XII.

Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers.

[Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauß, Braunschweig 1877, S. 1—55.]

Die erhabenen Schöpfungen von Carl Friedrich Gauß haben die Bewunderung der Mathematiker dieses Jahrhunderts vor allem deshalb erregt, weil sie in fast beispielloser Weise die Wissenschaft mit einer außerordentlichen Fülle ganz neuer Gedanken befruchtet und vorher gänzlich unbekannte Felder zum ersten Male der Forschung erschlossen haben. Im höchsten Maße gilt dies von Gauß' Entdeckungen im Gebiete der höheren Arithmetik, die ihn nach seinem eigenen Ausspruche das ganze Leben hindurch vor allen anderen Teilen der Mathematik gefesselt hat. Mit der Theorie der Kreisteilung ist von ihm nicht bloß der Grund zu einem neuen Teile der Mathematik gelegt, welcher von der algebraischen Verwandtschaft der Zahlen handelt, sondern sie hat auch das erste und bis jetzt noch immer fruchtbarste Beispiel des innigen Zusammenhangs zwischen der höheren Algebra und der Zahlentheorie geliefert, welche bis dahin zwei vollständig getrennte Gebiete gebildet hatten. In der nächsten Beziehung zu dieser Erweiterung der Grenzen der Wissenschaft steht der kühne Gedanke, den Begriff der ganzen Zahl durch die Einführung der ganzen komplexen Zahlen von seiner bisherigen Beschränkung zu befreien, wodurch Gauß abermals der arithmetischen Forschung ein heute noch unermeßliches Feld eröffnet hat. Aber es ist nicht bloß dieser wunderbare Reichtum an neuen Gedanken und großen Entdeckungen, durch welchen Gauß sein Wirken auf allen von ihm beschrittenen Gebieten der Wissenschaft für alle Zeiten bezeichnet hat, sondern es steht diesem vollständig ebenbürtig die Tiefe der Methoden gegenüber, durch welche er die größten Schwierig-

keiten überwunden und die verborgensten Wahrheiten, die *mysteria numerorum*, in das hellste Licht gesetzt hat. Es genügte seinem stets auf das Große und auf die zukünftige Entwicklung der Wissenschaft blickenden Geiste nicht, einen Beweis gefunden und damit die Wahrheit außer Zweifel gesetzt zu haben, sondern er kehrte, wie er selbst so eindringlich beschreibt, unablässig zu den schon überwundenen Schwierigkeiten zurück, in der Hoffnung, durch erneute Anstrengungen neue Waffen zu gewinnen, welche eine über das unmittelbar vorliegende Ziel weit hinausreichende Tragweite besäßen. Und so ist es gekommen, daß dieselben von Gauß erdachten Methoden unmittelbar oder mit geringen Modifikationen auch bei der Behandlung von ähnlichen, aber allgemeineren Problemen sich als vollständig ausreichend erweisen. Diese schon oft als ein besonders charakteristisches Kennzeichen der Gedankentiefe von Gauß hervorgehobene Erscheinung an einem neuen Beispiel zu bestätigen, ist der Zweck der gegenwärtigen Abhandlung, welche dem Andenken des großen Mathematikers gewidmet ist.

Die Theorie der binären quadratischen Formen, zu deren Entstehung einige Sätze von Fermat die Veranlassung gegeben haben verdankt ihre Begründung den hervorragenden Arbeiten von Euler und Lagrange, aber sie ist erst von Gauß durch die in der fünften Sektion der Disquisitiones Arithmeticae niedergelegten Untersuchungen zu einem wissenschaftlichen Ganzen gestaltet, und namentlich hat sie durch die daselbst zum ersten Male behandelte Lehre von der Komposition der Formen die höchste Bereicherung erhalten. Unter den Anwendungen, welche Gauß von dieser neuen Theorie gemacht hat, ist eine der bemerkenswertesten die Bestimmung des Verhältnisses der Klassen-Anzahlen der Formen, welche zu zwei verschiedenen Ordnungen derselben Determinante D gehören; bezeichnet man mit $h(D)$ die Klassen-Anzahl für diejenige Ordnung der Determinante D, welche nur primitive Formen (und zwar entweder nur die eigentlichen oder nur die uneigentlichen) enthält, so kommt diese Aufgabe darauf hinaus, für zwei gegebene, in quadratischem Verhältnis stehende Determinanten D und D' das Verhältnis $h(D):h(D')$ zu ermitteln. Die aus der Theorie der Komposition der Formen geschöpfte Beantwortung dieser Frage ist im Art. 256, V. und VI. enthalten, und sie ist für den Fall negativer Determinanten eine so vollständige, daß der Wert des Verhältnisses $h(D):h(D')$ unmittelbar

aus den Werten von D und D' entnommen werden kann; nicht ebenso vollständig durchgeführt ist der Fall positiver Determinanten, über welchen Gauß folgendes sagt: „*Pro casu tertio autem, ubi D est numerus positivus non quadratus, regulam generalem pro comparanda multitudine formarum pr. primitivarum in V, V', V'' etc. cum multitudine classium diversarum inde resultantium hucusque non habemus. Id quidem asserere possumus, hanc vel illi aequalem vel ipsius partem aliquotam esse; quin etiam nexum singularem inter quotientem horum numerorum et valores minimos ipsorum t, u aequationi* $tt - Duu = AA$ *satisfacientes deteximus, quem hic explicare nimis prolixum foret; an vero possibile sit, illum quotientem in omnibus casibus ex sola inspectione numerorum D, A cognoscere (ut in casibus praecc.), de hac re nihil certi pronunciare possumus.*“

Das umfassendere und noch viel schwierigere Problem, die Klassen-Anzahl $h(D)$ selbst, d. h. die Abhängigkeit dieser Anzahl von der Determinante D zu bestimmen, ist schon während des Druckes der fünften Sektion der Disquisitiones Arithmeticae, wie aus Art. 306, X. hervorgeht, ein Gegenstand des höchsten Interesses für Gauß gewesen, und es ist ihm in der Tat bald darauf gelungen, die vollständige Lösung desselben zu finden, was er noch am Schlusse des großen Werkes mit folgenden Worten ankündigen konnte: „*Quaestionem hic propositam plene solvere nuper successit, quam disquisitionem plures partes tum Arithmeticae sublimioris tum Analyseos mirifice illustrantem in continuatione hujus operis trademus quam primum licebit.*“ Allein die hier in Aussicht gestellte Veröffentlichung dieser Untersuchung ist zu Gauß' Lebzeiten nicht erfolgt; der hierauf bezügliche Teil seines Nachlasses, welchen ich in dem 1863 erschienenen zweiten Bande seiner gesammelten Werke herausgegeben habe, enthält namentlich zwei Fragmente, die aus den Jahren 1834 und 1837 stammen und den gemeinsamen Titel führen: „*De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earumque determinantem.*“ Obgleich jedes dieser Fragmente nach wenigen Seiten abbricht, so reicht ihr Inhalt doch aus, um den Weg vollständig überblicken zu lassen, auf welchem Gauß zu dem erstrebten Ziele gelangt ist.

Im Jahre 1839, also 38 Jahre nach dem Erscheinen der Disquisitiones Arithmeticae, trat Peter Gustav Lejeune Dirichlet,

der nach Gauß' eigenem Zeugnis zuerst von allen Mathematikern dieses Werk vollständig begriffen und die darin enthaltenen Untersuchungen selbständig weitergeführt hat, mit einer vollständigen und höchst eigentümlichen Lösung des Problems der Klassen-Anzahl hervor*). Ohne hier, was zu weit führen würde, auf eine nähere Vergleichung der Methode von Dirichlet mit derjenigen von Gauß einzugehen, bemerke ich nur, daß von beiden für die Klassen-Anzahl ein Ausdruck durch eine unendliche Reihe gewonnen wird, welche sich mit Hilfe gewisser, der Kreisteilung angehörender Sätze von Gauß summieren, also in geschlossener Form darstellen läßt. Aber es ist von Wichtigkeit, daß es schon vor Ausführung dieser Summation gelingt, aus dem erhaltenen Ausdruck den Wert des oben besprochenen Verhältnisses $h(D):h(D')$ abzuleiten. Auf diese Weise**) ist Dirichlet für den Fall negativer Determinanten zu demselben Resultat gelangt wie Gauß, und er hat außerdem für den Fall positiver Determinanten zum ersten Male das Gesetz vollständig ausgesprochen, nach welchem das gesuchte Verhältnis von den kleinsten Lösungen der unbestimmten Gleichungen $tt - Duu = 1$, $t't' - D'u'u' = 1$ abhängt. Aus der oben angeführten, auf diesen Fall bezüglichen Stelle der Disquisitiones Arithmeticae geht aber wohl mit Gewißheit hervor, daß Gauß ebenfalls dieses Gesetz schon vollständig gekannt hat, welches zwar einfach, aber doch keineswegs so einfach ist, daß man *ex sola inspectione numerorum* D, D' den Wert des gesuchten Verhältnisses erkennen könnte; auch habe ich gezeigt***), daß man wirklich auf dem von Gauß eingeschlagenen Wege, d. h. durch die Komposition der Formen, mit wenigen Schritten zu diesem, zuerst von Dirichlet ausgesprochenen Gesetz gelangen kann.

