. 342—354.

Die *Galoissche Theorie* liefert den Kern dieses Verfahrens. Die Wurzeln der Gleichung $\frac{z^p - 1}{z - 1} = 0$ seien mit

$$\alpha_i = \Theta^i(\alpha) = \alpha^{g^i} \qquad (i = 0, 1, 2, \ldots, p-2)$$

bezeichnet. Die Galoissche Gruppe $\mathfrak{G}$ der Gleichung $\frac{z^p - 1}{z - 1} = 0$ wird von der zyklischen Permutation $C = (\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{p-2})$ und ihren Potenzen gebildet. Die Permutation C^e und ihre Potenzen bilden eine Untergruppe $\mathfrak{G}_1$ von $\mathfrak{G}$ des Index e. Jede der e Perioden $\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}$ ist eine zu $\mathfrak{G}_1$ zugehörige natürliche Irrationalität. Die e Perioden vertauschen sich bei allen $\mathfrak{G}_1$ nicht angehörigen Permutationen von $\mathfrak{G}$ nur untereinander und genügen daher einer irreduziblen Normalgleichung $\Phi = 0$, deren Galoissche Gruppe zu $\mathfrak{G}/\mathfrak{G}_1$ isomorph ist und aus der zyklischen Permutation $T = (\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1})$ und ihren Potenzen besteht. Adjungiert man η_0 zum absoluten Rationalitätsbereich, so reduziert sich die Galoissche Gruppe $\mathfrak{G}$ unserer Gleichung $\frac{z^p - 1}{z - 1} = 0$ auf die intransitive Gruppe $\mathfrak{G}_1$ der Ordnung f. Ist $f = e'f'$, so erzeugt die Permutation $C^{ee'}$ mit ihren Potenzen eine Untergruppe $\mathfrak{G}_2$ von $\mathfrak{G}_1$ vom Index e'; die Funktionen $\eta_0', \eta_1', \ldots, \eta_{e'-1}'$ sind zu $\mathfrak{G}_2$ zugehörige natürliche Irrationalitäten, die sich bei allen $\mathfrak{G}_2$ nicht angehörigen Permutationen von $\mathfrak{G}_1$ nur untereinander permutieren.

Für eine ungerade Primzahl p kann man $p - 1$ in das Produkt $2 \cdot \frac{(p-1)}{2}$ zerlegen. Für $e = 2$, $f = \frac{p-1}{2}$ wird:

$$\eta_0 = \alpha + \alpha^{g^2} + \alpha^{g^4} + \cdots + \alpha^{g^{p-3}},$$
$$\eta_1 = \alpha^{g} + \alpha^{g^3} + \cdots + \alpha^{g^{p-2}}.$$

Die zwei Größen η_0 und η_1 genügen der quadratischen Gleichung $\Phi = \eta^2 + \eta + \frac{1 - (-1)^{\frac{p-1}{2}} p}{4} = 0$ mit ganzzahligen Koeffizienten. Es wird:

$$\eta_0 = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{(-1)^{\frac{p-1}{2}} \cdot p}, \quad \eta_1 = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{(-1)^{\frac{p-1}{2}} \cdot p},$$
$$\eta_0 - \eta_1 = \pm \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}.$$

Durch Adjunktion von $\sqrt{(-1)^{\frac{p-1}{2}} \cdot p}$ zum absoluten Rationalitätsbereich wird $\frac{z^p - 1}{z - 1} = 0$ reduzibel und zerfällt in zwei Faktoren des Grades $\frac{p-1}{2}$.

Bei η_0 sind die Exponenten von α die quadratischen Reste, bei η_1 die quadratischen Nichtreste unter den Zahlen $1, 2, \ldots, p - 1$ nach p. Daher ist: $\eta_0 - \eta_1 = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) \alpha^s$, wobei $\left(\frac{s}{p}\right)$ das Legendresche Symbol ist, das den Wert $+1$

oder -1 hat, je nachdem s quadratischer Rest oder Nichtrest der Primzahl p ist.

Ein berühmtes Problem, dem Gauß (1811) (*Ges. Werke* **2**, 9, deutsche Ausg. von E. Netto in *Die sechs Beweise des Fundamentaltheorems über quadratische Reste von Gauß* in Ostwalds *Klassikern der exakt. Wiss.* Nr. 122, S. 51) eine besondere Abhandlung gewidmet hat, ist die *Bestimmung des Vorzeichens* der oben auf der rechten Seite von $\eta_0 - \eta_1$ auftretenden Quadratwurzel, die davon abhängt, welche Einheitswurzel man für α wählt. Ist $\alpha = e^{\frac{2\pi i \mu}{p}}$, wobei μ zu p relativ prim ist, und demnach $\eta_0 - \eta_1 = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) e^{\frac{2\pi i \mu s}{p}}$, so hat die Summe $\sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) e^{\frac{2\pi i \mu s}{p}}$, *die man als Gaußsche Summe bezeichnet, den Wert* $+\left(\frac{\mu}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}$; *hierbei ist* $\left(\frac{\mu}{p}\right)$ *das Legendresche Symbol und* $i = \sqrt{-1}$. Mithin ergibt sich für $p \equiv 1 \pmod{4}$ die Wertbestimmung $\left(\frac{\mu}{p}\right) \cdot \sqrt{p}$ und für $p \equiv 3 \pmod{4}$ gleich $i\left(\frac{\mu}{p}\right)\sqrt{p}$. Die Gleichung

$$\sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) e^{\frac{2\pi i \mu s}{p}} = \left(\frac{\mu}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}$$

bleibt noch richtig, wenn p eine beliebige ganze, aber keine Primzahl mehr ist und $\left(\frac{s}{p}\right)$ das Jacobische Symbol bedeutet, das jedesmal, wenn s und p einen gemeinsamen Teiler besitzen, den Wert 0 zu erhalten hat.[1]) $\left(\frac{\mu}{p}\right)$ ist dann ebenfalls das Jacobische Symbol. Auch können μ und p einen Teiler gemein haben; in diesem Fall ist $\left(\frac{\mu}{p}\right) = 0$ zu nehmen. Eine Darstellung der in die Zahlentheorie gehörigen Gaußschen Summen findet man bei Bachmann, *Analytische Zahlentheorie*, Leipzig 1894, S. 145.

---

1) Sind s und p zwei relativ prime Zahlen und ist p in die Primzahlfaktoren $p = p_1 p_2 p_3 \ldots$ zerlegbar, so ist das Jacobische Symbol definiert durch

$$\left(\frac{s}{p}\right) = \left(\frac{s}{p_1}\right)\left(\frac{s}{p_2}\right)\left(\frac{s}{p_3}\right)\ldots, \text{ wobei } \left(\frac{s}{p_1}\right), \left(\frac{s}{p_2}\right), \left(\frac{s}{p_3}\right), \ldots$$

die Legendreschen Symbole sind.

Weitere Angaben über Einheitswurzeln findet man in der Monographie von Bachmann, *Die Lehre von der Kreisteilung*, Leipzig 1872, Weber, *Algebra* **1**, 596ff., **2**, 69 u. 736 und D. Hilbert, *Die Theorie der algebraischen Zahlkörper, Math.-Ver.* **4** (1897), S. 325 (der Kreiskörper). Vgl. auch § 11, S. 310.

Wir schließen diesen Paragraphen mit der Betrachtung der *reinen Gleichung* $z^n = a$, die auch als *binomische Gleichung* bezeichnet wird. *Ist n eine Primzahl p, so ist die Gleichung $z^p - a = 0$ in jedem Körper* P, *der a enthält, dann und nur dann reduzibel, wenn a die p^{te} Potenz einer Zahl aus* P *ist.* Ist also die Gleichung $z^p = a$ reduzibel, so hat sie eine dem Körper P angehörige Wurzel. (Abel, *Œuvres* **1**, 72, Jordan, *Traité*, p. 300, Mertens, *Monatsh. f. Math.* **2**, 291 (1891), Kneser, *Journ. f. Math.* **106**, 48 (1890)).

Für beliebiges n gilt folgender Satz (Capelli, *Rend. Acc. di Napoli*, Dez. 1897, Febr. 1898, *Math. Ann.* **54**, 602 (1901), Vahlen, *Acta math.* **19**, 195 (1895), Wendt, *Math. Ann.* **53**, 450 (1900)): *Die Gleichung $z^n - a = 0$ ist in einem beliebigen Körper* P, *der a enthält, dann und nur dann reduzibel, wenn a die h^{te} Potenz einer Zahl aus* P *ist, wobei h ein Teiler von n ist, oder wenn n durch 4 teilbar und $-a$ das Vierfache der vierten Potenz einer Zahl aus* P *ist.*

Ist α_0 eine Wurzel der Gleichung $z^n - a = 0$, so ergeben sich ihre sämtlichen Wurzeln in der Form $\alpha_i = \varepsilon^i \alpha_0$ $(i = 0, 1, 2, \ldots, n-1)$, wobei ε eine primitive n^{te} Einheitswurzel ist. Jede reine Gleichung $z^n - a = 0$ ist in einem Körper, der die n^{ten} Einheitswurzeln enthält, eine Abelsche Gleichung. In dem kleinsten Körper, der die Größe a enthält[1]*, ist die Gleichung $z^n - a = 0$ so beschaffen, daß sich alle ihre Wurzeln als rationale Funktionen von zwei geeigneten α_0, α_1 in der Form $\alpha_i = \left(\frac{\alpha_1}{\alpha_0}\right)^i \alpha_0$ $(i = 0, 1, 2, \ldots, n-1)$ ausdrücken lassen.*

§ 13. Algebraisch auflösbare Gleichungen.

Eine Gleichung $f(z) = 0$ mit Koeffizienten aus einem Körper P heißt *algebraisch auflösbar* (präziser eine im Körper P algebraisch auflösbare Gleichung), wenn sich ihre sämtlichen Wurzeln aus den Größen des Körpers P durch eine endliche Anzahl von Wurzelausziehungen finden lassen. Man sieht sofort, daß die Exponenten bei sämtlichen Wurzelausziehungen als Prim-

1) Also ohne Adjunktion von Einheitswurzeln.

zahlen angenommen werden können. Weber, *Algebra* **1**, 647 nennt die auflösbaren Gleichungen, wie man kürzer statt algebraisch auflösbar sagt, *metazyklisch*.

Die n Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ *einer auflösbaren Gleichung lassen sich stets in die Form:* $\alpha_i = r_i(\varphi_\lambda, \varphi_{\lambda-1}, \ldots, \varphi_2, \varphi_1)$ $(i = 1, 2, \ldots, n)$ *bringen, wobei die n Funktionen* r_i *ganze rationale Funktionen ihrer Argumente* $\varphi_1, \varphi_2, \ldots, \varphi_\lambda$ *mit Koeffizienten aus dem der Untersuchung zugrunde liegenden Körper* P *bedeuten. Die Größen* $\varphi_1, \varphi_2, \ldots, \varphi_\lambda$ *bestimmen sich hierbei nacheinander durch eine Kette reiner Gleichungen:* $\varphi_1^{\tau_1} = R_1$, $\varphi_2^{\tau_2} = R_2(\varphi_1)$,

$$\varphi_3^{\tau_3} = R_3(\varphi_1, \varphi_2), \ldots, \quad \varphi_\lambda^{\tau_\lambda} = R_\lambda(\varphi_1, \varphi_2, \ldots, \varphi_{\lambda-1}).$$

Die Zahlen $\tau_1, \tau_2, \ldots, \tau_\lambda$ *bedeuten Primzahlen; die Größen* R_i $(i = 2, \ldots, \lambda)$ *sind ganze rationale Funktionen von* $\varphi_1, \varphi_2, \ldots, \varphi_{i-1}$ *mit Koeffizienten aus* P, *und* R_1 *ist eine dem Körper* P *angehörige Zahl.* Man kann es stets so einrichten, daß die Größen $\varphi_1, \varphi_2, \ldots, \varphi_\lambda$, d. h. die auftretenden Radikale, ganze rationale Funktionen der n Wurzeln von $f(z) = 0$ sind, und die Koeffizienten dieser Funktionen dem durch Adjunktion von Einheitswurzeln erweiterten Körper P angehören. *Die Größen* $\varphi_1, \varphi_2, \ldots, \varphi_\lambda$ *sind also bei Zugrundelegung des Körpers* P *akzessorische Irrationalitäten, die aber in dem durch Adjunktion von Einheitswurzeln erweiterten Körper natürliche Irrationalitäten sind.* Abel hat in seiner grundlegenden Arbeit (vgl. oben S. 252, *Œuvres* **1**, 75) bei der Untersuchung der Form, die man den Radikalen φ bei algebraisch auflösbaren Gleichungen geben kann, das Auftreten der Einheitswurzeln nicht betont; dies geschah erst durch Jordan (*Traité*, p. 270) und Kronecker (*Monatsb. d. Berl. Akad.* (1879), 206). Daß die bei der Lösung der Gleichungen *dritten* und *vierten* Grades auftretenden Radikale in die Form rationaler Funktionen der Gleichungswurzeln und Einheitswurzeln gebracht werden können, geht bereits aus Lagranges Angaben in seinen Réflexions hervor. (Vgl. S. 283 und 287.)

Da die reinen Gleichungen sich auf Abelsche Gleichungen zurückführen lassen, folgt:

Damit eine Gleichung auflösbar sei, ist notwendig und hinreichend, daß ihre Behandlung auf eine Kette irreduzibler Abelscher Gleichungen vom Primzahlgrad reduziert werden kann. Diese Behandlungsweise verdankt man Jordan, *Traité*, p. 386. Vgl. hierzu auch Bendixson, *Acta math.* **27**, 317 (1903).

Eine Gleichung ist dann und nur dann auflösbar, wenn ihre Galoissche Gruppe eine auflösbare Gruppe ist. (Vgl. S. 199.)

