Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 6 (1934)

Artikel: Die Probleme der modernen Galoisschen Theorie.
Autor: Tschebotaröw, Nikolaj
DOI: https://doi.org/10.5169/seals-7592

Die Probleme der modernen Galoisschen Theorie[1)]

Von NIKOLAJ TSCHEBOTARÖW, Kasan

Das soeben verflossene 100-jährige Jubiläumsdatum des Todes von ÉVARISTE GALOIS gibt mir den Anlaß, den heutigen Stand seiner wichtigsten Schöpfung darzulegen, die unter dem Namen „Galoissche Theorie" bekannt ist. Zugleich erlaube ich mir, zu versuchen, einige Voraussagungen über die Galoissche Theorie des Zukünftigen zu machen. Der ursprüngliche Zielpunkt der Galoisschen Theorie, die Frage nach der Darstellung der Wurzeln von algebraischen Gleichungen durch Radikalausdrücke, wurde von Galois selbst und von seinen früheren Nachfolgern beinahe erledigt. Das Haupthilfsmittel aber, welches von Galois in seinen Untersuchungen benutzt wurde, die Beschreibung von algebraischen Zahlkörpern durch die ihnen entsprechenden Gruppen, erwies seine Macht auch für ziemlich entfernte Zweige der mathematischen Analysis. Auf diese Weise entstanden in der Mathematik neue Gebiete wie „Riemannsche Flächen", „automorphe Funktionen", „kontinuierliche Transformationsgruppen", u. s. w.

Außerdem sind in der klassischen Galoisschen Theorie selbst neue Aufgaben entstanden, welche einer wesentlichen Vertiefung des Galoisschen Grundgedankens bedürfen. Das Problem der Auffindung von Gleichungen mit vorgeschriebener Gruppe hat verlangt, die Theorie der allgemeinen rationalen Funktionenkörper zu studieren (das Problem von LÜROTH-STEINITZ). Eine Erweiterung des Problems der Radikallösung, das sogenannte Kleinsche Formenproblem, hat anderseits die Theorie der endlichen Gruppen mit der Theorie der kontinuierlichen Gruppen verknüpft. Die „lineare Gruppentheorie" ist eine wahre Brücke, welche diese beiden Zweige der Gruppentheorie verbindet.

Im vorliegenden Bericht will ich den gegenwärtigen Apparat durchgehen, welcher zur Beherrschung der Probleme der Galoisschen Theorie nützlich sein kann. Dabei fasse ich den Begriff der „Galoisschen Theorie" etwas weiter auf, als das bei Anwendung der Gruppentheorie auf algebraische Gleichungen üblich ist, indem ich in ihn alle Fragen einschließe, die den Begriff „das Rationale" dem Begriff „das algebraische Irrationale" gegenüberstellen. Dazu gehören einige recht schöne Resultate und Pro-

[1)] Der Auszug dieses Berichtes wurde am Internationalen Mathematiker-Kongreß in Zürich, 1932, als Vortrag gehalten.

bleme der algebraischen Funktionenkörper von mehreren Veränderlichen, die bis jetzt nur durch die Methoden der algebraischen Geometrie lösbar sind. Es ist das große Verdienst der alten deutschen und der italienischen Geometer, daß sie manche dieser Probleme mit Hilfe der algebraischen Geometrie gelöst haben, während wir Algebraiker dafür noch keine Methode besitzen.

Ich lege bei der Wahl des Materials hauptsächlich meinen eigenen Geschmack zugrunde, so daß ich für die Objektivität dieser Wahl keinen Anspruch erhebe.

Inhalt.

§ 1. Grundlagen der Galoisschen Theorie.
§ 2. Gleichungen mit vorgeschriebener Gruppe.
§ 3. Ueber die analytische Form der zu einer vorgeschriebenen Permutationsklasse gehörenden Primzahlen.
§ 4. Resolventenproblem.
§ 5. Weitere Fragen der allgemeinen Körpertheorie.

§ 1. Grundlagen der Galoisschen Theorie

1. Man kann die Arbeiten, die sich mit den Grundlagen der Galoisschen Theorie beschäftigen, in zwei Arten einteilen. Zur ersten Art gehören die Arbeiten, welche neue Wege zur Begründug der klassischen Galoisschen Theorie suchen, während die Arbeiten der zweiten Art den Begriff der Galoisschen Gruppen vertiefen und seine Anwendung auf viel weitere Gebiete möglich machen, als das die klassische Theorie zu tun imstande ist

2. Unter den Arbeiten der ersten Art sind die von F. Mertens (50), S. Schatunowski (62) und A. Loewy (46, 47) besonders zu erwähnen. Mertens erklärt den Begriff der Galoisschen Gruppe und beweist die dazu gehörigen Fundamentalsätze, ohne die Begriffe des Normalkörpers, der Galoisschen Resolvente usw. zu benutzen. Er geht vom Begriffe der Irreduzibilität in erweiterten Bereichen aus. Ist die gegebene Gleichung $f(x) = 0$ irreduzibel, und ist x_1 eine ihrer Wurzeln, so findet er einen Faktor $f_1(x; x_1)$ des Polynoms $\frac{f(x)}{x - x_1}$, welcher im Bereiche $K[x_1]$ irreduzibel ist. Dann findet er einen im Bereiche $K[x_1, x_2]$ irreduziblen Faktor des Polynoms $\frac{f_1(x; x_1)}{x - x_2}$, wobei x_2 eine Wurzel von $f_1(x; x_1)$ ist. Fährt er so fort, so kommt er zum System

$$(1.1) \qquad Z_0 = f(x),\ Z_1 = f_1(x; x_1),\ Z_2 = f_2(x; x_1, x_2),\ \ldots,\ Z_{n-1} = f_{n-1}(x; x_1, \ldots, x_{n-1})$$

von Polynomen, die ein System von Fundamentalmoduln bilden. Jede ganze rationale Funktion $\varphi(x_1, x_2, \ldots, x_n)$ ist dann und nur dann gleich Null, wenn sie (bei den veränderlichen x_i) in der Gestalt

$$(1.2) \qquad P_0 \cdot Z_0(x_1) + P_1 \cdot Z_1(x_2) + \ldots + P_{n-1} \cdot Z_{n-1}(x_n)$$

darstellbar ist, wobei die P_i Polynome sind. Die Galoissche Gruppe besteht aus den Permutationen, die jedes Polynom $Z_i(x_{i+1})$ in ein Polynom der Gestalt (1.2) überführen. Die Ordnung dieser Galoisschen Gruppe ist gleich dem Produkt der Grade der Polynome (1.1).

3. Schatunowski stellt eine Theorie auf, die sich formal mit der Mertensschen deckt, geht aber dabei von einem viel allgemeineren Standpunkt aus. Seine Arbeit steht auf dem Grunde der Kroneckerschen Idee der funktionalen Moduln, die darin besteht, daß man jede von einer Wurzel x_1 der Gleichung

$$(1.3) \qquad f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$$

abhängige Größe als eine Funktion einer unbestimmten Veränderlichen auffaßt und und als Gleichheitszeichen das Kongruenzzeichen modulo $f(x)$ zugrunde legt. Da man in der Galoisschen Theorie auch Funktionen von mehreren Wurzeln der Gleichung (1.3) betrachtet, so sucht Schatunowski, ein System von funktionalen Moduln der Veränderlichen $x_1, x_2, \ldots, x_n$ derart aufzustellen, daß das Restsystem nach diesen Moduln dem durch die Wurzeln der Gleichung (1.3) erzeugten algebraischen Zahlkörper isomorph ist. Das Modulsystem

$$(1.4) \quad \psi_1 = x_1 + x_2 + \ldots + x_n + a_1, \quad \psi_2 = x_1 x_2 + \ldots + x_{n-1} x_n - a_2, \ldots,$$
$$\psi_n = x_1 x_2 \ldots x_n - (-1)^n a_n$$

ist dazu nicht geeignet, da etwa die $f(x_i)$ nach diesem System nicht $\equiv 0$ sind. Das System

$$(1.5) \qquad f(x_1), f(x_2), \ldots, f(x_n)$$

kann auch nicht zu diesem Zwecke dienen, da etwa nicht

$$\psi_i \equiv 0 \pmod{f(x_1), f(x_2), \ldots, f(x_n)},$$

wohl aber $\psi_i V \equiv 0 \pmod{f(x_1), f(x_2), \ldots, f(x_n)}$ gilt, wobei V die Vandermondesche Determinante der Größen $x_1, x_2, \ldots, x_n$ bedeutet. Die Systeme (1.4) und (1.5) sind nach moderner Ausdruckweise keine Primideale.

Schatunowski stellt ein verlangtes Modulsystem auf, indem er die von ihm genannten Cauchyschen Moduln zugrunde legt. Man erhält diese Moduln folgendermaßen: als den ersten Modul nehme man $f(x_1)$; als den zweiten Modul den Quotienten der Division von $f(x_1)$ durch $x_1 - x_2$; als den dritten Modul den Quotienten der Division des nach Potenzen von x_2 geordneten zweiten Moduls durch $x_2 - x_3$, usw. Das Cauchysche Modulsystem gibt ein mit dem entsprechenden Zahlkörper isomorphes Restklassensystem dann und nur dann, wenn die Gleichung (1.3) affektlos ist. Dann ist jeder dieser Moduln irreduzibel nach dem System der ihm vorangehenden Moduln. Ist das nicht der Fall, so kommt Schatunowski zum allgemeinen Mertensschen Modulsystem. Die Grade dieser Moduln geben Aufschluß über die Transitivitäts- und Primitivitätsverhältnisse der Gleichung (1.3). Fallen z. B. die k ersten Moduln mit den Cauchyschen Moduln überein, so ist die Gruppe k-fach transitiv.

Die Arbeit von Schatunowski enthält die einleitenden Grundlagen der Theorie, die man heute *Theorie der Polynomideale* nennt. Sie beschäftigt sich mit den Bereichen, deren Moduln reduzibel sind. Kann man dabei eine neue (endliche) Anzahl Moduln adjungieren, so daß der Bereich sich in einen Körper verwandelt, so wird der ursprüngliche Bereich „*Halbkörper*" genannt.

Von Wichtigkeit ist der von Schatunowski eingeführte Begriff der *Erweiterungen zweiter Art.* Er nennt so die Bereiche, die aus den ursprünglichen Bereichen entstehen, wenn man zu ihren Modulsystemen neue Moduln adjungiert, mit anderen Worten, gewisse nicht verschwindende Größen des ursprünglichen Bereiches gleich Null setzt. Es wäre natürlicher, diese Erweiterungen *Faktorbereiche* zu nennen, in Uebereinstimmung mit dem Begriff *Faktorgruppe.* Es gilt der Satz, daß ein Körper keine Erweiterungen zweiter Art zuläßt. Es ist dabei angenommen, daß alle Körper nur die Charakteristik Null haben können. Gehen wir aber zu einer Primzahlcharakteristik p über, so läuft dies auf die Hinzufügung des neuen Moduls p hinaus, und ein Körper bleibt Körper.

Indem man von der Mertens-Schatunowskischen Definition der Galoisschen Gruppe ausgeht, kann man leicht den folgenden zuerst von I. Schur (70; vgl. auch 79) bewiesenen Satz beweisen:

Die Gruppe eines Faktorkörpers ist ein Teiler der Gruppe eines ursprünglichen Körpers.

4. Die Loewysche Begründung der Galoisschen Theorie hat einige Berührungspunkte mit der Mertens-Schatunowskischen Theorie, vor allem dadurch, daß sie die Zugrundelegung von normalen Körpern vermeidet.

Loewy geht nicht von einer, sondern von mehreren algebraischen Größen aus, die einen Körper P erzeugen mögen und *Dirigenten* genannt werden. Die erste Dirigente ϱ_1 ist Wurzel einer Gleichung mit den Koeffizienten aus dem Rationalitätsbereich; die zweite Dirigente ist Wurzel einer Gleichung vom Typ $f(\varrho_1; z) = 0$; die dritte vom Typ $f(\varrho_1, \varrho_2; z) = 0$, usw. Sind alle diese Gleichungen irreduzibel, so nennt Loewy *„Transmutation des Körpers P"* den Ersatz einer Dirigente ϱ_i durch eine konjugierte Wurzel in allen Gleichungen, wo ϱ_i vorkommt (was notwendig auch den Ersatz aller nachstehenden Dirigenten nach sich zieht), und beweist, daß jede Relation zwischen den Dirigenten nicht gestört wird, wenn man auf sie solche Transmutationen ausübt. Diese Transmutationen können wohl gewisse Körpergrößen aus dem Körper P hinausführen. Diejenigen Transmutationen, welche aus dem Körper P nicht hinausgehen, bilden eine Gruppe, welche Gruppe der *automorphen Transmutationen* genannt wird. Gruppentheoretisch bedeutet dies folgendes: Ein Körper P ist keineswegs, wenn er nicht normal ist, durch seine Gruppe bestimmt; er ist durch seine Galoissche Gruppe $\mathfrak{G}$ und ihre Untergruppe $\mathfrak{H}$ bestimmt, zu welcher eine primitive Größe von P gehört. Ist $\mathfrak{K}$ der Normalisator der Gruppe $\mathfrak{H}$ innerhalb $\mathfrak{G}$, so ist die automorphe Gruppe von P mit $\mathfrak{K}/\mathfrak{H}$ isomorph. Die Gesamtheit aller Transmutationen von P bildet aber keine Gruppe im gewöhnlichen Sinne. Loewy nennt solche Operationsmengen *Mischgruppen* und untersucht ihre Struktureigenschaften (47). Jede Mischgruppe $\mathfrak{T}$ enthält einen Kern $\mathfrak{G}$, d. h. die größte in $\mathfrak{T}$ enthaltene gewöhnliche Gruppe und besteht aus einigen Nebengruppen (Restklassen) nach $\mathfrak{G}$. Es ist wesentlich, daß eine Faktorgruppe von $\mathfrak{T}$ nach einer *beliebigen* (nicht notwendig normalen) Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ wieder eine Mischgruppe ist, deren Kern $\mathfrak{N}/\mathfrak{G}$ ist, wo $\mathfrak{N}$ den Normalisator von $\mathfrak{H}$ innerhalb $\mathfrak{G}$ bedeutet. Diese Tatsachen erlauben, eine Mischgruppe als ein mehr adäquates Bild eines Körpers zu betrachten.

Eine ähnliche Gruppenbildung hat H. Brandt (7) eingeführt, welche das *Brandtsche Gruppoid* genannt wird.

5. Ehe wir zu den Arbeiten der zweiten Art übergehen, müssen wir die moderne Auffassung des Begriffes „Galoissche Gruppe" darlegen, welche von der älteren Auffassung abweicht. Es ist für mich schwer, zu sagen, von wem die neuere Auffassung herrührt. Die ältere Galoissche Theorie betrachtete die Elemente der Galoisschen Gruppe, die *Substitutionen* (oder *Permutationen*), als Vertauschungen unter den Wurzeln einer erzeugenden Gleichung (die wohl auch reduzibel sein kann), welche sämtliche Relationen zwischen diesen Wurzeln nicht stören. Die moderne Galoissche Theorie betrachtet dagegen Uebergänge, welche

gleichzeitig alle Größen eines Körpers K erleiden, ohne die zwischen ihnen bestehenden Relationen zu stören. Mit anderen Worten, jedes Element der Galoisschen Gruppe ist eine Abbildung eines (normalen) Körpers K auf sich selbst, oder, wie man in der Gruppentheorie zu sagen braucht, ein Automorphismus, d. h. ein solcher Uebergang aller Größen des Körpers in andere Größen desselben Körpers, welcher die Summe und das Produkt in die Summe bzw. das Produkt überführt.

6. Für die Galoissche Theorie ist die gegenseitige Zuordnung der Unterkörper von K und der Untergruppen seiner Galoisschen Gruppe $\mathfrak{G}$ vor allem wesentlich. Man kann das genauer wie folgt formulieren (43; 74, Anhang; 3): Man ordne jedem Unterkörper U von K die größte Untergruppe $\mathfrak{H}(U)$ von $\mathfrak{G}$ zu, die die Größen von U nicht ändert. Andererseits ordne man jeder Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ den größten Unterkörper $U(\mathfrak{H})$ von K zu, deren Größen sich nicht gegenüber $\mathfrak{H}$ ändern. Ist $U_1 > U_2$, so ist $\mathfrak{H}(U_1) < \mathfrak{H}(U_2)$ und umgekehrt. Außerdem gilt:

$$U[\mathfrak{H}(U)] > U, \quad \mathfrak{H}[U(\mathfrak{H})] > \mathfrak{H}\,. \tag{1.6}$$

Man kann aber die Galoissche Theorie nur dann ohne weiteres entwickeln, wenn gilt:

$$U[\mathfrak{H}(U)] = U, \tag{1.7}$$

$$\mathfrak{H}[U(\mathfrak{H})] = \mathfrak{H}. \tag{1.8}$$

Damit (1.8) gelte, muß K über seinem Rationalitätsbereich endlich sein (Krull, 43).

Damit (1.7) gelte, muß K über seinem Rationalitätsbereich von der 1. Art sein (Baer-Hasse, 74, Anhang).

Besitzt K den Körper der rationalen Zahlen als Teiler (dann sagt man: K hat die Charakteristik Null), so ist K jedenfalls von der 1. Art. Hat K dagegen die Charakteristik p (d. h. gibt es eine Primzahl p, die innerhalb K gleich Null ist), so ist K dann und nur dann von der 1. Art, wenn eine den Körper K erzeugende Größe einer irreduziblen Gleichung mit lauter verschiedenen Wurzeln genügt.

K ist über seinem Rationalitätsbereich endlich, wenn es eine endliche Anzahl Basiszahlen gibt, so daß jede Größe von K linear durch diese Basiszahlen mit den Koeffizienten aus dem Rationalitätsbereich darstellbar ist.

7. Ist K unendlich, so hat Krull (43) den Hauptsatz der Galoisschen Theorie auch auf diesen Fall erweitert, indem er nicht alle Untergruppen von $\mathfrak{H}$, sondern nur die *abgeschlossenen* Untergruppen in Betracht zog.

Darunter versteht er folgendes. Ist γ ein Element von $\mathfrak{G}$ und $\varkappa$ ein endlicher normaler Unterkörper von K, so bewirkt γ eine Abbildung von $\varkappa$ auf sich selbst. Bewirken γ und γ^* eine gleiche Abbildung von $\varkappa$, so sagen wir, γ^* befinde sich in einer *$\varkappa$-Umgebung* von γ. Diese Definition der Umgebung erfüllt alle Hausdorffschen Umgebungsaxiome:

a) Jedes Element γ ist in jeder seiner Umgebungen enthalten.

b) Der Durchschnitt zweier Umgebungen von γ enthält eine neue Umgebung von γ. Er ist vielmehr selbst eine Umgebung von γ. Denn der Durchschnitt von den $\varkappa_1$- und $\varkappa_2$-Umgebungen ist die $\varkappa_3$-Umgebung, wobei $\varkappa_3$ als Vereinigungskörper von $\varkappa_1$ und $\varkappa_2$ endlich und normal ist.

c) Ist δ ein Element der $\varkappa$-Umgebung von γ, so gibt es eine Umgebung von δ, die ganz in der $\varkappa$-Umgebung von γ liegt. Vielmehr fallen die $\varkappa$-Umgebungen von γ und δ zusammen, da sie den Inbegriff der Elemente von $\mathfrak{G}$ enthalten, die unter den Elementen des Körpers $\varkappa$ eine und dieselbe Permutation bewirken.