Beide Methoden, das Verhältnis der Klassen-Anzahlen zu bestimmen, sowohl die von Gauß, welche auf die Komposition der Formen gegründet ist, als auch diejenige von Dirichlet, zeichnen sich nun dadurch aus, daß sie auf ähnliche Probleme von sehr allgemeinem Charakter mit demselben Erfolg anwendbar

---

*) Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres (Crelles Journal, Bd. 19, 21).

**) Ebenda, Bd. 21, § 8.

***) Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet. Zweite Auflage. 1871. §. 150, 151. — Ich werde dieses Werk in der Folge kurz mit D. zitieren.

sind*). Die binären quadratischen Formen, von welchen bisher ausschließlich gesprochen ist, bilden nämlich nur einen äußerst speziellen Fall der sogenannten zerlegbaren Formen, d. h. der homogenen Funktionen von beliebig hohem Grade n mit n Variabelen, welche rationale Koeffizienten haben und in n lineare Faktoren mit algebraischen Koeffizienten zerlegbar sind. Das Verdienst, diese Formen zuerst betrachtet und eine charakteristische Fundamental-Eigenschaft derselben erkannt zu haben, gebührt Lagrange**), und eine weitere Verfolgung seines Gedankens hätte leicht schon früher zu der Theorie der Komposition der Formen führen können. Erst viel später hat sich Dirichlet eingehend mit diesem Gegenstand beschäftigt; leider ist von seinen tiefen Untersuchungen — abgesehen von der ebenfalls hierhergehörigen, aber speziellen Theorie der quadratischen Formen mit komplexen Koeffizienten und Variabelen***) — nur eine einzige veröffentlicht, welche die Theorie der Transformation dieser Formen in sich selbst, oder, anders ausgedrückt, die Theorie der Einheiten in dem entsprechenden Gebiete algebraischer Zahlen behandelt. Der in äußerst kurzen Umrissen von Dirichlet mitgeteilte Beweis****) für die Existenz und für die allgemeine Form aller dieser Einheiten, welcher ihm erst nach großen und anhaltenden Anstrengungen gelungen ist, muß zu seinen bedeutendsten Leistungen gezählt werden, da derselbe ein unerläßliches Fundament für die ganze Theorie bildet; und Dirichlet selbst, der seinen eigenen Schöpfungen gegenüber sich immer ein ganz unbefangenes Urteil bewahrte, legte auf dies Resultat einen ebenso hohen Wert, wie auf die Prinzipien, welche ihn zu dem Beweise des Satzes über die arithmetische Progression und zur Bestimmung der Klassen-Anzahl der binären quadratischen Formen geführt haben. Dirichlet hat auch die Klassen-Anzahl für solche zerlegbare Formen bestimmt, welche aus der Theorie der

---

*) Ob dasselbe auch von der scharfsinnigen Methode gilt, welche R. Lipschitz zur Lösung derselben Aufgabe angewandt hat (Crelles Journal, Bd. 53), wage ich für jetzt nicht zu beurteilen; doch spricht dafür der Erfolg, mit welchem er diese Methode auf ein höheres Problem übertragen hat (Crelles Journal, Bd. 54).

**) Sur la solution des problèmes indéterminés du second degré. § VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. — Élémens d'Algèbre par L. Euler; Additions § IX.

***) Crelles Journal, Bd. 24.

****) Monatsberichte der Berliner Akademie vom Oktober 1841, April 1842, März 1846. — Comptes rendus der Pariser Akademie 1840, T. X, S. 286.

Kreisteilung entspringen, aber hiervon ist nichts veröffentlicht*). Es folgte zunächst im Jahre 1844 eine wertvolle Untersuchung von Eisenstein**) über gewisse kubische Formen, welche aus der Kreisteilung entspringen; doch scheint dieselbe wegen ihres sehr speziellen Charakters keinen bedeutenden Einfluß auf die Entwicklung der allgemeinen Theorie ausgeübt zu haben. Den größten und folgenreichsten Schritt aber hat Kummer***) im Jahre 1847 durch die Einführung der idealen Zahlen getan; denn wenn auch seine Untersuchungen ebenfalls sich zunächst nur auf die Kreisteilung und einige derselben nahestehende Gebiete beziehen, so sind doch die ihnen zugrunde liegenden Gedanken von viel allgemeinerer Bedeutung. Der außerordentliche, von Kummer erreichte Erfolg hat mich schon seit dem Jahre 1856 angetrieben, meine Kräfte hauptsächlich diesem Gegenstand zu widmen, und es ist mir endlich gelungen, eine allgemeine, ausnahmslose Theorie der ganzen algebraischen Zahlen aufzustellen, deren Grundlagen ich in dem zehnten Supplement der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie veröffentlicht habe****). Mit Hilfe dieser Prinzipien, welche ich hier als bekannt voraussetzen muß, läßt sich nun das auf die zerlegbaren Formen von beliebigem Grade oder auf die entsprechenden Ideal-Klassen übertragene Problem, das Verhältnis der Klassen-Anzahlen für verschiedene Ordnungen zu bestimmen, sowohl nach der Methode von Gauß, als auch nach derjenigen von Dirichlet vollständig lösen, und hierin besteht das Ziel der vorliegenden Abhandlung.

§ 1.

Theorie der ganzen Zahlen eines endlichen Körpers.

Obwohl diese Theorie, deren Mittelpunkt die Lehre von der Multiplikation der Ideale und von der Komposition der Ideal-Klassen bildet, hier als bekannt vorausgesetzt werden muß, so wird es doch

---

*) Vgl. Kummer, Gedächtnisrede auf G. P. Lejeune Dirichlet, 1860, S. 21—22.

**) Crelles Journal, Bd. 28.

***) Ebenda, Bd. 35.

****) Eine etwas ausführlichere Darstellung eines Teiles dieser Theorie erscheint gegenwärtig unter dem Titel *Sur la théorie des nombres entiers algébriques* in dem *Bulletin des sciences mathématiques et astronomiques* von Darboux und Houël. — Ich werde diese Abhandlung mit B. zitieren. [Vgl. Bd. 3 dieser Ausgabe.]

zweckmäßig sein, die wichtigsten ihr zugrunde liegenden Begriffe hier möglichst kurz in Erinnerung zu bringen, schon um den Anknüpfungspunkt der jetzigen Abhandlung an meine früheren Untersuchungen deutlicher hervorheben zu können.