Hat man eine im Körper P auflösbare Gleichung $f(z)=0$ mit der Galoisschen Gruppe $\mathfrak{G}$ der Ordnung g, deren Kompositionsreihe $\mathfrak{G}, \mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_{f-1}, 1$ lautet und deren Indexreihe $\frac{g}{g_1}, \frac{g_1}{g_2}, \ldots, \frac{g_{f-2}}{g_{f-1}}, g_{f-1}$ infolge der Auflösbarkeit aus lauter Primzahlen besteht, so gestaltet sich die *Behandlung der auflösbaren Gleichung $f(z)=0$ auf Grund der Galoisschen Theorie* folgendermaßen: Man bestimmt eine natürliche Irrationalität η_1 der Wurzeln von $f(z)=0$, die zur Gruppe $\mathfrak{G}_1$ gehört, ebenso eine natürliche Irrationalität η_2, die zur Gruppe $\mathfrak{G}_2$ gehört, usw., schließlich eine zur Gruppe $\mathfrak{G}_{f-1}$ gehörige natürliche Irrationalität η_{f-1} der Wurzeln von $f(z)=0$ und eine zur identischen Permutation 1 gehörige natürliche Irrationalität η_f. Dann ist η_1 eine rationale Funktion von η_2 mit Koeffizienten aus P, ebenso ist η_2 eine rationale Funktion von η_3 mit Koeffizienten aus P usw., schließlich η_{f-1} eine rationale Funktion von η_f mit Koeffizienten aus P. Die Größe η_1 genügt einer im Körper P irreduziblen einfachen Abelschen Gleichung vom Primzahlgrade $\frac{g}{g_1}$, deren Galoissche Gruppe mit der Faktorgruppe $\mathfrak{G}/\mathfrak{G}_1$ holoedrisch isomorph ist. Nach Adjunktion von η_1 genügt die Größe η_2 einer in dem erweiterten Körper (P, η_1) irreduziblen einfachen Abelschen Gleichung vom Primzahlgrade $\frac{g_1}{g_2}$, deren Galoissche Gruppe mit der Faktorgruppe $\mathfrak{G}_1/\mathfrak{G}_2$ holoedrisch isomorph ist. Nach Adjunktion von η_2 genügt die Größe η_3 einer irreduziblen einfachen Abelschen Gleichung vom Primzahlgrad $\frac{g_2}{g_3}$, deren Galoissche Gruppe mit der Faktorgruppe $\mathfrak{G}_2/\mathfrak{G}_3$ holoedrisch isomorph ist usw., schließlich genügt η_f in dem durch Adjunktion von η_{f-1} erweiterten Körper einer irreduziblen einfachen Abelschen Gleichung des Grades g_{f-1}, deren Galoissche Gruppe mit der Gruppe $\mathfrak{G}_{f-1}$ holoedrisch isomorph ist. Die Wurzeln der vorgelegten Gleichung $f(z)=0$ sind ganze rationale Funktionen von η_f mit Koeffizienten aus P. Dieses Verfahren reduziert, wie es dem Jordanschen Satz entspricht, die Auflösung der Gleichung $f(z)=0$ auf eine Kette von nacheinander zu lösenden einfachen Abelschen Gleichungen mit Gruppen von Primzahlordnung, die mit den Faktorgruppen $\mathfrak{G}/\mathfrak{G}_1, \mathfrak{G}_1/\mathfrak{G}_2, \ldots, \mathfrak{G}_{f-1}$ holoedrisch isomorph sind. Bei einer Reduktion auf Gleichungen mit einfachen Gruppen sind diese Gruppen nicht zu vermeiden, sie können eventuell nur in anderer

Reihenfolge auftreten. *Im Gegensatz zu den bei der Reduktion auf eine Kette von reinen Gleichungen oben* (S. 321) *eingeführten* φ *sind die Größen* $\eta_1, \eta_2, \ldots, \eta_f$ *natürliche Irrationalitäten des Körpers* P, *ohne daß man diesem Einheitswurzeln zu adjungieren braucht.*

Läßt sich auch nur eine Wurzel einer irreduziblen algebraischen Gleichung durch Wurzelausziehungen finden, so trifft dies für alle Wurzeln zu, und die Gleichung ist algebraisch auflösbar. (Abel, *Œuvres* **2**, 221, vgl. auch Selivanoff, *Acta math.* **19**, 88 (1895).)

Aus dem Satz von Galois (vgl. oben S. 210) und der Tatsache, daß die Ordnung jeder transitiven Permutationsgruppe durch ihren Grad teilbar ist, folgt der Satz von Abel (*Œuvres* **2**, 222 und 262): *Jede auflösbare irreduzible Gleichung, deren Grad sich durch wenigstens zwei verschiedene Primzahlen teilen läßt, ist imprimitiv. Ist also n durch zwei verschiedene Primzahlen teilbar, so zerfällt die vorgelegte Gleichung* n^{ten} *Grades durch Adjunktion der Wurzeln einer auflösbaren Gleichung* s^{ten} *Grades in Faktoren* r^{ten} *Grades, wobei* $n = rs$. *Die Behandlung auflösbarer Gleichungen läßt sich also auf das Studium der auflösbaren primitiven Gleichungen vom Primzahlpotenzgrad zurückführen.* (Vgl. Galois, *Œuvres,* p. 51.)

Hat man eine irreduzible primitive auflösbare Gleichung des Primzahlpotenzgrades p^k, so lassen sich ihre Wurzeln stets in der Form $\alpha_{\xi_1' \xi_2' \ldots \xi_k'}$ derartig anordnen, daß $\xi_1', \xi_2', \ldots, \xi_k'$ die Zahlen $0, 1, 2, \ldots, p-1$ durchlaufen und alle Permutationen der Galoisschen Gruppe der Gleichung das Aussehen $\begin{pmatrix} \alpha_{\xi_1' \xi_2' \cdots \xi_k'} \\ \alpha_{\xi_1 \xi_2 \cdots \xi_k} \end{pmatrix}$ haben; die Indices $\xi_1, \xi_2, \ldots, \xi_k$ ergeben sich hierbei aus $\xi_1', \xi_2', \ldots, \xi_k'$ durch Substitutionen der Form

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{ik}\xi_k' + a_{i,k+1}, \quad (i = 1, 2, \cdots, k)$$

wobei a_{ij} $(i = 1, 2, \ldots, k;\ j = 1, 2, \ldots, k+1)$ ganze Zahlen mod p mit nicht verschwindender Determinante $|a_{ij}|$ $(i, j = 1, 2, \ldots, k)$ bedeuten.

Die Galoissche Gruppe einer irreduziblen primitiven auflösbaren Gleichung des Primzahlpotenzgrades p^k *ist also entweder mit der allgemeinen vollen linearen Kongruenzgruppe der Ordnung* $(p^k - 1)(p^k - p)(p^k - p^2) \cdots (p^k - p^{k-1})p^k$ *in k Variablen mit ganzzahligen Koeffizienten mod p oder mit einer ihrer Untergruppen isomorph.* (Vgl. S. 247.) Für $k = 1$ erhält man die von Kronecker sog. *metazyklische Gruppe* des Grades p und der Ordnung $p(p-1)$, die stets auflösbar ist. (Vgl. S. 213,

Z. 21 auf S. 213 lies $|z, \alpha + \beta z|$ statt $|z, \alpha z + \beta|$). Hieraus ergeben sich die für $k = 1$ gültigen Galoisschen Theoreme:

Eine irreduzible Gleichung vom Primzahlgrad ist dann und nur dann auflösbar, wenn ihre Wurzeln sich so schreiben lassen, daß ihre Galoissche Gruppe die metazyklische Gruppe oder eine ihrer transitiven Untergruppen ist. (Galois, *Œuvres*, p. 48.)

Eine irreduzible Gleichung vom Primzahlgrad ist dann und nur dann auflösbar, wenn alle ihre Wurzeln rationale Funktionen zweier beliebiger Wurzeln mit Koeffizienten aus dem der Betrachtung zugrunde liegenden Körper sind. (Galois, *Œuvres*, p. 49.)

Hat eine irreduzible Gleichung vom Primzahlgrad mit reellen Koeffizienten mehr als eine reelle Wurzel, so ist sie bei Zugrundelegung eines reellen Körpers sicher nicht auflösbar, wenn sie nicht lauter reelle Wurzeln hat.

Aus der Natur der metazyklischen Gruppe und ihrer Untergruppen (vgl. S. 213) folgt:

Jede im Körper P *irreduzible auflösbare Gleichung vom Primzahlgrade* p *kann mittelst zweier irreduzibler einfacher Abelscher Gleichungen des Grades* $p-1$ *bezw.* $\frac{p-1}{\delta}$ *und des Grades* p *gelöst werden.* Die Wurzeln einer im Körper P irreduziblen auflösbaren Gleichung p^{ten} Grades lassen sich nämlich so anordnen, daß zwischen ihnen die Beziehungen stattfinden $\alpha_1 = \Theta(\alpha_0)$, $\alpha_2 = \Theta(\alpha_1)$, ..., $\alpha_0 = \Theta(\alpha_{p-1})$. Die Operation Θ ist hierbei eine ganze rationale Funktion mit Koeffizienten aus einem Körper (P, φ); dieser geht aus dem der Betrachtung zugrunde liegenden Körper P durch Adjunktion einer Wurzel φ einer im Körper P irreduziblen einfachen Abelschen Gleichung des Grades $p-1$ oder $\frac{p-1}{\delta}$ hervor, wobei δ ein Teiler von $p-1$ ist. (Kronecker, *Monatsb. d. Berl. Akad.* (1853), 369.)

Als Endziel der Behandlung algebraisch auflösbarer Gleichungen sah bereits Abel (*Œuvres* **2**, 222ff., 266) an, *Ausdrücke zu konstruieren,* die aus dem gegebenen Körper P durch Wurzelziehungen hervorgehen und die Doppeleigenschaft besitzen, daß jede Wurzel einer irreduziblen auflösbaren Gleichung vorgegebenen Grades in ihnen enthalten ist und sie umgekehrt nur solche Werte annehmen, die irreduziblen auflösbaren Gleichungen des vorgegebenen Grades genügen. Eine Lösung des Problems in voller Allgemeinheit hat für einen *Primzahlgrad* Kronecker (*Monatsb. d. Berl. Akad.* (1853), 365) ohne Beweis gegeben; der erste völlig durchgeführte Beweis stammt von

H. Weber. Vgl. das zusammenfassende Resultat bei Weber, *Algebra* **1**, 694. Vgl. ferner Wiman, *Acta math.* **27**, 163 (1903). Die gewöhnliche kurze Angabe, daß die Wurzeln jeder im Körper P irreduziblen auflösbaren Gleichung p^{ten} Grades von der Form $A + \sqrt[p]{R_1} + \sqrt[p]{R_2} + \cdots + \sqrt[p]{R_k}$ sind, wobei A dem Körper P angehört und $R_1, R_2, \ldots, R_k$ die Wurzeln einer im Körper P einfachen Abelschen Gleichung k^{ten} Grades sind, wobei k gleich $p-1$ oder $\frac{p-1}{\delta}$, und δ ein Teiler von $p-1$ ist, hat den Nachteil, daß der angegebene Ausdruck p^k- statt p-wertig ist. Die Lösung des Abelschen Problems der Wurzeldarstellung für auflösbare Gleichungen, die nicht vom Primzahlgrad sind, gibt für den Grad 8: Weber, *Algebra* **2**, 383, für den Grad 9, später allgemein für den Grad p^2: Wiman, *Arkiv för mat., Svenska Vetenskapsakademien* **1**, 665 (1904), ebenda **3**, Nr. 27 (1907), *Verhandl. d. 3. Math.-Kongr.*, S. 190 (1905). Zu den auflösbaren Gleichungen neunten Grades gehören die *Gleichungen für die neun Wendepunkte der Kurven 3. Ordnung.* (Vgl. S. 247.) Die Herstellung eines Wurzelausdruckes für die auflösbaren Gleichungen von beliebigem Primzahlpotenzgrad ist eine noch nicht abgeschlossene Aufgabe. Vgl. Bucht, *Arkiv för mat.*, **5**, Nr. 23 (1909).

Für die *Geometrie* wichtig ist die Frage: *Unter welchen Bedingungen können die Wurzeln einer algebraischen Gleichung nur durch Ausziehen von Quadratwurzeln, also bloß mittelst einer Kette quadratischer Gleichungen, gefunden werden. Hierzu ist notwendig und hinreichend, daß die Ordnung der Galoisschen Gruppe der Gleichung eine Potenz von 2 ist. Dann und nur dann, wenn sich die Lösung einer geometrischen Aufgabe auf eine solche Gleichung zurückführen läßt, können die in der Aufgabe gesuchten Größen mittelst Zirkels und Lineals allein gefunden werden* (Descartes, *Géométrie* (1637), livre premier). Von den berühmten geometrischen Problemen, die das Altertum schon beschäftigten, sind das *delische Problem* (Verdoppelung des Würfels) und die *Trisektion eines beliebigen Winkels* mit Hilfe von Zirkel und Lineal allein unlösbar; diese Aufgaben führen nämlich auf irreduzible Gleichungen dritten Grades. Literatur: Die Bücher von Klein und Enriques (vgl. S. 316). Über *die Teilung des Kreises in n gleiche Teile* mit Hilfe von Zirkel und Lineal vgl. S. 315.

§ 14. Gleichungen fünften und höheren Grades. Einige funktionentheoretische und geometrische, nicht algebraisch auflösbare Gleichungen höheren Grades.

Zum Mittelpunkt für die Behandlung der *Gleichungen fünften Grades* kann die *Ikosaedergleichung:* $\frac{H_{20}^3}{1728 f_{12}^5} = Z$ gewählt werden, die ausführlich geschrieben:

$$(-\vartheta^{20} - 1 + 228\vartheta^{15} - 228\vartheta^5 - 494\vartheta^{10})^3$$
$$- 1728\vartheta^5 Z(\vartheta^{10} + 11\vartheta^5 - 1)^5 = 0$$

lautet. (Vgl. oben S. 240.) In dem Körper, der außer den rationalen Zahlen noch den Parameter Z enthält, hat die Ikosaedergleichung eine Galoissche Gruppe der Ordnung $4 \cdot 60$. *Nach Adjunktion der fünften Einheitswurzeln wird die Ikosaedergleichung eine Normalgleichung, deren Wurzeln lineare Funktionen einer einzigen sind und durch die bekannten 60 Kollineationen der Ikosaedergruppe $\mathfrak{J}_{60}$ aus ihr hervorgehen. Die Galoissche Gruppe wird die einfache transitive Permutationsgruppe des Grades und der Ordnung 60, die mit der Ikosaedergruppe $\mathfrak{J}_{60}$ isomorph ist.*

Da die Ikosaedergruppe $\mathfrak{J}_{60}$ Tetraederuntergruppen $\mathfrak{T}_{12}$, also Untergruppen des Index 5, besitzt, so existieren für die Ikosaedergleichung rationale Resolventen fünften Grades.

Setzt man $u = \frac{12 f_{12}^2 \cdot f_6}{T}$, $v = \frac{12 f_{12} \cdot H_8}{H_{20}}$, wobei H_8 und f_6 Invarianten der Oktaedergruppe (vgl. S. 239) und f_{12}, T und H_{20} Invarianten der Ikosaedergruppe (vgl. S. 240) sind, so hängen u und v von dem Verhältnis $\vartheta = \frac{x_1}{x_2}$ ab, und die Funktion $Y = mv + nuv$ genügt, wenn m und n willkürliche Größen sind, einer rationalen Resolvente fünften Grades der Ikosaedergleichung, der von Klein (*Ikosaeder,* S. 106) sog. *Hauptresolvente*

$$Y^5 + \frac{5}{Z}\left(8m^3 + 12m^2 n + \frac{6mn^2 + n^3}{1 - Z}\right) Y^2$$
$$+ \frac{15}{Z}\left(-4m^4 + \frac{6m^2n^2 + 4mn^3}{1 - Z} + \frac{3n^4}{4(1 - Z)^2}\right) Y$$
$$+ \frac{3}{Z}\left(48m^5 - \frac{40m^3n^2}{1 - Z} + \frac{15mn^4 + 4n^5}{(1 - Z)^2}\right) = 0.$$

Diese Hauptresolvente hat in dem durch die Gleichungskoeffizienten bestimmten Körper, nachdem man ihm die fünften Einheitswurzeln adjungiert hat — es genügt sogar die Adjunktion von $\sqrt{5}$ —, *die alternierende Permutationsgruppe von fünf Symbolen, also eine mit der* $\mathfrak{J}_{60}$ *isomorphe Gruppe, zur Galoisschen Gruppe.*[1])

Ist eine beliebige Hauptgleichung fünften Grades, d. h. eine Gleichung (vgl. S. 278) *der Form* $Y^5 + 5\alpha Y^2 + 5\beta Y + \gamma = 0$ *gegeben, so sind zur Bestimmung ihrer Wurzeln folgende Schritte erforderlich:*

(1.) Das Ausziehen der Quadratwurzel aus der Diskriminante der Gleichung. Adjungiert man diese Quadratwurzel dem durch die Gleichungskoeffizienten bestimmten Körper, so hat die vorgelegte Hauptgleichung die alternierende Permutationsgruppe von fünf Symbolen zur Galoisschen Gruppe.

(2.) Nach Adjunktion der Quadratwurzel aus der Diskriminante kann man die vorgelegte Hauptgleichung direkt mit der Hauptresolvente identifizieren. Setzt man:

$$\alpha = \frac{8m^3}{Z} + \frac{12m^2n}{Z} + \frac{6mn^2 + n^3}{Z(1-Z)},$$

$$\beta = 3\left(-\frac{4m^4}{Z} + \frac{6m^2n^2 + 4mn^3}{Z(1-Z)} + \frac{3n^4}{4Z(1-Z)^2}\right),$$

$$\gamma = 3\left(\frac{48m^5}{Z} - \frac{40m^3n^2}{Z(1-Z)} + \frac{15mn^4 + 4n^5}{Z(1-Z)^2}\right),$$

so drücken sich m, n, Z aus diesen Gleichungen rational durch α, β, γ und die Quadratwurzel der Diskriminante aus; die numerischen Koeffizienten sind abgesehen von $\sqrt{5}$ rationale Zahlen (vgl. Klein, *Ikosaeder,* S. 192).