Sind γ und δ verschiedene Elemente von $\mathfrak{G}$, so gibt es eine Umgebung von γ, die das Element δ nicht enthält. Denn sind γ und δ verschieden, so gibt es in K Größen, die sich gegenüber γ und δ verschieden verhalten. Da jede dieser Größen einen endlichen Körper erzeugt, so entsprechen diesen Körpern verschiedene Umgebungen von γ und δ.

Diese Definition erlaubt, *Häufungselemente* (H.-E.) zu definieren. Ist $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$, so soll ein Häufungselement (kurz H.-E.) von $\mathfrak{H}$ Elemente von $\mathfrak{H}$ in jeder seiner Umgebungen enthalten. Ein H.-E. von $\mathfrak{H}$ braucht wohl selbst in $\mathfrak{H}$ nicht enthalten zu sein. Enthält aber eine Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ alle ihre H.-E., so heißt sie *abgeschlossen.* Jede Gruppe, zu der ein Unterkörper von K gehört, ist abgeschlossen. Umgekehrt: zu jeder abgeschlossenen Gruppe $\mathfrak{H}$ muß ein Unterkörper U von K gehören, so daß $\mathfrak{H}[U(\mathfrak{H})] = \mathfrak{H}$ gilt. Um also die Fundamentalsätze der Galoisschen Theorie auf unendliche Körper erweitern zu können, muß man nur diejenigen Untergruppen von $\mathfrak{H}$ in Betracht nehmen, welche abgeschlossen sind.

8. Die Bedingungen für das Bestehen der Relation (1.7) wurden von R. Baer (3) ausführlich untersucht. Er fand, daß es jedenfalls einen Zwischenkörper S gibt, den er den *starren Körper* zwischen K und dem Rationalitätsbereich nennt. Der starre Körper ist dadurch charakterisiert, daß K *ordentlich* ist (d. h. stets (1.8) gilt), wenn man S als Rationalitätsbereich nimmt, während alle Größen von S gegenüber allen Automorphismen von K invariant bleiben. Ich kann hier nicht in die weiteren interessanten Ausführungen dieser Arbeit eingehen.

9. Es ist sehr schwer, die Galoissche Gruppe für die Fälle zu defi-

nieren, wo der zu untersuchende Körper K einen höheren Transzendenzgrad hat als sein Rationalitätsbereich. Der Grund dazu liegt darin, daß die *universelle Norm* eines solchen Körpers (d. h. der Körper, welcher alle mit den Unterkörpern von K konjugierten Körper enthält) ein unendlicher Körper ist, dessen Definition schwer analytisch aufzufassen ist. Um eine Gruppe, welche die Haupteigenschaften der Galoisschen Gruppe besitzen soll, mindestens theoretisch aufzustellen, kann man folgendes Schema skizzieren. Es seien $x_1, x_2, \ldots, x_n$ die erzeugenden Größen eines Körpers K, zwischen denen gewisse algebraische Relationen bestehen mögen, die wir mit (I) bezeichnen wollen. Man kann jeden Unterkörper U von K analog durch erzeugende Größen $\xi_1, \xi_2, \ldots, \xi_m$ bestimmen, wobei die ξ_i sich rational durch die x_i ausdrücken:

$$\xi_i = \xi_i(x_1, x_2, \ldots, x_n) \qquad (i = 1, 2, \ldots, m) .$$

Die Gleichungen

$$(\text{II}) \qquad \xi_i(x_1, x_2, \ldots, x_n) = \xi_i(y_1, y_2, \ldots, y_n) \qquad (i = 1, 2, \ldots, m)$$

bestimmen einen neuen Körper, dessen Erzeugenden $[x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n; y_1', y_2', \ldots, y_n'; \ldots]$ durch die Relationen (I) und (II) verbunden sind. Diesen Körper kann man *relative Norm* (in bezug auf U) von K nennen. Der Uebergang von $(x_1, x_2, \ldots, x_n)$ zu $(y_1, y_2, \ldots, y_n)$ wird als Transmutation von K oder Permutation seiner Relativnorm bezeichnet. Durchläuft U sämtliche Unterkörper von K, so erzeugen die entsprechenden Relativnormen die gesuchte universelle Norm. Das Kompositum sämtlicher soeben aufgestellter Permutationen ist eine Gruppe, die alle Haupteigenschaften der Galoisschen Gruppe besitzt.

10. Man kann die Galoissche Gruppe eines Körpers algebraischer Funktionen etwas anders aufstellen, indem man nicht die Funktionen des Körpers, sondern die Gesamtheit ihrer Wertesysteme ins Auge faßt, die die sogenannte *absolute Riemannsche Fläche* bilden (vgl. 86). Dann führt jede Transformation der Galoisschen Gruppe jeden Wert einer Funktion von K in einen andern Wert über, so daß zwischen den Werten verschiedener Funktionen dieselben Relationen bestehen bleiben. Da jede Funktion durch die Gesamtheit ihrer Werte vollständig bestimmt ist, so werden durch eine solche Transformation auch die Funktionen bestimmt, in welche die gegebenen Funktionen übergehen. Die verschiedenen *Monodromiegruppen*, die gewisse Rationalitätsbereiche in Ruhe lassen, sind in dieser Gruppe enthalten. Es kann sehr wohl eintreten, daß eine Transformation einige Funktionen von K aus K hinausführt. Das findet im Falle einer unabhängigen Veränderlichen seinen Ausdruck

darin, daß eine durch ihre Null- und Unendlichkeitsstellen bis auf eine multiplikative Konstante bestimmte Funktion

$$f \underline{\sim} \frac{\mathfrak{p}_1' \mathfrak{p}_2' \dots \mathfrak{p}_m'}{\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m}$$

in ein Produkt

$$\frac{\bar{\mathfrak{p}}_1' \bar{\mathfrak{p}}_2' \dots \bar{\mathfrak{p}}_m'}{\bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_2 \dots \bar{\mathfrak{p}}_m}$$

übergeht, worin der Zähler und der Nenner in verschiedenen Idealklassen liegen. Jede Transformation, welche Divisoren in äquivalente Divisoren überführt, gehört zu der sogenannten *Gruppe der Transformationen in sich* (38), die eine analoge Rolle spielt wie die von A. Loewy (47) eingeführte Gruppe der *automorphen Transformationen.*

11. Es ist in der Theorie der algebraischen Funktionen eine Gruppe von Wichtigkeit, die mit der soeben definierten Galoisschen Gruppe in engem Zusammenhange steht.

Es seien $u_1^{\mathfrak{p},\mathfrak{p}'}$, $u_2^{\mathfrak{p},\mathfrak{p}'}$, ..., $u_p^{\mathfrak{p},\mathfrak{p}'}$ die auf der Riemannschen Fläche von K definierten linear unabhängigen Abelschen Integrale 1. Gattung. Das Jacobische Umkehrungsproblem besteht in der Lösung des Gleichungssystems

$$(1.9) \qquad u_i^{\mathfrak{p}_1,\mathfrak{p}_1'} + u_i^{\mathfrak{p}_2,\mathfrak{p}_2'} + \dots + u_i^{\mathfrak{p}_p,\mathfrak{p}'_p} \equiv v_i \quad (i = 1, 2, \dots, p),$$

wobei die unteren Grenzen $\mathfrak{p}_i$ gegeben und die oberen Grenzen $\mathfrak{p}_i'$ gesucht sind und die Kongruenzen nach den Periodensystemen als Moduln genommen sind. Dieses Problem ist bei „allgemeiner Lage" der Punkte $\mathfrak{p}_i$ eindeutig lösbar (54; 4). Fassen wir die $\mathfrak{p}_i$, $\mathfrak{p}_i'$ als Koordinaten der Punkte P, P' eines p-dimensionalen Raumes auf, so bestimmt jedes Wertesystem der Parameter v_i eine Transformation, welche jeden Punkt P in einen bestimmten Punkt P' überführt (hier muß man die sich durch die Ordnung der Koordinatenwerte unterscheidenden Punkte als nicht verschieden betrachten, so daß man diese Punkte eindeutig mittels der Werte der symmetrischen Funktionen von $\mathfrak{p}_i$ bestimmen kann). Die Gruppe dieser Transformationen ist mit der p-gliedrigen Gruppe der parallelen Verschiebungen *im kleinen isomorph* (vgl. 67) und findet ihren analytischen Ausdruck in den Additionsformeln der Abelschen Funktionen. Sie ist Untergruppe einer erweiterten Galoisschen Gruppe, die die Koordinaten des Punktes P voneinander unabhängig transformiert. Im folgenden wollen wir diese Gruppe *Jacobische Gruppe* nennen.

§ 2. Gleichungen mit vorgeschriebener Gruppe

Das Problem der Auffindung von Gleichungen mit vorgeschriebener Gruppe gehört zu den wichtigsten Problemen der modernen Galoisschen Theorie und ist bis jetzt noch nicht gelöst. Es kann in den folgenden drei Arten aufgefaßt werden:

I. Man finde irgendwelche Gleichungen, deren Gruppe mit einer gegebenen Gruppe $\mathfrak{G}$ isomorph ist.

II. Man finde die allgemeinste parametrische Form der Koeffizienten einer Gleichung, deren Gruppe mit $\mathfrak{G}$ oder einem Teiler von $\mathfrak{G}$ isomorph ist. Die Darstellbarkeit der Koeffizienten in dieser Form soll notwendige und hinreichende Bedingung dafür sein, daß die Gruppe der Gleichung entweder mit $\mathfrak{G}$ oder mit einem Teiler von $\mathfrak{G}$ isomorph ist.

III. Man stelle ein Verfahren auf zur Bestimmung von Gleichungen, deren Gruppe mit $\mathfrak{G}$ isomorph ist. Dieses Verfahren soll alle Gleichungen dieser Art erschöpfen, falls es hinlänglich weit fortgesetzt wird.

2. Die Aufgabe II läßt stets eine Lösung zu, wenn für eine gegebene Gruppe $\mathfrak{G}$ der verallgemeinerte Lürothsche Satz (welcher auch Satz von der *rationalen Minimalbasis* heißt) gilt. Dieser Satz kann folgendermaßen formuliert werden:

Ist $K_n(x_1, x_2, \ldots, x_n)$ der Körper der rationalen Funktionen der Veränderlichen $x_1, x_2, \ldots, x_n$, so ist jeder Unterkörper von $K_n(x_1, x_2, \ldots, x_n)$ mit $K_m(x_1, x_2, \ldots, x_m)$ $(m \leqq n)$ isomorph. (Man kann auch sagen: dieser Körper ist *rein transzendent*).

Diesen Satz hat Lüroth (48) für den Fall $n = 1$ bewiesen. Castelnuovo (15) hat den Beweis für $n = 2$ gefunden. Für den Fall $n = 3$ haben G. Fano (21) und F. Enriques (20) ein Gegenbeispiel gefunden. Für die Lösung der Aufgabe II ist aber dieser Satz nicht in seinem vollen Umfange notwendig. Beschränken wir uns auf den Fall, daß der zu untersuchende Unterkörper den Körper der elementar-symmetrischen Funktionen von $x_1, x_2, \ldots, x_n$ enthält, so ist die Richtigkeit des Satzes mit der Lösbarkeit der Aufgabe II vollständig äquivalent. Nun ist aber die Frage nach der Richtigkeit dieses Satzes „in engerer Fassung" bis jetzt offen (vgl. 74, Bemerkung von B. L. Van der Waerden). Trifft auch dies nicht allgemein zu, so kann man für jede abstrakt gegebene endliche Gruppe $\mathfrak{G}$ entscheiden, ob sie „Lürothsch" ist oder nicht, d. h. ob der Körper $K(a_1, a_2, \ldots, a_n; \varphi)$ rein transzendent ist, wobei $\mathfrak{G}$ als Permutationsgruppe von $x_1, x_2, \ldots, x_n$ dargestellt ist, $a_1, a_2, \ldots, a_n$ die

elementar-symmetrischen Funktionen von $x_1, x_2, \ldots, x_n$ sind, und φ eine zu $\mathfrak{G}$ gehörende Funktion von $x_1, x_2, \ldots, x_n$ ist.

3. E. Noether (55) hat aus der Aufgabe II die Aufgabe I gefolgert, indem sie den Hilbertschen Irreduzibilitätssatz (35) heranzog, nach welchem man bei jedem irreduziblen Polynom für den einen Teil der Variablen solche Zahlenwerte wählen kann, daß sich ein irreduzibles Polynom der übrigen Variablen ergibt.

Man kann dieses Ergebnis etwas verschärfen, indem man nicht nur die Aufgabe I, sondern auch die Aufgabe III aus der Aufgabe II folgert. Dazu benutzt man das folgende von M. Bauer (5,6) angegebene Verfahren. Es ist bekannt, daß die Galoissche Gruppe $\mathfrak{G}$ einer algebraischen Gleichung

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \tag{2.1}$$

sich in eine ihrer Untergruppen verwandelt, wenn man die Größen des Rationalitätsbereiches nicht absolut, sondern modulo einer Primzahl (oder eines Primideals) dieses Rationalitätsbereichs betrachtet, wenn man also den Rationalitätsbereich durch seinen Faktorbereich ersetzt (16, 70, 79). Es ist andererseits bekannt, daß die Galoissche Gruppe einer Primzahlmodulkongruenz zyklisch ist, und daß dabei eine erzeugende Permutation der letzteren Gruppe aus den Zyklen von den Ordnungen besteht, die den Graden der irreduziblen Bestandteile unserer Kongruenz gleich sind. Daraus folgt: gilt

$$f(x) \equiv X_{n_1}^{(p)} X_{n_2}^{(p)} \ldots X_{n_k}^{(p)} \pmod{p}, \tag{2.2}$$

wobei $X_{n_i}^{(p)}$ ein modulo p irreduzibles Polynom vom Grade n_i bedeutet $(n_1 + n_2 + \ldots + n_k = n)$, so enthält die Gruppe von (2.1) eine Permutation mit den n_1-, n_2-, ..., n_k-gliedrigen Zyklen.

4. Wir nehmen an, der Körper $K(a_1, a_2, \ldots, a_n; \varphi)$ sei rein transzendent (vgl. die Bezeichnungen der N° 2). D. h. es gibt rationale Funktionen $\pi_1, \pi_2, \ldots, \pi_n$ von $a_1, a_2, \ldots, a_n; \varphi$ derart, daß umgekehrt $a_1, a_2, \ldots, a_n; \varphi$ sich durch die π_i ausdrücken lassen. Nun sei $\mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_s$ ein System der Untergruppen von $\mathfrak{G}$ derart, daß jede echte Untergruppe von $\mathfrak{G}$ ein Teiler wenigstens des einen von den $\mathfrak{G}_i$ ist. Ein solches System kann man sicher aufstellen, indem man als die $\mathfrak{G}_i$ z. B. alle echten Untergruppen von $\mathfrak{G}$ nimmt.

Es sei φ_i eine zu $\mathfrak{G}_i$ gehörende Funktion von $x_1, x_2, \ldots, x_n$ $(i = 1, 2, \ldots, s)$, und es sei $F_i(x_i)$ das Polynom des niedrigsten Grades, dessen Koeffi-

zienten rationale Funktionen von $\pi_1, \pi_2, \ldots, \pi_n$ sind und dessen Wurzel φ_i ist $(i = 1, 2, \ldots, s)$. Man erkennt, daß der Grad von $F_i(z_i)$ dem Index $(\mathfrak{G} : \mathfrak{G}_i)$ gleich ist $(i = 1, 2, \ldots, s)$.

Die Gruppe der Gleichung $F_i(z_i) = 0$ enthält als transitive Permutationsgruppe eine Permutation $\overline{S_i}$, welche alle Ziffern ändert. Dieser Permutation entspricht wenigstens eine Permutation von $\mathfrak{G}$. Es sei S_i eine solche Permutation, deren Zyklen von den Ordnungen $n_1, n_2, \ldots, n_k$ sein mögen. Man nehme eine beliebige Primzahl $p_i > n - 2$ und man setze

$$(2.3) \qquad f(x) \equiv X_{n_1}^{(p_i)} X_{n_2}^{(p_i)} \ldots X_{n_k}^{(p_i)} \pmod{p_i},$$

wobei $X_{n_j}^{(p_i)}$ ein modulo p_i irreduzibles Polynom vom Grade n_j bedeutet. Dadurch werden für die a_i die Kongruenzklassen modulo p_i bestimmt. Wir setzen diese in die Ausdrücke der Koeffizienten der Gleichung $F(z) = 0$ ein und erhalten die Kongruenz

$$F(z) \equiv 0 \pmod{p_i},$$

welche sicher eine oder mehrere rationale Wurzeln hat. Es sei φ_i eine dieser Wurzeln. Dann gehe φ_i in die anderen rationalen Wurzeln über mittels einiger Permutationen $\Sigma_1, \Sigma_2, \ldots, \Sigma_\nu$ der symmetrischen Permutationsgruppe $\mathfrak{S}$ von $x_1, x_2, \ldots, x_n$.

Durch die Festsetzung (2.3) ist die „breite" Klasse der Permutation bestimmt, zu der p_i gehört, d. h. die Gesamtheit aller mit S_i innerhalb $\mathfrak{S}$ ähnlichen Permutationen. Wählen wir aber die Kongruenzklasse von φ_i fest, so wird dadurch eine *Abteilung* von S_i innerhalb $\mathfrak{G}$ bestimmt. Ist $\mathfrak{A}$ die Abteilung von S_i, so sind

$$\Sigma_1^{-1} \mathfrak{A} \Sigma_1, \ \Sigma_2^{-1} \mathfrak{A} \Sigma_2, \ \ldots, \ \Sigma_\nu^{-1} \mathfrak{A} \Sigma_\nu$$

gerade diejenigen Abteilungen von $\mathfrak{G}$, welche den Zyklentyp von S_i haben. Einer dieser Abteilungen muß die Abteilung der von uns gewählten Permutation $\overline{S_i}$ entsprechen. Setzen wir die Werte von $\varphi_i^{\Sigma_j}$ $(j = 1, 2, \ldots, \nu)$ in die Ausdrücke der Koeffizienten der Gleichung $F_i(z_i) \equiv 0$ ein, so entspricht mindestens eine der daraus entstandenen Kongruenzen $F_i(z_i) \equiv 0 \pmod{p_i}$ der Permutation $\overline{S_i}$ und besitzt demnach keine rationale Wurzeln. D. h. p_i gehört in $K(x_1, x_2, \ldots, x_n)$ zu einer Permutationsklasse, welche nicht in $\mathfrak{G}_i$ enthalten ist.

Nehmen wir $i = 1, 2, \ldots, s$, so erhalten wir für $a_1, a_2, \ldots, a_n$; φ und also für $\pi_1, \pi_2, \ldots, \pi_n$ die Kongruenzklassen modulo $P = p_1 p_2 \ldots p_s$.

Wählen wir dabei die π_i innerhalb der soeben bestimmten Kongruenzklassen fest und setzen diese Werte in die Ausdrücke der Kongruenzen der Gleichung $f(x) = 0$ ein, so ist die Gruppe der so entstehenden Gleichung genau $\mathfrak{G}$. Denn sie ist einerseits kraft der parametrischen Ausdrücke von den a_i in $\mathfrak{G}$ enthalten. Andererseits ist sie wegen der aufgestellten Kongruenzbedingungen in keiner der Gruppen $\mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_s$ enthalten.