Ist θ eine algebraische Zahl, und zwar eine Wurzel einer irreduktiblen Gleichung

$$f(\theta) = \theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0$$

vom $n$ten Grade, deren Koeffizienten $a_1, a_2 \cdots a_{n-1}, a_n$ rationale Zahlen sind, und betrachtet man die sämtlichen Zahlen von der Form

$$\omega = \varphi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1},$$

wo $x_0, x_1, x_2 \cdots x_{n-1}$ willkürliche rationale Zahlen bedeuten, so besitzt der Inbegriff Ω aller dieser Zahlen ω die charakteristische Eigenschaft eines Körpers (D. § 159), welche darin besteht, daß die Summen, Differenzen, Produkte und Quotienten von je zwei solchen Zahlen ω ebenfalls in Ω enthalten sind; ein Körper Ω, dessen Zahlen auf die angegebene Art aus einer Wurzel θ einer irreduktiblen Gleichung $n$ten Grades gebildet sind, heißt speziell ein endlicher Körper vom Grade n. Hat man n Zahlen

$$\omega_1 = \varphi_1(\theta), \quad \omega_2 = \varphi_2(\theta) \cdots \omega_n = \varphi_n(\theta)$$

nach Belieben, nur mit der einzigen Beschränkung aus Ω ausgewählt, daß die aus den n^2 rationalen Koeffizienten x gebildete Determinante einen von 0 verschiedenen Wert besitzt, so läßt sich jede beliebige Zahl ω des Körpers Ω stets und nur auf eine einzige Weise in der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

darstellen, wo $h_1, h_2 \cdots h_n$ rationale Zahlen bedeuten. Ein solches System von n Zahlen $\omega_1, \omega_2 \cdots \omega_n$ heißt eine Basis des Körpers Ω, und die n rationalen Zahlen $h_1, h_2 \cdots h_n$ heißen die Koordinaten der Zahl ω in bezug auf diese Basis. Offenbar bilden die Zahlen $1, \theta, \theta^2 \cdots \theta^{n-1}$ selbst eine solche Basis.

Ist θ' ebenfalls eine Wurzel derselben irreduktiblen Gleichung $f(\theta') = 0$, so entspricht jeder bestimmten Zahl $\omega = \varphi(\theta)$ des Körpers Ω eine bestimmte Zahl $\omega' = \varphi(\theta')$, und der Inbegriff aller dieser Zahlen ω' bildet einen mit Ω konjugierten Körper Ω'; diese Korrespondenz besitzt die charakteristische Eigenschaft, daß, wenn α, β zwei beliebige Zahlen des Körpers Ω bedeuten, stets

$$(\alpha + \beta)' = \alpha' + \beta', \quad (\alpha - \beta)' = \alpha' - \beta', \quad (\alpha\beta)' = \alpha'\beta', \quad \left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}$$

ist; die Substitution, durch welche jede Zahl $\omega = \varphi(\theta)$ des Körpers Ω in die korrespondierende oder konjugierte Zahl $\omega' = \varphi(\theta')$ des Körpers Ω' übergeht, heiße eine Permutation des Körpers Ω. Sind $\theta', \theta'' \cdots \theta^{(n)}$ die sämtlichen Wurzeln der obigen irreduktiblen Gleichung, so entspricht einer jeden von ihnen, $\theta^{(r)}$, eine Permutation $P^{(r)}$ des Körpers Ω, durch welche jede in ihm enthaltene Zahl $\omega = \varphi(\theta)$ in die konjugierte Zahl $\omega^{(r)} = \varphi(\theta^{(r)})$ des Körpers $\Omega^{(r)}$ übergeht. Die n mit ω konjugierten Zahlen $\omega', \omega'' \cdots \omega^{(n)}$ sind dann immer die Wurzeln einer Gleichung $n$ten Grades mit rationalen Koeffizienten, welche aber nicht notwendig irreduktibel ist. Das Produkt $\omega'\omega'' \cdots \omega^{(n)}$ aus diesen n Zahlen ist eine rationale Zahl, welche die Norm der Zahl ω heißt und mit $N(\omega)$ bezeichnet wird; sie verschwindet nur dann, wenn $\omega = 0$ ist, und die Norm eines Produkts ist das Produkt aus den Normen der Faktoren. Sind ferner $\alpha_1, \alpha_2 \cdots \alpha_n$ beliebige Zahlen des Körpers, so ist das Quadrat der Determinante

$$\sum \pm \alpha_1' \alpha_2'' \cdots \alpha_n^{(n)},$$

welche aus den n^2 konjugierten Zahlen $\alpha_i^{(i)}$ gebildet ist, ebenfalls eine rationale Zahl, welche die Diskriminante des Systems $\alpha_1, \alpha_2 \cdots \alpha_n$ heißt und mit $\Delta(\alpha_1, \alpha_2 \cdots \alpha_n)$ bezeichnet wird; dieselbe ist stets und nur dann von 0 verschieden, wenn die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden; dies ergibt sich leicht aus dem bekannten Satze

$$\Delta(1, \theta, \theta^2 \cdots \theta^{n-1}) = (-1)^{1/2\, n\,(n-1)} N[f'(\theta)],$$

wo $f'(t)$ die Derivierte der Funktion $f(t)$ bedeutet.

Alle algebraischen Zahlen, deren Gesamtheit ebenfalls einen Körper, aber keinen endlichen Körper bildet, zerfallen nun in ganze und in gebrochene Zahlen; eine algebraische Zahl η heißt eine ganze Zahl, wenn sie die Wurzel einer Gleichung von der Form

$$\eta^m + c_1 \eta^{m-1} + c_2 \eta^{m-2} + \cdots + c_{m-1}\eta + c_m = 0$$

ist, wo $c_1, c_2 \cdots c_{m-1}, c_m$ ganze Zahlen im alten Sinne des Wortes bedeuten, die von nun an immer rationale ganze Zahlen genannt werden sollen. Aus dieser Definition, welche wohl die höchste Verallgemeinerung des ursprünglich so beschränkten Begriffes der ganzen Zahl enthält, folgt unmittelbar, daß die Summen, Differenzen und Produkte von je zwei ganzen Zahlen wieder ganze Zahlen sind, und hieran knüpft sich wieder der Begriff der Teilbarkeit der ganzen Zahlen: eine ganze Zahl α heißt teilbar durch eine ganze Zahl β,

oder ein Vielfaches (Multiplum) von β, wenn $\alpha = \beta\gamma$, und γ wieder eine ganze Zahl ist; zugleich heißt γ ein Teiler (Divisor) von α, oder man sagt auch, β gehe in α auf. Eine ganze Zahl ε, welche in der Zahl 1 und folglich auch in allen ganzen Zahlen aufgeht, heißt eine Einheit; zwei ganze Zahlen, deren jede in der anderen aufgeht, und deren Quotient notwendig eine Einheit ist, heißen assoziierte Zahlen*) oder Gefährten.

Kehrt man mit diesen allgemeinen Begriffen zu einem endlichen Körper Ω zurück, und bezeichnet man mit o den Inbegriff aller in Ω enthaltenen ganzen Zahlen, zu welchen auch alle ganzen rationalen Zahlen gehören, so ergibt sich ohne Schwierigkeit die Existenz einer aus n ganzen Zahlen $\omega_1, \omega_2 \cdots \omega_n$ bestehenden Basis des Körpers Ω von der Beschaffenheit, daß die Koordinaten $h_1, h_2 \cdots h_n$ einer jeden in o enthaltenen Zahl

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

ganze rationale Zahlen sind; die Diskriminante

$$D = \Delta(\omega_1, \omega_2 \cdots \omega_n)$$

eines solchen Systems $\omega_1, \omega_2 \cdots \omega_n$, welches auch eine Basis des Gebietes o heißen soll, ist eine ganze rationale, von 0 verschiedene Zahl, die ich ihrer Wichtigkeit wegen die Grundzahl oder die Diskriminante des Körpers Ω nenne und mit $\Delta(\Omega)$ bezeichne. Die Norm einer jeden von 0 verschiedenen Zahl μ des Gebietes o ist eine ganze rationale, von 0 verschiedene Zahl, welche die folgende, wichtige Bedeutung besitzt; nennt man zwei ganze Zahlen α, β kongruent oder inkongruent in bezug auf den Modulus μ, je nachdem ihre Differenz $\alpha - \beta$ durch μ teilbar oder nicht teilbar ist, so ist die Anzahl aller in o enthaltenen, nach μ inkongruenten Zahlen $= \pm N(\mu)$; die Kongruenz der Zahlen α, β in bezug auf μ wird durch $\alpha \equiv \beta \pmod{\mu}$ bezeichnet. Eine in o enthaltene Einheit ist dadurch charakterisiert, daß ihre Norm $= \pm 1$ ist.