(3.) Bestimmung einer Wurzel ϑ der Ikosaedergleichung $\frac{H_{20}^3}{1728 f_{12}^5} = Z$, deren rechte Seite nach (2) zu finden ist.

(4.) $Y = mv(\vartheta) + nu(\vartheta)v(\vartheta)$ liefert die Wurzeln der vorgelegten Hauptgleichung, hierbei bedeuten m und n die nach (2) bestimmten Werte und u und v sind die oben angegebenen Funktionen von ϑ. *Um die Wurzeln einer Hauptgleichung fünften Grades zu bestimmen, sind also außer rationalen Operationen und dem Ziehen der Quadratwurzel aus der Zahl* 5 (*Operation* (2)) *nur das Ausziehen der Quadratwurzel aus der Diskriminante* (*Operation* (1)) *und die Bestimmung einer Wurzel der Ikosaedergleichung* (*Operation* (3)) *erforderlich.*

---

1) Die Hauptresolvente ist auch ohne Adjunktion von $\sqrt{5}$ eine rationale Resolvente der Ikosaedergleichung; bei Unterlassung der Adjunktion von $\sqrt{5}$ hat sie die symmetrische Gruppe von fünf Buchstaben zur Galoisschen Gruppe.

Um die Operation (3) zu leisten, muß man den algebraischen Bereich verlassen; denn die *Bestimmung der Ikosaederirrationalität* ϑ *ist transzendenter Natur. Sie kann mittels hypergeometrischer Reihen oder elliptischer Modulfunktionen geschehen.*

Die *hypergeometrische Reihe*

$$x = F(\alpha, \beta, \gamma, Z) = 1 + \frac{\alpha \cdot \beta}{1 \cdot \gamma} Z + \frac{\alpha \cdot (\alpha + 1) \cdot \beta \cdot (\beta + 1)}{1 \cdot 2 \cdot \gamma \cdot (\gamma + 1)} Z^2 + \cdots$$

genügt der Gaußschen Differentialgleichung:

$$Z(1 - Z) \frac{d^2 x}{d Z^2} + (\gamma - (\alpha + \beta + 1) Z) \frac{d x}{d Z} - \alpha \beta x = 0.$$

Der Quotient $\vartheta = \frac{x_1}{x_2}$ irgend zweier partikulärer Integrale dieser linearen homogenen Differentialgleichung befriedigt die Differentialgleichung 3. Ordnung:

$$\frac{\vartheta'''}{\vartheta'} - \frac{3}{2}\left(\frac{\vartheta''}{\vartheta'}\right)^2 = \frac{1 - \frac{1}{\nu_1^2}}{2(1 - Z)^2} + \frac{1 - \frac{1}{\nu_2^2}}{2 Z^2} - \frac{\frac{1}{\nu_1^2} - \frac{1}{\nu_3^2} + \frac{1}{\nu_2^2} - 1}{2 Z (1 - Z)};$$

hierbei bedeuten, falls α, β, γ reell vorausgesetzt werden, die Größen $\frac{1}{\nu_1}, \frac{1}{\nu_2}, \frac{1}{\nu_3}$ der Reihe nach die absoluten Beträge von $|\gamma - \alpha - \beta|$, $|1 - \gamma|$ und $|\alpha - \beta|$. Das allgemeine Integral der Differentialgleichung lautet $\frac{a\vartheta + b}{c\vartheta + d}$, wobei a, b, c, d Integrationskonstanten sind. Jedes partikuläre Integral ϑ der Differentialgleichung 3. Ordnung vermittelt die konforme Abbildung der positiven Halbebene der Variablen Z auf die Fläche ϑ eines von Kreisen begrenzten Dreiecks mit den Winkeln $\frac{\pi}{\nu_1}, \frac{\pi}{\nu_2}, \frac{\pi}{\nu_3}$. Das spezielle Wertsystem $\nu_1 = 2$, $\nu_2 = 3$, $\nu_3 = 5$, bei dem die Gaußsche Differentialgleichung der hypergeometrischen Funktion

$$F\left(\frac{11}{60}, -\frac{1}{60}, \frac{2}{3}, Z\right)$$

entspricht, steht in innigster Beziehung zu der durch ein Ikosaeder bewirkten Kugeleinteilung in 120 abwechselnd kongruente und symmetrische sphärische Dreiecke mit den Winkeln $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{5}$. Die Funktion $Z = \frac{H_{20}^3}{1728 f_{12}^5}$ vermittelt nämlich die konforme Abbildung der Fläche ϑ eines sphärischen Dreiecks mit den Winkeln $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{5}$ auf die positive Halbebene der Z. *Die Ikosaederirrationalität läßt sich daher als Quotient zweier geeigneter partikulärer Lösungen der Gaußschen Differentialgleichung finden, also mittels hyper-*

geometrischer Reihen bestimmen. (Vgl. die grundlegende Arbeit von H. A. Schwarz, *Journ. f. Math.* **75**, 292 (1873), *Ges. Abhdlgn.*, Berlin 1890, **2**, 211, Klein, *Math. Ann.* **12**, 512 (1877).)

Um die *Ikosaederirrationalität durch elliptische Modulfunktionen* auszudrücken, setze man $Z = J(\omega) = \frac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)}$, wobei J die absolute Invariante, g_2 und Δ homogene transzendente Funktionen $(-4)^{\text{ter}}$ und $(-12)^{\text{ter}}$ Dimension aus der Theorie der elliptischen Funktionen sind, und bestimme hieraus ω. (Wie dies geschehen kann, vgl. Klein, *Math. Ann.* **14**, 111 (1879).) Ist $q = e^{i\pi\omega} = e^{-\pi\frac{K'}{K}}$ in Jacobischer Bezeichnung, so ergibt sich die Ikosaederirrationalität ϑ als Quotient zweier elliptischer Thetareihen in der Form:

$$\vartheta = -q^{\frac{3}{5}} \frac{\vartheta_1(2\omega\pi, q^5)}{\vartheta_1(\pi\omega, q^5)}$$

(Klein, *Math. Ann.* **61**, 560 (1905)). Die Benützung dieser Formel an Stelle von Reihen, die der Gaußschen Differentialgleichung genügen, kommt auf einen Umweg hinaus, wie wenn man sich zur Lösung der reinen Gleichung $z^n = a$ des Logarithmus bedient, zuerst $\frac{1}{n} la$ berechnet und dann z als Numerus zu $\frac{1}{n} la$ bestimmt (vgl. S. 254).

Da die Ikosaedergruppe Diederuntergruppen $\mathfrak{D}_{10}$, *also Untergruppen des Index 6, besitzt, so existieren für die Ikosaedergleichung auch rationale Resolventen sechsten Grades.* Setzt man $\varphi = \frac{5 x_1^2 x_2^2 H_{20}}{12 f_{12}^2}$, so genügt die von dem Quotienten $\vartheta = \frac{x_1}{x_2}$ abhängige Größe φ der Gleichung (vgl. Klein, *Ikosaeder*, S. 134 f.):

$$\varphi^6 - 10 Z \varphi^3 + 12 Z^2 \varphi + 5 Z^2 = 0.$$

Die Galoissche Gruppe dieser Gleichung sechsten Grades ist bei Adjunktion der fünften Einheitswurzeln — es genügt sogar schon die Adjunktion von $\sqrt{5}$ — die der Primzahl $p = 5$ entsprechende Modulargruppe $(p+1)^{\text{ten}}$ Grades der Ordnung $\frac{p(p^2-1)}{2}$, welche mit $\mathfrak{J}_{60}$ holoedrisch isomorph ist (vgl. S. 253 u. 214).[1] Setzt man $Z = \frac{g_2^3}{\Delta}$ und $\xi^2 = -\frac{\varphi}{g_2}$, so erhält man für

1) Ohne Adjunktion von $\sqrt{5}$ ist die Gleichung sechsten Grades für φ auch eine rationale Resolvente der Ikosaedergleichung; ihre Galoissche Gruppe ist bei Unterlassung der Adjunktion von der Ordnung 120.

die Unbekannte ξ die in der Theorie der elliptischen Funktionen auftretende Gleichung:

$$\xi^{12} + \frac{10}{\Delta}\xi^6 - \frac{12 g_2}{\Delta^2}\xi^2 + \frac{5}{\Delta^2} = 0,$$

die durch $\dfrac{1}{\wp\left(\frac{2\omega}{5}\right) - \wp\left(\frac{4\omega}{5}\right)}$ befriedigt wird. (Kiepert, *Journ. f. Math.* **87**, 114 (1879).) Führt man in dieser Gleichung $\xi^2 = u$ ein, so erhält man:

$$u^6 + \frac{10}{\Delta}u^3 - \frac{12 g_2}{\Delta^2}u + \frac{5}{\Delta^2} = 0.$$

Diese Gleichung gehört zum Typus der sog. *allgemeinen Jacobischen Gleichungen sechsten Grades. Hierunter versteht man Gleichungen sechsten Grades, bei denen sich die Quadratwurzeln ihrer sechs mit $u_\infty, u_0, u_1, u_2, u_3, u_4$ bezeichneten Wurzeln als lineare Funktionen von drei Parametern $\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2$ in der bereits von Jacobi* (*Journ. f. Math.* **3**, 308 (1828), *Ges. Werke* **1**, 261) *angegebenen Form:*

$$\sqrt{u_\infty} = \sqrt{5}\,\mathsf{A}_0, \quad \sqrt{u_m} = \mathsf{A}_0 + \varepsilon^m \mathsf{A}_1 + \varepsilon^{4m}\mathsf{A}_2 \qquad (m = 0, 1, 2, 3, 4)$$

darstellen lassen, wobei ε eine primitive fünfte Einheitswurzel ist. Die von Brioschi (vgl. die Angaben auf S. 255, sowie die Darstellung bei Klein, *Ikosaeder,* S. 150) *aufgestellte allgemeine Jacobische Gleichung sechsten Grades mit den Wurzeln u_∞, u_0, u_1, u_2, u_3, u_4 lautet:*

$$(u - A)^6 - 4A(u - A)^5 + 10B(u - A)^3 - C(u - A) + 5B^2 - AC = 0;$$

hierbei ist:

$$A = \mathsf{A}_0^2 + \mathsf{A}_1\mathsf{A}_2,$$
$$B = 8\mathsf{A}_0^4\mathsf{A}_1\mathsf{A}_2 - 2\mathsf{A}_0^2\mathsf{A}_1^2\mathsf{A}_2^2 + \mathsf{A}_1^3\mathsf{A}_2^3 - \mathsf{A}_0(\mathsf{A}_1^5 + \mathsf{A}_2^5),$$
$$C = 320\mathsf{A}_0^6\mathsf{A}_1^2\mathsf{A}_2^2 - 160\mathsf{A}_0^4\mathsf{A}_1^3\mathsf{A}_2^3 + 20\mathsf{A}_0^2\mathsf{A}_1^4\mathsf{A}_2^4 + 6\mathsf{A}_1^5\mathsf{A}_2^5 - 4\mathsf{A}_0(32\mathsf{A}_0^4 - 20\mathsf{A}_0^2\mathsf{A}_1\mathsf{A}_2 + 5\mathsf{A}_1^2\mathsf{A}_2^2)\cdot(\mathsf{A}_1^5 + \mathsf{A}_2^5) + \mathsf{A}_1^{10} + \mathsf{A}_2^{10}.$$

Eliminiert man die Parameter A_0, A_1, A_2 aus der oben für die Gleichungswurzeln gegebenen Darstellung, so erhält man folgende zwischen den Wurzeln bestehende Relationen:

$$\sqrt{u_0}+\sqrt{u_1}+\sqrt{u_2}+\sqrt{u_3}+\sqrt{u_4}=\sqrt{5u_\infty},$$
$$\sqrt{u_0}+\varepsilon^2\sqrt{u_1}+\varepsilon^4\sqrt{u_2}+\varepsilon\sqrt{u_3}+\varepsilon^3\sqrt{u_4}=0,$$
$$\sqrt{u_0}+\varepsilon^3\sqrt{u_1}+\varepsilon\sqrt{u_2}+\varepsilon^4\sqrt{u_3}+\varepsilon^2\sqrt{u_4}=0.$$

Der Nachweis, wie man aus der allgemeinen Gleichung fünften Grades nach Adjunktion der Quadratwurzel ihrer Diskriminante allgemeine Jacobische Gleichungen sechsten Grades als rationale Resolventen herleiten kann, und der Zusammenhang spezieller Jacobischer Gleichungen mit der Theorie der elliptischen Funktionen bildet den Kern der Kroneckerschen und Brioschischen Untersuchungen über die Gleichungen fünften Grades. Eine Jacobische Gleichung mit $A=0$ hat Kronecker seiner Auflösung der Gleichung fünften Grades (*C. R.* (1858)) zugrunde gelegt. (Vgl. Klein, *Math. Ann.* **14**, 147 (1879).) $A=0$, $B=\frac{1}{\Delta}$, $C=+\frac{12g_2}{\Delta^2}$ liefert auch die oben angeführte spezielle Gleichung sechsten Grades aus der Theorie der elliptischen Funktionen, von der wir ausgingen. Die Jacobischen Gleichungen für $B=0$ charakterisieren nach Brioschi die aus der Theorie der elliptischen Funktionen stammenden *Multiplikatorgleichungen*. Die spezielle $B=0$, $A=1$, $C=-256k^2(1-k^2)$ entsprechende Jacobische Gleichung verwendet Brioschi zur Lösung der Gleichung fünften Grades (vgl. S. 255).

Die allgemeine Jacobische Gleichung sechsten Grades hängt von zwei wesentlichen Parametern, nämlich $\frac{B}{A^3}$ und $\frac{C}{A^5}$ ab, wie ihre Form:

$$\left(\frac{u}{A}-1\right)^6-4\left(\frac{u}{A}-1\right)^5+10\frac{B}{A^3}\left(\frac{u}{A}-1\right)^3-\frac{C}{A^5}\left(\frac{u}{A}-1\right)$$
$$+5\left(\frac{B}{A^3}\right)^2-\frac{C}{A^5}=0$$

lehrt, wenn man $\frac{u}{A}=U$ setzt. Hingegen hängt die Ikosaedergleichung nur von einem Parameter ab. Das gleiche trifft auch für die speziellen Jacobischen Gleichungen zu, die $A=0$ bezw. $B=0$ entsprechen und die wir durch die elliptischen Funktionen beherrschen. Die $A=0$ entsprechende Jacobische Gleichung sechsten Grades lautet:

$$u^6+10Bu^3-Cu+5B^2=0$$

oder

$$\varphi^6-10Z\varphi^3+12Z^2\varphi+5Z^2=0,$$

wenn $\varphi = -\frac{C}{12 B^2} u$, $Z = \frac{C^3}{12^3 B^5}$ gesetzt wird. Die letztere Gleichung ist die Ausgangsgleichung auf Seite 329.