5. Will man insbesondere die affektlosen Gleichungen aufstellen, so kann man nach einem Vorgang von M. Bauer drei beliebige Primzahlen p, q, r $(r \geqq n-2)$ nehmen und dann das Polynom $f(x)$ durch drei Kongruenzbedingungen

$$\begin{aligned} f(x) &\equiv X_n^{(p)} \pmod{p}, \\ f(x) &\equiv X_{n-1}^{(q)}\,(x-b) \pmod{q}, \\ f(x) &\equiv X_2^{(r)}\,(x-b_1)\,(x-b_2)\ldots(x-b_{n-2}) \pmod{r} \end{aligned}$$

beschränken. Die Gruppe der Gleichung $f(x) = 0$ enthält einen n-gliedrigen, einen $(n-1)$-gliedrigen Zyklus und eine Transposition und ist demnach die symmetrische Gruppe (5, 6, 79).

6. Das in N° 4 dargelegte Verfahren erlaubt, alle möglichen Gleichungen mit der Gruppe $\mathfrak{G}$ zu erschöpfen, wenn man es hinlänglich weit fortsetzt. Das folgt aus dem folgenden Ergebnis von Frobenius (23):

Enthält die Gruppe der Gleichung $f(x) = 0$ eine Permutation mit den Zyklen $n_1, n_2, \ldots, n_k$ $(\Sigma n_i = n)$, so gibt es unendlich viele Primzahlen p derart, daß die Kongruenz $f(x) \equiv 0 \pmod{p}$ in irreduzible Polynome von den Graden $n_1, n_2, \ldots, n_k$ zerfällt.

Der etwas vage Begriff „alle Gleichungen" kann dadurch präzisiert werden, daß wir uns die Aufgabe stellen, sämtliche Gleichungen mit der Gruppe $\mathfrak{G}$ aufzustellen, deren Koeffizienten eine gegebene Grenze nicht übersteigen. Dazu muß man das Frobeniussche Resultat folgendermaßen verschärfen:

Man finde die Grenzen, unterhalb deren sich gewiß eine vorgeschriebene Anzahl der Primzahlen von verlangter Beschaffenheit befindet.

Solche Grenzen haben L. Kronecker (42) und F. Mertens (49) für den Fall der arithmetischen Progressionen angegeben. Ich habe diese Abschätzung für die Frobeniussche Aufgabe durchgeführt (81). Das Ergebnis ist wie folgt. Ist

$$x = \operatorname{Max}\left\{ 2\left(\frac{2A_d}{g_d h_d} + 2W\right)^{\frac{1}{a}} \right\} \text{ für alle } d \mid f, \tag{2.4}$$

so sind im Intervalle $(1, x)$ sicher V Primzahlen enthalten, die zur Abteilung von S gehören. Die Konstanten A_d, g_d, h_d, W hängen von den gewissen Unterkörpern von K und von der Zahl V ab. Um diese Grenze explizite durch die Koeffizienten der Gleichung (2.1) auszudrücken, ist es nötig, für gewisse Konstanten von K Abschätzungen anzugeben. Ganz neuerdings hat R. Remak (61) für den Regulator eines Körpers eine obere und eine untere Grenze aufgestellt, was für die Abschätzung der Formel (2.4) besonders wichtig ist.

7. Suchen wir nur die Lösung der Aufgabe I, so ist die Lösbarkeit der Lürothschen Aufgabe nicht notwendig. Ist $F(\varphi) = 0$ die Gleichung, der eine zu $\mathfrak{G}$ gehörende Funktion φ genügt, so sind die Koeffizienten des Polynoms $F(\varphi)$ rationale Funktionen der Koeffizienten $a_1, a_2, \ldots, a_n$ des Polynoms $f(x)$. Nehmen wir $f(x) \equiv X_{n_1}^{(p_j)} X_{n_2}^{(p_j)} \ldots X_{n_k}^{(p_j)} \pmod{p_j}$, so werden dadurch die a_i modulo p_j bestimmt. Setzen wir ihre Werte in die Kongruenz $F(z) \equiv 0 \pmod{p_j}$ ein, so muß diese Kongruenz wenigstens eine rationale Wurzel haben. Hat sie mehrere Wurzeln, so wählen wir unter ihnen diejenige, welche einer für uns nötigen Abteilung entspricht. Durchläuft j die Werte $1, 2, \ldots, s$, so werden $a_1, a_2, \ldots, a_n$; φ modulis $p_1, p_2, \ldots, p_s$, also modulo $P = p_1 p_2 \ldots p_s$ bestimmt, sind also in der Form $a_i = a_i^{(0)} + Pt_i$, $\varphi = \varphi_0 + Pu$ darstellbar, wo $a_1^{(0)}, a_2^{(0)}, \ldots, a_n^{(0)}$; φ Konstanten bedeuten. Setzen wir dies in die *Gleichung* $F(\varphi) = 0$ ein, so erhalten wir eine Diophantische Gleichung $\Phi(t_1, t_2, \ldots, t_n; u) = 0$. Die Aufgabe läuft demnach auf die Lösung dieser Gleichung hinaus. Man beachte dabei, daß diese Gleichung folgende Eigenschaften besitzt:

1) Sie ist stets in gebrochenen rationalen Zahlen lösbar. Man kann nämlich statt der a_i die elementar-symmetrischen Funktionen der n willkürlichen rationalen Zahlenwerte einsetzen, so daß die Lösung n „Freiheitsgrade“ besitzt.

2) Sie ist stets in ganzen p-adischen Zahlen lösbar, wobei die Primzahl p ganz beliebig zu wählen ist.

Die Lösbarkeit der Gleichung $\Phi = 0$ hängt von der Wahl der zu $\mathfrak{G}$ gehörenden Funktion nicht ab.

8. Es sind der Lösung der in Rede stehenden Aufgaben für einige spezielle Gruppen viele Arbeiten gewidmet. An der ersten Linie steht die Arbeit von D. Hilbert (35), in welcher die Aufgabe I auf Grund des Irreduzibilitätssatzes für symmetrische und alternierende Gruppen jeder Ordnung gelöst ist. Die wirkliche Aufstellung von Gleichungen mit alternierender Gruppe wurde neuerdings von I. Schur (72) fast vollständig

durchgeführt. Ist nämlich $n \equiv 0 \pmod 4$, so zeigt Schur, daß die Gleichung

$$E_n(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} = 0$$

die alternierende Gruppe als Galoissche Gruppe besitzt. Andererseits beweist er (Crelle: 165, 1931), daß bei $n \equiv 1 \pmod 2$ die Gleichung

$$1 - \binom{n}{1}\frac{x}{2!} + \binom{n}{2}\frac{x^2}{3!} - \ldots + (-1)^n \frac{x^n}{(n+1)!} = 0$$

ebenfalls die alternierende Gruppe als Galoissche Gruppe hat.

9. Bei der Lösung der Aufgabe II ist es wichtig, die Lürothsche Aufgabe durch *rationalzahlige* rationale Funktionen zu lösen. Dieser Frage für den Fall auflösbarer Gruppen vom Primzahlgrad sind die Arbeiten von S. Breuer (10, 11) und Ph. Furtwängler (27) gewidmet. Furtwängler hat für den Fall zyklischer Gruppen vom Primzahlgrad p folgendes hinreichendes Kriterium aufgestellt:

Die Aufgabe läßt eine Lösung zu, wenn es gelingt, ein ganzzahliges Zahlensystem $e_0, e_1, \ldots, e_{p-2}$ aufzustellen, so daß 1) die Hankelsche Determinante

$$\begin{vmatrix} e_0, & e_1, & \ldots, & e_{p-2} \\ e_{p-2}, & e_0, & \ldots, & e_{p-3} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ e_1, & e_2, & \ldots, & e_0 \end{vmatrix} = \pm p$$

ist, 2) die Kongruenzen $\sum_{i=0}^{p-2} e_i g^i \equiv 0 \pmod p$ gelten, wobei g eine Primitivwurzel von p ist.

Dieses Kriterium ist z. B. für $p = 47$ nicht erfüllt. Nachträglich gibt Furtwängler einige allgemeine Vorschriften für die Aufstellung der rationalen Minimalbasen von metazyklischen Gruppen.

Breuer hat mehrere ähnliche Kriterien hergeleitet, indem er seinen Satz über die Zerspaltung eines Körpers der rationalen Funktionen von n Veränderlichen in zwei Unterkörper benutzte, von denen einer von den vollmetazyklischen Funktionen der erzeugenden Veränderlichen abhängt.

10. Die Aufgaben I und III wurden auf Relativkörper erweitert. Zunächst kann die Aufgabe III als für Relativkörper gelöst betrachtet werden, wenn eine bekannte Rationalbasis nicht rationalzahlig ist, son-

dern gewisse Kreiskörperzahlen unter den Koeffizienten enthält (vgl. z. B. E. Fischer, 22). Das ist aber keine Erweiterung der Aufgabe. Eine Lösung der Aufgaben I und III kann nur dann als befriedigende Erweiterung der Aufgaben auf Relativkörper betrachtet werden, wenn wir auch über die absolute Galoissche Gruppe etwas sagen können.

Man kann die Arbeiten von O. Ore (57) und H. Hasse (30, 31) als die ersten in dieser Richtung nennen, obwohl sie sich nicht unmittelbar mit diesen Aufgaben beschäftigen. Hasse legt einen Zahlkörper k und eine Anzahl der darin enthaltenen Primideale $\mathfrak{p}_i$ zugrunde. Dann findet er unendlich viele Oberkörper K, in denen die $\mathfrak{p}_i$ in Primideale von vorgeschriebener Ordnung und Multiplizität zerfallen. Sodann macht er eine wesentliche Verschärfung dieses Resultats, indem er die vorgeschriebenen Zerlegungen *regulär* annimmt und verlangt, daß K/k relativ Abelsch ist. Er gibt den Existenzbeweis unter gewissen einschränkenden Voraussetzungen.

11. Die allgemeine Aufgabe I für Relativkörper kann folgendermaßen formuliert werden (vgl. 84):

Aufgabe A. Es sei ein algebraischer Zahlkörper k gegeben, dessen Gruppe $\mathfrak{g}$ sein möge. Es sei außerdem eine abstrakte Gruppe $\mathfrak{G}$ mit einem Normalteiler $\mathfrak{H}$ gegeben, so daß die Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ mit $\mathfrak{g}$ isomorph ist. Man finde die notwendigen und hinreichenden Bedingungen dafür, daß es einen Oberkörper K von k gibt, dessen Gruppe mit $\mathfrak{G}$ isomorph ist.

Das nachstehende Beispiel zeigt, daß diese Aufgabe in manchen Fällen nicht lösbar ist. Es sei k zyklisch vom Primzahlgrade l. $\mathfrak{G}$ sei zyklisch von der Ordnung l^2. Die *kritischen* Primzahlen von k seien wohl $\equiv 1 \pmod{l}$, aber nicht $\equiv 1 \pmod{l^2}$. Aus dem *zahlentheoretischen Monodromiesatz* folgt, daß K wenigstens eine Trägheitsgruppe von der Ordnung l^2 enthalten muß (vgl. 82). Die einer solchen Trägheitsgruppe entsprechende Primzahl p muß auch in k kritisch sein, was unmöglich ist, da sie bekanntlich die Kongruenz $p \equiv 1 \pmod{l^2}$ befriedigt.

Dieses Beispiel zeigt auch, daß die Lösbarkeit der Aufgabe A nicht durch die blosse Struktur der Gruppe $\mathfrak{G}$, sondern auch durch gewisse arithmetische Eigenschaften des Körpers k bestimmt wird.

12. Für die Aufgabe A in bezug auf Abelsche Gruppen hat A. Scholz (63, 64) besonders wichtige Ergebnisse erhalten. Seine Untersuchungen betreffen meistens die zweistufigen Gruppen (d. h. Gruppen mit Abelschen Kommutatorgruppen) und schreiten wesentlich in zwei Richtungen fort. Erstens hat er eine sehr zweckmäßige Klassifikation von zwei-

stufigen Gruppen durchgeführt. Die einfachste seiner Klassen, welche er *Dispositionsgruppen* nannte, läßt eine Lösung der Aufgabe A unabhängig von den arithmetischen Eigenschaften des Körpers k zu (63). Man kann die Dispositionsgruppe als Gruppe $\mathfrak{G}$ definieren, deren Abelsche Normalteiler $\mathfrak{H}$ das direkte Produkt aller zyklischen Gruppen ist, die mit einer von ihnen konjugiert sind. Außerdem soll jede dieser zyklischen Gruppen keinen Normalisator außer $\mathfrak{H}$ besitzen.

Scholz hat für die Dispositionsgruppen folgende zwei Sätze bewiesen:

1) Eine Dispositionsgruppe $\mathfrak{G}$ wird vollständig bestimmt, sobald man die Gruppe $\mathfrak{G}/\mathfrak{H}$ und die Ordnung eines erzeugenden Elements von $\mathfrak{H}$ kennt.

2) Ist ein algebraischer Zahlkörper k mit der Gruppe $\mathfrak{G}/\mathfrak{H}$ gegeben, so kann man stets einen Oberkörper K finden, dessen Gruppe mit $\mathfrak{G}$ isomorph ist.

Später hat Scholz den ersten dieser Sätze auf den Fall erweitert, wo sowohl $\mathfrak{G}/\mathfrak{H}$ als auch $\mathfrak{H}$ nicht Abelsch, sondern ganz beliebig sind (65).

Zweitens hat Scholz andere mögliche Typen von zweistufigen Gruppen eingehend untersucht (64). Er hat nämlich unter allen zweistufigen Gruppen zwei *Maximaltypen* (d. h. solche Typen, daß eine jede zweistufige Gruppe als Faktorgruppe eines Produkts von Gruppen dieser Typen dargestellt werden kann) gefunden: *Ringgruppen* und *Zweiggruppen*. Ringgruppen sind stets Faktorgruppen gewisser Potenzen von Dispositionsgruppen. Zweiggruppen besitzen dagegen eine Eigenschaft, die eine solche Darstellung nicht zuläßt: sie haben keine Abelsche Obergruppe der Kommutatorgruppe. Demnach bleibt die Frage nach der Existenz von Relativkörpern mit Zweiggruppen offen.

13. Ich habe der Aufgabe A eine Arbeit gewidmet (84). Darin habe ich den Begriff der Dispositionsgruppe etwas verallgemeinert, indem ich die Forderung, daß jede erzeugende zyklische Untergruppe von $\mathfrak{H}$ keinen Normalisator außer $\mathfrak{G}$ zuläßt, weggeworfen habe. Dann entstehen die sogenannten *Scholzschen Gruppen*, denen die *reinverzweigten* (d. h. keine unverzweigte Oberkörper von k enthaltenden) Körper mit den Relativdiskriminanten entsprechen, deren Primidealteiler innerhalb k nicht kritisch sind. Die Frage nach der Einzigkeit einer Scholzschen Gruppe, wenn die Faktorgruppe $\mathfrak{G}/\mathfrak{H}$, die Ordnung eines erzeugenden Elements von $\mathfrak{H}$ und sein Normalisator gegeben sind, bleibt offen. Die Frage nach der Existenz eines Relativkörpers mit einer gegebenen Scholzschen Gruppe ist auf die Existenzfrage von Hauptprimidealen $\mathfrak{p}$ mit vorgeschriebenen Werten des Hasseschen Normenrestsymbols $\left(\frac{\mathfrak{p}, K}{\mathfrak{p}}\right)$ (vgl.

Hasse, 32 III) zurückgeführt. Diese Frage liegt aber außer dem Rahmen der bis jetzt bekannten analytischen Idealtheorie.

14. Gehört die Gruppe $\mathfrak{G}$ nicht zum Typ der Scholzschen Gruppen, so kann man nur dann die Existenz eines entsprechenden Oberkörpers erwarten, wenn er entweder einen absoluten Teilklassenkörper enthält oder seine relativ kritischen Primideale auch innerhalb k kritisch sind. In diesem Falle bleiben wir unter der vollen Herrschaft der individuellen Eigentümlichkeiten des Körpers k.

Die Gruppen der absoluten Klassenkörper können ebenfalls nicht ganz willkürlich sein. Einerseits sind sie durch den schon obenerwähnten Monodromiesatz beschränkt, nach welchem alle Trägheitsgruppen durch Komposition die volle Galoissche Gruppe des Körpers erzeugen, während die Trägheitsgruppen eines relativ unverzweigten Körpers eine eineindeutige Abbildung auf die Trägheitsgruppen des Grundkörpers k zulassen. Ich habe, indem ich von diesem Prinzip ausging, eine Klassifikation der möglichen Gruppentypen von absoluten Klassenkörpern durchgeführt (82). Andererseits haben F. Pollaczek (60) und Scholz (66) eine durch die Eigenschaften des Grundeinheitensystems beeinflußte Einschränkung der absoluten Klassenkörper entdeckt und entwickelt.

§ 3. Ueber die analytische Form der zu vorgeschriebener Permutationsklasse gehörenden Primzahlen

1. Ein algebraischer Zahlkörper ist bekanntlich nicht durch seine Galoissche Gruppe vollständig bestimmt. Die bekannten Invarianten, die den Körper vollständig bestimmen, sind die sogenannten Artin-Symbole $\left(\frac{K}{\mathfrak{p}}\right)$ (32 III, S. 6), d. h. die Permutationsklassen, zu denen einzelne Primzahlen gehören. Die Anzahl dieser Invarianten ist unendlich, woraus folgt, daß sie nicht voneinander unabhängig sein können. Die zwischen ihnen bestehenden Relationen können hergeleitet werden, wenn wir die analytische Form kennen, in welcher die Primzahlen darstellbar sind, die zu gewissen Permutationsklassen gehören, d. h. einem und demselben Wert von $\left(\frac{K}{\mathfrak{p}}\right)$ entsprechen. Es erweist sich, daß solche analytische Formen von den Struktureigenschaften der entsprechenden Gruppen $\mathfrak{G}$ abhängen. Dieser Zusammenhang liefert einen tiefen Einblick in die arithmetische Struktur eines Körpers mit bekannter Galoisschen Gruppe.

2. Zunächst erinnere ich an den klassischen Fall eines Abelschen Körpers. Damit eine Primzahl zu einer gegebenen Permutation (in

diesem Fall besteht jede Permutationsklasse nur aus einer Permutation) gehöre, muß sie in der Form einer der verschiedenen arithmetischen Progressionen $ax + b$ darstellbar sein, die der Permutation der Galoisschen Gruppe eindeutig entsprechen. Die Zahl a ist für alle Permutationen dieselbe und besteht aus den Primzahlen, die in der Diskriminante des Körpers aufgehen, während die b den verschiedenen Permutationen der Galoisschen Gruppe zugeordnet sind.

3. Der weitere klassisch gewordene Fall entspricht der komplexen Multiplikation der elliptischen Funktionen. Ist ein Zahlkörper relativ Abelsch über einem imaginär-quadratischen Körper, so ist jede zu einer gegebenen Permutationsklasse gehörende Primzahl durch eine oder mehrere positive quadratische Formen darstellbar, deren Diskriminante von dem Körper abhängt (genauer: gleich der Diskriminante des imaginär-quadratischen Körpers ist) und deren Klassen den Permutationsklassen zugeordnet sind.