Die wichtigste Frage ist aber die nach der Zerlegung einer in o enthaltenen Zahl μ in solche Faktoren, welche, wie im folgenden immer stillschweigend vorausgesetzt wird, ebenfalls dem Gebiet o angehören. Die Divisoren einer Einheit sind sämtlich selbst Einheiten; ist aber μ keine Einheit, so sind zwei Fälle möglich; ist μ

*) Vgl. Gauß, Theoria residuorum biquadraticorum II, Art. 31.

das Produkt aus zwei Faktoren, von denen keiner eine Einheit, und folglich auch keiner mit μ assoziiert ist, so soll μ eine zerlegbare Zahl heißen; im entgegengesetzten Falle, d. h. wenn jeder Divisor von μ entweder ein Gefährte von μ oder eine Einheit ist, heißt μ unzerlegbar. Aus dem Satze über die Norm eines Produktes folgt nun offenbar, daß jede zerlegbare Zahl stets als Produkt aus einer endlichen Anzahl von unzerlegbaren Faktoren darstellbar ist; während aber in der Theorie der rationalen Zahlen (d. h. im Falle $n = 1$) diese Zerlegung, abgesehen von den Einheitsfaktoren ± 1, eine völlig bestimmte, einzige ist, so tritt bei Körpern höheren Grades sehr häufig die merkwürdige Erscheinung auf, daß eine Zahl μ als Produkt von unzerlegbaren Faktoren auf mehrere Arten darstellbar ist, welche in dem Sinne wesentlich verschieden sind, daß z. B. ein unzerlegbarer Faktor α der einen Darstellung $\mu = \alpha\beta\gamma\cdots$ mit keinem der unzerlegbaren Faktoren $\alpha_1, \beta_1 \cdots$ der anderen Darstellung $\mu = \alpha_1\beta_1\cdots$ assoziiert ist. Es folgt hieraus, daß eine unzerlegbare Zahl durchaus nicht immer den Charakter einer eigentlichen Primzahl besitzt, welcher darin besteht, daß ein Produkt nur dann durch eine Primzahl teilbar ist, wenn diese wenigstens in einem der Faktoren aufgeht. Diese unwillkommene Erscheinung, welche auf den ersten Blick jeden weiteren Fortschritt auf diesem Felde zu verbieten schien, ist aber die Quelle von einer der schönsten und fruchtbarsten Entdeckungen in der höheren Arithmetik geworden: in der Tat ist Kummer bei der Untersuchung solcher Gebiete o, welche aus der Kreisteilung entspringen, dahin gelangt, die Gesetze der Teilbarkeit durch Einführung idealer Zahlen in völligen Einklang mit denjenigen zu bringen, welche in der alten Theorie der rationalen Zahlen herrschen.

Es ist das Ziel meiner langjährigen Bemühungen gewesen, dasselbe Resultat für jeden endlichen Körper Ω zu erreichen, also diejenigen allgemeinen Gesetze der Teilbarkeit festzustellen, welche ohne Ausnahme jedem Gebiete o von der oben beschriebenen Art zukommen. Bei der Begründung dieser Theorie (D. § 163) habe ich den von Kummer eingeschlagenen Weg verlassen und statt der idealen Zahlen einen anderen Begriff, den des Ideals, einführen müssen, welcher von jeder, einem speziellen Körper Ω eigentümlichen Färbung frei ist und gerade deshalb die erforderliche Allgemeinheit besitzt, um als Grundlage der Theorie dienen zu können. Zum Ver-

ständnis der nachfolgenden Untersuchungen ist es unerläßlich, an die Hauptsätze dieser Theorie kurz zu erinnern.

1°. Ein System $\mathfrak{m}$ von unendlich vielen Zahlen des Gebietes $\mathfrak{o}$ heißt ein Ideal, wenn es die beiden folgenden Eigenschaften besitzt:

I. Die Summen und Differenzen von je zwei Zahlen des Systems $\mathfrak{m}$ sind ebenfalls in $\mathfrak{m}$ enthalten.

II. Jedes Produkt aus einer Zahl des Systems $\mathfrak{m}$ und aus einer Zahl des Systems $\mathfrak{o}$ ist eine Zahl des Systems $\mathfrak{m}$.

Bedeutet μ eine bestimmte, ω jede beliebige Zahl in $\mathfrak{o}$, so kommen diese beiden Eigenschaften offenbar dem System $\mathfrak{m}$ aller durch μ teilbaren Zahlen $\mu\omega$ zu; ein solches Ideal $\mathfrak{m}$ heißt ein Hauptideal und wird mit $\mathfrak{o}(\mu)$ oder kürzer mit $\mathfrak{o}\mu$ oder $\mu\mathfrak{o}$ bezeichnet*); es bleibt ungeändert, wenn μ durch eine mit μ assoziierte Zahl ersetzt wird. Ist μ eine Einheit, so ist $\mathfrak{o}\mu = \mathfrak{o}$, und umgekehrt. Da die Kongruenz zweier Zahlen α, β in bezug auf den Modulus μ darin besteht, daß die Differenz $\alpha - \beta$ dem Ideal $\mathfrak{o}\mu$ angehört, so wird man zu der folgenden allgemeineren Definition der Kongruenz geführt:

2°. Zwei Zahlen α, β heißen kongruent in bezug auf ein Ideal $\mathfrak{m}$, und dies wird durch die Kongruenz $\alpha \equiv \beta \pmod{\mathfrak{m}}$ angedeutet, wenn $\alpha - \beta$ eine Zahl des Ideals $\mathfrak{m}$ ist; im entgegengesetzten Falle heißen α, β inkongruent nach $\mathfrak{m}$. Die immer endliche Anzahl aller in $\mathfrak{o}$ enthaltenen, in bezug auf $\mathfrak{m}$ inkongruenten Zahlen heißt die Norm des Ideals $\mathfrak{m}$ und wird mit $N(\mathfrak{m})$ bezeichnet; die Norm eines Hauptideals $\mathfrak{o}\mu$ ist $= \pm N(\mu)$; das Hauptideal $\mathfrak{o}$ ist das einzige Ideal, dessen Norm $= 1$ ist.

Die Teilbarkeit einer Zahl $\mu = \alpha\beta$ durch eine Zahl α besteht darin, daß alle Zahlen $\mu\omega = \alpha(\beta\omega)$ des Ideals $\mathfrak{o}\mu$ auch in dem Ideal $\mathfrak{o}\alpha$ enthalten sind; dies veranlaßt zu der folgenden Definition der Teilbarkeit der Ideale:

3°. Ein Ideal $\mathfrak{m}$ heißt teilbar durch ein Ideal $\mathfrak{a}$ oder ein Vielfaches von $\mathfrak{a}$, wenn alle Zahlen des Ideals $\mathfrak{m}$ auch dem Ideal $\mathfrak{a}$ angehören; zugleich heißt $\mathfrak{a}$ ein Teiler von $\mathfrak{m}$, oder man sagt auch, $\mathfrak{a}$ gehe in $\mathfrak{m}$ auf.

---

*) Früher habe ich die weniger zweckmäßige Bezeichnung $\mathfrak{i}(\mu)$ angewendet (D. § 163).

Da hiernach die Teilbarkeit der Zahlen nur einen speziellen Fall von der Teilbarkeit der Ideale bildet, so kommt es lediglich darauf an, die tatsächlich einfacheren Gesetze der letzteren festzustellen. Dies geschieht durch die folgenden Begriffe und Sätze:

4°. Ist das Ideal $\mathfrak{m}$ teilbar durch das Ideal $\mathfrak{a}$, und letzteres teilbar durch das Ideal $\mathfrak{b}$, so ist auch $\mathfrak{m}$ teilbar durch $\mathfrak{b}$.

5°. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so bildet das System $\mathfrak{m}$ aller den Idealen $\mathfrak{a}$, $\mathfrak{b}$ gemeinschaftlich angehörenden Zahlen ein Ideal, welches das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ heißt, weil es in jedem gemeinschaftlichen Vielfachen von $\mathfrak{a}$, $\mathfrak{b}$ aufgeht.

6°. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bildet das System $\mathfrak{d}$ aller in der Form $\alpha + \beta$ darstellbaren Zahlen ein Ideal, welches der größte gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ heißt, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideal $\mathfrak{d}$ aufgeht.

7°. Zwei Ideale, deren größter gemeinschaftlicher Teiler das Ideal $\mathfrak{o}$ ist, heißen relative Primideale.

8°. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$ heißt ein Primideal, wenn es kein von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenes Ideal zum Teiler hat; im entgegengesetzten Falle heißt $\mathfrak{p}$ ein zusammengesetztes Ideal.