Die Hauptgleichung $Y^5 + 5\alpha Y^2 + 5\beta Y + \gamma = 0$ *hat, wenn die fünften Einheitswurzeln als bekannt gelten, nach Adjunktion der Quadratwurzel ihrer Diskriminante die Ikosaedergleichung zur rationalen Resolvente.* Für die *allgemeine* Gleichung fünften Grades gilt folgender von Kronecker (*Monatsber. d. Berl. Akad.* (1861), 609) stammende und zuerst von Klein (*Ikosaeder*), dann von Gordan (*Math. Ann.* **29**, 318 (1887), vgl. auch Weber, *Algebra* **2**, 470) bewiesene Satz: *Ohne Einführung akzessorischer Irrationalitäten ist es, wenn auch alle numerischen Konstanten als bekannt gelten, selbst nach Adjunktion der Quadratwurzel aus der Diskriminante unmöglich, aus der allgemeinen Gleichung fünften Grades Jacobische Gleichungen mit nur einem Parameter oder überhaupt rationale Resolventen mit nur einem Parameter abzuleiten. Um die Wurzeln einer allgemeinen Gleichung fünften Grades zu finden, kann man die vorgelegte Gleichung zuerst durch Ziehen einer Quadratwurzel auf eine Hauptgleichung reduzieren* (vgl. S. 278). *Dieses Ziehen einer Quadratwurzel geht bei einer allgemeinen Gleichung fünften Grades den mit* (1)—(4) *numerierten Operationen voraus, die wir S. 327 zur Bestimmung der Wurzeln einer Hauptgleichung fünften Grades angaben. Diese bei der Behandlung einer allgemeinen Gleichung fünften Grades noch hinzutretende Quadratwurzel ist eine akzessorische Irrationalität* (vgl. S. 301); *diese trägt nicht zur Erniedrigung der Galoisschen Gruppe der Gleichung bei. Eine solche akzessorische Irrationalität ist nach dem Kroneckerschen Satze nicht zu vermeiden, wenn man mit einparametrigen Gleichungen arbeiten will.* Bei der Lösung der allgemeinen Gleichung fünften Grades durch Jacobische Gleichungen, die $A = 0$ bezw. $B = 0$ entsprechen, tritt daher auch notwendigerweise eine akzessorische Irrationalität auf.

Für die Gleichungen fünften Grades vgl. man außer der im voraufgehenden und auf S. 253 ff. zitierten Literatur den Artikel von Wiman, *Endliche Gruppen linearer Substitutionen in der Enzyklopädie der math. Wiss.* **1**, 522, ferner Scheibner, *Beiträge zur Theorie der linearen Transformationen,* Leipzig 1907. Zur Einführung vgl. man: Vivanti, *Funzioni poliedriche e modulari,* Mailand 1906, Netto, *Algebra* **2**, 487, Bianchi, *Lezioni dei gruppi etc.,* p. 234.

Hat man eine *Gleichung beliebigen Grades,* so kann man sie nach der Galoisschen Theorie zunächst stets durch eine Kette von Gleichungen mit einfachen Galoisschen Gruppen ersetzen (vgl. S. 303). *Für die Behandlung einer Gleichung $f(z) = 0$ beliebigen Grades mit einfacher Galoisscher Gruppe* $\mathfrak{G}$ *hat* Klein, (*Math. Ann.* **15**, 251 (1879), vgl. auch Weber, *Algebra* **2**, 235) *folgendes Verfahren angegeben:* Für die Gruppe $\mathfrak{G}$ gibt es, wie für jede Gruppe eine Gruppe linearer homogener Substitutionen von niedrigstem Grade μ, die mit $\mathfrak{G}$ isomorph ist. (*Kleinsches Normalproblem,* vgl. S. 232.) Aus den Wurzeln der vorgelegten Gleichung $f(z) = 0$ kann man stets ganze homogene Funktionen bilden, und zwar genau in der oben definierten Zahl μ, daß sich diese, wenn die Wurzeln von $f(z) = 0$ den Permutationen der Gruppe $\mathfrak{G}$ unterworfen werden, nach einer mit $\mathfrak{G}$ isomorphen linearen homogenen Substitutionsgruppe Γ des Grades μ transformieren. (Vgl. auch Burkhardt, *Math. Ann.* **41**, 309 (1893).) Mit der Gruppe Γ ist wie mit jeder Gruppe linearer homogener Substitutionen das auf S. 228 besprochene sog. *Kleinsche Formenproblem* verbunden, nämlich aus den Invarianten der Gruppe Γ die Variablen zu berechnen. Hierbei gelangt man zu einer Normalgleichung, deren Grad gleich der Ordnung von Γ ist und deren Galoissche Gruppe mit Γ holoedrisch isomorph ist. Die Behandlung der Gleichung $f(z) = 0$ wird durch die angegebene Normalgleichung oder eine andere mit ihr äquivalente rationale Resolvente ersetzt. Existiert eine zu der Gruppe $\mathfrak{G}$ holoedrisch isomorphe Kollineationsgruppe des Grades μ', wobei μ' kleiner als μ ist, und will man die Behandlung der Gleichung $f(z) = 0$ mittels dieser Kollineationsgruppe durchführen, so wird die Adjunktion akzessorischer Irrationalitäten erforderlich.

Hat man eine *einfache Abelsche Gleichung* $f(z) = 0$ (vgl. S. 306) mit den Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$, deren Galoissche Gruppe $\mathfrak{G}$ aus der zyklischen Permutation $C = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ und ihren Potenzen besteht, so wird die fragliche lineare homogene Substitutionsgruppe Γ vom Grade $\mu = 1$. Ist ε eine primitive n^{te} Einheitswurzel und adjungiert man diese dem durch die Koeffizienten von $f(z) = 0$ bestimmten Körper, so stellt die in dem erweiterten Körper natürliche Irrationalität $Y_1 = (\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3 + \cdots + \varepsilon^{n-1}\alpha_n)^{n-1}$ eine ganze rationale Funktion der Wurzeln von $f(z) = 0$ dar, die bei der Permutation $C^\varkappa$ in $\varepsilon^\varkappa Y_1$ $(\varkappa = 1, 2, \ldots, n)$ übergeht. Einfacher verwendet man die sich mit Y_1 kogredient transformierende Größe $Z_1 = \dfrac{1}{\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3 + \cdots + \varepsilon^{n-1}\alpha_n}$. Die Invariante dieser Gruppe in einer Variablen ist Z_1^n. Die Bestimmung von Z_1 kommt auf das Ziehen einer n^{ten} Wurzel aus der bekannten Größe 1: $(\alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3 + \cdots + \varepsilon^{n-1}\alpha_n)^n$ heraus. Die Größe $\frac{1}{Z_1}$ ist die Lagrangesche Resolvente (vgl. S. 307). *Die durch Wurzelzeichen lösbaren Gleichungen und auch nur sie allein führen auf Formenprobleme ersten Grades.*

Bei der nicht algebraisch auflösbaren Gleichung niedrigsten Grades, der *Gleichung fünften Grades*, liegt es so: Nach Adjunktion der Quadratwurzel aus der Diskriminante hat sie die alteenierende Gruppe von fünf Symbolen zur Galoisschen Gruppe. Dr. Gruppe linearer homogener Substitutionen niedrigsten Gradeis die mit dieser einfachen Gruppe der Ordnung 60 isomorph islt ist eine solche des Grades 3, die ternäre Ikosaedergruppe (vgl. S. 242). Das Kleinsche Formenproblem wird ungefähr gleichbedeutend mit dem Studium der allgemeinen Jacobischen Gleichungen sechsten Grades. (Klein, *Math. Ann.* **15**, 259 (1879), *Ikosaeder*, S. 211). Da es keine einfache binäre Gruppe linearer homogener Substitutionen 60. Ordnung gibt, erfordert die Behandlung der Gleichung fünften Grades mit Hilfe der binären Kollineationsgruppe $\mathfrak{J}_{60}$ die Zuziehung einer akzessorischen Quadratwurzel.

Die *allgemeine Gleichung sechsten Grades* hat nach Adjunktion der Quadratwurzel aus der Diskriminante die alternierende Gruppe von sechs Symbolen zur Galoisschen Gruppe. Die Valentinersche Gruppe (vgl. S. 242) ist die Kollineationsgruppe niedrigsten Grades 3, die mit der einfachen Gruppe der Ordnung 360 isomorph ist. Die Valentinersche Gruppe ist mit keiner Gruppe linearer homogener Substitutionen in drei Variablen isomorph. Unter Zuziehung akzessorischer Irrationalitäten läßt sich die Auflösung der Gleichung sechsten Grades mit der Valentinerschen Gruppe in Zusammenhang bringen (vgl. Klein, *Journ. f. Math.* **129**, 151 (1905), Gordan, *Math. Ann.* **61**, 453 (1905), Lachtin, *Math. Ann.* **56**, 445 (1903)).

Ehe die Valentinersche Gruppe entdeckt war, haben Maschke (*Rend. Lincei* 4_1, 181 (1888)) und Brioschi, *Acta math.* **12**, 83 (1889) und *Ann. de l'école normale* (3) **12**, 343 (1895) die Wurzeln der Gleichung sechsten Grades durch hyperelliptische ϑ-Nullwerte ausgedrückt, analog wie man die Wurzeln der Gleichung fünften Grades durch elliptische Modulfunktionen bestimmen kann. Der tiefere Grund hierfür liegt darin, daß die Gruppe der Borchardtschen Moduln $\mathfrak{G}_{11520}$ eine invariante Untergruppe der Ordnung 16 besitzt und daher mit der symmetrischen Gruppe $\mathfrak{S}_6$ von sechs Symbolen meroedrisch isomorph ist. (Vgl. S. 243.)

Da die alternierende Gruppe $\mathfrak{A}_{\frac{7!}{2}}$ von sieben Symbolen mit einer quaternären Kollineationsgruppe holoedrisch isomorph ist, so kann die *allgemeine Gleichung siebenten Grades* mit einer quaternären Kollineationsgruppe in Zusammenhang gebracht werden (vgl. S. 236 u. 243, sowie Klein, *Math. Ann.* **28**, 499 (1887)). Auch die *Gleichung sechsten Grades* kann mit einer quaternären Kollineationsgruppe behandelt werden, da die symmetrische Gruppe $\mathfrak{S}_{6!}$ von sechs Symbolen mit einer solchen holoedrisch isomorph ist (vgl. Klein, *Math. Ann.* **28**, 499 (1887).) Für die Gleichung siebenten Grades ist die quaternäre Kollineationsgruppe die niedrigste mögliche, hingegen nicht für die Gleichung sechsten Grades (vgl. oben). Sowohl die mit $\mathfrak{S}_{6!}$ als auch mit $\mathfrak{A}_{\frac{7!}{2}}$ holoedrisch isomorphen quaternären Kollineationsgruppen erfordern, wenn man zu einer homogenen linearen Substitutionsgruppe übergeht, die doppelte Zahl von Substitutionen. Die Behandlung der Gleichungen sechsten und siebenten Grades auf diesem Wege erfordert daher akzessorische Irrationalitäten.

Die allgemeinen Gleichungen achten und höheren Grades können, wenn n der Grad der Gleichung ist, mit keiner Kollineationsgruppe von niedrigerem als $(n-1)^{\text{tem}}$ Grade in Zusammenhang gebracht werden (Folge des Satzes von Wimann, vgl. S. 235). Die allgemeine Gleichung n^{ten} Grades läßt sich sofort auf ein Formenproblem $(n-1)^{\text{ten}}$ Grades reduzieren, indem man die zu permutierenden Größen der Bedingung unterwirft, daß ihre Summe verschwinden soll. *Die allgemeine Gleichung n^{ten} Grades gestattet daher für $n \geqq 8$ keine Reduktion auf einfachere Formenprobleme; die fraglichen Gleichungen bilden ihre eigenen Normalprobleme.*

Eine Bestimmung der Wurzeln der allgemeinen Gleichung n^{ten} Grades durch transzendente Funktionen geben die Aufsätze von Lindemann, *Gött. Nachr.* (1884) und (1892).

Über *spezielle, nicht algebraisch auflösbare Gleichungen* mögen folgende Angaben gemacht werden: *Daß gewisse aus der Theorie der elliptischen Funktionen stammende Gleichungen $(p+1)^{\text{ten}}$ Grades (p ungerade Primzahl) die Modulargruppe der Ordnung $\frac{1}{2}p(p^2-1)$ als Galoissche Gruppe* besitzen, hat bereits Galois (*Œuvres,* p. 27) gezeigt (vgl. S. 253). Kronecker (*Monatsber. d. Berl. Akad.* (1861) 615, (1879) 220) hat dann die Aufmerksamkeit auf die *allgemeinen Gleichungen $(p+1)^{\text{ten}}$ Grades (p ungerade Primzahl) mit der Modulargruppe als Galoisscher Gruppe* gelenkt. Für $p = 3, 5, 7$ und 11 und auch nur für diese Werte haben die fraglichen Gleichungen vierten, sechsten, achten und zwölften Grades infolge der Eigenschaften der Modulargruppe (vgl. S. 215, letzte Zeile) rationale Resolventen dritten, fünften, siebenten und elften Grades. Die Behandlung jeder Gleichung siebenten und achten Grades, deren Galoissche Gruppe eine einfache Gruppe der Ordnung 168 ist ($p = 7$ entsprechend), läßt sich auf das Formenproblem einer ternären linearen homogenen Substitutionsgruppe der Ordnung 168 zurückführen (vgl. S. 242). Ebenso kann die Behandlung jeder Gleichung 11. und 12. Grades mit einer einfachen Galoisschen Gruppe der Ordnung 660 ($p = 11$ entsprechend) auf das Formenproblem einer quinären linearen homogenen Substitutionsgruppe zurückgeführt werden; die Kollineationsgruppe niedrigsten Grades, die mit der $p = 11$ entsprechenden Modulargruppe isomorph ist, geht nämlich aus einer quinären Gruppe linearer homogener Substitutionen derselben Ordnung hervor (vgl. S. 244). Für alle Gleichungen siebenten und achten Grades mit einer einfachen Galoisschen Gruppe der Ordnung 168 hat Klein (*Math. Ann.* **15**, 265 (1879)) bewiesen, daß sie sich unter Heranziehung einer akzessorischen Hilfsgleichung vierten Grades mittels der speziellen, durch die Theorie der elliptischen Funktionen gelieferten Modulargleichung lösen lassen. (Rechnerische Ausführung bei Gordan, Literatur auf S. 242 bei der Kleinschen Gruppe.)

Die Dreiteilung der hyperelliptischen Funktionen liefert eine Gleichung 27. Grades mit einer Galoisschen Gruppe der Ordnung 51840, die eine invariante einfache Untergruppe der Ordnung 25920 besitzt. Die Lösung jeder Gleichung 27. Grades mit einer derartigen Galoisschen Gruppe der Ordnung 51840 läßt sich auf die obige Gleichung aus der Theorie der hyperelliptischen Funktionen zurückzuführen. Zu dieser Gattung von Gleichungen gehört im besonderen auch die *Gleichung 27. Grades für die 27 Geraden einer allgemeinen Fläche dritter Ordnung.* (Literaturangaben oben auf S. 244.)

Die Gleichung 16. Grades für die 16 Knotenpunkte einer Kummerschen Fläche hat eine Galoissche Gruppe der Ordnung 11520, die eine invariante Untergruppe $\mathfrak{G}_{16}$ der Ordnung 16 besitzt. Die Quotientengruppe $\mathfrak{G}_{11520}/\mathfrak{G}_{16}$ ist mit der symmetrischen Permutationsgruppe in sechs Symbolen holoedrisch isomorph, und die Gleichung 16. Grades kann mit Hilfe der allgemeinen Gleichung sechsten Grades und vier Quadratwurzelausziehungen gelöst werden (Literatur oben auf S. 243). Hingegen erfordert die *Gleichung 16. Grades für die 16 Geraden einer Fläche*

4. Ordnung mit einem Doppelkegelschnitt außer der Auflösung quadratischer Gleichungen nur die Lösung einer allgemeinen Gleichung fünften Grades. Die Ordnung der Galoisschen Gruppe dieser Gleichung 16. Grades ist 16. 5!. (Jordan, *Traité*, p. 309, Klein, *Math. Ann.* **4**, 357 (1871), Pereno, *Annali di mat.* (2) **21**, 57 (1893).)