4. Diese Tatsache wurde von Kronecker vermutet („Jugendtraum") und von R. Fueter (24, 25) bewiesen. Die Prinzipien, auf denen sie beruht, folgen aus der verallgemeinerten Klassenkörpertheorie. Faßt man nämlich nur diejenigen Zahlen eines Körpers k als Hauptideale auf, welche gewissen Kongruenzen modulo eines Ideals $\mathfrak{f}$ (welches man Führer nennt) genügen, und ist h die Klassenzahl in diesem neuen Sinne, so gibt es einen relativ Abelschen Körper K vom Relativgrade h, sogenannten Klassenkörper, der die Eigenschaft besitzt, daß innerhalb K diejenigen und nur diejenigen Primideale von k vollständig zerfallen, welche in der Hauptklasse liegen (Ph. Furtwängler, 26; T. Takagi, 76). Man kann umgekehrt jeden über k relativ Abelschen Körper als einen Klassenkörper mit geeignet gewähltem Führer betrachten (Fueter, 24; Takagi, 76; Hasse, 32).

5. Nun stellen wir uns die allgemeine Frage nach der analytischen Form der Primzahlen, welche zu durch die Potenzen einer Permutation S erzeugten Klassen gehören. Es sei ein normaler algebraischer Zahlkörper K gegeben, dessen Gruppe sei $\mathfrak{G}$. Es sei ferner S eine Permutation von $\mathfrak{G}$. Damit eine Primzahl p zu einer der Klassen gehöre, die durch Potenzen von S erzeugt sind, ist notwendig und hinreichend, daß der zu $\mathfrak{Z}_S$ gehörende Unterkörper K_S von K ein Primidealteiler $\mathfrak{p}$ von p ersten Grades enthält, wobei $\mathfrak{Z}_S$ die durch Potenzen von S erzeugte zyklische Untergruppe von $\mathfrak{G}$ ist.

Es sei $\mathfrak{a}_1 \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ ein System der Repräsentanten aller verschiedenen Idealklassen von K_S, und es sei $(\mu_1^{(i)}, \mu_2^{(i)}, \ldots, \mu_n^{(i)})$ eine Basis des Ideals

$\mathfrak{a}_i$ $(i = 1,2, \ldots, h)$. Dann ist $N(\mu_1^{(i)} x_1 + \mu_2^{(i)} x_2 + \ldots + \mu_n^{(i)} x_n)$ die (zerlegbare) Form n-ten Grades der Veränderlichen $x_1, x_2, \ldots, x_n$, deren Koeffizienten die Zahl $N(\mathfrak{a}_i)$ als größten gemeinsamen Teiler haben. Der Quotient

$$(3.1) \quad \frac{N(\mu_1^{(i)} x_1 + \mu_2^{(i)} x_2 + \ldots + \mu_n^{(i)} x_n)}{N(\mathfrak{a}_i)} = f_i(x_1, x_2, \ldots, x_n) \quad (i = 1, 2, \ldots, h)$$

ist also eine primitive Form n-ten Grades. Ergeben wir den x_i alle ganzen rationalen Zahlenwerte, so durchlaufen die Werte der Form $f_i(x_1, x_2, \ldots, x_n)$ die Normen aller Ideale, deren Klasse zu der Klasse von $\mathfrak{a}_i$ entgegengesetzt ist. Denn liegt b in der zu $\mathfrak{a}_i$ entgegengesetzten Idealklasse, so ist $b\mathfrak{a}_i$ ein Hauptideal, welches mit einer Zahl $x_1 \mu_1^{(i)} + x_2 \mu_2^{(i)} + \ldots + x_n \mu_n^{(i)}$ des Ideals $\mathfrak{a}_i$ assoziiert sein möge. Es gilt also:

$$N(b)\, N(\mathfrak{a}_i) = N(x_1 \mu_1^{(i)} + x_2 \mu_2^{(i)} + \ldots + x_n \mu_n^{(i)}) = N(\mathfrak{a}_i)\, f_i(x_1, x_2, \ldots, x_n).$$

Ist $\mathfrak{p}$ ein Primideal ersten Grades von K_S, gilt also $N(\mathfrak{p}) = p$, so suche man denjenigen Repräsentant $\mathfrak{a}_i$, dessen Klasse zur Klasse von $\mathfrak{p}$ entgegengesetzt ist. Dann ist $\mathfrak{p}$ in der Form $f_i(x_1, x_2, \ldots, x_n)$ darstellbar. Ist umgekehrt $\mathfrak{p}$ in der Form $f_i(x_1, x_2, \ldots, x_n)$ darstellbar, so ist $N(\mathfrak{a}_i)\mathfrak{p}$ in der Form $N(x_1 \mu_1^{(i)} + x_2 \mu_2^{(i)} + \ldots + x_n \mu_n^{(i)})$ darstellbar. Die Zahl $x_1 \mu_1^{(i)} + x_2 \mu_2^{(i)} + \ldots x_n \mu_n^{(i)}$ ist durch $\mathfrak{a}_i$ teilbar, und die Norm des Quotientenideals $\frac{x_1 \mu_1^{(i)} + x_2 \mu_2^{(i)} + \ldots + x_n \mu_n^{(i)}}{\mathfrak{a}_i}$ ist gleich p. Daraus folgt, daß es ein Ideal mit der Norm p gibt. Dieses Ideal muß ein Primideal vom Grade 1 sein.

6. Um die Bedingung für die Zugehörigkeit einer Primzahl p zur *Abteilung* von S aufzustellen, müssen wir ihre Zugehörigkeit zu den Potenzen S^k von S ausschließen, deren Exponenten k nicht zur Ordnung f von S relativ prim sind. Dazu muß p in K_S mindestens ein Primideal ersten Grades enthalten, während dies für kein K_{S^k} zutrifft, wenn $(k, f) \neq 1$ ist. Sind

$$(3.2) \qquad g_i(x_1, x_2, \ldots, x_n), \quad h_i(x_1, x_2, \ldots, x_n), \ldots$$

die den Körpern K_{S^k} entsprechenden Formen, die ebenso wie die Form $f_i(x_1, x_2, \ldots, x_n)$ gebaut sind, so gehört p zur Abteilung von S dann und nur dann, wenn sie durch eine der Formen (3.1), aber durch keine der Formen (3.2) darstellbar ist.

7. Wie kann man die Zugehörigkeit einer Primzahl p zur *Klasse* von S charakterisieren? Ich kann das nur dann dartun, wenn ich eine Zahl a derart kenne, daß $p^f \equiv 1 \pmod{a}$ ist, aber keine niedere als die f-te Potenz von $p \equiv 1 \pmod{a}$ ist. Bildet man dann den Unterkörper $K(\eta)$ des Körpers der a-ten Einheitswurzeln, so bleibt p in $K(\eta)$ unzerlegbar. Ist $p \equiv b \pmod{a}$, so gilt: $\eta^p \equiv \eta^b \pmod{p}$. Nun bilden wir die Größe

$$\xi = \eta\omega + \eta^b\omega^S + \ldots + \eta^{b^{f-1}}\omega^{S^{f-1}},$$

wobei ω eine Größe von K ist, und die Gleichung $\Phi(\xi) = 0$, der ξ genügt. Hält man schon für festgestellt, daß p zur *Abteilung* von S gehört, so gehört p zur *Klasse* von S dann und nur dann, wenn die Kongruenz $\Phi(\xi) \equiv 0 \pmod{p}$ rationale Wurzeln besitzt, d. h. wenn p im Körper $K(\xi)$ mindestens einen Primidealteiler vom Grade 1 hat. Man kann also ein Formensystem derart aufstellen, daß p durch sie dann und nur dann darstellbar ist, wenn p zur Klasse von S gehört. Man kann für jedes p gewiß die entsprechende Zahl a finden; den verschiedenen p entsprechen aber verschiedene Formen. Ich kann demnach nicht eine endliche Anzahl von Formen aufstellen, die für sämtliche Primzahlen gültig wären.

8. Aus diesem Kriterium folgen die in N° N° 2,3 betrachteten klassischen Kriterien nicht. Um ein allgemeineres Kriterium aufzustellen, betrachten wir den Fall, daß $\mathfrak{G}$ einen Abelschen Normalteiler $\mathfrak{H}$ hat. Dann kann man K als einen relativ Abelschen Körper in bezug auf den zu $\mathfrak{H}$ gehörigen Körper k auffassen. K ist also ein Klassenkörper von k. Nach dem allgemeinen Reziprozitätsgesetze von E. Artin (2) besteht zwischen den Permutationen von $\mathfrak{H}$ und den Idealklassen (genauer: den Restklassen nach einer gewissen Idealklassenuntergruppe) von k eine eineindeutige Beziehung, welche den Charakter eines Isomorphismus hat. Die dem Körper k entsprechenden Formen (3.1) zerfallen demnach in die Formensysteme $\mathfrak{B}_i$, von denen jedes einer der erwähnten Restklassen entspricht. Die Anzahl der Formensysteme ist gleich der Ordnung von $\mathfrak{H}$. Das Artinsche Reziprozitätsgesetz besagt, daß eine Primzahl p dann und nur dann durch eine der Formen des Systems $\mathfrak{B}_i$ darstellbar ist, wenn sie zur Klasse von S_i gehört, wobei S_i eine dem System $\mathfrak{B}_i$ entsprechende Permutation von $\mathfrak{H}$ ist. Dieses Formensystem hat den Vorteil, daß der Grad der ihnen entsprechenden Formen im allgemeinen niedriger ist. Ist z. B. K absolut Abelsch, so ist k der rationale Körper, so daß die Normen mit den Zahlen selbst zusammenfallen. Die Klasseneinteilung der Zahlen des rationalen Körpers im „engeren“ Sinne ist nichts anderes als ihre Verteilung unter den Kongruenzklassen nach

einem gewissen Modul, den man *Führer* nennt. Ist k quadratisch, so kommen wir zu den quadratischen Formen, in voller Uebereinstimmung mit der allgemeinen Theorie.

9. Wir bemerken noch, daß die dem Körper k entsprechenden Formen die sogenannte Formenkomposition zulassen. Ist z. B.

$$N(\mathfrak{a}) = f_1(x_1, x_2, \ldots, x_n), \quad N(\mathfrak{b}) = f_2(y_1, y_2, \ldots, y_n),$$

so ist

$$N(\mathfrak{ab}) = f_1(x_1, x_2, \ldots, x_n) \cdot f_2(y_1, y_2, \ldots, y_n).$$

Liegt andererseits $\mathfrak{ab}$ etwa in der zu $\mathfrak{a}_3$ entgegengesetzten Idealklasse, so ist $N(\mathfrak{ab}) = f_3(x_1, x_2, \ldots, x_n)$, wobei $z_1, z_2, \ldots, z_n$ gewisse ganzzahlige bilineare Ausdrücke in $x_1, x_2, \ldots, x_n$ und $y_1, y_2, \ldots, y_n$ sind, welche man erhalten kann, indem man im bilinearen Ausdruck $\sum_{i,j} \mu_i^{(1)} \mu_j^{(2)} x_i x_j$, wo $(\mu_1^{(1)}, \mu_2^{(1)}, \ldots, \mu_n^{(n)})$, $(\mu_1^{(2)}, \mu_2^{(2)}, \ldots, \mu_n^{(2)})$ die Basen der Ideale $\mathfrak{a}_1$, $\mathfrak{b}_2$ sind, die $\mu_i^{(1)} \mu_j^{(2)}$ durch eine Basis $(\mu_1^{(3)}, \mu_2^{(3)}, \ldots, \mu_n^{(3)})$ des Ideals $\mathfrak{a}_1 \mathfrak{b}_2$ ausdrückt: $\mu_i^{(1)} \mu_j^{(2)} = \sum_s c_{ij}^s \mu_s^{(3)}$, d. h. $\mathfrak{a}_1 \mathfrak{a}_2 \mathfrak{a} \mathfrak{b} = \sum_{i,j,s} c_{ij}^s x_i x_j \mu_s^{(3)}$, und die Koeffizienten von $\mu_s^{(3)}$ mit z_s bezeichnet: $z_s = \sum_{i,j} c_{ij}^s x_i x_j$. Es ist leicht zu verstehen, daß diese Komposition der Formen der Multiplikation der ihnen entsprechenden Formen entspricht.

10. Um eine einfachste analytische Gestalt der zu verschiedenen Permutationsklassen eines gegebenen Zahlkörpers gehörenden Primzahlen zu erhalten, brauchen wir, maximale Abelsche Normalteiler seiner Gruppe $\mathfrak{G}$ zu finden. Dazu beachten wir, daß eine Permutation S von $\mathfrak{G}$ dann und nur dann in einem Abelschen Normalteiler von $\mathfrak{G}$ enthalten sein kann, wenn *ihre Klasse Abelsch ist*, d. h. wenn alle Permutationen ihrer Klasse miteinander vertauschbar sind. Ist $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_k$ die Gesamtheit aller Abelschen Klassen von $\mathfrak{G}$, so besteht jeder Abelsche Normalteiler von $\mathfrak{G}$ aus denjenigen Permutationen dieser Klassen, welche auch miteinander vertauschbar sind. Sind z. B. $\mathfrak{C}_1$ und $\mathfrak{C}_2$ vertauschbar, so ist ihre *Hülle*, d. h. die kleinste $\mathfrak{C}_1$ und $\mathfrak{C}_2$ enthaltende Gruppe, ein Abelscher Normalteiler von $\mathfrak{G}$. Die Einzigkeit des maximalen Abelschen Normalteilers kann nicht erwartet werden, da die Vertauschbarkeit eine nicht transitive Eigenschaft ist.

Das folgende Beispiel zeigt, daß es wirklich Fälle gibt, wo $\mathfrak{G}$ mehrere verschiedene maximale Abelsche Normalteiler enthält. Es sei $\mathfrak{G}$ mittels

3 erzeugender Elemente s_1, s_2, s_3 definiert, die durch folgende Relationen verbunden sind:

$$s_1^p = s_2^p = s_3^p = 1, \quad s_1 s_2 = s_2 s_1, \quad s_1 s_3 = s_3 s_1, \quad s_2 s_3 = s_3 s_2 s_1$$

(p ist eine Primzahl). Beide Untergruppen (s_1, s_2) und (s_1, s_3) sind Abelsche Normalteiler von $\mathfrak{G}$. Beide sind maximal, da die einzige echte Obergruppe jeder dieser Gruppen, $\mathfrak{G}$ selbst, nicht Abelsch ist. Andererseits sind sie voneinander verschieden.

11. Als Beispiel betrachten wir einen allgemeinen kubischen Zahlkörper K. Zu seiner alternierenden Gruppe gehört ein quadratischer Unterkörper k, und man kann nach der Fueter-Takagischen Theorie K als Ringklassenkörper von k betrachten. Den zu betrachtenden Ringklassen von k entspricht ein System von binären quadratischen Formen, welches sich in drei Untersysteme $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3$ zerspaltet, von denen jedes einer der 3 Permutationen von $\mathfrak{H}$ entspricht. Ist D die Diskriminante dieses Formensystems, so ist $\left(\frac{D}{p}\right) = +1$ die notwendige und hinreichende Bedingung dafür, daß p durch eine dieser Formen darstellbar sei. Dasjenige der Systeme $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3$, etwa $\mathfrak{B}_1$, welche die Eigenschaft $\mathfrak{B}_1 \mathfrak{B}_1 = \mathfrak{B}_1$ besitzt, soll das *Hauptsystem* genannt werden. Dann zerfallen alle zur Diskriminante von K relativ primen Primzahlen in folgende drei Arten:

1) $\left(\frac{D}{p}\right) = -1$, p gehört zu $\mathfrak{H}$ nicht, also gehört es zu einer der Transpositionen.

2) $\left(\frac{D}{p}\right) = +1$, p ist durch eine der Formen $\mathfrak{B}_2, \mathfrak{B}_3$ darstellbar. p gehört zu einem der dreigliedrigen Zyklen.

3) $\left(\frac{D}{p}\right) = +1$, p ist durch eine der Formen $\mathfrak{B}_1$ darstellbar. p gehört zur identischen Permutation.

Den kubischen Körper haben in dieser Hinsicht Dedekind, (17), Voronoi (85) und Takagi untersucht. Neuerdings hat Hasse (33) den kubischen Körper auf klassenkörpertheoretischer Grundlage untersucht, indem er auch die kritischen Primideale mitbetrachtete. Auf diese Aufgabe hat mich B. Delaunay freundlicherweise aufmerksam gemacht.

12. Nun will ich ein sehr elegantes Verfahren von A. Speiser (73) erwähnen, das dazu dient, um die Ordnung f der Permutation zu

bestimmen, zu deren Klasse eine Primzahl p gehört. Ich erlaube mir, den Beweis etwas abzuändern. Ist

$$(3.3) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0$$

die zu untersuchende Gleichung, so betrachten wir die Differenzengleichung

$$(3.4) \quad y(m+n) + a_1 y(m+n-1) + \ldots + a_{n-1} y(m+1) + a_n y(m) = 0.$$

Ihre allgemeinste Lösung ist bekanntlich

$$(3.5) \qquad y(m) = C_1 \alpha_1^m + C_2 \alpha_2^m + \ldots + C_n \alpha_n^m ,$$

wobei $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Wurzeln der Gleichung (3.3) und $C_1, C_2, \ldots, C_n$ willkürliche Konstanten sind. Setzen wir $y(1) = y(2) = \ldots = y(n-1) = 0$, $y(n) = 1$, so ist $C_i = \frac{1}{f'(\alpha_i)}$. Nun betrachten wir den $GF[p^f]$ als Grundkörper. Ist u die kleinste (ganzzahlige) Periode der Funktion $y(m)$ modulo p, so ist $\alpha_i^u \equiv 1 \pmod{p}$ $(i = 1, 2, \ldots, n)$ und umgekehrt. Denn ist $y(u) \equiv y(u+1) \equiv \ldots \equiv y(u+n-1) \equiv 0 \pmod{p}$, $y(u+n) \equiv 1 \pmod{p}$, so folgt daraus $C_i \equiv \frac{1}{\alpha_i^u f'(\alpha_i)} \pmod{p}$, d. h. $\alpha_i^u \equiv 1 \pmod{p}$. Da aber $(\alpha_i \to \alpha_i^p)$ eine erzeugende Permutation der Gruppe der Kongruenz $f(x) \equiv 0 \pmod{p}$ ist und demnach ihre Ordnung gleich der kleinsten Zahl f ist, für welche gilt: $\alpha_i^{p^f} \equiv \alpha_i \pmod{p}$, so ist f dem kleinsten Exponenten gleich, für den gilt: $p^f \equiv 1 \pmod{u}$.

13. Hasse hat neuerdings die Frage nach der arithmetischen Struktur von Zahlkörpern auf einen ganz neuen Boden gestellt, indem er die Theorie der Zahlkörper mit den sogenannten *„Algebren"* (d. h. *hyperkomplexen Systemen*) verknüpfte (34, 9). Jedem Körper entspricht ein *„zyklisches"* hyperkomplexes System, welches von E. Noether unter dem Namen *verschränktes Produkt* eingeführt wurde. Da aber umgekehrt einer zyklischen Algebra mehrere Körper mit verschiedenen Galoisschen Gruppen, insbesondere zyklische Körper entsprechen, so wurden dadurch die arithmetischen Eigenschaften von Körpern mit denjenigen von zyklischen Körpern in innigsten Zusammenhang gebracht.

§ 4. Resolventenproblem

1. Es gibt in der allgemeinen algebraischen Körpertheorie eine Frage, die das Resolventenproblem als speziellen Fall enthält:

Es sei ein Körper K rationaler Funktionen mehrerer Veränderlichen $x_1, x_2, \ldots, x_n$ gegeben. Man bestimme den *wahren Transzendenzgrad* von K in bezug auf seinen gewissen Unterkörper k, d. h. die kleinste Zahl m, so daß K als direktes Produkt eines Körpers *algebraischer* Funktionen von m Veränderlichen, die in k aufgehen, und eines gewissen Unterkörpers von k erscheint (vgl. unten § 5).