9°. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bilden die sämtlichen Produkte $\alpha\beta$ und alle Summen von solchen Produkten ein durch $\mathfrak{a}$ und durch $\mathfrak{b}$ teilbares Ideal, welches das Produkt aus den Faktoren $\mathfrak{a}$ und $\mathfrak{b}$ heißt und mit $\mathfrak{ab} = \mathfrak{ba}$ bezeichnet wird; zugleich ist $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Die Ausdehnung dieses Begriffes auf beliebig viele Faktoren und die Bedeutung einer Potenz ist selbstverständlich.

10°. Umgekehrt: ist das Ideal $\mathfrak{m}$ teilbar durch das Ideal $\mathfrak{a}$, so gibt es ein und nur ein Ideal $\mathfrak{b}$ von der Art, daß $\mathfrak{ab} = \mathfrak{m}$ wird.

11°. Ein Produkt von Idealen ist nur dann durch ein Primideal teilbar, wenn dieses wenigstens in einem der Faktoren aufgeht.

12°. Jedes zusammengesetzte Ideal ist als Produkt von lauter Primidealen darstellbar, und zwar nur auf eine einzige Weise.

13°. Damit ein Ideal $\mathfrak{m}$ durch ein Ideal $\mathfrak{a}$ teilbar sei, ist erforderlich und hinreichend, daß alle in $\mathfrak{a}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{m}$ aufgehen.

14°. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so gibt es ein durch $\mathfrak{a}$ teilbares Hauptideal $\mathfrak{a}\mathfrak{m}$ von der Art, daß $\mathfrak{m}$ und $\mathfrak{b}$ relative Primideale werden.

Für den Fall $n = 1$, in welchem alle Ideale Hauptideale sind, gehen die vorstehenden Sätze, deren strenge Beweise mir erst nach Überwindung von erheblichen Schwierigkeiten gelungen sind, in die Fundamentalsätze über die Teilbarkeit der ganzen rationalen Zahlen über. Dieselben Gesetze gelten daher auch für jeden Körper Ω von beliebigem Grade n, sobald alle seine Ideale Hauptideale sind, und für einen solchen Körper ist offenbar die Einführung der Ideale gänzlich überflüssig. Dies ist aber, wie schon oben bemerkt, im allgemeinen keineswegs der Fall, und hieran knüpft sich die Einteilung aller Ideale eines Körpers Ω in bestimmte Ideal-Klassen (D. § 164). Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen äquivalent, wenn es ein Ideal $\mathfrak{c}$ gibt, für welches beide Produkte $\mathfrak{a}\mathfrak{c}$, $\mathfrak{b}\mathfrak{c}$ Hauptideale werden; da aus dieser Definition unmittelbar folgt, daß zwei mit einem dritten äquivalente Ideale auch miteinander äquivalent sind, so bildet das System A aller Ideale, welche einem bestimmten Ideal $\mathfrak{a}$ äquivalent sind, eine Klasse, welche ungeändert bleibt, wenn ihr Repräsentant $\mathfrak{a}$ durch ein beliebiges, derselben Klasse A angehörendes Ideal ersetzt wird. Die Anzahl h dieser Klassen ist immer eine endliche; wählt man aus jeder Klasse nach Belieben ein bestimmtes Ideal als Repräsentanten, so ist jedes Ideal mit einem und nur mit einem dieser h Ideale äquivalent. Das System aller Hauptideale bildet die Hauptklasse O; zu jeder Klasse A von Idealen $\mathfrak{a}$ gehört eine bestimmte entgegengesetzte oder reziproke, inverse Klasse A^{-1}, welche aus allen denjenigen Idealen besteht, die durch Multiplikation mit den Idealen $\mathfrak{a}$ in Hauptideale verwandelt werden. Durchläuft nun $\mathfrak{a}$ alle Ideale einer Klasse A, ebenso $\mathfrak{b}$ alle Ideale einer Klasse B, so gehören die sämtlichen Produkte $\mathfrak{a}\mathfrak{b}$ ein und derselben Klasse an, welche die aus A und B zusammengesetzte Klasse oder das Produkt aus A, B heißt und mit AB bezeichnet wird; diese Komposition oder Multiplikation der Ideal-Klassen gehorcht den Gesetzen $AB = BA$, $(AB)C = A(BC)$, $OA = A$, $AA^{-1} = O$, $A^r A^s = A^{r+s}$, $A^h = O$, und aus $AB = AC$ folgt $B = C$.

Aus dem Satze $A^h = O$ folgt beiläufig, wenn man von dem endlichen Körper Ω wieder zu dem Gebiete aller ganzen algebraischen Zahlen übergeht, das wichtige Resultat, daß je zwei ganze Zahlen

α, β, die nicht beide verschwinden, einen größten gemeinschaftlichen Divisor δ besitzen, welcher in der Form $\delta = \alpha\alpha_1 + \beta\beta_1$ darstellbar ist, wo α_1, β_1 ebenfalls ganze Zahlen bedeuten; natürlich kann auch hier δ durch jeden Gefährten von δ ersetzt werden.

Das größte Interesse nimmt aber die Bestimmung der Klassen-Anzahl h in Anspruch (D. § 167). Die Übertragung der Prinzipien, welche Dirichlet bei dem Beweise des Satzes über die arithmetische Progression und bei der Bestimmung der Klassen-Anzahl der binären quadratischen Formen geschaffen hat, führt zu der Betrachtung unendlicher Reihen und Produkte von der Form

$$\sum f(\mathfrak{a}) = \prod \frac{1}{1 - f(\mathfrak{p})},$$

wo $\mathfrak{a}$ alle Ideale, $\mathfrak{p}$ alle Primideale durchläuft, und $f(\mathfrak{a})$ eine reelle oder komplexe Funktion bedeutet, die der Bedingung $f(\mathfrak{ab}) = f(\mathfrak{a})f(\mathfrak{b})$ genügt und außerdem so beschaffen ist, daß die unendliche Reihe linker Hand eine von der Anordnung ihrer Glieder unabhängige endliche Summe besitzt. Diese Bedingungen sind erfüllt, wenn man

$$f(\mathfrak{a}) = \frac{1}{N(\mathfrak{a})^s}, \quad s > 1$$

nimmt; multipliziert man mit $(s-1)$ und teilt die Totalsumme in h Partialsummen, deren jede einer bestimmten Klasse von Idealen $\mathfrak{a}$ entspricht, so nähern sich diese Summen für unendlich kleine positive Werte von $(s-1)$ einem gemeinschaftlichen, endlichen, von 0 verschiedenen Grenzwert g, der sich nach den fundamentalen Untersuchungen Dirichlets über die Einheiten ohne Schwierigkeit bestimmen läßt, und man erhält folglich

$$gh = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = \lim (s-1) \prod \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}.$$

Das Problem der Klassen-Anzahl wird daher gelöst sein, sobald es gelingt, den Grenzwert der unendlichen Reihe oder des mit ihr identischen Produkts noch auf eine zweite Art, nämlich unmittelbar aus der Natur der sämtlichen, dem Körper Ω angehörenden Primideale $\mathfrak{p}$ zu bestimmen. Dies ist bis jetzt nur für Kreisteilungskörper geglückt (zu welchen auch alle quadratischen Körper gehören), und eine aufmerksame Betrachtung dieser Fälle führt zu der

Überzeugung — in welcher ich durch meine demnächst zu veröffentlichenden Untersuchungen über die Anzahl der Ideal-Klassen in kubischen Körpern bestärkt werde —, daß die allgemeine Lösung des Problems der Klassen-Anzahl auf diesem Wege erst dann gelingen wird, wenn die algebraische Konstitution eines jeden Körpers und ihr Zusammenhang mit seinen Idealen uns vollständig bekannt sein wird — ein Ziel, von welchem wir noch außerordentlich weit entfernt sind; außerdem scheint auch eine viel genauere Ausbildung der Theorie der transzendenten Funktionen erforderlich zu sein.