Die *28 Doppeltangenten einer allgemeinen Kurve 4. Ordnung* hängen von einer Gleichung 28. Grades mit einer einfachen Galoisschen Gruppe der Ordnung 1451520 ab (vgl. S. 249). Die Verallgemeinerung dieses Problems ist folgende: *Ist C_n eine Kurve n^{ter} Ordnung ohne Doppelpunkte vom Geschlechte $p = \frac{1}{2}(n-1)(n-2)$, so hängt die Bestimmung der $2^{p-1}(2^p-1)$ Kurven der Ordnung $n-3$, die die gegebene C_n in $\frac{1}{2}n(n-3)$ Punkten zweipunktig berühren, von einer Gleichung $2^{p-1}(2^p-1)^{ten}$ Grades ab.* Die Untersuchung der zugehörigen Galoisschen Gruppe bei Jordan, *Traité*, p. 329, Dickson, *Trans. Am. M. S.* **3**, 38 und 377 (1902), *Annals of math.* (2) **6**, 141 (1905). Weiteres über Gruppen geometrischer Gleichungen bei Jordan, *Traité*, p. 301, Maillet, *C. R.* **138**, 890 (1904), *Ann. de Toulouse* (2) **6**, 277 (1904), E. Pascal, *Annali di mat.* (2) **20**, 269 (1893), **21**, 85 (1893).

§ 15. Bestimmung der Anzahl der reellen und komplexen Wurzeln einer Gleichung.

Eine Gleichung $f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$ mit reellen Koeffizienten hat zwischen zwei reellen Zahlen A und B eine gerade (einschl. 0) oder eine ungerade Anzahl von Wurzeln, je nachdem $f(A)$ und $f(B)$ gleiche oder entgegengesetzte Vorzeichen haben; hierbei ist jede Wurzel entsprechend ihrer Vielfachheit zu zählen. Für reelle Größen A, deren absoluter Betrag genügend groß ist, entscheidet über das Vorzeichen von $f(A)$ das erste Glied $a_0 A^n$.

Eine Gleichung ungeraden Grades mit reellen Koeffizienten hat stets wenigstens eine reelle Wurzel. Ist[1] *$sign(a_0) = -sign(a_n)$, so hat die Gleichung wenigstens eine positive Wurzel und, wenn n eine gerade Zahl ist, auch noch wenigstens eine negative Wurzel.*

Ist $f(z)$ eine ganze Funktion mit reellen Koeffizienten, $f'(z)$ ihre erste Abgeleitete und durchläuft z die reelle Zahlenreihe von

1) sign = Vorzeichen.

$-\infty$ bis $+\infty$, so geht der Quotient $\frac{f(z)}{f'(z)}$ bei seinem Verschwinden jedesmal von einem negativen Wert zu einem positiven über.

Hieraus folgt der Satz von Rolle, *Traité d'algèbre* (1690), 2tes Buch, Kap. 6, vgl. auch Lagrange, *Œuvres* **8**, 190—199:

Sind A und B zwei unmittelbar aufeinanderfolgende reelle Wurzeln einer Gleichung $f(z) = 0$ mit reellen Koeffizienten, so liegt zwischen A und B (die Grenzen sind nicht mitzuzählen) eine ungerade Zahl von Wurzeln (mehrfache Wurzeln sind ihrer Vielfachheit nach zu zählen) der Gleichung $f'(z) = 0$, also mindestens eine.

Korollare zum Satz von Rolle: I. Hat die Gleichung $f(z) = 0$ mit reellen Koeffizienten ϱ reelle Wurzeln, so hat die Gleichung $f'(z) = 0$ stets $\varrho - 1 + 2k$ reelle Wurzeln, wobei $k \geqq 0$ ist. II. *Zwischen zwei aufeinanderfolgenden reellen Wurzeln der Gleichung $f'(z) = 0$ kann höchstens eine Wurzel von $f(z) = 0$ gelegen sein.* Den Satz II benützt Rolle, um Grenzen für die reellen Gleichungswurzeln zu finden. Vgl. auch Lagrange, a. a. O.

Aus dem Satze von Rolle ergibt sich das Theorem von Waring (*Meditationes algebraicae* (1770), vgl. Cajori bei Cantor, *Vorl. über Geschichte der Math.* **4**, 106): *Sind A und B zwei unmittelbar aufeinanderfolgende reelle Wurzeln einer Gleichung $f(z) = 0$ mit reellen Koeffizienten, so liegt zwischen A und B (die Grenzen sind nicht mitzuzählen) eine ungerade Anzahl von Wurzeln (mehrfache Wurzeln sind ihrer Vielfachheit nach zu zählen) der Gleichung $F(z) = C_0 f(z) + C_1 f'(z) = 0$, also mindestens eine. C_0 und C_1 sind beliebige reelle Größen; $C_1 \neq 0$* (vgl. auch Cesàro, *Nouv. Ann. de math.* (3) **4**, 326 (1885)).

Korollare zum Waringschen Satz: I. Hat die Gleichung $f(z) = 0$ mit reellen Koeffizienten ϱ reelle Wurzeln, so hat die Gleichung $F(z) = C_0 f(z) + C_1 f'(z) = 0$, wobei C_0 und C_1 beliebige reelle Größen sind $(C_0 \neq 0)$, $\varrho + 2l$ reelle Wurzeln; hierbei ist $l \geqq 0$. II. Zwischen zwei aufeinanderfolgenden reellen Wurzeln der Gleichung $F(z) = 0$ kann höchstens eine Wurzel von $f(z) = 0$ gelegen sein.

Verallgemeinerung des Korollars I zum Waringschen Satz: Hat die Gleichung $C_0 z^m + C_1 z^{m-1} + C_2 z^{m-2} + \cdots + C_m = 0$ von beliebigem Grade m mit reellen Koeffizienten lauter reelle Wurzeln und die Gleichung $f(z) = 0$ vom Grade $n \geqq m$ mit reellen Koeffizienten ϱ reelle Wurzeln, so hat die Gleichung $C_0 f(z) + C_1 f'(z) + C_2 f''(z) + \cdots + C_m f^{(m)}(z) = 0$, bei der $f'(z)$, $f''(z), \ldots f^{(m)}(z)$ die sukzessiven Abgeleiteten bedeuten, $\varrho + 2l$

reelle Wurzeln ($l \geqq 0$) (Poulain, *Nouv. Ann. de math.* (2) **6**, 23 (1867), Realis, ebenda, p. 417, Fouret, *C. R.* **106**, 1135 u. 1220 (1888)).

Hat die Gleichung $f(z) = 0$ vom n^{ten} Grade mit reellen Koeffizienten ϱ reelle Wurzeln, so hat die Gleichung

$$f(z) + tf'(z) + t^2 f''(z) + \cdots + t^n f^{(n)}(z) = 0,$$

wobei t eine beliebige reelle Größe ist und $f'(z), f''(z), \ldots, f^{(n)}(z)$ die sukzessiven Abgeleiteten bedeuten, $\varrho - 2k$ reelle Wurzeln, $k \geqq 0$ (Poulain, *Nouv. Ann. de math.* (2) **6**, 22 (1867), Realis, ebenda, p. 416).

Satz von Hermite *und* Biehler (Hermite, *Bull. soc. math.* **7**, 131 (1879), Biehler, *Journ. f. Math.* **87**, 350 (1879), Laguerre, *Œuvres* **1**, 109 und 360, Auric, *C. R.* **137**, 967 (1903), Hurwitz, *Math. Ann.* **46**, 284 (1895)): *Ist $(z - \alpha_1 - \beta_1 i)(z - \alpha_2 - \beta_2 i) \ldots (z - \alpha_n - \beta_n i) = \varphi(z) + i\psi(z)$ und haben die Größen $\beta_1, \beta_2, \ldots, \beta_n$ ausnahmslos das gleiche Vorzeichen*[1]*, so hat die Gleichung $p\varphi(z) + q\psi(z) = 0$, wobei p und q beliebige reelle Größen bedeuten, nur reelle Wurzeln. Alle reellen Wurzeln von $\varphi(z) = 0$ sind untereinander verschieden und werden durch diejenigen von $\psi(z) = 0$ getrennt, die gleichfalls reell und verschieden sind.*

Die *genaue Anzahl reeller Wurzeln* einer beliebigen Gleichung $f(z) = 0$ mit reellen Koeffizienten zwischen zwei reellen Zahlen A und B ($A < B$) liefert der *Satz von* Sturm (vgl. S. 256). Wir führen zunächst den Begriff der *Sturmschen Kette* ein: Ist $f(z) = 0$ eine Gleichung mit reellen Wurzeln, die im Intervall A bis B keine mehrfachen Wurzeln hat, so heißt eine Reihe ganzer rationaler Funktionen $f(z), f_1(z), f_2(z), \ldots, f_r(z)$ mit reellen Koeffizienten eine Sturmsche Kette, wenn sie folgende Bedingungen erfüllt:

1. Die letzte Funktion $f_r(z)$ ändert nie ihr Vorzeichen, wenn z alle reellen Werte des Intervalls von A bis B[2] durchläuft.

2. Zwei unmittelbar aufeinanderfolgende Funktionen $f_{k-1}(z)$ und $f_k(z)$ verschwinden nie gleichzeitig für denselben reellen Wert $z = b$ des Intervalls von A bis B.

3. Verschwindet eine Funktion $f_k(z)$ ($k = 1, 2, \ldots, r - 1$) für einen reellen Wert $z = b$ des Intervalls von A bis B, so ist sign $f_{k-1}(b) = -$ sign $f_{k+1}(b)$.

---

1) i ist die imaginäre Einheit.

2) Die Grenzen A und B sind bei den Bedingungen 1—4 einzuschließen.

4. Wenn $f(z)$ für einen reellen Wert des Intervalls von A bis B verschwindet, so hat für diesen die erste Funktion $f_1(z)$ jedesmal dasselbe Vorzeichen wie die erste Abgeleitete $f'(z)$.

Sturmscher Satz (I): *Bilden für eine Gleichung $f(z) = 0$ mit reellen Koeffizienten, die im Intervall von A bis B keine mehrfachen Wurzeln hat, die Funktionen $f(z)$, $f_1(z)$, $f_2(z), \ldots$, $f_r(z)$ eine Sturmsche Kette und sind A und B zwei reelle Zahlen $(A < B)$, so hat die Gleichung $f(z) = 0$ zwischen den Grenzen A und B, die selbst keine Wurzeln sein sollen, soviel reelle Wurzeln, wie die Reihe*

$$f(A),\ f_1(A),\ f_2(A), \ldots, f_r(A)$$

mehr Vorzeichenwechsel besitzt als die Reihe

$$f(B),\ f_1(B),\ f_2(B), \ldots, f_r(B).$$

Zwei aufeinanderfolgende reelle Größen, die nicht verschwinden, besitzen einen *Vorzeichenwechsel* oder eine *Vorzeichenfolge*, je nachdem sie verschiedene oder gleiche Vorzeichen haben. In den zwei obigen Reihen können Nullen nur in der Mitte, jedoch nie am Ende (Bedingung 1 für die Sturmsche Kette) und nie am Anfang ($f(A) \neq 0$, $f(B) \neq 0$) auftreten; die Nullen kommen nur isoliert vor (Bedingung 2 für die Sturmsche Kette) und sind beim Abzählen der Vorzeichenwechsel einfach fortzulassen.

Eine besondere Sturmsche Kette liefert das *von Sturm angegebene Divisionsverfahren.* Man wähle für $f_1(z)$ die erste Abgeleitete $f'(z)$. Durch fortgesetzte Division bilde man die Gleichungskette:

$$\begin{aligned}
f(z) &= f'(z)\,G_1(z) - f_2(z),\\
f'(z) &= f_2(z)\,G_2(z) - f_3(z),\\
f_2(z) &= f_3(z)\,G_3(z) - f_4(z),\\
&\;\vdots\\
f_{r-2}(z) &= f_{r-1}(z)\,G_{r-1}(z) - f_r,
\end{aligned}$$

in der die sukzessiv auftretenden Reste immer mit entgegengesetzten Vorzeichen verwendet werden. Hat $f(z) = 0$ keine mehrfachen Wurzeln, so sind $f(z)$ und $f'(z)$ relativ prim, und man gelangt schließlich zu einem von Null verschiedenen letzten konstanten Rest: $-f_r$. *Die gefundenen Funktionen $f(z)$, $f'(z)$, $f_2(z)$, $f_3(z), \ldots, f_r$ bilden eine Sturmsche Kette.*

Sturmscher Satz (II): *Hat die Gleichung $f(z) = 0$ reelle Koeffizienten und keine mehrfachen Wurzeln und setzt man in* *die durch das Sturmsche Divisionsverfahren gefundene Funktionenkette* $f(z)$, $f'(z)$, $f_2(z)$, $f_3(z)$, ..., f_r *die reellen Zahlen* A *und* B $(A < B)$, *die selbst keine Wurzeln der Gleichung sein sollen, so gibt die Anzahl der Vorzeichenwechsel, welche die Reihe*

$$f(A),\ f'(A),\ f_2(A), \ldots, f_{r-1}(A),\ f_r$$

mehr als die Reihe

$$f(B),\ f'(B),\ f_2(B), \ldots, f_{r-1}(B),\ f_r$$

hat, die genaue Anzahl reeller Wurzeln von $f(z) = 0$, *die zwischen den Grenzen* A *und* B *liegen.*

Zusatz (Sturm, a. a. O., Artikel 18): *Bei einer Gleichung mit mehrfachen Wurzeln verschwindet der Rest* $-f_r$; *der Satz* II *bleibt trotzdem noch richtig, nur ist das verschwindende* f_r *fortzulassen und jede zwischen den Grenzen* A *und* B *gelegene mehrfache Wurzel auch bloß einfach zu zählen.*

Wählt man $A = -\infty$ und $B = +\infty$, so liefert das Sturmsche Theorem die genaue Anzahl aller reellen Wurzeln von $f(z) = 0$.