Um den Zusammenhang dieser Frage mit dem Resolventenproblem zu erläutern, betrachten wir den Körper K aller rationalen Funktionen der Veränderlichen $x_1, x_2, \ldots, x_n$, während k aus den elementaren symmetrischen Funktionen $a_1, a_2, \ldots, a_n$ der Veränderlichen $x_1, x_2, \ldots, x_n$ und ihren rationalen Funktionen besteht. Man finde eine Gleichung n-ten Grades *(Resolvente)*, deren Koeffizienten rationale Funktionen von $a_1, a_2, \ldots, a_n$ sind, von denen eine möglichst kleine Anzahl m funktional unabhängig ist, und deren Wurzeln den ganzen Körper K erzeugen. Mit anderen Worten, es handelt sich um eine Tschirnhausensche Transformation der Gleichung

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \tag{4.1}$$

mit den unbeschränkt veränderlichen Koeffizienten $a_1, a_2, \ldots, a_n$ in eine Gleichung, deren Koeffizienten eine möglichst kleine Anzahl Freiheitsgrade haben.

Es ist zweckmäßig, die Aufgabe dadurch zu erweitern, daß man im *Koeffizientenkörper* k auch irrationale Funktionen von $a_1, a_2, \ldots, a_n$ einführt, die aber ebenfalls von einem nicht größeren als m wahren Transzendenzgrade sind, z. B. $\sqrt{D}$, wo D die Diskriminante der Gleichung (4.1) bedeutet.

Diese Aufgabe kann als eine natürliche Erweiterung der ursprünglichen Grundaufgabe der Galoisschen Theorie, der Radikallösung, aufgefaßt werden. Denn die Darstellung von Wurzeln durch Radikalausdrücke hat den Vorteil, daß sie erlaubt, die Wurzeln durch eine Folge von Operationen zu ermitteln, von denen jede nur mit einer Veränderlichen zu tun hat. Man kann demnach eine Tabelle bewerkstelligen, die jedem Radikand sein Radikal zuordnet, so daß solche Tabellen uns ermöglichen, Wurzeln aller auflösbaren Gleichungen vom gegebenen Grade zu berechnen.

2. Die soeben erwähnte Eigenschaft ist keineswegs für auflösbare Gleichungen charakteristisch. Man kann vielmehr die Auffindung von Gleichungswurzeln durch Operationen ganz anderer Art aufstellen, von denen jeder diese Eigenschaft zukommt. Man kann zunächst die

allgemeine Gleichung 5-ten Grades erwähnen. Es war schon lange bekannt (Bring, 12), daß man sie auf die sogenannte Bring-Jerrardsche Form

$$y^5 + py + q = 0 \tag{4.2}$$

bringen kann, wenn man auf sie eine Tschirnhausensche Transformation anwendet, deren Koeffizienten Wurzeln der Gleichungen von den Graden $\leqq 4$ sind, also Darstellungen durch Radikalausdrücke zulassen (vgl. J. J. Sylvester, 75). Andererseits war der Zusammenhang der Gleichungen 5-ten Grades mit dem Teilungsproblem der Perioden von elliptischen Funktionen (also des Argumentes von Modulfunktionen) durch 5 seit langem bekannt. Dies ermöglicht, eine allgemeine Gleichung 5-ten Grades auf einem transzendenten Wege zu lösen (vgl. 29, 86).

3. Diese Aufgabe wurde von F. Klein auf eine Weise gelöst, die einen Einblick auf das allgemeine Resolventenproblem liefert (41). Er hat nämlich die allgemeine Gleichung 5-ten Grades auf eine etwas andere Normalform

$$y^5 + 15y^4 - 10\gamma \cdot y^2 + 3\gamma^2 = 0 \tag{4.3}$$

mit Hilfe von nur quadratischen Irrationalitäten gebracht, von denen die eine $\sqrt{D}$ und die andere $\sqrt{5}$ ist.

Das zweite, viel wichtigere Verdienst von Klein für das Resolventenproblem besteht darin, daß er den inneren Grund entwickelte, warum das Resolventenproblem für Gleichungen 5-ten Grades lösbar ist. Er knüpfte nämlich dieses Problem an das sogenannte *Formenproblem*, welches im folgenden besteht. Betrachten wir die höchste endliche Gruppe $\mathfrak{G}$ binärer linearer Substitutionen, die Ikosaedergruppe, so kann man für sie eine Gleichung 60-ten Grades

$$(\mathfrak{D}^{30} + 522\,\mathfrak{D}^{25} - 10005\,\mathfrak{D}^{20} - 10005\,\mathfrak{D}^{10} - 522\,\mathfrak{D}^5 + 1)^2 = z \cdot \mathfrak{D}^5 (\mathfrak{D}^{10} + 11\mathfrak{D}^5 - 1)^5 \tag{4.4}$$

aufstellen, deren Koeffizienten von einer Form z der Veränderlichen x_1, x_2 abhängen, die gegenüber den Substitutionen von $\mathfrak{G}$ invariant ist, während ihre Wurzeln ineinander mit Hilfe dieser Substitutionen übergehen. Die Galoissche Gruppe dieser Gleichung ist als Ikosaedergruppe mit der alternierenden Gruppe 5-ten Grades isomorph. Daraus kann man schließen, daß jede Gleichung 5-ten Grades auf die Gestalt (4.4) (oder auch (4.3)) gebracht werden kann, wenn man sie einer rationalen

Transformation unterwirft, deren Koeffizienten eventuell $\sqrt{D}$ enthalten, wobei D die Diskriminante dieser Gleichung bedeutet.

Die Grundidee der Reduktion von Gleichungen 5-ten Grades auf einparametrige Resolventen läuft darauf hinaus, daß die Kompositionsreihe der symmetrischen Gruppe 5-ten Grades aus zwei Gliedern besteht, von denen die eine Gruppe 2-ten Grades ist, während die andere mit der Ikosaedergruppe isomorph ist, welche als Gruppe gebrochener linearer Substitutionen einer Veränderlichen dargestellt werden kann.

4. Diese Idee wurde von Klein auf andere Gleichungen angewandt, nämlich auf die einfache Gruppe von der Ordnung 168, die durch ternäre lineare homogene Substitutionen darstellbar ist. Dieser Gruppe entspricht eine spezielle Klasse von Gleichungen 7-ten Grades, die diese Gruppe als Galoissche Gruppe haben. Da die ternäre lineare homogene Substitutionsgruppe mit der Gruppe der gebrochenen linearen Substitutionen von zwei Veränderlichen isomorph ist, so können wir ganz ebenso schließen, daß die in Rede stehenden Gleichungen eine zweiparametrige Resolvente besitzen.

Etwas komplizierter war der Sachverhalt bei den alternierenden Gleichungen 6-ten Grades. Die alternierende Gruppe 6-ten Grades besitzt keine Darstellung durch ternäre lineare homogene Substitutionen. Deswegen dachte Klein, daß die allgemeinen Gleichungen 6-ten Grades nicht eine 2-parametrige Resolvente besitzen, und suchte für sie 3-parametrige Resolventen. A. Wiman (89) beachtete, daß diese Gruppe trotzdem eine Darstellung durch gebrochene lineare Substitutionen von zwei Veränderlichen zuläßt. Denn man kann diese Gruppe als eine Faktorgruppe einer gewissen Gruppe von der Ordnung 1080 auffassen, welche als lineare homogene Gruppe von drei Veränderlichen dargestellt werden kann. Der ihr entsprechende Normalteiler $\mathfrak{H}$ dritter Ordnung liegt im Zentrum der Gruppe und erscheint also als Gruppe, deren Substitutionen nur die Multiplikationen der Veränderlichen mit den 3-ten Einheitswurzeln bewirken. Fassen wir nun die Verhältnisse der Veränderlichen ins Auge, so erleiden diese eine gebrochene lineare Substitutionsgruppe. Ueben wir auf die ursprünglichen Veränderlichen die Substitutionen von $\mathfrak{H}$ aus, so erleiden ihre Verhältnisse keine Aenderung. Die auf diese Weise konstruierte Gruppe gebrochener linearer Substitutionen ist also mit ihrer Faktorgruppe, d. h. mit der alternierenden Gruppe 6-ten Grades isomorph.

5. Die Frage nach der Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen wurde von I. Schur (69, 70) allgemein untersucht. Es erwies sich, daß diese Aufgabe stets durch eine endliche

Anzahl von Operationen erledigt werden kann. Um nämlich alle solche Darstellungen von einer gegebenen endlichen Gruppe $\mathfrak{G}$ zu ermitteln, muß man eine zu $\mathfrak{G}$ entsprechende *Darstellungsgruppe* $\mathfrak{K}$ finden, die folgende Eigenschaften besitzen soll:

I. $\mathfrak{G}$ soll mit einer Faktorgruppe $\mathfrak{K}/\mathfrak{M}$ isomorph sein.

II. $\mathfrak{M}$ soll im Zentrum von $\mathfrak{K}$ liegen.

III. Die Kommutatorgruppe von $\mathfrak{G}$ ist die Faktorgruppe $\mathfrak{D}/\mathfrak{M}$, wobei $\mathfrak{D}$ die Kommutatorgruppe von $\mathfrak{K}$ ist.

Jeder Gruppe $\mathfrak{G}$ entspricht nur eine endliche Anzahl der verschiedenen Darstellungsgruppen $\mathfrak{K}$. Findet man alle Darstellungen von $\mathfrak{K}$ durch lineare homogene Substitutionen, so ergibt jede dieser Darstellungen eine Darstellung von $\mathfrak{G}$ durch gebrochene lineare Substitutionen. Das ist der allgemeinste Weg zur Bildung sämtlicher Darstellungen dieser Art von $\mathfrak{G}$.

6. A. Wiman (90) hat die Frage nach den Darstellungen der symmetrischen und alternierenden Gruppen von höheren Graden untersucht. Es erwies sich, daß bei $n \geqq 8$ die symmetrischen Gruppen S_n als lineare homogene Gruppen von nicht weniger als $n-1$ Veränderlichen dargestellt werden können und dasselbe von den alternierenden Gruppen gilt.

7. D. Hilbert (36) hat ein Problem („13. Problem") gestellt, das mit dem oben besprochenen Kleinschen Problem viele Berührungspunkte hat. Die Wurzeln der Gleichung (4.1) seien als Funktionen von n Veränderlichen aufgefaßt. Man fragt, ob sie nicht als Superpositionen von Funktionen einer kleineren Anzahl k Veränderlichen und rationaler Operationen dargestellt werden können. Später (37) fand er die folgenden Werte für die k bei $n \leqq 9$:

n	5	6	7	8	9
$k \leqq$	1	2	3	4	4

.

Wiman (91) verallgemeinerte dies Resultat, indem er zeigte, daß für alle $n \geqq 9$ die Ungleichung $k \leqq n-5$ gilt, d. h. daß man jede allgemeine Gleichung vom Grade $n \geqq 9$ mindestens um 5 Variablen vermindern kann, wenn man sie einer Tschirnhausenschen Transformation unterwirft. (Vgl. auch R. Garver, 28).

8. Ich (83) habe mir den Zweck gestellt, den Zusammenhang zwischen der Reduktionsfähigkeit einer Gleichung und der Darstellbarkeit ihrer Galoisschen Gruppe als Transformationsgruppe von einer möglichst

kleinen Anzahl Variablen näher zu untersuchen. Dazu führe ich den folgenden Begriff der *Einkleidungsgruppe* (kurz E. G.) ein:

Ist $\mathfrak{G}$ eine gegebene endliche Gruppe, so heißt eine kontinuierliche Gruppe Γ dann und nur dann E. G. von $\mathfrak{G}$, wenn sie den folgenden Bedingungen genügt:

1) Γ enthält eine mit $\mathfrak{G}$ isomorphe Gruppe als Teiler.
2) Es gibt keinen echten Teiler von Γ, welcher die Eigenschaft 1) besitzt.
3) Es gibt keine echte Faktorgruppe von Γ, welche die Eigenschaft 1) besitzt.

Dann beweise ich den folgenden

Satz. Eine algebraische Gleichung mit unbeschränkt veränderlichen Koeffizienten besitzt eine Resolvente mit k Parametern dann und nur dann, wenn ihre Galoissche Gruppe $\mathfrak{G}$ eine E. G. hat, welche im k-dimensionalen Raume darstellbar ist.

Um den ersten Teil dieses Satzes zu beweisen, nehmen wir an, die Gruppe $\mathfrak{G}$ sei einfach, was zu unseren Zwecken hinreichend ist. Dann ist jede E. G. von $\mathfrak{G}$ ebenfalls eine einfache Gruppe. Hat dann eine $\mathfrak{G}$ als Teiler enthaltende kontinuierliche Gruppe Γ einen echten Normalteiler Γ_1, so kann Γ_1 entweder die ganze Gruppe $\mathfrak{G}$ oder kein Element von $\mathfrak{G}$ außer 1 enthalten. Im ersten Falle widerspricht dies der Bedingung 2). Im zweiten Falle hat die Faktorgruppe Γ/Γ_1 einen mit $\mathfrak{G}$ isomorphen Teiler, was der Bedingung 3) widerspricht.

Man kann vielmehr folgendes beweisen: ist eine $\mathfrak{G}$ als Teiler enthaltende kontinuierliche Gruppe Γ im k-dimensionalen Raume darstellbar (oder kurz: ist Γ eine k-Gruppe), so ist derjenige Teiler einer Faktorgruppe von Γ, welcher E. G. von $\mathfrak{G}$ ist, ebenfalls eine k-Gruppe. Daß ein Teiler einer k-Gruppe wieder eine k-Gruppe ist, ist evident. Um zu beweisen, daß eine einfache Faktorgruppe einer k-Gruppe wieder eine k-Gruppe ist, erinnern wir uns an einen zuerst allgemein von E. E. Levi (44) bewiesenen Satz:

Hat eine kontinuierliche Gruppe Γ eine einfache Faktorgruppe Γ_1, so besitzt sie auch einen mit Γ_1 isomorphen Teiler.

9. Läßt $\mathfrak{G}$, als Transformation der Wurzeln als Veränderlichen aufgefaßt, eine E. G. zu, die zu einer k-Gruppe nicht nur *isomorph*, sondern auch *ähnlich* ist, so erhält man unmittelbar eine Lösung der Aufgabe. Dann kann man nämlich k gewisse Funktionen $z_1, z_2, \ldots, z_k$ der Veränderlichen $x_1, x_2, \ldots, x_n$ aufstellen, welche eine mit Γ isomorphe Gruppe beschreiben, indem man die x_i den Transformationen von Γ unterwirft. Man kann dabei, den Untersuchungen von Lie-Engel (45, S. 522) zufolge,

die z_i auf rationalem Wege finden, da sie Imprimitivitätssysteme von Γ bilden. Ist die Gruppe Γ transitiv, so kann man als die z_i rationale Funktionen von $x_1, x_2, \ldots, x_n$ nehmen. Im Gegenfalle hängen sie von einer Irrationalität θ ab, die von den Invarianten der Gruppe Γ abhängt. Fassen wir etwa z_i als rationale Funktion von $x_1, x_2, \ldots, x_n$ auf, so erzeugen alle mit z_i konjugierten Größen den mit $k[x_1, x_2, \ldots, x_n]$ zusammenfallenden Körper. Andererseits hängen diese Größen nur von $z_1, z_2, \ldots, z_k$ ab, da sie durch Ausübung der Transformationen der Gruppe $\mathfrak{G}$ erzeugt werden, während die Transformationen von $\mathfrak{G}$ in der Gruppe Γ auftreten, welche die z_i in Funktionen der z_i überführt. Daraus folgt, daß z_i einer Gleichung genügt, deren Koeffizienten nur von k Parametern abhängen, während die x_i sich durch die z_i rational ausdrücken.

10. Ist eine E. G. Γ der Gruppe $\mathfrak{G}$ mit einer k-Gruppe isomorph, aber nicht ähnlich, so kann man das Cartansche Prinzip anwenden, welches im folgenden besteht (14):

Sind zwei kontinuierliche Gruppen Γ und Γ_1 isomorph, so kann man die Gruppe Γ so erweitern, daß man die Gruppe Γ_1 erhält, indem man auf die gewissen Funktionen der erweiterten Gruppe entsprechenden Variablen die Transformationen von Γ ausübt.

Unter einer Erweiterung der Gruppe Γ versteht man folgendes. Sind $x_1, x_2, \ldots, x_n$ die der Gruppe Γ entsprechenden Variablen, so führe man neue Folgen

$$
\begin{array}{l}
x_1, \quad x_2, \quad \ldots, x_n, \\
x_1^{(1)}, \quad x_2^{(1)}, \quad \ldots, x_n^{(1)} \\
\ldots\ldots\ldots \cdot \ldots\ldots\ldots\ldots \\
x_1^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}
\end{array} \tag{4.5}
$$

von Variablen ein, so daß man die erweiterte Gruppe Γ' erhält, indem man auf jede Folge

$$x_1^{(\lambda)}, x_2^{(\lambda)}, \ldots, x_n^{(\lambda)} \qquad (\lambda = 0, 1, 2, \ldots, m-1)$$

gleichzeitig Transformationen der ursprünglichen Gruppe Γ ausübt.

Um in diesem Falle eine k-parametrige Resolvente zu bilden, führen wir statt der $x_1^{(\lambda)}, x_2^{(\lambda)}, \ldots, x_n^{(\lambda)}$ $(\lambda = 1, 2, \ldots, m-1)$ neue Veränderliche $\alpha_0^{(\lambda)}, \alpha_1^{(\lambda)}, \ldots, \alpha_{n-1}^{(\lambda)}$ nach den Formeln

$$
\begin{array}{l}
x_1^{(\lambda)} = \alpha_0^{(\lambda)} + \alpha_1^{(\lambda)} x_1 + \ldots + \alpha_{n-1}^{(\lambda)} x_1^{n-1}, \\
x_2^{(\lambda)} = \alpha_0^{(\lambda)} + \alpha_1^{(\lambda)} x_2 + \ldots + \alpha_{n-1}^{(\lambda)} x_2^{n-1}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x_n^{(\lambda)} = \alpha_0^{(\lambda)} + \alpha_1^{(\lambda)} x_n + \ldots + \alpha_{n-1}^{(\lambda)} x_n^{n-1}
\end{array} \qquad (\lambda = 1, 2, \ldots, m-1) \tag{4.6}
$$

ein. Ueben wir auf die Veränderlichen (4.5) die Transformationen U von Γ aus, so erleiden die $\alpha_i^{(\lambda)}$ gewisse Transformationen, die sich in die identische Transformation verwandeln, wenn man in der Rolle von U Transformationen von $\mathfrak{G}$ nimmt. Setzen wir diese Ausdrücke in eine der Funktionen

$$z_i(x_1, x_2, \ldots, x_n; x_1^{(1)}, x_2^{(1)}, \ldots, x_n^{(1)}; \ldots; x_1^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}),$$

etwa z_1, ein, welche eine Transformation einer k-Gruppe erleidet, wenn man auf die $x_i^{(\lambda)}$ die Transformationen von Γ ausübt, so hängen die Funktionen $z, z_1^{s_1}, \ldots, z_1^{s_{N-1}}$ nur von k Parametern ab, wobei $\mathfrak{G} = 1 + s_1 + \ldots + s_{N-1}$ ist. Da bei diesen Transformationen die Veränderlichen $\alpha_i^{(\lambda)}$ invariant bleiben, so können wir ihnen willkürliche rationale Zahlenwerte zuschreiben, indem man nur besorgt, daß die Differenzen $z_1^{s_i} - z_1$ $(i = 1, 2, \ldots, N-1)$ lauter von Null verschieden sind. Es entsteht dadurch eine Galoissche Resolvente mit k Parametern. Um aber zu einer k-parametrigen Gleichung überzugehen, die mit der Gleichung (4.1) durch eine Tschirnhausensche Transformation verbunden ist, brauchen wir, eine zu derjenigen Gruppe gehörige Funktion von den $z_1^{s_i}$ zu bilden, zu welcher etwa x_1 gehört.