Es ist nun noch mit einigen Worten die Beziehung zwischen den Idealen eines Körpers und den zugehörigen zerlegbaren Formen zu besprechen (D. § 165). Ist $\mathfrak{a}$ ein bestimmtes Ideal, so gibt es immer n partikuläre, in $\mathfrak{a}$ enthaltene Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ von der Beschaffenheit, daß die sämtlichen Zahlen α des Ideals $\mathfrak{a}$ durch den Ausdruck

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

dargestellt werden, wenn die Variabelen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen. Das System der Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ heißt eine Basis von $\mathfrak{a}$. Bildet man das Produkt aus allen n mit α konjugierten Ausdrücken, so erhält man

$$N(\alpha) = N(\mathfrak{a})X,$$

wo X eine homogene Funktion $n$ten Grades von den Variabelen $x_1, x_2 \cdots x_n$ bedeutet; die Koeffizienten dieser zerlegbaren Form X sind immer ganze rationale Zahlen ohne gemeinschaftlichen Teiler. Da das Ideal $\mathfrak{a}$ unendlich viele verschiedene Basen besitzt, so entspricht demselben eine Klasse von unendlich vielen äquivalenten Formen X, welche durch lineare Substitutionen mit ganzen rationalen Koeffizienten gegenseitig ineinander übergehen. Dieselben Formen entspringen aber auch aus jedem mit $\mathfrak{a}$ äquivalenten Ideal, und folglich entspricht jeder Ideal-Klasse eine bestimmte Formen-Klasse. Die Multiplikation der Ideale und der Ideal-Klassen führt zu der Komposition der Formen und der Formen-Klassen.

Aber diese Formen X umfassen nur einen unendlich kleinen Teil aller möglichen zu dem Körper Ω gehörenden Formen. Versteht man nämlich unter der Determinante einer aus n homogenen linearen Faktoren $f_1, f_2 \cdots f_n$ gebildeten Funktion F von

n Variabelen $h_1, h_2 \cdots h_n$ das Quadrat der Funktional-Determinante

$$\sum \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \cdots \frac{\partial f_n}{\partial h_n},$$

so ergibt sich leicht, daß die Determinante aller oben betrachteten Formen X mit der Grundzahl $D = \Delta(\Omega)$ des Körpers Ω übereinstimmt; für den Fall $n = 2$ würde man z. B. nur zu solchen binären Formen $ax^2 + bxy + cy^2$ gelangen, deren Determinante $b^2 - 4ac = D$ durch kein ungerades Quadrat teilbar und entweder $\equiv 1 \pmod 4$, oder $\equiv 8, 12 \pmod{16}$ ist*).

Um nun eine allgemeinere Theorie der zu einem Körper Ω gehörenden Formen aufzustellen, muß man, wie ich schon früher bemerkt habe (D. § 165), den Begriff des Ideals so erweitern, daß an Stelle des bisher betrachteten Gebietes $\mathfrak{o}$, welches alle ganzen Zahlen des Körpers umfaßt, beschränktere Gebiete $\mathfrak{o}'$ treten, welche ich mit Rücksicht auf die in der Theorie der binären quadratischen Formen von Gauß gebrauchte Ausdrucksweise Ordnungen genannt habe. Diese Erweiterung bildet den nächsten Gegenstand dieser Abhandlung.

§ 2.

Sätze aus der Theorie der Moduln.

Um hierzu zu gelangen, und namentlich um beständige Wiederholungen über die Art zu vermeiden, in welcher aus gewissen Systemen von Zahlen neue Systeme gebildet werden, ist es notwendig, hier einige sehr einfache und zugleich sehr allgemeine Sätze über solche Systeme einzuschalten, die ich Moduln genannt habe (D. § 161). Da der Begriff eines Ideals in demjenigen eines Moduls als spezieller Fall enthalten ist, so wird bei einer systematischen Darstellung die Theorie der Moduln zweckmäßig der Theorie der Ideale vorausgeschickt werden. Hier wird es genügen, einige Hauptbegriffe zu entwickeln und einige Sätze anzuführen, deren Beweise ich unterdrücke, weil jeder sie leicht finden wird (vgl. D. § 161 und B. §§ 1

*) Die obige Erklärung einer Formen-Determinante stimmt für den Fall $n = 2$ nicht ganz mit derjenigen von Gauß überein; dies läßt sich aber kaum vermeiden, wenn sie allgemein für jeden Grad n gelten soll, und selbst in dem speziellen Falle $n = 2$ sprechen viele Erscheinungen zugunsten derselben, was ich aber hier nicht näher begründen kann.

bis 4). Da manche dieser Sätze sich in Worten nur ziemlich umständlich aussprechen lassen, so wage ich es, die Ausdrucksweise durch Einführung einer Zeichensprache abzukürzen, und ich hoffe, daß man aus diesem Grunde die Benutzung der Zeichen $>$, $<$, $+$, $-$ entschuldigen wird. Ich bemerke nur noch, daß im folgenden die Einschränkung auf die Zahlen eines endlichen Körpers gänzlich wegfällt, also das Wort Zahl immer in seiner allgemeinsten Bedeutung gebraucht wird.

1°. Ein System $\mathfrak{m}$ von reellen oder komplexen Zahlen heißt ein Modul, wenn alle Summen und Differenzen dieser Zahlen demselben System $\mathfrak{m}$ angehören. Die Zahl 0 findet sich in jedem Modul, und sie bildet auch für sich allein einen Modul. Ein Modul $\mathfrak{m}$ heißt teilbar durch einen Modul $\mathfrak{a}$ oder ein Vielfaches von $\mathfrak{a}$, wenn alle Zahlen des Moduls $\mathfrak{m}$ auch in $\mathfrak{a}$ enthalten sind; zugleich heißt $\mathfrak{a}$ ein Teiler von $\mathfrak{m}$, und wir bezeichnen die Teilbarkeit von $\mathfrak{m}$ durch $\mathfrak{a}$ sowohl durch $\mathfrak{m} > \mathfrak{a}$, als durch $\mathfrak{a} < \mathfrak{m}$. Ist jeder der beiden Moduln $\mathfrak{m}$, $\mathfrak{a}$ durch den anderen teilbar, so sind sie identisch, was durch $\mathfrak{m} = \mathfrak{a}$ angedeutet wird. Aus $\mathfrak{m} > \mathfrak{a}$, $\mathfrak{a} > \mathfrak{b}$ folgt $\mathfrak{m} > \mathfrak{b}$. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so ist das System aller derjenigen Zahlen, welche beiden Moduln gemeinschaftlich angehören, selbst ein Modul, und zwar ein Vielfaches von $\mathfrak{a}$ und von $\mathfrak{b}$, welches durch $\mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a}$ bezeichnet werden soll; dasselbe heißt das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ durch $\mathfrak{a} - \mathfrak{b}$ teilbar ist. Durchläuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so ist das System aller Zahlen von der Form $\alpha + \beta$ ein Modul, und zwar ein Teiler von $\mathfrak{a}$ und von $\mathfrak{b}$, der mit $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$ bezeichnet werden soll; derselbe heißt der größte gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ auch ein Teiler von $\mathfrak{a} + \mathfrak{b}$ ist. Diese Begriffe lassen sich leicht auf beliebig viele, sogar auf unendlich viele Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ··· ausdehnen, und man beweist leicht die beiden folgenden charakteristischen Sätze

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c})),$$
$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c})),$$

in welchen sich der zwischen den Begriffen des kleinsten gemeinschaftlichen Vielfachen und des größten gemeinschaftlichen Teilers durchgängig herrschende Dualismus kundgibt.