Eine Gleichung $f(z) = 0$ *vom* n^{ten} *Grade mit reellen Koeffizienten besitzt dann und nur dann lauter reelle verschiedene Wurzeln, wenn die durch das Sturmsche Divisionsverfahren gewonnene Sturmsche Kette* $f, f', f_2, \ldots, f_r$ *aus* $n+1$ *Funktionen besteht, und die Koeffizienten der höchsten Potenzen in allen Funktionen das nämliche Vorzeichen haben.*

Ebenso wie das Sturmsche Verfahren leistet auch die Theorie der reellen quadratischen Formen (Hermite, *C. R.* **35**, 52 (1852), ebenda **36**, 407 (1853), *Journ. f. Math.* **52**, 39 (1856), *Œuvres* **1**, 281, 284, 397, Sylvester, *Phil. Trans.* **143** (1853), *Coll. math. papers* **1**, 429) *die Bestimmung der genauen Anzahl reeller Wurzeln, welche eine Gleichung* $f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$ *mit reellen Koeffizienten zwischen zwei gegebenen reellen Zahlen* A *und* B $(A < B)$ *hat.*

Es seien $\alpha_1, \alpha_2, \ldots, \alpha_n$ die n verschiedenen Wurzeln der Gleichung $f(z) = 0$, die keine mehrfachen Wurzeln habe. Man bilde die quadratische Form:

$$h_1 = \sum_{k=1}^{k=n} (\xi - \alpha_k)^q (U_1 + \alpha_k U_2 + \alpha_k^2 U_3 + \cdots \alpha_k^{n-1} U_n)^2$$

der n Variablen $U_1, U_2, \ldots, U_n$; die Größe q bedeute eine positive oder negative ungerade Zahl, ξ einen reellen willkürlichen Parameter. Die Koeffizienten von h_1 lassen sich als symmetrische Funktionen der Gleichungswurzeln durch die reellen Koeffizienten von $f(z) = 0$ reell ausdrücken. *Transformiert man die reelle quadratische Form h_1 durch eine reelle lineare homogene Substitution von nicht verschwindender Determinante in eine Summe reeller Quadrate* (vgl. S. 121) *und findet man, wenn man $\xi = A$ setzt, N_A, wenn man $\xi = B$ wählt, N_B Quadrate mit negativen Vorzeichen, so ist die genaue Anzahl der zwischen A und B gelegenen Wurzeln von $f(z) = 0$ gleich $N_A - N_B$.*

Man kann statt h_1 auch andere reelle quadratische Funktionen wählen, die dasselbe leisten, z. B. die aus h_1 durch reelle lineare homogene Transformation von nicht verschwindender Determinante: $U_i = a_0 u_i + a_1 u_{i+1} + a_2 u_{i+2} + \cdots + a_{n-i} u_n$ $(i = 1, 2, \ldots, n)$ hervorgehende reelle quadratische Form H_1 der n Variablen $u_1, u_2, \ldots u_n$, nämlich:

$$H_1 = \sum_{k=1}^{k=n} (\xi - \alpha_k)^q \cdot [a_0 u_1 + (a_0 \alpha_k + a_1) u_2 + (a_0 \alpha_k^2 + a_1 \alpha_k + a_2) u_3 + \cdots (a_0 \alpha_k^{n-1} + a_1 \alpha_k^{n-2} + \cdots a_{n-1}) u_n]^2.$$

Besonders bequem gestaltet sich die Berechnung der $q = 1$ entsprechenden quadratischen Form H_1. Sie ist nämlich die *Bézoutiante* (vgl. S. 271) der zwei ganzen Funktionen $f(x)$ und $g(x) = f'(x) \cdot (x - \xi)$ vom n^{ten} Grade, wobei $f'(x)$ die erste Abgeleitete bedeutet. Es ergibt sich folgende Vorschrift: *Man entwickle*

$$\frac{f(x) \cdot f'(y) \cdot (y - \xi) - f(y) f'(x) \cdot (x - \xi)}{y - x} = \sum_{i=0}^{i=n-1} \sum_{k=0}^{k=n-1} d_{ik} x^i y^k$$

nach ganzen positiven Potenzen der Variablen x, y und führe für $x^i y^k$ die Produkte $u_{n-i} u_{n-k}$ ein. Die $q = 1$ entsprechende quadratische Form H_1 lautet alsdann

$$H_1 = \sum_{i=0}^{i=n-1} \sum_{k=0}^{k=n-1} d_{ik} u_{n-i} u_{n-k}.$$

Die Differenz der Anzahl negativer Quadrate, welche die Bézoutiante $\sum_{i=0}^{i=n-1} \sum_{k=0}^{k=n-1} d_{ik} u_{n-i} u_{n-k}$, deren Koeffizienten von dem Parameter ξ abhängen, für $\xi = A$ und $\xi = B$ liefert, ist gleich der Zahl der Gleichungswurzeln von $f(z) = 0$ zwischen den Grenzen A und B (Hermite, *Journ. f. Math.* **52**, 51 (1856), *Œuvres* **1**, 413).

Die für $q = 0$ aus h_1 hervorgehende quadratische Form sei mit g_1 bezeichnet.

$$g_1 = \sum_{k=1}^{k=n} (U_1 + \alpha_k U_2 + \alpha_k^2 U_3 + \cdots + \alpha_k^{n-1} U_n)^2 = \sum_{i=1}^{i=n} \sum_{l=1}^{l=n} s_{i+l-2} U_i U_l,$$

wobei $s_i = \sum_{k=1}^{k=n} \alpha_k^i$ die Summe der i^{ten} Potenzen der Gleichungswurzeln bedeutet. *Die reelle quadratische Form g_1 hat bei jeder reellen linearen homogenen Substitution in eine Summe von Quadraten soviel Quadrate mit negativen Vorzeichen als die Gleichung $f(z) = 0$ Paare imaginärer Wurzeln hat.* Hieraus ergibt sich der Satz von Borchardt (*Journ. de math.* **12**, 58 (1847), *Ges. Werke,* S. 24):

Die Gleichung $f(z) = 0$ mit reellen Koeffizienten und verschiedenen Wurzeln hat soviel Paare imaginärer Wurzeln als die Reihe der Determinanten:

$$\sigma_1 = s_0, \quad \sigma_2 = \begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix},$$

$$\sigma_3 = \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}, \ldots, \sigma_n = \begin{vmatrix} s_0 & s_1 \ldots s_{n-1} \\ s_1 & s_2 \ldots s_n \\ \vdots & \\ s_{n-1} & s_n \ldots s_{2n-2} \end{vmatrix}$$

Vorzeichenwechsel aufweist. Das Borchardtsche Theorem bleibt auch richtig, wenn in der Größenreihe $\sigma_1, \sigma_2, \ldots, \sigma_n$ isolierte Nullen auftreten; diese sind einfach zu streichen. Bei mehrfach unmittelbar aufeinanderfolgenden Nullen kann das Borchardtsche Kriterium versagen, wie beispielsweise die Gleichung $z^4 + 1 = 0$ lehrt.

Eine charakteristische Bedingung dafür, daß eine Gleichung $f(z) = 0$ mit reellen Koeffizienten ohne mehrfache Wurzeln nur reelle Wurzeln hat, besteht darin, daß $\sigma_2 > 0$, $\sigma_3 > 0, \ldots$, $\sigma_n > 0$ sind.

Die quadratische Form g_1 und das Trägheitsgesetz der reellen quadratischen Formen hat Jacobi bereits vor Veröffentlichung der Hermiteschen und Sylvesterschen Arbeiten zur Bestimmung der reellen Wurzeln einer Gleichung $f(z) = 0$ mit reellen Koeffizienten verwendet (vgl. Borchardt, *Journ. f. Math.* **53**, 281 (1857), *Ges. Werke,* S. 469, siehe oben S. 122).

Wir schließen diese Betrachtungen (vgl. zu dem hier behandelten Gegenstand noch die Aufsätze von Kronecker, *Ges. Werke* **1**, 227, 303, **2**, 37, 113, die *Monographie* von Hattendorff, *Die Sturmschen Funktionen*, 2. Aufl. Hannover 1874, Frobenius, *Journ. f. Math.* **114**, 187 (1895), Hurwitz, *Math. Ann.* **46**, 273 (1895), die Anmerkungen zu Sturms Abhandlung in Ostwalds *Klass. der exakten Wiss.* Nr. 143) mit einem Satz von Sylvester (*Phil. Trans.* (1853), *Coll. math. papers* **1**,547):

Sei $f(z)=0$ eine Gleichung n^{ten} Grades ohne mehrfache Wurzeln und mit reellen Koeffizienten und $f_1(z)=nf(z)-zf'(z)$, wobei $f'(z)$ die erste Abgeleitete von $f(z)$ ist, so hat die Gleichung $f(z)=0$ soviel Paare imaginärer Wurzeln, wie die Bézoutiante von $f'(z)$ und $f_1(z)$ bei einer reellen Transformation in eine Summe von Quadraten negative Quadrate aufweist. Die Bézoutiante von $f'(z)$ und $f_1(z)$ ist eine reelle quadratische Form

$$\sum_{i=0}^{i=n-2}\ \sum_{k=0}^{k=n-2} d_{ik}u_{n-i}u_{n-k}$$

von nur $n-1$ Variablen $u_2, u_3, \ldots, u_n$ und wird gefunden, indem man

$$\frac{f'(x)\cdot f_1(y)-f'(y)f_1(x)}{y-x}=\sum_{i=0}^{i=n-2}\ \sum_{k=0}^{k=n-2} d_{ik}x^i y^k$$

bildet und für $x^i y^k$ das Produkt $u_{n-i}u_{n-k}$ setzt.

Nicht die genaue Anzahl, aber eine *obere Grenze* für die Zahl der Wurzeln einer Gleichung mit reellen Koeffizienten, die zwischen zwei reellen Zahlen liegen, liefert der *Satz von* Fourier (vgl. S. 256): *Ist $f(z)=0$ eine Gleichung n^{ten} Grades mit reellen Koeffizienten und bedeuten $f'(z), f''(z), \ldots, f^{(n)}(z)$ die Abgeleiteten von $f(z)$, so ist die Anzahl der Wurzeln von $f(z)=0$, die zwischen den zwei reellen Zahlen A und B $(A<B)$ liegen, wenn A und B keine Wurzeln von $f(z)=0$ sind, gleich oder um eine gerade Zahl kleiner als die Differenz der Vorzeichenwechsel in den zwei Reihen:*

$$f(A),\ f'(A), \ldots,\ f^{(n)}(A)$$

und

$$f(B),\ f'(B), \ldots,\ f^{(n)}(B).$$

Etwaige in den zwei Reihen auftretende Nullen sind zu streichen. Jede mehrfache Wurzel, welche die Gleichung $f(z)=0$ im Intervall A bis B hat, ist beim Fourierschen Satz entsprechend ihrer

Vielfachheit zu zählen. Für eine Gleichung mit lauter reellen Wurzeln gibt der Fouriersche Satz die genaue Anzahl ihrer reellen Wurzeln zwischen irgend zwei Grenzen A und B. Der Fouriersche Satz wird mit Unrecht auch nach Fouriers Zeitgenossen Budan genannt (vgl. Darboux, *Œuvres de Fourier* **2**, 310).

Satz von Laguerre (*Journ. de math.* (3) **9**, 102 (1883), (*Nouv. Ann. de math.* (2) **18**, 9 (1879), ebenda **19**, 52 (1880), *Œuvres* **1**, 6, 68 und 75, Paris 1898): *Ist A eine positive Größe und $f(z) = 0$ eine Gleichung mit reellen Koeffizienten, so ist die Zahl der Zeichenwechsel, welche die Reihe:*

$$\begin{aligned}
f(z) &= a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n\,, \\
f_1(z) &= a_0 z^{n-1} + a_1 z^{n-2} + \cdots \qquad\quad + a_{n-1}\,, \\
f_2(z) &= a_0 z^{n-2} + a_1 z^{n-3} + \cdots \qquad\quad + a_{n-2}\,, \\
&\vdots \\
f_n \;\; &= a_0
\end{aligned}$$

für $z = A$ aufweist, wenigstens gleich der Zahl der Wurzeln von $f(z) = 0$ (mehrfache Wurzeln sind entsprechend ihrer Vielfachheit zu zählen), die größer als A sind. Übertrifft die Anzahl der Zeichenwechsel die Zahl der Wurzeln, die größer als A sind, so ist die Differenz eine gerade Zahl.

Descartessche Zeichenregel (vgl. S. 251): *Hat man eine Gleichung $f(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n = 0$ mit reellen Koeffizienten, so ist die Zahl der positiven Wurzeln von $f(z) = 0$ (mehrfache Wurzeln sind entsprechend ihrer Vielfachheit zu zählen) gleich oder um eine gerade Zahl kleiner als die Zahl der Vorzeichenwechsel der Gleichung. Etwa vorhandene Wurzeln 0 sind nicht als positive Wurzeln mitzuzählen. Unter den Zeichenwechseln bezw. Zeichenfolgen der Gleichung $f(z) = 0$ versteht man die Zahl der Zeichenwechsel bezw. Zeichenfolgen der Koeffizientenreihe a_0, a_1, a_2, . . ., a_n; etwaige verschwindende Koeffizienten sind fortzulassen.*

Die Descartessche Regel ergibt sich aus dem Fourierschen Satz, indem man $A = 0$, $B = \infty$ wählt, und aus dem Laguerreschen Satz, wenn man $A = 0$ setzt. Einen Beweis der Descartesschen Regel hat Gauß, *Ges. Werke* **3**, 65, gegeben, vgl. ferner Laguerre, *Journ. de math.* (3) **9**, 99 (1883), *Œuvres* **1**, 3. Die Descartessche Regel wird irrtümlicherweise auch Harriot, *Artis analyticae praxis* (1631), zugeschrieben. Bei Harriot findet sich die Regel überhaupt nicht (vgl. auch die Anm. in *Ostwalds Klass. d. exakt. Wiss.* Nr. 127, S. 247).

Zusätze zur Descartesschen Zeichenregel:

1. *Die Zahl der negativen Wurzeln von* $f(z) = 0$ *ist gleich oder um eine gerade Zahl kleiner als die Zahl der Vorzeichenwechsel der Gleichung* $f(-z) = 0$.

2. *Gauß' Korollar zum Descartesschen Satz* (Gauß, *Ges. Werke* **3**, 70): *Fehlen in einer Gleichung mit reellen Koeffizienten e Glieder und ist c und d die Anzahl der durch eine ungerade Zahl fehlender Glieder unterbrochenen Zeichenwechsel bezw. Zeichenfolgen in der gegebenen Gleichung, so hat die Gleichung mindestens* $e - c + d$ *imaginäre Wurzeln.*

3. Aus dem Gaußschen Korollar oder aus der am Schluß des Fourierschen Satzes gemachten Bemerkung folgt: *Eine Gleichung mit lauter reellen Wurzeln besitzt genau soviel positive Wurzeln, als* $f(z)$ *Zeichenwechsel aufweist, und soviel negative Wurzeln, wie* $f(-z)$ *Zeichenwechsel hat. Abgesehen von den letzten Gliedern können nur isolierte Glieder der Gleichung verschwinden, diese müssen stets zwischen zwei Gliedern mit verschiedenen Vorzeichen stehen.*

Eine *obere Grenze* für die Anzahl der reellen Wurzeln einer Gleichung gibt auch ein von Sylvester, *Coll. math. papers* **2**, 376, 489, 491, 493, 498, 542, 704 aufgestelltes Theorem, das eine bereits von Newton (*Arithmetica universalis* (1707), Bd. 2, Kap. 2, Maclaurin, *Algebra* (1748), Teil 2, Sect. 1, Kap. 13, Cantor, *Vorl. über Geschichte der Math.* **3**, 404 u. 561) stammende Regel als besonderen Fall enthält. Literatur: Genocchi, *Nouv. Ann. de math.* (2) **6**, 5 (1867), Petersen, *Theorie der algebraischen Gleichungen*, S. 203, Weber, *Algebra* **1**, 345, Netto, *Algebra* **1**, 225.

Die Bestimmung der Gesamtzahl der reellen Gleichungswurzeln hängt mit der für ein Intervall auf folgende Weise zusammen:

Jede Gleichung $f(z) = 0$ *mit reellen Koeffizienten hat halb so viele Wurzeln, die größer als irgendeine reelle Zahl A sind, als die Gesamtzahl reeller Wurzeln von* $f(y^2 + A) = 0$ *beträgt.* Bestimmt man also $A = 0$ entsprechend die Gesamtzahl reeller Wurzeln von $f(y^2) = 0$ nach dem Borchardtschen oder Sylvesterschen Satz, so ist die Zahl der positiven Wurzeln von $f(z) = 0$ halb so groß.

Jede Gleichung $f(z) = 0$ *mit reellen Koeffizienten hat* *zwischen den Grenzen A und B $(A < B)$ soviel Wurzeln als die Gleichung* $\varphi(u) = (1+u)^n f\left(\frac{A+Bu}{1+u}\right) = 0$ *positive Wurzeln besitzt.* Die auf $\varphi(u) = 0$ angewandte Descartessche Zeichenregel gibt also analog dem Fourierschen Satz eine approximative obere Grenze für die im Intervall A bis B gelegenen Wurzeln von $f(z) = 0$ (Jacobi, *Journ. f. Math.* **13**, 348 (1835), *Ges. Werke* **3**, 279).

Die Gleichung $f(z) = 0$ *hat zwischen den Grenzen A und B $(A < B)$ halb so viele Wurzeln wie* $\varphi(y^2) = (1+y^2)^n f\left(\frac{A+By^2}{1+y^2}\right) = 0$ *reelle Wurzeln besitzt, und die Gesamtzahl reeller Wurzeln von* $\varphi(y^2) = 0$ *ist gleich der Differenz der Gesamtzahl reeller Wurzeln von* $f(y^2 + A) = 0$ *und der von* $f(y^2 + B) = 0$.