11. Es ist nicht ausgeschlossen, daß der Uebergang von den x_i zu den Z_i nicht rational ist, sondern eine Irrationalität θ enthält, die von den Invarianten der erweiterten Gruppe Γ abhängt. Wir wollen die irreduzible Gleichung $R(\theta) = 0$, der θ genügt, *Nebenresolvente* nennen. Es entsteht die wesentliche Frage, ob nicht eine Nebenresolvente mehr wesentliche Parameter als die Gleichung (4.1) selbst enthält. Ich kann heute diese Frage allgemein nicht beantworten. Es ist nur bekannt, daß für symmetrische $\mathfrak{G}$ die Nebenresolvente 0-parametrig, also numerisch, und für alternierende $\mathfrak{G}$ höchstens 1-parametrig ist.

12. Nun beweisen wir den zweiten Teil des gestellten Satzes. Es seien $Z_1, Z_2, \ldots, Z_n$ sämtliche Wurzeln einer k-parametrigen Resolvente der Gleichung (4,1), welche in der Gestalt einer normalen Gleichung gegeben sein möge. Die Z_i sind Funktionen von $x_1, x_2, \ldots, x_n$, die zur Einheitsgruppe gehören. Ueben wir auf die x_i die Permutationen der Gruppe $\mathfrak{G}$ aus, so erleiden die Z_i gewisse Permutationen, die eine mit $\overline{\mathfrak{G}}$ isomorphe Gruppe bilden, die sich von $\mathfrak{G}$ nur durch eine andere Bezeichnung der Veränderlichen unterscheidet.

Wir fassen zunächst $Z_1, Z_2, \ldots, Z_n$ als unabhängige Veränderliche auf

und kleiden $\overline{\mathfrak{G}}$ mittels einer kontinuierlichen Gruppe Γ folgendermaßen ein: wir nehmen aus $\overline{\mathfrak{G}}$ ein System von Permutationen $A, B, \ldots$, die durch Komposition die ganze Gruppe $\overline{\mathfrak{G}}$ erzeugen. Wir fassen jede dieser Permutationen, etwa A, als eine lineare homogene Transformation auf und bringen sie in eine normale Gestalt:

$$u_i \to \varepsilon^{k_i} u_i \qquad (i = 1, 2, \ldots, n),$$

wo $\varepsilon = e^{\frac{2\pi i}{m}}$ eine Einheitswurzel ist und die u_i gewisse lineare Funktionen von $Z_1, Z_2, \ldots, Z_n$ bedeuten. Dann nehmen wir

$$u_i \to e^{k_i t} u_i \qquad (i = 1, 2, \ldots, n)$$

als eine der erzeugenden Transformationen der Gruppe Γ_1, die sich in A verwandelt, wenn wir darin $t = \frac{2\pi i}{m}$ setzen. Kehren wir zu den ursprünglichen Variablen $Z_1, Z_2, \ldots, Z_n$ zurück und verfahren so mit allen erzeugenden Transformationen $A, B, \ldots$, so erhalten wir eine kontinuierliche Gruppe Γ, die die Gruppe $\overline{\mathfrak{G}}$ einkleidet. Γ hat als lineare Gruppe der n Veränderlichen nur eine endliche Anzahl Parameter.

Nun fassen wir die Z_i als Funktionen von x_i auf und betrachten die x_i als Koordinaten eines Raumes $\mathfrak{R}$, wobei zwei Punkte $(x_1, x_2, \ldots, x_n)$ und $(x_1', x_2', \ldots, x_n')$ dann und nur dann als nicht verschieden betrachtet sein sollen, wenn

$$Z_i(x_1, x_2, \ldots, x_n) = Z_i(x_1', x_2', \ldots, x_n') \qquad (i = 1, 2, \ldots, n)$$

gilt. Da unter den Funktionen $Z_1, Z_2, \ldots, Z_n$ genau k funktional unabhängig sind, so hat der Raum $\mathfrak{R}$ k Dimensionen. Die Gruppe Γ induziert im Raume $\mathfrak{R}$ eine kontinuierliche Gruppe, die mit Γ „im kleinen isomorph“ ist (67) und die mit $\mathfrak{G}$ isomorphe Gruppe als Teiler enthält, da etwa Z_1 zur identischen Gruppe von $\mathfrak{G}$ gehört. Somit läßt $\mathfrak{G}$ eine k-Gruppe als E. G. zu, w. z. b. w.

13. Beim Beweise dieses Satzes ist es wesentlich, daß jedes Wertesystem der Parameter der Gruppe Γ eindeutig den Punkt des Raumes $\mathfrak{R}$ bestimmt. Demnach trifft für unsere Gruppe die Schreiersche Definition (67) zu, so daß hier die ganze Schreiersche Theorie anwendbar ist. Ist aber diese Bedingung nicht erfüllt, so können wir z. B. der Erscheinung begegnen, daß eine nicht zyklische Monodromiegruppe einer algebraischen

Funktion einer Veränderlichen eine eingliedrige kontinuierliche Gruppe als E. G. zuläßt. Zum Beispiel: die durch die Gleichungen

$$x+y+z=C_1, \quad x^2+y^2+z^2=C_2, \quad x^3+y^3+z^3=C_3$$

definierte kontinuierliche Gruppe enthält als Teiler die symmetrische Permutationsgruppe 3-ten Grades, die sogar nicht Abelsch ist.

14. Es sei eine endliche Gruppe $\mathfrak{G}$ ohne Zentrum gegeben. Wie kann man diejenigen ihrer E. G. bestimmen, welche im Raume von möglichst kleiner Dimensionszahl darstellbar sind? Um diese Frage zu beantworten, beachte man, daß jede der gesuchten kontinuierlichen Gruppen stets mit einer gewissen linearen homogenen Gruppe Γ „im kleinen isomorph" ist. Dabei muß Γ entweder $\mathfrak{G}$ selbst oder eine endliche Gruppe als Teiler enthalten, welche $\mathfrak{G}$ als Faktorgruppe in bezug auf ihr Zentrum enthält. Das folgt aus der Schreierschen Theorie der „im kleinen isomorphen Gruppen" (67), nach welcher alle „im kleinen isomorphen" Gruppen Faktorgruppen einer Ueberlagerungsgruppe in bezug auf diskrete Untergruppen sind, die im Zentrum der Ueberlagerungsgruppe liegen. Dann folgt aus den Untersuchungen von I. Schur (69, 70), daß man alle „Darstellungsgruppen" in Betracht ziehen muß. Ihre Anzahl ist bekanntlich endlich.

Diese Frage läßt eine ziemlich leichte Beantwortung zu, falls $\mathfrak{G}$ eine einfache Gruppe ist. Denn dann sind auch ihre E. G. einfach. Es folgt aber aus den Untersuchungen von W. Killing (40) und E. Cartan (13), daß es außer einer endlichen leicht angebbaren Anzahl von Ausnahmen nur drei verschiedene Typen einfacher Gruppen gibt: 1) volle unimodulare lineare Gruppen; 2) orthogonale Gruppen; 3) Komplexgruppen. Es ist außerdem bekannt (Cartan, 13) daß n-dimensionale Gruppen vom Typ 1) $(n-1)$-Gruppen und von den Typen 2), 3) $(n-2)$-Gruppen sind. Daraus folgt, daß man nur die linearen homogenen Gruppen von höchstens $n-1$ Dimensionen untersuchen muß, ob sie nicht $\mathfrak{G}$ einkleiden können, wobei n den Grad der Gleichung (4.1) bedeutet. Andererseits hat Wiman (91; vgl. auch R. Garver, 28) bewiesen, daß die alternierenden Gruppen n-ten Grades ($n \geqq 8$) nicht durch lineare homogene Substitutionen vom weniger als $(n-1)$-tem Grade darstellbar sind. Das erlaubt uns noch nicht, die Aufgabe der Auffindung von Resolventen mit weniger als $n-3$ Parameter als unmöglich anzusehen. Denn man muß nicht nur die Darstellbarkeit der alternierenden Gruppen selbst, sondern auch ihrer Darstellungsgruppen untersuchen. Wir haben uns am Beispiel $n=6$ überzeugt, daß dies manchmal die Parameterzahl der

Resolvente zu erniedrigen erlaubt. Indessen muß ich noch einmal ausdrücklich betonen, daß die Sylvester-Hilbert-Wimansche Aufgabe, die für $n \geqq 9$ die Reduktion mindestens um 5 Parameter ergibt, nicht als einen speziellen Fall des Kleinschen Problems betrachtet werden kann. Mit anderen Worten, wir können a priori nicht behaupten, daß eine Parameterreduktion, die mit Hilfe elner Kette von Resolventen gelungen ist, auch mit Hilfe nur einer Resolvente geschehen muß. Der für die klassische Galoissche Theorie gültige Satz von den natürlichen Irrationalitäten kann nicht unmittelbar auf das Resolventenproblem erweitert werden. Die Erledigung der Frage nach den Ketten von Resolventen erfordert ein eingehendes Studium des Resolventenproblems im Falle, wo die Koeffizienten der Gleichung (4.1) nicht frei, sondern durch einige Relationen verbunden sind. (Vgl. § 5, N 8). Dann kann es eintreten, daß die sich einzukleidende endliche Gruppe nicht mit der Monodromiegruppe der Gleichung (4.1) zusammenfällt. Wir haben in N° 13 ein Beispiel dieser Erscheinung gesehen.

15. Das Einkleidungsproblem von endlichen Gruppen durch kontinuierliche ist auch von selbstständigem Interesse. Ich kann bis jetzt nicht aussagen, ob eine endliche Gruppe eine endliche oder eine unendliche Anzahl nicht isomorpher kontinuierlicher Gruppen als E. G. zuläßt. Es ist für die Lösung dieser Aufgabe die Darstellungstheorie von kontinuierlichen Gruppen von Nutzen (Cartan, 13; Schur, 71; R. Brauer, 8; H. Weyl, 88). Es ist aber sehr ungünstig, daß jede kontinuierliche Gruppe unendlich viele irreduzible lineare homogene Darstellungen zuläßt.

Die Umkehrung dieser Aufgabe wurde schon seit langem gestellt. Das ist das Problem der Aufsuchung von allen endlichen Gruppen, die in einer gegebenen kontinuierlichen Gruppe enthalten sind. C. Jordan (39) hat für dieses Problem folgenden fundamentalen Satz bewiesen;

Jede kontinuierliche lineare homogene Gruppe Γ enthält nur solche nicht isomorphe endliche Untergruppen $\mathfrak{G}$, deren Faktorgruppen in bezug auf Abelsche Normalteiler zu einer endlichen für jede Gruppe Γ angebbaren Anzahl von endlichen Gruppen gehört.

§ 5. Weitere Fragen der allgemeinen Körpertheorie

1. Die Fragen der algebraischen Zahlkörpertheorie, die die algebraischen Zahlen in bezug auf ihre Rationalität betrachten, sind meistens durch die Methoden der Galoisschen Theorie lösbar. Enthalten aber die zu untersuchenden Körper gewisse transzendente (veränderliche) Grössen,

so lassen die diesen Körpern entsprechenden Strukturfragen nicht eine unmittelbare gruppentheoretische Einkleidung zu. Wenn ich nichtsdestoweniger diese Fragen in den Galoisschen Ideenkreis einschließe, so mache ich dies aus folgenden Gründen: Es ist erstens nicht naturgemäß, die Galoissche Theorie als denjenigen Ideenkreis zu definieren, dessen Probleme mit Hilfe der Galoisschen Gruppe gelöst werden können, da die Galoissche Gruppe ein Lösungsmittel ist, während sogar dieselben Probleme mit Hilfe wesentlich verschiedener Mittel lösbar sein können, so daß ein Lösungsmittel keineswegs geeignet ist, ein Wissenschaftsgebiet abzugrenzen. Zweitens können wir von vornherein nicht sagen, ob ein zu untersuchendes Problem nicht mit Hilfe eines zweckmäßig eingeführten Begriffes der Galoisschen Gruppe gelöst werden kann. Es ist vielmehr zweckmäßiger, die Galoissche Theorie als den Problemenkreis zu definieren, dessen Probleme sich mit der rationalen Abhängigkeit von Körpern und einzelnen Körpergrößen beschäftigen.

2. *Identität von zwei algebraischen Körpern.* Ein Körper ist keineswegs durch seine Galoissche Gruppe bestimmt. Man kann vielmehr verschiedene Körper mit isomorphen Gruppen aufstellen. Die Frage nach der Identität von Körpern liegt also eigentlich außer dem Rahmen der Galoisschen Theorie. Ist K ein Zahlkörper, so ist diese Frage im wesentlichen zahlentheoretisch. Ihre Beantwortung wäre am besten dadurch geleistet, daß wir ein vollständiges Invariantensystem von Zahlkörpern aufstellen. Für dieses letztere Problem sind zwei Methoden bekannt. Die eine folgt aus der Dedekind-Frobeniusschen Theorie (vgl. § 3). Diese Methode ist unbequem wegen der unendlichen Anzahl von Invarianten, die miteinander durch wenig bekannte Relationen verbunden sind. — Die zweite Methode beruht auf dem Verhalten der Körperdiskriminanten. Es gibt nur eine endliche Anzahl von Körpern mit gegebener Körperdiskriminante. Es ist aber kein Invariantensystem dieser Art bekannt, welches den Körper eindeutig bestimmt. Außerdem kann die Körperdiskriminante nicht jeden ganzzahligen Wert annehmen, und wir wissen bis heute nicht, welche Zahlenwerte sie annehmen kann.

3. Es gibt dennoch eine rein algebraische Methode für die Lösung des Identitätsproblems. Sind K und K_1 die zu untersuchenden Körper, deren Gruppen mit $\mathfrak{G}$ isomorph sind, so hat das Kompositum KK_1 im allgemeinen das direkte Produkt $\mathfrak{G} \times \mathfrak{G}$ als Galoissche Gruppe. Haben aber K und K_1 einen nicht rationalen Durchschnitt, so verwandelt sich die Gruppe von KK_1 in einen echten Teiler von $\mathfrak{G} \times \mathfrak{G}$. Sind insbesondere K und K_1 identisch, so ist die Gruppe von KK_1 mit $\mathfrak{G}$ iso-

morph. Daraus kann man ein brauchbares Kriterium der Identität von K und K_1 herleiten. Sind nämlich

$$(5.1) \qquad x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0,\ y^n + b_1 y^{n-1} + \ldots + b_{n-1} y + b_n = 0$$

die Gleichungen, deren einzelne Wurzeln die Körper K bzw. K_1 erzeugen, so ist $K = K_1$ dann und nur dann, wenn eine der Größen

$$x_1^k y_1 + x_2^k y_2 + \ldots + x_n^k y_n \qquad (k = 1, 2, \ldots, n-1)$$

rational ist, wobei $x_1, x_2, \ldots, x_n$ und $y_1, y_2, \ldots, y_n$ sämtliche Wurzeln der Gleichungen (5.1) bedeuten. Jede der Größen $x_1^k y_1 + x_2^k y_2 + \ldots + x_n^k y_n$ genügt einer Gleichung vom Grade $n!$, deren Koeffizienten man rational durch die a_i, b_i ausdrücken kann. Die Körper K und K_1 sind dann und nur dann identisch, wenn diese Gleichung wenigstens eine rationale Wurzel besitzt. Hat dabei $\mathfrak{G}$ bekannte Normalteiler, so kann man den Grad dieser („gemischten") Gleichung mit Hilfe gemischter Resolventen erniedrigen (78).

4. Wir betrachten näher die Fälle $n = 3$ und $n = 4$. Sind

$$x^3 + p x + q = 0, \qquad y^3 + \bar{p} y + \bar{q} = 0$$

die zu untersuchenden Gleichungen, so muß erstens das Produkt ihrer Diskriminanten ein vollständiges Quadrat sein. Die Größe $z = x_1 y_1 + x_2 y_2 + x_3 y_3$ genügt einer der gemischten Gleichungen

$$z^3 - 3 p \bar{p} z - \frac{27}{2} q \bar{q} \pm \sqrt{D \bar{D}} = 0 .$$

Ist z eine ihrer rationalen Wurzeln, und ist $z^2 - p \bar{p} \neq 0$, so kann man die Koeffizienten des rationalen Uebergangs $y = \alpha_0 + \alpha_1 x + \alpha_2 x^2$ aus den Gleichungen

$$3 \alpha_0 - 2 p \alpha_2 = 0,\ -2 p \alpha_1 - 3 q \alpha_2 = z,\ -2 p \alpha_0 - 3 q \alpha_1 + 2 p^2 \alpha_2 = u$$

bestimmen, wobei $u = x_1^2 y_1 + x_2^2 y_2 + x_3^2 y_3 = \dfrac{3 (q \bar{p} z - p^2 \bar{q})}{z^2 - p \bar{p}}$ ist.

Nun gehen wir zu dem Fall $n = 4$ über. Sind

$$x^4 + p_2 x^2 + p_3 x + p_4 = 0,\ \bar{x}^4 + \bar{p}_2 \bar{x}^2 + \bar{p}_3 \bar{x} + \bar{p}_4 = 0$$

die zu untersuchenden Gleichungen, so lösen wir das Problem zunächst für die kubischen Gleichungen

$$z^3 - p_2 z^2 - 4 p_4 z - p_3^2 + 4 p_2 p_4 = 0, \quad \bar{z}^3 - \bar{p}_2 \bar{z}^2 - 4 \bar{p}_4 z - \bar{p}_3^2 + 4 \bar{p}_2 \bar{p}_4 = 0,$$

denen bekanntlich die Größen $z = x_1 x_2 + x_3 x_4$ bzw. $\bar{z} = \bar{x}_1 \bar{x}_2 + \bar{x}_3 \bar{x}_4$ genügen. Führen wir dann die Bezeichnungen

$$\zeta = z_1 \bar{z}_1 + z_2 \bar{z}_2 + z_3 \bar{z}_3, \quad u = z_1^2 \bar{z}_1 + z_2^2 \bar{z}_2 + z_3^2 \bar{z}_3, \quad \bar{u} = z_1 \bar{z}_1^2 + z_2 \bar{z}_2^2 + z_3 \bar{z}_3^2$$

ein, so muß die Gleichung

$$F(T) = T^4 - (2 p_2 \bar{p}_2 + 2\zeta) T^2 - 8 p_3 \bar{p}_3 T - \tfrac{1}{3} \zeta^2 - \tfrac{8}{3} p_2 \bar{u} - \tfrac{8}{3} \bar{p}_2 u + \\ + \tfrac{14}{3} p_2 \bar{p}_2 \zeta + p_2^2 \bar{p}_2^2 + 16 p_2^2 \bar{p}_4 + 16 \bar{p}_2^2 p_4 + \tfrac{64}{3} p_4 \bar{p}_4 = 0$$

mindestens eine rationale Wurzel haben. Ist dabei $F'(T) \neq 0$, so kann man die Koeffizienten $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ des Uebergangs $\bar{x} = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3$ aus den Gleichungen

$$4\alpha_0 - 2p_2 \alpha_2 - 3p_3 \alpha_3 = 0, \quad -2p_2 \alpha_1 - 3p_3 \alpha_2 + (2p_2^2 - 4p_4) \alpha_3 = T,$$
$$-2p_2 \alpha_0 - 3p_3 \alpha_1 + (2p_2^2 - 4p_4) \alpha_2 + 5p_2 p_3 \alpha_3 = \theta,$$
$$3p_3 \alpha_0 + (2p_2^2 - 4p_4) \alpha_1 + 5p_2 p_3 \alpha_2 + (-2p_2^3 + 3p_3^2 + 6p_2 p_4) \alpha_3 = Z$$

bestimmen, wobei ist:

$$\theta = x_1^2 \bar{x}_1 + x_2^2 \bar{x}_2 + x_3^2 \bar{x}_3 + x_1^2 \bar{x}_1,$$

$$Z = x_1^3 \bar{x}_1 + x_2^3 \bar{x}_2 + x_3^3 \bar{x}_3 + x_4^3 \bar{x}_4 .$$

5. Ist K ein algebraischer Funktionskörper, so läßt die Galoissche Theorie keine Anwendung auf die Lösung des Identitätsproblems zu. Besitzt K nur eine unabhängige Variable, so ist das Problem mit Hilfe funktionentheoretischer Mittel gelöst. Ist nämlich sein Geschlecht $p > 1$, so wird K durch $3p-3$ unabhängige kontinuierliche Parameterwerte bestimmt. Für die solche Körper erzeugenden Gleichungen sind Normalformen bekannt. Finden wir für jeden der zu vergleichenden Körper je eine Normalform, so wird das Problem durch ihre Zusammenstellung gelöst (3, S. 90—92).