2°. Zwei Zahlen α, β heißen kongruent oder inkongruent in bezug auf einen Modul $\mathfrak{m}$, je nachdem ihre Differenz $\alpha - \beta$ in $\mathfrak{m}$ enthalten ist oder nicht; die Kongruenz wird durch $\alpha \equiv \beta \pmod{\mathfrak{m}}$ ausgedrückt. Alle mit einer bestimmten Zahl nach $\mathfrak{m}$ kongruenten Zahlen bilden eine Zahl-Klasse (mod. $\mathfrak{m}$). Mehrere Zahlen heißen inkongruent (mod. $\mathfrak{m}$), wenn jede derselben mit jeder der übrigen inkongruent (mod. $\mathfrak{m}$) ist. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so kann es sein, daß $\mathfrak{a}$ nur eine endliche Anzahl inkongruenter Zahlen in bezug auf $\mathfrak{b}$ enthält, und dann soll diese Anzahl durch das Symbol $(\mathfrak{a}, \mathfrak{b})$ bezeichnet werden; gibt es aber in $\mathfrak{a}$ unendlich viele, in bezug auf $\mathfrak{b}$ inkongruente Zahlen, so soll $(\mathfrak{a}, \mathfrak{b}) = 0$ gesetzt werden, weil dann gewisse Determinanten-Sätze allgemein gültig bleiben. In beiden Fällen ist

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}, \mathfrak{b});$$

ist $\mathfrak{a} > \mathfrak{b}$, so ist $(\mathfrak{a}, \mathfrak{b}) = 1$, und umgekehrt. Ist ferner $\mathfrak{m} > \mathfrak{a} > \mathfrak{b}$, so ist

$$(\mathfrak{b}, \mathfrak{m}) = (\mathfrak{b}, \mathfrak{a})(\mathfrak{a}, \mathfrak{m}).$$

Durch Kombination beider Sätze erhält man viele andere Sätze, die hier übergangen werden können. Sind ϱ, σ zwei gegebene Zahlen, so hat das System der beiden Kongruenzen

$$\omega \equiv \varrho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}}$$

stets und nur dann gemeinschaftliche Wurzeln ω, wenn

$$\varrho \equiv \sigma \pmod{\mathfrak{a} + \mathfrak{b}}$$

ist, und die sämtlichen Zahlen ω bilden eine bestimmte Zahlklasse (mod. $\mathfrak{a} - \mathfrak{b}$).

3°. Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ Konstanten, während $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, so bilden die sämtlichen, in der Form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

darstellbaren Zahlen α einen Modul $\mathfrak{a}$, der ein endlicher Modul heißen und mit $[\alpha_1, \alpha_2 \cdots \alpha_n]$ bezeichnet werden soll; die Konstanten $\alpha_1, \alpha_2 \cdots \alpha_n$ bilden eine Basis des Moduls $\mathfrak{a}$. Der Modul [1] ist das System aller ganzen rationalen Zahlen. Wenn alle Zahlen eines solchen endlichen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ durch Multiplikation mit rationalen, von 0 verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{b}$ verwandelt werden können, so ist $(\mathfrak{a}, \mathfrak{b})$ von 0 verschieden, und $\mathfrak{a} - \mathfrak{b}$

ist ein endlicher Modul; man kann die ganzen rationalen Zahlen a so wählen, daß die n Zahlen

$$\begin{aligned}
\mu_1 &= a_1' \alpha_1, \\
\mu_2 &= a_1'' \alpha_1 + a_2'' \alpha_2, \\
\mu_3 &= a_1''' \alpha_1 + a_2''' \alpha_2 + a_3''' \alpha_3, \\
&\cdots\cdots\cdots\cdots \\
\mu_n &= a_1^{(n)} \alpha_1 + a_2^{(n)} \alpha_2 + a_3^{(n)} \alpha_3 + \cdots + a_n^{(n)} \alpha_n
\end{aligned}$$

eine Basis von $\mathfrak{a} - \mathfrak{b}$ bilden, und daß zugleich

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = a_1' a_2'' a_3''' \cdots a_n^{(n)}$$

wird; unterwirft man die n ganzen rationalen Zahlen $x_1', x_2' \cdots x_n'$ den n Bedingungen

$$0 \leqq x_r' < a_r^{(r)},$$

so sind die entsprechenden, in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha' = x_1' \alpha_1 + x_2' \alpha_2 + \cdots + x_n' \alpha_n,$$

deren Anzahl $= (\mathfrak{a}, \mathfrak{b})$ ist, sämtlich inkongruent (mod. $\mathfrak{b}$) und deshalb auch inkongruent (mod. $\mathfrak{a} - \mathfrak{b}$).

4°. Ein System von n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ soll ein irreduktibeles System, und diese Zahlen sollen voneinander unabhängig heißen, wenn die Summe

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n$$

für jedes System von rationalen, nicht sämtlich verschwindenden Zahlen $x_1, x_2 \cdots x_n$ einen von 0 verschiedenen Wert erhält. Ist nun wieder $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$, und sind die Basiszahlen eines Moduls $\mathfrak{m} = [\mu_1, \mu_2 \cdots \mu_n]$ von der Form

$$\begin{aligned}
\mu_1 &= a_1' \alpha_1 + a_2' \alpha_2 + \cdots + a_n' \alpha_n, \\
\mu_2 &= a_1'' \alpha_1 + a_2'' \alpha_2 + \cdots + a_n'' \alpha_n, \\
&\cdots\cdots\cdots\cdots \\
\mu_n &= a_1^{(n)} \alpha_1 + a_2^{(n)} \alpha_2 + \cdots + a_n^{(n)} \alpha_n,
\end{aligned}$$

wo die Koeffizienten a ganze rationale Zahlen bedeuten, so ist

$$(\mathfrak{a}, \mathfrak{m}) = \pm \sum \pm a_1' a_2'' \cdots a_n^{(n)}.$$

Von besonderer Wichtigkeit ist noch der folgende Satz: besteht eine Basis eines endlichen Moduls $\mathfrak{a}$ aus m Zahlen $\alpha_1', \alpha_2' \cdots \alpha_m'$, von denen aber nur n voneinander unabhängig sind, so gibt es immer eine aus n unabhängigen Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ bestehende Basis desselben Moduls $\mathfrak{a}$.

5°. Durchläuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so bilden die Produkte $\alpha\beta$ und alle Summen solcher Produkte einen Modul, der das Produkt aus den Faktoren $\mathfrak{a}$, $\mathfrak{b}$ heißen und mit $\mathfrak{ab}$ bezeichnet werden soll, aber keineswegs durch $\mathfrak{a}$ oder $\mathfrak{b}$ teilbar zu sein braucht. Offenbar ist $\mathfrak{ab} = \mathfrak{ba}$ und $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc}) = \mathfrak{abc}$; die Bedeutung einer Potenz $\mathfrak{a}^r$ ist selbstverständlich. Aus $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{b}' > \mathfrak{b}$ folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{ab}$; ferner ist

$$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{ac} + \mathfrak{bc},$$
$$(\mathfrak{a} - \mathfrak{b})\mathfrak{c} > \mathfrak{ac} - \mathfrak{bc},$$
$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} - \mathfrak{b}) > \mathfrak{ab};$$

ist ferner $[1] > \mathfrak{o}$, so ist $\mathfrak{a} > \mathfrak{oa}$, weil $\mathfrak{a}[1] = \mathfrak{a}$ ist. Ist $\mathfrak{b}$ ein eingliedriger Modul $[\mu]$, so besteht das Produkt $\mathfrak{ab}$ aus den Produkten $\alpha\mu$, wo α alle Zahlen des Moduls $\mathfrak{a}$ durchläuft; ein solches Produkt $\mathfrak{a}[\mu]$ soll bequemer durch $\mathfrak{a}\mu = \mu\mathfrak{a}$ bezeichnet werden; dann ist $(\mathfrak{a}\mu)\nu = \mathfrak{a}(\mu\nu)$, und aus $\mathfrak{a}\mu = \mathfrak{a}'\mu$ folgt immer $\mathfrak{a} = \mathfrak{a}'$, wenn μ von 0 verschieden ist.

6°. Ist $\mathfrak{a}$ ein beliebiger Modul, so bildet das System $\mathfrak{o}$ aller derjenigen Zahlen ω, für welche das Produkt $\mathfrak{a}\omega > \mathfrak{a}$ wird, einen Modul, welcher die Ordnung des Moduls $\mathfrak{a}$ heißen soll und offenbar stets ein Teiler des Moduls $[1]$ ist; hieraus folgt unmittelbar, daß $\mathfrak{ao} = \mathfrak{a}$, und $\mathfrak{o}^2 = \mathfrak{o}$ ist. Umgekehrt ist jeder Modul $\mathfrak{o}$, der ein Teiler von $[1]$ und von $\mathfrak{o}^2$ ist, eine Ordnung, nämlich diejenige des Moduls $\mathfrak{o}$ selbst. Der Begriff einer Ordnung bildet eigentlich nur einen speziellen Fall des Begriffes des Quotienten $\mathfrak{a} : \mathfrak{b}$ von zwei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, worunter der größte gemeinschaftliche Teiler aller derjenigen Moduln $\mathfrak{c}$ zu verstehen ist, für welche das Produkt $\mathfrak{bc}$ durch $\mathfrak{a}$ teilbar wird; die Ordnung $\mathfrak{o}$ eines Moduls $\mathfrak{a}$ ist nämlich identisch mit dem Quotienten $\mathfrak{a} : \mathfrak{a}$, und die charakteristische Eigenschaft einer jeden Ordnung $\mathfrak{o}$ wird durch die Gleichung $\mathfrak{o} : \mathfrak{o} = \mathfrak{o}$ ausgedrückt. Doch wird von dem Begriff des Quotienten in dieser Abhandlung kein Gebrauch gemacht werden.