Über eine von Klein angegebene geometrische Vergleichung der verschiedenen Abschätzungskriterien für die Anzahl der reellen Gleichungswurzeln vgl. Weber, *Algebra* **1**, 354.

Mit Hilfe des Sturmschen Divisionsverfahrens läßt sich für eine rationale Funktion auch der von Cauchy eingeführte *Index der Funktion* bestimmen. $\varphi(t)$ sei irgendeine in dem Intervall $A \leqq t \leqq B$ (A und B reelle Zahlen) reelle und, abgesehen von ν in dem Intervall gelegenen Ausnahmestellen $t_1, t_2, \ldots, t_\nu$, eindeutige und stetige Funktion von t; die Unstetigkeitsstellen seien derartig, daß der Wert von φ mit bestimmtem Vorzeichen unendlich wird, sowohl wenn t von links her als von rechts her sich dem t_i $(i = 1, 2, \ldots, \nu)$ nähert. Für jede einzelne Unstetigkeitsstelle sei $\varepsilon(t_i) = 0$, $+1$ oder -1, je nachdem φ beim Überschreiten von t_i sein Vorzeichen nicht ändert oder von einem negativen zu einem positiven oder von einem positiven zu einem negativen Wert übergeht. *Unter dem Index* $J_A^B(\varphi)$ *der Funktion φ für das Intervall* $A \leqq t \leqq B$ *versteht man nach Cauchy* (*J. éc. polyt.*, Cah. **25**, 176 (1837)) *die Summe* $J_A^B(\varphi) = \varepsilon(t_1) + \varepsilon(t_2) + \cdots + \varepsilon(t_\nu)$. *Ist φ für das ganze Intervall stetig, so ist* $J_A^B(\varphi) = 0$.

Hat auch $\frac{1}{\varphi}$ ebenso wie φ für das Intervall A bis B nur einzelne im Innern des Intervalls liegende polare Unstetigkeiten, so besteht die Relation:

$$J_A^B(\varphi) + J_A^B\left(\frac{1}{\varphi}\right) = \frac{1}{2}\Big(\operatorname{sign}\varphi(B) - \operatorname{sign}\varphi(A)\Big).$$

Ist $\varphi = \frac{f_1}{f}$ *eine rationale Funktion, wobei f und f_1 teiler-*

fremde ganze Funktionen bedeuten, und ist f mindestens von dem gleichen Grade wie f_1, so findet man den Index $J_A^B\left(\frac{f_1}{f}\right)$ auf folgende Weise: Man bilde nach dem Sturm*schen Divisionsverfahren die Funktionenreihe $f, f_1, f_2, \ldots, f_r$, die erhalten wird, indem man f durch f_1 dividiert und die sukzessiv auftretenden Reste immer mit entgegengesetzten Vorzeichen nimmt. $J_A^B\left(\frac{f_1}{f}\right)$ ist gleich der Anzahl der Vorzeichenwechsel, welche die Reihe*

$$f(A),\ f_1(A),\ f_2(A), \ldots,\ f_r(A)$$

mehr aufweist als die Reihe

$$f(B),\ f_1(B),\ f_2(B), \ldots,\ f_r(B).$$

(Sturm in der S. 256 zitierten Arbeit Artikel 20, ferner *Journ. de math.* **1**, 305 (1836), Cauchy, a. a. O., S. 187.)

Ist f_1 von höherem Grade als f und hat man den Index $J_A^B\left(\frac{f_1}{f}\right)$ zu bestimmen, so geschieht dies mit Hilfe der oben zwischen $J_A^B(\varphi)$ und $J_A^B\left(\frac{1}{\varphi}\right)$ angegebenen Relation.

Ist f' die erste Abgeleitete von f, so ist $J_A^B\left(\frac{f'}{f}\right)$ gleich der Anzahl der zwischen A und B gelegenen reellen Wurzeln von $f(z) = 0$. (Sturmscher Satz vgl. S. 340.)

Die Anzahl der Wurzeln einer Gleichung $f(z) = 0$ mit beliebigen (auch komplexen) Koeffizienten im Innern einer einfach geschlossenen regulären Kurve C wird durch ein Cauchysches Integral bestimmt. *Ist $f(z)$ eine überall im Innern und auf dem Rande von C holomorphe und auf dem Rande auch von Null verschiedene Funktion, so ist die Anzahl ihrer innerhalb von C gelegenen Nullstellen (jede nach ihrer Vielfachheit gezählt) gleich $\frac{1}{2\pi i}\int\limits_C \frac{f'(z)}{f(z)}\,dz$, wobei das Integral über den Rand von C in positivem Sinne zu erstrecken ist. Ist $z = x + iy$ und trennt man $f(z)$ in seinen reellen und imaginären Bestandteil, setzt also $f(x + iy) = X(x, y) + i\,Y(x, y)$, so wird*

$$\frac{1}{2\pi i}\int \frac{f'(z)}{f(z)}\,dz = \frac{1}{2}\,J\left(\frac{X}{Y}\right);$$

der Index ist längs der Kurve C zu erstrecken, d. h. er wird gleich der stets geraden Zahl $p - p'$, wenn p bezw. p' die An-

zahl von Punkten auf C angibt, in denen Y verschwindet und hierbei der Quotient $\frac{X}{Y}$ *vom Negativen zum Positiven bzw. vom Positiven zum Negativen übergeht. Man kann statt X, Y auch — Y, X verwenden* (Cauchy, vgl. Sturm u. Liouville, *Journ. de math.* **1**, 278 (1836), Sturm, ebenda, S. 290). Betreffs des Cauchyschen Index vgl. ferner Hermite, *Journ. f. Math.* **52**, 39 (1856), *Œuvres* **1**, 410, Hurwitz, *Math. Ann.* **46**, 273 (1895), **64**, 517 (1907).

$f(z)$ sei eine ganze rationale Funktion und C werde von λ Bogen unicursaler Kurven gebildet. Ein Bogen C_l werde durch die rationalen Funktionen $x = \varphi(t)$, $y = \psi(t)$ dargestellt, wobei die reelle Variable t das Intervall A bis B durchlaufe und auf diese Weise den Bogen C_l einmal beschreibe. Längs des Bogens C_l geht $f(z) = X(x, y) + iY(x, y)$ über in die rationale Funktion $X(\varphi, \psi) + iY(\varphi, \psi) = R(t) + iR_1(t)$; längs des Bogens C_l wird $J\left(\frac{X}{Y}\right)$ daher gleich $J_A^B\left(\frac{R(t)}{R_1(t)}\right)$ und ist als Index einer rationalen Funktion mittels des Sturmschen Divisionsverfahrens zu finden. Der Index längs der Kurve C ist die Summe der Indizes längs $C_1, C_2, \ldots, C_\lambda$. So kann man auf rationalem Wege die Anzahl der Wurzeln innerhalb eines von Geraden und Kreisbogen begrenzten Bereiches finden. Wählt man für C einen genügend großen Kreis, dessen Zentrum der Koordinatenursprung der Gaußschen Ebene ist, so läßt sich auf die Theorie des Index ein Beweis des *Fundamentalsatzes der Algebra* gründen. Hierauf beruhen auch ihrem Gedankengang nach der erste und vierte Gaußsche Beweis des Fundamentalsatzes der Algebra (vgl. Zitat oben S. 251, siehe auch Weber, *Algebra* **1**, 333).

Die Untersuchungen über den Cauchyschen Index sind ein spezieller Fall der von Kronecker (*Monatsb. d. Berl. Akad.* (1869), (1873) u. (1878), *Ges. Werke* **1**, 175, 213, 303, **2**, 37, 113) stammenden *Charakteristikentheorie.* Sie bestimmt die mehreren Gleichungen mit reellen Koeffizienten und reellen Variablen gemeinsamen Wurzeln. Vgl. Picard, *Traité d'analyse,* **2**. Aufl., Bd. **1**, 136 und **2**, 205, Weber, *Algebra* **1**, 323.

§ 16. Approximation der Wurzeln.

Jede Gleichung $b_0 + b_1 z^{\nu_1} + b_2 z^{\nu_2} + \cdots + b_k z^{\nu_k} = 0$, *bei der* $0 < \nu_1 < \nu_2 < \cdots < \nu_k$ *und* $b_0 \neq 0$, $b_1 \neq 0$ *ist, hat, wenn man ihre Wurzeln in der sog. Gaußschen Ebene der komplexen*

Zahlen darstellt, innerhalb oder am Rande eines jeden der vier Kreise mit den Radien:

$$(1)\qquad \left(\frac{\nu_2\nu_3\ldots\nu_k}{(\nu_2-\nu_1)(\nu_3-\nu_1)\ldots(\nu_k-\nu_1)}\right)^{\frac{1}{\nu_1}}\left|\frac{b_0}{b_1}\right|^{\frac{1}{\nu_1}},$$

$$(2)\qquad \left(\frac{(\nu_1+1)(\nu_1+2)\ldots(\nu_1+k-1)}{1\cdot 2\ldots k-1}\right)^{\frac{1}{\nu_1}}\cdot\left|\frac{b_0}{b_1}\right|^{\frac{1}{\nu_1}},$$

$$(3)\qquad k\left|\frac{b_0}{b_1}\right|^{\frac{1}{\nu_1}},$$

$$(4)\qquad kB$$

mindestens eine Wurzel. Die bei (4) *auftretende Größe* B *bedeutet jene der zwei positiven Zahlen* 1 *und* $\left|\frac{b_0}{b_1}\right|$, *die nicht kleiner als die andere ist* (Fejér, *Math. Ann.* **65**, 413 (1908)). Die Kreisradien hängen außer von den Anfangsgliedern b_0 und b_1 noch von der Gliederanzahl der Gleichung oder den Exponenten ab; b_0 und b_1 *allein* bestimmen keinen endlichen Kreis, der mindestens eine Gleichungswurzel enthält.

Hingegen gilt folgendes Theorem (Landau, *Sitzungsb. d. Berl. Akad.* (1904), 1118, *Viertelsjahrhefte der naturf. Ges. zu Zürich* **51**, 252 (1906)): *Für jede ganze rationale (sogar ganze transzendente) Funktion* $f(z)=c_0+c_1z+c_2z^2+\cdots$, *bei der der Koeffizient* c_1 *von Null verschieden ist, existiert eine nur von den zwei Größen* c_0 *und* c_1 *abhängige positive Zahl* R, *so daß in einem mit dem Radius* R *um den Koordinatenursprung geschlagenen Kreise mindestens eine der beiden Gleichungen* $f(z)=0$ *oder* $f(z)=1$ *eine Wurzel besitzt.*

Ist $f'(z)$ *die erste Abgeleitete irgendeiner ganzen rationalen Funktion* $f(z)$, *so stellt sich in der Gaußschen Ebene der komplexen Zahlen keine der Wurzeln der Gleichung* $f'(z)=0$ *außerhalb jenes kleinsten konvexen geradlinigen Polygons dar, das sich um die Wurzeln von* $f(z)=0$ *spannen läßt* (vgl. die Literaturangaben von Fejér, *Math. Ann.* **65**, 417 (1908), ferner Cesàro, *Nouv. Ann. de math.* (3) **4**, 329 (1885), Cesàro-Kowalewski, *Elementares Lehrbuch der algebraischen Analysis* usw., S. 434).

Stellt man die Wurzeln irgendeiner Gleichung

$$f(z)=a_0z^n+a_1z^{n-1}+a_2z^{n-2}+\cdots+a_n=0$$

mit beliebigen reellen oder komplexen Koeffizienten in der sog. Gaußschen Ebene der komplexen Zahlen dar, so liegt keine von *ihnen außerhalb des mit dem Radius G um den Koordinatenursprung geschlagenen Kreises, wo G die einzige positive Wurzel der Gleichung:*

$$|a_0|u^n - \{|a_1|u^{n-1} + |a_2|u^{n-2} + |a_3|u^{n-3} + \cdots + |a_n|\} = 0$$

ist, d. h. G ist eine obere Grenze für den absoluten Betrag der Gleichungswurzeln (Cauchy, *Exercices de math.* (1829), *Œuvres* (2) **9**, 122). Diese Grenze ist schärfer als die von Gauß beim vierten Beweise des Fundamentalsatzes im Jahre 1849 (*Ges. Werke* **3**, 76, vgl. oben S. 251) verwendete. Aus den unten angegebenen Kriterien für die obere Grenze der positiven Wurzeln einer Gleichung mit reellen Koeffizienten folgt: Ist A die größte Zahl unter den absoluten Beträgen von $|a_1|, |a_2|, \ldots, |a_n|$, so ist die angegebene Größe G nicht größer als $1 + \frac{A}{|a_0|}$. Ist k die Anzahl der von Null verschiedenen Größen $a_1, a_2, \ldots, a_n$, so ist G nicht größer als die größte unter den Zahlen

$$\frac{k|a_1|}{|a_0|}, \quad \sqrt{\frac{k|a_2|}{|a_0|}}, \quad \sqrt[3]{\frac{k|a_3|}{|a_0|}}, \ldots, \sqrt[n]{\frac{k|a_n|}{|a_0|}}.$$

Setzt man $z = \frac{1}{t}$, so erhält man für t die Gleichung $a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n = 0$; ist G' eine obere Grenze für die absoluten Beträge $|t|$ der Wurzeln der transformierten Gleichung $t^n f\left(\frac{1}{t}\right) = 0$, so ist $K = \frac{1}{G'}$ eine untere Grenze für die absoluten Beträge der Wurzeln von $f(z) = 0$, d. h. $|z| \geqq K$.

Eine Zahl G heißt eine *obere Grenze für die positiven Gleichungswurzeln, wenn alle positiven Wurzeln nicht größer als G sind;* eine solche wird durch folgende Sätze geliefert:

Ist $f(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n = 0$ *eine Gleichung mit reellen Koeffizienten und* $a_0 > 0$, *so ist jede Zahl G, für die* $f(z)$ *und sämtliche sukzessive Abgeleitete* $f'(z), f''(z), \ldots, f^{(n-1)}(z)$ *positiv werden, eine obere Grenze für die positiven Gleichungswurzeln von* $f(z) = 0$ (Newton, *Arithmetica universalis,* Bd. 2, Kap. 4, Folge des Fourierschen Satzes auf S. 344). *Ist ebenfalls* $a_0 > 0$, *so ist auch jede Zahl G, für die alle Funktionen*

$$f_i(z) = a_0 z^{n-i} + a_1 z^{n-i-1} + \cdots a_{n-i} \quad (i = n-1, n-2, \ldots, 0)$$

positiv ausfallen, eine obere Grenze für die positiven Wurzeln (Laguerre, *Nouv. Ann. de math,* (2) **19**, 49 (1880), *Œuvres* **1**, 72, Folge des Laguerreschen Satzes auf S. 345).

Ist in der Gleichung $a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$ *mit reellen Koeffizienten* a_j *der erste der negativen Koeffizienten, also* $a_0, a_1, \ldots, a_{j-1}$ *positiv, und ist* N *der absolute Betrag des dem absoluten Betrage nach größten negativen Koeffizienten, so ist jede der Größen*

$$1 + \sqrt[j-f]{\frac{N}{a_0 + a_1 + \cdots a_f}},$$

wobei f *jeden der Werte* $0, 1, 2, \ldots, j-1$ *annehmen kann, eine obere Grenze für die positiven Gleichungswurzeln. Im besonderen sind also*

$$1 + \sqrt[j]{\frac{N}{a_0}}, \quad 1 + \frac{N}{a_0 + a_1 + \cdots a_{j-1}}$$

(und a fortiori $1 + \frac{N}{a_0}$, *die sog. Maclaurinsche Grenze, die aber schon Rolle, Traité d'algèbre (1690), 2*[tes] *Buch, Kap. 6 hat) obere Grenzen für die positiven Gleichungswurzeln.* Vgl. auch Lagrange, *Rés. des équ. num.* (oben S. 256), *Œuvres* **8**, 32, Longchamps, *Nouv. Ann. de math.* (2) **19**, 71 (1880).