Hängt K von mehreren unabhängigen Veränderlichen ab, so ist das Problem im allgemeinen unerledigt. Die alten deutschen und die italienischen Geometer haben in diesem Gebiete mehrere außerordentlich wichtige Resultate erhalten. Dennoch fürchte ich, daß wir darüber noch heute folgende Phrase wiederholen müssen, die im Züricher Vortrag von F. Enriques enthalten ist (19):

«Malheureusement la plupart de ces problèmes demeurent aujourd'hui sans réponse, et les contributions qu'on a portées dans ce champ de recherches ressemblent en vérité à de rares flambeaux au milieu d'une obscurité épaisse.»

6. *Rationale Minimalbasis.* Betrachten wir den Körper K_n aller rationalen Funktionen von n unabhängigen Veränderlichen $x_1, x_2, \ldots, x_n$, so entsteht die Frage nach allen möglichen Typen seiner Unterkörper. Man kann leicht „triviale Typen" solcher Unterkörper aufstellen: man nehme nämlich eine Anzahl $m \leqq n$ funktional unabhängiger Elemente von K_n (d. h. rationaler Funktionen von $x_1, x_2, \ldots, x_n$) als erzeugende Elemente eines Unterkörpers. Der auf diese Weise gebildete Körper ist offenbar entweder mit K_n oder mit dem Körper K_m der rationalen Funktionen von m ($m < n$) Veränderlichen isomorph. Man kann aber die Existenz von anderen Körpern erwarten: man nehme als erzeugende Elemente eines Unterkörpers irgendwelche Elemente von K_n, die miteinander durch algebraische Relationen verbunden sein können. Es entsteht die Frage, ob die „trivialen" Typen von Unterkörpern alle möglichen Typen erschöpfen. Mit anderen Worten, fragt man nach der Existenz eines Systems unabhängiger Elemente des Unterkörpers, durch welche alle Elemente dieses Unterkörpers rational darstellbar sind. Ein solches System nennt man *rationale Minimalbasis.*

Diese Frage wurde für $n = 1$ von Lüroth (48; vgl. auch E. Netto, 53) bejahend beantwortet. G. Castelnuovo (15) hat dieses Resultat auf den Fall $n = 2$ erweitert. Sein Beweis beruht auf den Methoden der algebraischen Geometrie. Für den Fall $n = 3$ haben G. Fano (21) und F. Enriques (20) ein Gegenbeispiel gefunden, indem sie einen Unterkörper der Körpers der rationalen Funktionen von drei Veränderlichen aufgestellt haben, welcher keine rationale Minimalbasis besitzt.

Das Problem der rationalen Minimalbasis hat eine Anwendung in der klassischen Galoisschen Theorie, nämlich in der Frage nach der Existenz von Körpern mit vorgeschriebener Galoisscher Gruppe (§ 2). Um diese letztere Frage zu beantworten, ist es nötig, das Problem der rationalen Minimalbasis nur für den Fall zu lösen, daß der zu untersuchende Unter-

körper den Körper der elementar-symmetrischen Funktionen eines Systems erzeugender Elemente von K_n enthält. Bei dieser Beschränkung ist das Problem der rationalen Minimalbasis weder erledigt noch widerlegt (vgl. 74).

Dieses Problem kann auch als Problem der Identität von Körpern aufgefaßt werden. Denn sind unter den erzeugenden Elementen eines Unterkörpers $\overline{K}$ von K_n etwa m ($m \leqq n$) funktional unabhängig, so wird die Frage darauf zurückgeführt, die Identität (genauer: Isomorphismus) von $\overline{K}$ und K_m nachzuweisen.

7. *Einfachste Auflösung von Gleichungen mit mehreren Veränderlichen.* Es sei ein Körper K der rationalen Funktionen von n Veränderlichen $x_1, x_2, \ldots, x_n$ gegeben, zwischen denen eine algebraische Relation $f(x_1, x_2, \ldots, x_n) = 0$ besteht (der Fall mehrerer Relationen kann sehr leicht auf diesen Fall zurückgeführt werden). Man soll neue erzeugende Größen $y_1, y_2, \ldots, y_n$ von K so wählen, daß die zwischen den y_i bestehende Gleichung von möglichst niedrigem Grade in bezug auf eine von ihnen, etwa von y_1, ist. Was kann man von dieser Gradzahl sagen?

Diese Frage wurde von Enriques (19) am ersten internationalen Mathematiker-Kongreß (Zürich, 1897) ausführlich behandelt. Ich erlaube mir, einige der dort betrachteten schönen Resultate zu wiederholen.

1) Wir fassen x_1, x_2 als Veränderliche und $x_3, x_4, \ldots, x_n$ als Parameter auf. Ist das Geschlecht der Gleichung $f(x_1, x_2) = f(x_1, x_2, x_3, \ldots, x_n) = 0$ beständig gleich Null, so kann man eine Veränderliche t derart auswählen, daß x_1, x_2 sich rational durch $t, x_3, x_4, \ldots, x_n$ und eine Quadratwurzel einer rationalen Funktion von $x_3, x_4, \ldots, x_n$ ausdrücken (M. Noether, 56).

Ist $n = 3$, so kann man sich durch zweckmäßige Wahl von t auch von der quadratischen Irrationalität befreien.

Man kann vermuten, daß dieser Satz von Bedeutung für die Auffindung von Körpern mit vorgeschriebener Gruppe $\mathfrak{G}$ ist. Das letztere Problem scheint leichter lösbar zu sein, wenn die Gruppe $\mathfrak{H}/\mathfrak{G}$ von ungerader Ordnung ist, wobei $\mathfrak{H}$ den *Holomorph* der Gruppe $\mathfrak{G}$ bedeutet.

2) Ist das Geschlecht p der Gleichung $f(x_1, x_2) = 0 > 1$, so kann der Körper K durch Adjunktion einer Irrationalität vom Grade $\leqq 2p - 2$ gelöst werden.

Nur im Falle $p = 1$ kann man die obere Grenze für den Grad dieser Irrationalität nicht von vornherein angeben.

8. *„Wahrer Transzendenzgrad" eines Oberkörpers.* Es sei ein Körper

k der rationalen Funktionen von $u_1, u_2, \ldots, u_n$ gegeben, die miteinander eventuell durch eine algebraische Relation

$$f(u_1, u_2, \ldots, u_n) = 0 \tag{5.2}$$

verbunden sein können. Es sei außerdem ein Oberkörper K von demselben Transzendenzgrad gegeben, dessen erzeugende Größen $x_1, x_2, \ldots, x_n$ mit den u_i durch die Gleichungen

$$\varphi_1(x_1, x_2, \ldots, x_n) = u_1, \varphi_2(x_1, x_2, \ldots, x_n) = u_2, \ldots, \varphi_n(x_1, x_2, \ldots, x_n) = u_n \tag{5.3}$$

verbunden sind. Man finde einen Unterkörper K_1 von K derart, daß
1) das Kompositum von K_1 und k genau den Körper K ergibt;
2) der Transzendenzgrad von K_1 möglichst klein ist.

Den Transzendenzgrad von K_1 wollen wir den wahren Transzendenzgrad von K/k nennen. Es ist ersichtlich, daß jedes Problem der Körpertheorie wesentlich vereinfacht wird, wenn man den Transzendenzgrad eines zu untersuchenden Körpers vermindert. Darin liegt die Bedeutung dieses Problems.

Dieses Problem verwandelt sich als Spezialfall in das sogenannte Resolventenproblem (§ 4). Um zum Resolventenproblem überzugehen, muß man die Gleichungen (5.3) folgendermaßen spezialisieren:

$$x_1 + x_2 + \ldots + x_n = -u_1, x_1 x_2 + \ldots + x_{n-1} x_n = u_2,$$
$$\ldots, x_1 x_2 \ldots x_n = (-1)^n u_n .$$

Die x_i sind mit anderen Worten die Wurzeln der Gleichung

$$x^n + u_1 x^{n-1} + \ldots u_{n-1} x + u_n = 0 ,$$

während k durch $u_1, u_2, \ldots, u_n$ und eine zu einer gegebenen Permutationsgruppe $\mathfrak{G}$ gehörende Funktion Φ erzeugt wird, die mit den u_i durch eine leicht angebbare Gleichung verbunden ist.

Das Resolventenproblem und seine Erweiterung — das Problem nach den Ketten von Resolventen — sind zugleich extreme Aufgaben der klassischen Galoisschen Theorie. Das Resolventenproblem läßt eine Lösung zu mit Hilfe der kontinuierlichen Gruppentheorie (§ 4).

9. *Rationalitätsfragen für die Perioden elliptischer und Abelscher Integrale.* Wir betrachten zunächst den Fall eines elliptischen Gebildes.

Es sei ein algebraischer Funktionskörper $K(x, y)$ gegeben, wobei zwischen x und y die Gleichung

$$y^2 - (1 - x^2)(1 - k^2 x^2) = 0 \tag{5.4}$$

besteht. Dann kann man x und y bekanntlich durch elliptische Funktionen

$$x = sn(u, k), \quad y = cn(u, k)\, dn(u, k) \tag{5.5}$$

uniformisieren. Es sei außerdem auf dem Gebilde (5.4) ein Punkt (x_0, y_0) gegeben, der dem Werte $u = u_0$ des Arguments u entspricht:

$$x_0 = sn(u_0, k), \quad y_0 = cn(u_0, k)\, dn(u_0, k) .$$

u_0 ist eindeutig bis auf ein ganzzahliges Vielfaches der Perioden $4K$, $4K'$ bestimmt. Es ist zu entscheiden, ob u_0 ein rationales Vielfaches von $4K$, $4K'$ ist.

Diese Aufgabe kann auch als Aufgabe der klassischen Galoisschen Theorie formuliert werden. In der Tat, wir können annehmen, k, x_0, y_0 seien algebraische Zahlen, da dieser Fall allein Schwierigkeiten bietet. Wir nehmen noch an, der Rationalitätsbereich R enthalte den Modul k. Ist $u_0 \equiv \dfrac{m K + m' K'}{n} \pmod{4K, 4K'}$, wobei m, m', n ganze rationale Zahlen sind, so genügt $x_0 = sn\left(\dfrac{m K + m' K'}{n}, k\right)$ einer sogenannten Teilungsgleichung

$$\Phi_n(x_0, k) = 0 , \tag{5.6}$$

die bei veränderlichem k irreduzibel ist, kann aber innerhalb R zerfallen, wenn k gewisse Zahlenwerte annimmt. Es sei nun $f(x_0) = 0$ die irreduzible Gleichung, der x_0 genügt. Die Frage ist, ob es Werte von n gibt, bei denen $\Phi_n(x, k)$ durch $f(x)$ teilbar ist.

10. Bezeichnen wir die Punkte der Riemannschen Fläche, für welche $sn\, u = sn\, u_0$ gilt, mit P_1 und P_2, so kann unsere Bedingung folgendermaßen aufgefaßt werden:

$$n\, u(P_1) - n\, u(P_2) \equiv 0 \pmod{4K, 4K'} ,$$

wobei $u(P)$ das Integral erster Gattung ist. Daraus folgt nach dem Abelschen Theorem, daß es eine Funktion $\varphi(x, y)$ des Körpers $K(x, y)$ gibt, die in P_1 eine einzige n-fache Null und in P_2 einen einzigen n-fachen

Pol hat. Man kann auch sagen, daß das Ideal $\frac{P_1^n}{P_2^n}$ ein Hauptideal ist. Dann kann man φ durch Primfunktionen ausdrücken, d. h. in der Gestalt $\varphi = e^{n \cdot \Pi(P_1, P_2)}$ darstellen, wobei $\Pi(P_1, P_2)$ das Integral dritter Gattung mit den Residuen $+ 2\pi i$ in P_1 und $- 2\pi i$ in P_2 bedeutet.

Man kann die Funktion z zweiter Ordnung aufstellen, die in P_1 und P_2 unendlich wird (dazu setze man z. B. nach Zolotareff $z = \frac{sn^2(u, k)}{sn^2(u, k) - sn^2(u_0, k)}$). Dann wird $\Pi(P_1, P_2)$ in die Gestalt

$$\int \frac{z + A}{\sqrt{z(z-1)(z-\alpha)(z-\beta)}}\, dz$$

gebracht, wobei $\alpha = \frac{1}{dn^2 u_0}$, $\beta = \frac{1}{cn^2 u_0}$ ist, und es handelt sich darum zu erkennen, ob dieses Integral (bei geeignetem Werte von A, dessen Wahl der Normierung der Perioden in $\Pi(P_1, P_2)$ entspricht) durch Logarithmen integrierbar ist oder nicht.

11. Diese Frage wurde zum erstenmal von Abel (1) gestellt. Abel löste dieses Problem auf algebraischem Wege, indem er die Tatsache benutzte, daß $\varphi = \frac{P_1^n}{P_2^n}$ eine *funktionale Einheit* ist, d. h. daß die Norm von φ etwa Konstante ist, und die sich für $\varphi = \frac{p + q\sqrt{R}}{p - q\sqrt{R}}$ ergebende Diophantische Gleichung $p^2 - q^2 R = 1$ mit Hilfe der Kettenbruchentwicklung von $\sqrt{R(x)}$ zu lösen suchte. Damit dies möglich sei, ist notwendig und hinreichend, daß die Kettenbruchentwicklung von $\sqrt{R(x)}$ periodisch ist. Diese Periodizität kann aber nicht ohne weiteres nach einer endlichen Anzahl von Schritten bestätigt oder widerlegt werden. Es war dazu notwendig, für die mögliche Periode eine obere Schranke anzugeben. Diese Aufgabe wurde von P. Tchebycheff (77) für den Fall rationaler Koeffizienten von $R(x)$ und von G. Zolotareff (92) für allgemeine reelle $R(x)$ erledigt.

Tchebycheff und Zolotareff ermitteln dies Resultat, indem sie auf die Veränderlichen folgende Transformationen:

(I) $u \to u + u_0$, $k \to k$, $u_0 \to 2u_0$, $\alpha \to \left(\frac{\beta + \alpha - 1}{1 + \beta - \alpha}\right)^2$, $\beta \to \left(\frac{\beta + \alpha - 1}{1 + \alpha - \beta}\right)^2$,

(II) $u \to (1 + k')u$, $k \to \frac{1 - k'}{1 + k'}$, $\alpha \to \left(\frac{\sqrt{(\beta - \alpha)(\beta - 1)} - \sqrt{\alpha}}{1 + \alpha - \beta}\right)^2$,

$\beta \to \left(\frac{\sqrt{(\beta - \alpha)(\beta - 1)} + \sqrt{\alpha}}{1 + \alpha - \beta}\right)^2$

nach und nach ausüben. Die Transformation (II) hat den Zweck, ein gerades n in ein ungerades n überzuführen, und ist nichts anderes als die Landensche Transformation. Liegt nach einigen Schritten die Größe $\frac{2\sqrt{k}}{1+k}$ nicht im Körper $K(\alpha, \beta)$, so ist das ein Merkmal dafür, daß das auf diese Weise transformierte Integral einem ungeraden n entspricht. Dann muß man die Transformation (I) anwenden. Die Antwort ist positiv, wenn die Folge dieser Transformationen eine Periode aufweist. Andererseits zeigen schon nach einer endlichen Anzahl von Schritten gewisse Teilbarkeitsbedingungen, daß die Aufgabe unmöglich ist.

12. Die Frage nach der Kommensurabilität elliptischer Integrale ist noch auf einen ganz anderen Zweig der Mathematik, nämlich auf eine Frage der Diophantischen Analysis anwendbar. Es sei eine Gleichung

$$f(x, y) = 0 \tag{5.7}$$

gegeben, deren Koeffizienten einem algebraischen Zahlkörper K angehören und deren Geschlecht $p = 1$ ist. Es handelt sich um die Existenz der Werte x_0, y_0, die der Gleichung (5.7) genügen und im Körper K enthalten sind. Sie seien kurz rationale Punkte der Kurve (5.7) genannt. Man kann die Gleichung (5.7) in die Gestalt

$$y^2 = 4x^3 - g_2 x - g_3 \tag{5.8}$$

transformieren, indem man nötigenfalls den Körper K erweitert. Die Kurve (5.8) kann folgendermaßen parametrisch dargestellt werden:

$$x = p(u), \quad y = p'(u) . \tag{5.9}$$

Entsprechen einige Werte u_1, u_2 des Arguments u rationalen Punkten von (5.8), so folgt aus dem Additionstheorem, daß auch die $u_1 \pm u_2$ rationalen Punkten entsprechen. Die Argumente der rationalen Punkte der Kurve (5.8) bilden mit anderen Worten einen *additiven Modul*, den wir im folgenden *K-Rationalitätsmodul* nennen wollen. H. Poincaré (59) hat vermutet und L. J. Mordell (51) hat bewiesen, daß jeder Rationalitätsmodul eine endliche Basis besitzt.

Ist $(u_1, u_2, \ldots, u_n)$ eine solche Basis, so entsteht die Frage nach der Struktur der durch diese Basis erzeugten additiven Abelschen Gruppe $\mathfrak{A}$. Da man jeden Wert des Arguments u modulis ω_1, ω_2 reduzieren kann, wo ω_1, ω_2 die Perioden von $p(u), p'(u)$ sind, so ist die Anzahl unab-

hängiger erzeugender Elemente unendlicher Ordnung *(Rang)* dieser Gruppe dann und nur dann gleich n, wenn es zwischen den u_i keine Kongruenz der Gestalt

$$(5.10) \qquad m_1 u_1 + m_2 u_2 + \ldots + m_n u_u \equiv 0 \pmod{\omega_1, \omega_2}$$

gibt, wobei die m_i ganze rationale Zahlen sind. Im allgemeinen besteht aber die Basis von $\mathfrak{A}$ aus einer Anzahl ϱ der Elemente $A_1, A_2, \ldots, A_\varrho$ von unendlicher Ordnung und einer Anzahl der Elemente $B_1, B_2, \ldots, B_\sigma$ $(\varrho + \sigma \leqq n)$ von endlichen Ordnungen. Die Zahl ϱ heißt nach Kronecker *Rationalitätsrang* des Systems $u_1, u_2, \ldots, u_n \pmod{\omega_1, \omega_2}$, d. h. die größte Anzahl von rational unabhängigen Elementen. Das Zolotareffsche Verfahren ermöglicht uns, den Rationalitätsrang im Falle $n = 1$ zu bestimmen[2]), und läßt hoffentlich eine unmittelbare Erweiterung auf den allgemeinen Fall zu.

13. Man kann die aus diesen Ueberlegungen entstehenden Aufgaben folgendermaßen formulieren:

I. Man finde eine Methode zur Unterscheidung, ob der durch die Gleichungen $sn\, a = x_0, cn\, a \,.\, dn\, a = y_0$ (oder: $p(a) = x_0, p'(a) = y_0$) definierte Wert a des Arguments u mit den Perioden kommensurabel ist oder nicht.

Es handelt sich nur darum, die Frage für den Fall zu erledigen, daß die Landensche Transformation einer gegebenen elliptischen Funktion periodisch ist. Dieser Fall tritt nicht ein, wenn die Kurve (5.4) (oder (5.8)) reell ist.

II. Man bestimme den Rationalitätsrang eines Moduls $(u_1, u_2, \ldots, u_n) \pmod{\omega_1, \omega_2}$, wobei die u_i aus den Gleichungen $p(u_i) = x_i, p'(u_i) = y_i$ zu bestimmen sind und ω_1, ω_2 die Perioden der elliptischen Funktion $p(u)$ bedeuten.

III. Es seien ein elliptischer Funktionskörper (etwa durch Angabe des Moduls k) und ein die Größe k enthaltender algebraischer Zahlkörper K gegeben. Man finde eine Basis des entsprechenden K-Rationalitätsmoduls. Ist eine Basis $(u_1, u_2, \ldots, u_n)$ (durch explizite Angabe der Werte von $p(u_i)$) gegeben, so entscheide man, ob sie eine Basis des K-Rationalitätsmoduls ist oder nicht.

14. Man kann die Formulierungen der soeben erwähnten Aufgaben ohne große Mühe auf allgemeinere Körper algebraischer Funktionen

[2]) *T. Nagell* (52, S. 96, Z. 10—11 v. o.) meint, «on n'a pas de méthode générale pour reconnaître si l'argument d'un point donné (x, y) est commensurable avec une période ou non.» Tatsächlich ist diese Aufgabe in den erwähnten Zolotareffschen Untersuchungen gelöst.

übertragen. Zunächst liegt es nahe, daß die Frage nach der Endlichkeit einer algebraisch angegebenen Transformation der in § 1, N° 9 beschriebenen „Jacobischen Gruppe“ mit der Frage nach der Integrabilität der Abelschen Integrale durch Logarithmen nahe verwandt ist. Andererseits kann man die Ueberlegungen des N° 10 ohne weiteres auf den allgemeinen Fall übertragen. Dies zeigt, daß auch zwischen der Jacobischen Gruppe und der Idealklassengruppe eines algebraischen Funktionskörpers ein gewisser Zusammenhang besteht. Andererseits ist mit diesem Problem die Frage nach den funktionalen Einheiten verbunden.[3])

A. Weil (87) hat mit Hilfe einer ähnlichen Methode Diophantische Gleichungen $f(x, y) = 0$ bei beliebigem p untersucht. Er hat insbesondere das Mordellsche Resultat über die Endlichkeit von K-Rationalitätsmoduln auf beliebige $p \geqq 1$ erweitert. Dazu benutzte er die Jacobische Gruppe, während Mordell (51) implizite die Teilung der elliptischen Funktionen benutzte.

15. Das Diophantische Problem kann als Spezialfall des Hilbert-Doergeschen Irreduzibilitätsproblems betrachtet werden:

Es sei eine Gleichung $f(z, t) = 0$ gegeben. Man finde alle Werte t_i von t, bei welchen $f(z, t_i)$ ein in einem vorgegebenen Zahlkörper k reduzibles Polynom ist.

Nach K. Doerge folgt aus den Untersuchungen von Weil (87), daß es bei $p > 1$ nur dann unendlich viele Werte dieser Art von t gibt, wenn $f(z, t)$ sich nach einer gewissen Substitution der Gestalt

$$t = c_{-m} u^{-m} + c_{-m+1} u^{-m+1} + \ldots + c_0 + c_1 n + \ldots + c_m u^m$$

in ein identisch zerfallendes Polynom von z und u verwandelt[4]).

Die in Rede stehende Arbeit von Doerge ist dem Fall gewidmet, daß z eine funktionale Einheit ist. Dann erhält Doerge sehr einfache Bedingungen dafür, daß $f(z, t)$ nur bei einer endlichen Anzahl der Werte von t in k reduzibel wird. Es ist bemerkenswert, daß sich dadurch ein neuer unmittelbarer Zusammenhang zwischen den Diophantischen Gleichungen und den funktionalen Einheiten ergibt.

(Eingegangen den 12. September 1932)

---

[3]) Auf diesen Zusammenhang hat mich mein hochverehrter Lehrer Prof. Dr. D. Grave aufmerksam gemacht. Vergl. z. B. Verh. Russ. Math. Kongreß in Moskau (1927), S. 215 (russisch).

[4]) Zusatz bei Korrektur. In dieser Richtung hat C. R. Siegel (Abh. preuss. Akad., Berlin, 1930, N° 1) wesentliche neue Resultate erhalten.

Literatur

1. *N. H. Abel,* Sur l'intégration de la formule etc. Oeuvres, Christ. 1881, Tome I, S. 104—144.
2. *E. Artin,* Beweis des allgemeinen Reziprozitätsgesetzes. Hamb. Abh. 5 (1927), S. 353—363.
3. *R. Baer,* Abbildungseigenschaften algebraischer Erweiterungen. Math. Zeitschrift 33 (1931), S. 451—479.
4. *H. F. Baker,* Abel's Theorem and the allied Theory etc. Cambridge 1897.
5. *M. Bauer,* Ganzzahlige Gleichungen ohne Affekt. Math. Ann. 64 (1907), S. 325—327.
6. *M. Bauer,* Ganzzahlige Gleichungen ohne Affekt. Math. Zeitschrift 16 (1923), S. 318—319.
7. *H. Brandt,* Ueber eine Verallgemeinerung des Gruppenbegriffes. Math. Ann. 96 (1926), S. 360—366.
8. *R. Brauer,* Ueber die Darstellung der Drehungsgruppe durch Gruppen linearer Substitutionen. Berl. Diss. 1925.
9. *R. Brauer, H. Hasse, E. Noether,* Beweis eines Hauptsatzes in der Theorie der Algebren. Crelle 167 (1931; Hensel-Festband), S. 399—404.
10. *S. Breuer,* Zur Bestimmung der metazyklischen Minimalbasis vom Primzahlgrad. Math. Ann. 92 (1924).
11. *S. Breuer,* Metazyklische Minimalbasis und komplexe Primzahlen. Crelle 156 (1927), S. 13—42.
12. *E. S. Bring,* Meletamata quaedam mathematica circa transformationem etc. Diss. Lund, 1786.
13. *É. Cartan,* Sur la structure des groupes finis et continus. Thèse. Paris 1894.
14. *É. Cartan,* Sur la structure des groupes infinis. C R. 135 (1902), S. 851—854.
15. *G. Castelnuovo,* Sulla razionalità delle involuzioni piane. Math. Ann. 44 (1894), S. 125—155.
16. *R. Dedekind,* Zur Theorie der Ideale. Gött. Nachr. 1894, S. 272—277.
17. *R. Dedekind,* Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. Crelle 121 (1900), S. 40—123
18. *K. Doerge,* Bemerkung zum Hilbertschen Irreduzibilitätssatz. Math. Ann. 102 (1929), S. 521—530.
19. *F. Enriques,* Sur les problèmes qui se rapportent à la résolution des équations algébriques etc. Math. Ann. 51 (1899), S. 134—153.
20. *F. Enriques,* Sopra una involuzione non razionale dello spazio. Rendic. Linc. 21 (1912), S. 81—83.
21. *G. Fano,* Sopra alcune varietà algebriche a tre dimensioni etc. Atti Acc. Torino 43 (1908), S. 973—981.
22. *E. Fischer,* Zur Theorie der endlichen Abelschen Gruppen. Math. Ann. 77 (1916) S. 81—88.
23. *G. Frobenius,* Ueber Beziehungen zwischen Primidealen eines algebraischen Körpers und den Substitutionen usw. Sitzber. Berl. Akad. 1896, S. 689—705.
24. *R. Fueter,* Die Theorie der Zahlstrahlen. I, Crelle 130 (1905), S. 197—257; II, Crelle 132 (1907), S. 255—269.
25. *R. Fueter,* Abelsche Gleichungen in quadratisch imaginären Zahlkörpern. Math. Ann. 75 (1914), S. 177—255.

26. *Ph. Furtwängler,* Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen Zahlkörpers. Math. Ann. 63 (1907), S. 1—37.
27. *Ph. Furtwängler,* Ueber Minimalbasen für Körper rationaler Funktionen. Sitzber. Wiener Akad. 134 (1925), S. 69—80.
28. *R. Garver,* On the removal of four terms from an equation by means of a Tschirnhaus transformation. Bull. Amer. Math. Soc. 35 (1929), S. 73—78.
29. *G. H. Halphen,* Traité des fonctions élliptiques et leurs applications etc. Tome 3. Paris 1891.
30. *H. Hasse,* Zwei Existenztheoreme über algebraische Zahlkörper. Math. Ann. 95 (1925), S. 229—238.
31. *H. Hasse,* Ein weiteres Existenztheorem in der Theorie der algebraischen Zahlkörper. Math. Zeitschrift 24 (1925), S. 149—160.
32. *H. Hasse,* Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. I, Jahresber. D. M. V. 35 (1926), S. 1—55; Ia, ibid. 36 (1927), S. 233—311; II, ibid. VI. Ergänzbd. (1930).
33. *H. Hasse,* Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Math. Zeitschrift 31 (1930) S. 565—582.
34. *H. Hasse,* Theory of Cyclic Algebras over an Algebraic Number Field. Trans. Amer. Math. Soc. 34 (1932), S. 171—214.
35. *D. Hilbert,* Ueber die Irreducibilität ganzer rationaler Funktionen usw. Crelle 110 (1892), S. 104—129.
36. *D. Hilbert,* Mathematische Probleme. Gött. Nachr. 1900, S. 253—297.
37. *D. Hilbert,* Ueber die Gleichung neunten Grades. Math. Ann. 97 (1926), S. 243—250.
38. *A. Hurwitz,* Ueber algebraische Gebilde mit eindeutigen Transformationen in sich. Math. Ann. 41 (1893), S. 403—442.
39. *C. Jordan,* Mémoire sur les équations différentielles etc. Crelle 84 (1878), S. 89—215.
40. *W. Killing,* Die Zusammensetzung der stetigen endlichen Transformationsgruppen. I, Math. Ann. 31 (1888), S. 252—290; II, Math. Ann. 33, S. 1—48; III, Math. Ann. 34, S. 57—122; IV, Math. Ann. 36, S. 161—189.
41. *F. Klein,* Gesammelte mathematische Abhandlungen. Bd. 2. Berlin 1922. S. 255—504.
42. *L. Kronecker,* Vorlesungen über Zahlentheorie. Lpz. 1901. S. 452—492.
43. *W. Krull,* Galoissche Theorie der unendlichen algebraischen Erweiterungen. Math. Ann. 100 (1928), S. 687 - 698.
44. *E. E. Levi,* Sulla struttura dei gruppi finiti e continui. Atti Acc. Torino 40 (1905), S. 423—437.
45. *S. Lie,* Theorie der Transformationsgruppen. Bd. I. Lpz. 1888.
46. *A. Loewy,* Neue elementare Begründung und Erweiterung der Galoisschen Theorie. Sitzber. Heidlb. Akad. I, 7. Abh., 1925; II, 1 Abh. 1927.
47. *A. Loewy,* Ueber abstrakt definierte Transmutationssysteme oder Mischgruppen. Crelle 157 (1927), S. 239—254.
48. *Lüroth,* Beweis eines Satzes über rationale Curven. Math. Ann. 9 (1876), S. 163—165.
49. *F. Mertens,* Ueber Dirichlet's Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren Differenz zu ihren Gliedern

teilerfremd ist, unendlich viele Primzahlen enthält. Sitzber. Wiener Akad. 106 (1897), S. 254—286.

50. *F. Mertens,* Ein Beweis des Galois'schen Fundamentalsatzes. Sitzber. Wiener Akad. 111 (1902), S. 17—37.

51. *L. J. Mordell,* On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees. Proc. Cambr. Phil. Soc. 21 (1922), S. 179—192.

52. *T. Nagell,* Sur les propriétés arithmétiques des cubiques planes du premier genre. Acta Math. 52 (1928), S. 93—126.

53. *E. Netto,* Ueber einen Lüroth-Gordan'schen Satz. Math. Ann. 46 (1895), S. 310—318.

54. *C. Neumann,* Vorlesungen über Riemann's Theorie der Abel'schen Integrale. 2. Aufl. Lpz. 1884.

55. *E. Noether,* Gleichungen mit vorgeschriebener Gruppe. Math. Ann. 78 (1918), S. 221—227.

56. *M. Noether,* Ueber Flächen, welche Schaaren rationaler Curven besitzen. Math. Ann. 3 (1871), S. 161—227.

57. *O. Ore,* Zur Theorie der Eisensteinschen Gleichungen. Math. Zeitschrift 20 (1924), S. 267—279.

58. *O. Perron,* Ueber Gleichungen ohne Affekt. Sitzber. Heidlb. Akad. 1923, 3. Abh.

59. *H. Poincaré,* Sur les propriétés arithmétiques des courbes algébriques. Journ. de Math. (5) 17 (1901), S. 161.

60. *F. Pollaczek,* Ueber die Einheiten relativ-Abelscher Zahlkörper. Math. Zeitschrift 30 (1929), S. 520—551.

61. *R. Remak,* Ueber die Abschätzung des absoluten Betrages des Regulators eines algebraischen Zahlkörpers nach unten. Crelle 167 (Hensel-Festband, 1931), S. 360—378.

62. *S. Schatunowski,* Algebra als Lehre von den Kongruenzen nach funktionalen Moduln (russisch). Diss Odessa 1917.

63. *A. Scholz,* Ueber die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe. Math. Zeitschrift 30 (1929), S. 332—356.

64. *A. Scholz,* Reduktion der Konstruktion von Körpern mit zweistufiger (metabelscher) Gruppe. Sitzber. Heidlb. Akad. 1929, 14. Abh.

65. *A. Scholz,* Ein Beitrag zur Theorie der Zusammensetzung endlicher Gruppen. Math. Zeitschrift 32 (1930), S. 187—189.

66. *A. Scholz,* Ueber das Verhältnis von Idealklassen- und Einheitengruppe in Abelschen Körpern von Primzahlpotenzgrad. Sitzber. Heidlb. Akad. 1930, 3. Abh., S. 31—55.

67. *O. Schreier,* Die Verwandtschaft stetiger Gruppen im großen. Hamb. Abh. 5 (1927), S. 233—244.

68. *I. Schur,* Ueber eine Klasse von Matrizen, die sich einer gegebenen Matrix zuordnen lassen. Diss. Berlin 1901.

69. *I. Schur,* Ueber die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. Crelle 127 (1904), S. 20—50; II, Crelle 132 (1907), S. 85—137.

70. *I. Schur,* Beispiele für Gleichungen ohne Affekt. Jahresber. DMV. 29 (1920).

71. *I. Schur,* Ueber die stetigen Darstellungen der allgemeinen linearen Gruppe. Sitzber. Berl. Akad. 1928, S. 96 – 124.

72. *I. Schur,* Gleichungen ohne Affekt. Sitzber. Berl. Akad. 1930, S. 443—449.

73. *A. Speiser,* Die Zerlegung von Primzahlen in algebraischen Zahlkörpern. Trans. Amer. Math. Soc. 23 (1922), S. 173—178.

74. *E. Steinitz,* Algebraische Theorie der Körper. Crelle 137 (1910), S. 167—308; neu herausgeg. (1930), mit Anhang von *R. Baer* und *H. Hasse:* Abriß der Galoisschen Theorie.

75. *J. J. Sylvester,* On the so-called Tschirnhausen Transformation. Crelle 100 (1886), S. 465—487.

76. *T. Takagi,* Ueber eine Theorie des relativ Abel'schen Zahlkörpers. Journ. Coll. Sc. Tokyo 41 (1920), Art. 9.

77. *P. Tchebycheff,* Sur l'intégration de la différentielle $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}dx$. Oeuvres 1, S. 517—530.

78. *N. Tschebotaröw,* Die der Tschirnhausenschen umgekehrte Aufgabe. Journal des Sciences 1 (1922) (russisch).

79. *N. Tschebotaröw,* Zur Aufgabe der Bestimmung von algebraischen Gleichungen mit vorgeschriebener Gruppe (russisch). Bull. Soc. Math. Kasan, (3) 1 (1926), S. 26—32.

80. *N. Tschebotaröw,* Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Ann 95 (1925), S. 191—228.

81. *N. Tschebotaröw.* Studien über Primzahlendichtigkeiten. Bull. Soc. Math. Kasan: I, (3) 2 (1927), S. 14—20; II, (3) 3 (1928), S. 1—17.

82. *N. Tschebotaröw,* Zur Gruppentheorie des Klassenkörpers. Crelle 161 (1929), S. 179—193.

83. *N. Tschebotaröw,* Ueber ein algebraisches Problem von Herrn Hilbert. Math. Ann.: I, 104 (1931), S. 459—471; II, 105 (1931), S. 240—255.

84. *N. Tschebotaröw,* Untersuchungen über relativ Abelsche Zahlkörper. Crelle 167 (Hensel-Festband; 1931), S. 98—121.

85. *G. Voronoi,* Ueber ganze algebraische Zahlen, die von einer Wurzel einer Gleichung 3. Grades abhängen (russisch). Mag. Diss. S-Pb. 1894.

86. *H. Weber,* Lehrbuch der Algebra, Bd. 3. Braunschweig 1908.

87. *A. Weil,* L'arithmétique sur les courbes algébriques. Acta Math. 52 (1929), S. 281—315.

88. *H. Weyl,* Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen. Math. Zeitschrift: I, 23 (1925), S. 271—309; II, 24 (1925), S. 328—376; III, 24 (1925), S. 377—395.

89. *A. Wiman,* Ueber eine einfache Gruppe von 360 ebenen Collineationen. Math. Ann. 47 (1896), S. 531—556.

90. *A. Wiman,* Ueber die Darstellung der symmetrischen und alternierenden Vertauschungsgruppen usw. Math. Ann. 52 (1899), S. 243—270.

91. *A. Wiman,* Ueber die Anwendung der Tschirnhausentransformation auf die Reduktion algebraischer Gleichungen. Nova Acta Uppsala 1927, S. X + 3—8.

92. *G. Zolotareff,* Théorie des nombres complexes entiers avec une application vers le calcul intégral (russisch). Diss. S.-Pb. 1874. Oeuvres tome I, Leningrad 1931, S. 161—360.