Ist $a_0 > 0$ *und hat die Gleichung*

$$a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

mit reellen Koeffizienten im ganzen k *negative Koeffizienten, die* $a_j, a_m, a_p, a_s, \ldots$ *lauten mögen, so ist die größte der* k *Größen*

$$\sqrt[j]{k\frac{|a_j|}{a_0}}, \quad \sqrt[m]{k\frac{|a_m|}{a_0}}, \quad \sqrt[p]{k\frac{|a_p|}{a_0}}, \quad \sqrt[s]{k\frac{|a_s|}{a_0}}, \cdots$$

eine obere Grenze für die positiven Gleichungswurzeln (Cauchy, *Œuvres* (2) **9**, 152, Abel Transon, *Nouv. Ann. de math.* (2) **11**, 256 (1872)).

Ist G' eine obere Grenze für die positiven Wurzeln von $f(-z) = 0$, so ist $-G'$ eine untere Grenze für die negativen Wurzeln von $f(z) = 0$, d. h. keine der Wurzeln ist kleiner als $-G'$. Sind L und $-L'$ obere bezw. untere Grenzen für die positiven bezw. negativen Wurzeln von $z^n f\left(\frac{1}{z}\right) = 0$, so liegt keine Wurzel von $f(z) = 0$ zwischen $\frac{1}{L}$ und $-\frac{1}{L'}$.

Mittels des Sturmschen oder Fourierschen Satzes kann man zuerst die reellen Wurzeln einer Gleichung mit reellen Koeffizienten *separieren*, d. h. ein Intervall finden, in dem nur eine Wurzel der Gleichung liegt. Die zunächst folgenden Methoden setzen eine auf irgendwelche Weise vorgenommene Separation der Wurzeln voraus.

Regula falsi (Regel des doppelten falschen Ansatzes, Historisches bei Cantor, Vorl. über Geschichte der Math. unter dem Stichwort *Falscher Ansatz* des Registers, vgl. auch Rudolf Wolf, *Handbuch der Astronomie* **1**, 87, Zürich 1890): *Sind A und B zwei reelle Zahlen, $f(z)$ irgendeine Funktion mit reellen Koeffizienten und sign $f(A) = -$ sign $f(B)$, so liegt*

$$B_1 = \frac{Bf(A) - Af(B)}{f(A) - f(B)} = A - \frac{(A-B)f(A)}{f(A)-f(B)} = B - \frac{(A-B)f(B)}{f(A)-f(B)}$$

stets zwischen A und B. Eine Gleichung $f(z) = 0$, die zwischen A und B eine einzige Wurzel α hat, besitzt diese daher in einem der zwei kleineren Intervalle A bis B_1 oder B_1 bis B; die Wurzel α liegt zwischen $B_1 - L$ und $B_1 + L$, wobei

$$L = \frac{|A-B|^3}{8} \cdot \frac{M}{|f(A) - f(B)|}$$

ist und M den größten Wert bedeutet, den der absolute Betrag $|f''(z)|$ der zweiten Abgeleiteten im Intervall A bis B annehmen kann (vgl. Lüroth, *Vorl. über numerisches Rechnen*, Leipzig 1900, S. 175 u. 193).

Zwischen den zwei reellen Zahlen A und B habe die Gleichung $f(z) = 0$ mit reellen Koeffizienten nur eine reelle Wurzel α, mithin ist also sign $f(A) = -$ sign $f(B)$. Das Intervall A bis B sei so klein gewählt, daß die zweite Abgeleitete $f''(z)$ in dem ganzen Intervall A bis B keine Wurzel besitzt. Dies ist möglich, nachdem $f(z)$ und $f''(z)$ vorher von etwaigen gemeinsamen Teilern befreit wurden. $f''(z)$ hat dann im ganzen Intervall A bis B dasselbe Vorzeichen. Mit A sei, unabhängig davon, ob sie die größere oder kleinere Zahl ist, diejenige der zwei Grenzen bezeichnet, für die $f(z)$ und $f''(z)$ *dasselbe Vorzeichen* haben. Auf die Grenze A kann man dann die *Newtonsche Näherungsmethode in der von Fourier verbesserten Form* anwenden (Newton (1669) vgl. oben S. 256, zuerst publiziert in Wallis' *Algebra* (1685), Lagrange, *Rés. des équ. num.*, *Œuvres* **8**, 159, Fourier, *Anal. des équ. dét.*, vgl. oben S. 256, Darboux, *Nouv. Ann. de math.* (2) **8**, 17 (1869), Fouret, ebenda (2) **9**, 567 (1890)): *Bildet man sukzessiv*

$$A_1 = A - \frac{f(A)}{f'(A)}, \quad A_2 = A_1 - \frac{f(A_1)}{f'(A_1)}, \ldots$$

$$A_{n+1} = A_n - \frac{f(A_n)}{f'(A_n)}, \ldots,$$

so wird die erste Abgeleitete $f'(z)$ im ganzen Intervall A bis α nicht Null; A_1 liegt stets zwischen A und α, A_2 zwischen A_1 und α usw. und, die Größen $A, A_1, A_2, \ldots$ konvergieren nach α. Es ist α stets zwischen $A_{n+1} - L_1$ und $A_{n+1} + L_1$ gelegen; dabei ist

$$L_1 = \frac{|A_n - B|^2}{2} \frac{M_1}{|f'(A_n)|},$$

und M_1 bedeutet den größten Wert des absoluten Betrages von $f''(z)$ im Intervall A_n bis B.

Die *Kombination der Regula falsi mit der Newtonschen Näherungsmethode* (Fourier, *Anal. des équ. dét.*) ergibt unter den gleichen Bedingungen und bei Verwendung der gleichen Bezeichnungen wie beim Newtonschen Näherungsverfahren folgendes Theorem:

Bildet man sukzessiv

$$B_1 = \frac{Bf(A) - Af(B)}{f(A) - f(B)}, \quad B_{n+1} = \frac{B_n f(A_n) - A_n f(B_n)}{f(A_n) - f(B_n)} \quad (n = 1, 2, \ldots),$$

so liegt B_1 stets zwischen α und B, B_2 zwischen B_1 und α usw., und die Größen $B, B_1, B_2, \ldots$ konvergieren nach α. Die Wurzel α liegt stets zwischen A_n und B_n.

Bildet man ferner sukzessiv (Fourier a. a. O.)

$$C_1 = B - \frac{f(B)}{f'(A)}, \quad C_2 = C_1 - \frac{f(C_1)}{f'(A_1)}, \cdots C_{n+1} = C_n - \frac{f(C_n)}{f'(A_n)},$$

so liegt C_1 stets zwischen B und α, C_2 zwischen C_1 und α, C_3 zwischen C_2 und α usw., und die Zahlen $C_1, C_2, \ldots$ konvergieren nach α. Die Wurzel α liegt stets zwischen A_n und C_n.

Die Newtonsche Näherungsmethode ist nur ein Spezialfall des von Legendre-Cauchy (Cauchy, *Analyse algébrique* (1821), *Œuvres* (2) **3**, 381) stammenden Verfahrens *sukzessiver Approximation*. Aus einem geeigneten Anfangswert A ist mittels einer stetigen Funktion $\varphi(z)$ sukzessiv eine Wertreihe $A_1 = \varphi(A)$, $A_2 = \varphi(A_1), \ldots, A_{n+1} = \varphi(A_n), \ldots$ herzuleiten, so daß die Größen $A_1, A_2, \ldots$ nach einem Wert α konvergieren, der Wurzel einer vorgegebenen Gleichung $f(z) = 0$ ist. Hierzu muß $\alpha = \varphi(\alpha)$ sein. Vgl. Schroeder, *Math. Ann.* **2**, 317 (1870), Isenkrahe, ebenda **31**, 309 (1888), Netto, *Algebra* **1**, 300, Lüroth, *Vorl. über numerisches Rechnen*, S. 179, Pellet, *C. R.* **133**, 917 u. 1186 (1901), Perrin, ebenda, 1189.

Lagranges Kettenbruchmethode: Hat man eine Gleichung $f(z) = 0$ mit reellen Koeffizienten und weiß man, daß sie

λ positive Wurzeln zwischen den zwei positiven ganzen Zahlen g und $g + 1$ besitzt, so setze man $z = g + \frac{1}{z_1}\cdot$ Die sich dann aus $f(z) = 0$ für z_1 ergebende Gleichung $f_1(z_1) = 0$ hat soviel positive reelle Wurzeln, die größer als 1 sind, wie $f(z) = 0$ reelle Wurzeln zwischen den Grenzen g und $g + 1$ hat. Ist g_1 eine derartig gewählte ganze positive Zahl, daß $f_1(z_1) = 0$ zwischen den Grenzen g_1 und $g_1 + 1$ wenigstens eine Wurzel hat, so setze man $z_1 = g_1 + \frac{1}{z_2}$ und operiere mit der sich aus $f_1(z_1) = 0$ ergebenden Gleichung $f_2(z_2) = 0$ weiter. Auf diese Weise werden die zwischen g und $g + 1$ liegenden positiven Wurzeln von $f(z) = 0$ in Kettenbrüche

$$z = g + \cfrac{1}{g_1 + \cfrac{1}{g_2 \ddots}}$$

entwickelt. Lagrange, *Rés. des équ. num.*, *Œuvres* **8**, 41, M. A. Stern, *Journ. f. Math.* **11**, 142, 277 (1834), Sturm in der S. 256 zitierten Arbeit, Art. 16.

Lagrange-Bernoullisches Verfahren: Ist s_ν ($\nu = 1, 2 \ldots$) die Summe der ν^{ten} Potenzen der Gleichungswurzeln, so nähert sich $\frac{s_{\nu+1}}{s_\nu}$ für wachsendes ν der ihrem absoluten Betrage nach größten Gleichungswurzel, falls eine solche existiert (Lagrange, *Rés. des équ. num.*, *Œuvres* **8**, 170). Am einfachsten findet man die s_ν, indem man $\frac{f'(z)}{f(z)}$ nach fallenden Potenzen von z entwickelt, also $\frac{f'(z)}{f(z)} = \frac{n}{z} + \frac{s_1}{z^2} + \frac{s_2}{z^3} + \cdots$ bildet (vgl. S. 267). Dieses Verfahren ordnet sich als Spezialfall in die von Daniel Bernoulli (*Comm. Acad. Petrop.* **3**, 92 (1728)) stammende und dann von Euler (*Introductio in analysin infinitorum* (1748), Bd. 1, Kap. 17) aufgenommene Methode der Berechnung der Gleichungswurzeln mittels *rekurrenter Reihen* und läßt sich so ausgestalten (Fourier, *Anal. des équ. dét.*, *Ostwalds Klass.* Nr. 127, S. 63, Stern, *Journ. f. Math.* **11**, 293 (1834), Jacobi, ebenda **13**, 349 (1835), *Ges. Werke* **3**, 280, F. Cohn, *Math. Ann.* **44**, 473 (1894)), daß es zur Herleitung *sämtlicher* Wurzeln einer beliebigen Gleichung mit reellen oder imaginären Koeffizienten dienen kann.

Gräffesche Methode: Ist eine Gleichung $f(z) = 0$ mit den

Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ gegeben und schreibt man $f(z) = g_1(z^2) + z g_2(z^2)$, faßt man also die Glieder mit geraden und ungeraden Potenzen zusammen, so hat die Gleichung

$$f_1(y) = g_1(y)^2 - y^2 g_2(y)^2 = 0$$

die Wurzeln $\alpha_1^{\,2}, \alpha_2^{\,2}, \ldots, \alpha_n^{\,2}$. Durch sukzessives Fortsetzen dieses Verfahrens findet man eine Gleichung:

$$f_\nu(u) = d_0 u^n + d_1 u^{n-1} + d_2 u^{n-2} + \cdots + d_n = 0$$

mit den Wurzeln $\alpha_1^{\,\tau}, \alpha_2^{\,\tau}, \ldots, \alpha_n^{\,\tau}$, wobei $\tau = 2^\nu$ ist. Befriedigen die absoluten Beträge der Wurzeln der vorgelegten Gleichung die Ungleichheiten $|\alpha_1| > |\alpha_2| \ldots > |\alpha_n|$, so ist für genügend große ν angenähert

$$\alpha_1^{\,\tau} = -\frac{d_1}{d_0}, \quad \alpha_2^{\,\tau} = -\frac{d_2}{d_1}, \quad \alpha_3^{\,\tau} = -\frac{d_3}{d_2}, \cdots, \alpha_n^{\,\tau} = -\frac{d_n}{d_{n-1}},$$

und man findet $\alpha_1, \alpha_2, \ldots, \alpha_n$ durch Ziehen τ^{ter} Wurzeln.

Ist

$$|\alpha_1| = |\alpha_2| \cdots = |\alpha_j|$$

aber größer als

$$|\alpha_{j+1}|, |\alpha_{j+2}|, \ldots, |\alpha_n|,$$

so befriedigen die Größen $\alpha_1^{\,\tau}, \alpha_2^{\,\tau}, \ldots, \alpha_j^{\,\tau}$ für genügend große τ angenähert die Gleichung $d_0 u^j + d_1 u^{j-1} \cdots + d_j = 0$ und die Größen $\alpha_{j+1}^{\,\tau}, \alpha_{j+2}^{\,\tau}, \ldots, \alpha_n^{\,\tau}$ die Gleichung

$$d_j u^{n-j} + d_{j+1} u^{n-j-1} + d_{j+2} u^{n-j-2} + \cdots + d_n = 0.$$

Man kann die Methode so ausgestalten, daß sie *alle* Gleichungswurzeln liefert. Gräffe, *Die Auflösung der höheren numerischen Gleichungen*, Zürich 1837. Encke, *Journ. f. Math.* **22**, 193 (1841), Carvallo, *Ann. de la faculté de Toulouse* **3** (1889) (*Thèse de Paris*).

Wir schließen mit der Aufsuchung der *rationalen Wurzeln einer Gleichung mit rationalen Koeffizienten:*

Die rationalen Wurzeln einer Gleichung mit ganzzahligen Koeffizienten, bei der der Koeffizient der höchsten Potenz gleich 1 *ist, müssen ganzzahlig sein.*

Die rationalen Wurzeln einer Gleichung

$$a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n = 0$$

mit ganzzahligen Koeffizienten findet man, indem man $a_0 z = y$ *setzt und die ganzzahligen Wurzeln von*

$$y^n + a_1 y^{n-1} + a_2 a_0 y^{n-2} + a_3 a_0^2 y^{n-3} + \cdots + a_n a_0^{n-1} = 0$$

sucht (Rolle, *Traité d'algèbre* (1690), 2tes Buch, Kap. 5).

Man findet die etwa vorhandenen ganzzahligen Wurzeln der Gleichung

$$z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

mit ganzzahligen Koeffizienten, indem man alle ganzzahligen positiven und negativen Teiler von a_n *sucht, die innerhalb der Wurzelgrenzen liegen. Ist* α *ein solcher Wert, so ist* α *dann und nur dann Gleichungswurzel, wenn sämtliche Größen*

$$\frac{a_n}{\alpha} = b_1, \quad \frac{b_1 + a_{n-1}}{\alpha} = b_2, \quad \frac{b_2 + a_{n-2}}{\alpha} = b_3, \ldots,$$

$$\frac{b_{n-2} + a_2}{\alpha} = b_{n-1}$$

ganzzahlig ausfallen und schließlich $\frac{b_{n-1} + a_1}{\alpha} = \mp 1$ *wird.*