§ 3.

Ordnungen in einem endlichen Körper.

Nach diesen allgemeinen Vorbereitungen kehren wir definitiv zu den Zahlen eines endlichen Körpers Ω vom Grade n zurück, und beschränken zunächst den Begriff des Moduls in der Weise, daß unter einem Modul $\mathfrak{a}$ stets ein endlicher Modul $[\alpha_1, \alpha_2 \cdots \alpha_n]$ verstanden

wird, dessen Basiszahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ zugleich eine Basis des Körpers Ω bilden (§ 1) und folglich voneinander unabhängig sind (§ 2, 4°). Da hiernach jede Zahl des Körpers Ω durch Multiplikation mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Moduls $\mathfrak{a}$ verwandelt werden kann, so ergibt sich aus den vorhergehenden allgemeinen Sätzen sehr leicht, daß das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler, und ebenso das Produkt (und auch der Quotient) von je zwei solchen Moduln $\mathfrak{a}$, $\mathfrak{b}$ stets wieder ein solcher Modul, und daß $(\mathfrak{a}, \mathfrak{b})$ stets von 0 verschieden ist. Versteht man ferner wie früher, und wie es auch in der Folge stets geschehen soll, unter $\mathfrak{o}$ das Gebiet aller ganzen Zahlen des Körpers Ω, so kommt die Definition eines Ideals $\mathfrak{m}$ (§ 1, 1°) darauf hinaus, daß $\mathfrak{m}$ ein durch $\mathfrak{o}$ teilbarer Modul ist (I), welcher der Bedingung $\mathfrak{o}\mathfrak{m} = \mathfrak{m}$ genügt (II); die dortigen Sätze 5°, 6°, 9° enthalten nur noch die Behauptung, daß das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler und das Produkt von zwei beliebigen Idealen wieder Ideale sind; die Norm eines Ideals $\mathfrak{m}$ ist $= (\mathfrak{o}, \mathfrak{m})$.

Für die in Aussicht genommene Erweiterung des Ideal-Begriffs ist nun vor allem die Konstitution der Ordnung $\mathfrak{o}'$ eines beliebigen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ von Wichtigkeit (§ 2, 6°). Damit eine Zahl ω' der Ordnung $\mathfrak{o}'$ des Moduls $\mathfrak{a}$ angehöre, ist offenbar erforderlich und hinreichend, daß die n Produkte $\omega'\alpha_1, \omega'\alpha_2 \cdots \omega'\alpha_n$ in $\mathfrak{a}$ enthalten sind, daß also

$$\begin{aligned}
\omega'\alpha_1 &= x_1'\alpha_1 + x_2'\alpha_2 + \cdots + x_n'\alpha_n,\\
\omega'\alpha_2 &= x_1''\alpha_1 + x_2''\alpha_2 + \cdots + x_n''\alpha_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\omega'\alpha_n &= x_1^{(n)}\alpha_1 + x_2^{(n)}\alpha_2 + \cdots + x_n^{(n)}\alpha_n
\end{aligned}$$

ist, wo die n^2 Koeffizienten x sämtlich ganze rationale Zahlen bedeuten. Aus jeder einzelnen dieser Gleichungen folgt zunächst, daß ω' eine Zahl des Körpers Ω ist, und wenn man die n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eliminiert, so erhält man

$$\begin{vmatrix}
x_1' - \omega', & x_2' & \cdots & x_n'\\
x_1'' & x_2'' - \omega' & \cdots & x_n''\\
\cdots & \cdots & \cdots & \cdots\\
x_1^{(n)} & x_2^{(n)} & \cdots & x_n^{(n)} - \omega'
\end{vmatrix} = 0,$$

d. h. ω' ist eine ganze algebraische Zahl, also in dem Gebiete $\mathfrak{o}$ enthalten; mithin ist $\mathfrak{o}'$ ein Vielfaches von $\mathfrak{o}$. Versteht man jetzt für

einen Augenblick unter ω' eine beliebige Zahl des Körpers Ω, so gehören auch die n Produkte $\omega'\alpha_1$, $\omega'\alpha_2 \cdots \omega'\alpha_n$ dem Körper Ω an, und folglich werden, da $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden, wieder n Gleichungen von der obigen Form stattfinden, in welchen aber die n^2 rationalen Koeffizienten x nicht mehr notwendig ganze Zahlen sind; es wird dann immer eine von 0 verschiedene, rationale Zahl m von der Art geben, daß die sämtlichen n^2 Produkte mx ganze Zahlen werden, und folglich wird das Produkt $m\omega'$ eine Zahl der Ordnung $\mathfrak{o}'$ sein; jede Zahl des Körpers Ω, also auch jede Zahl des Gebietes $\mathfrak{o}$ kann daher durch Multiplikation mit einer von 0 verschiedenen rationalen Zahl in eine Zahl der Ordnung $\mathfrak{o}'$ verwandelt werden, und da das Gebiet $\mathfrak{o} = [\omega_1, \omega_2 \cdots \omega_n]$ ein Teiler von $\mathfrak{o}'$ ist, so ist (nach § 2, 3⁰) $\mathfrak{o}'$ ein endlicher Modul $[\omega_1', \omega_2' \cdots \omega_n']$, dessen Basiszahlen mit denen von $\mathfrak{o}$ durch n Gleichungen von der Form

$$\begin{aligned}
\omega_1' &= k_1'\omega_1 + k_2'\omega_2 + \cdots + k_n'\omega_n, \\
\omega_2' &= k_1''\omega_1 + k_2''\omega_2 + \cdots + k_n''\omega_n, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\omega_n' &= k_1^{(n)}\omega_1 + k_2^{(n)}\omega_2 + \cdots + k_n^{(n)}\omega_n
\end{aligned}$$

verbunden sind, deren Koeffizienten ganze rationale Zahlen sind und eine von 0 verschiedene, positive Determinante

$$\sum \pm k_1' k_2'' \cdots k_n^{(n)} = (\mathfrak{o}, \mathfrak{o}') = k$$

besitzen. Die charakteristischen Eigenschaften einer solchen Ordnung $\mathfrak{o}'$ sind daher (§ 2, 6⁰) die folgenden:

1⁰. $\mathfrak{o}'$ ist ein durch $\mathfrak{o}$ teilbarer Modul im obigen beschränkten Sinne des Wortes; alle in $\mathfrak{o}'$ enthaltenen Zahlen sind ganze Zahlen des Körpers Ω.

2⁰. $\mathfrak{o}'$ ist ein Teiler von [1], d. h. alle ganzen rationalen Zahlen sind in $\mathfrak{o}'$ enthalten.

3⁰. $\mathfrak{o}'$ ist ein Teiler von $\mathfrak{o}'^2$, d. h. jedes Produkt von zwei in $\mathfrak{o}'$ enthaltenen Zahlen gehört ebenfalls dem System $\mathfrak{o}'$ an. Aus 2⁰ folgt dann $\mathfrak{o}'^2 = \mathfrak{o}'$.

Aus den obigen Gleichungen folgt nun durch Umkehrung, daß die n Produkte $k\omega_1$, $k\omega_2 \cdots k\omega_n$ der Ordnung $\mathfrak{o}'$ angehören, und folglich ist das Hauptideal $\mathfrak{o}k$ teilbar durch $\mathfrak{o}'$. Da ferner der größte gemeinschaftliche Teiler von je zwei durch $\mathfrak{o}'$ teilbaren Idealen selbst wieder ein durch $\mathfrak{o}'$ teilbares Ideal ist, so gibt es unter diesen, durch

$\mathfrak{o}'$ teilbaren Idealen ein einziges, völlig bestimmtes Ideal $\mathfrak{k}$ von kleinster Norm, und die genannten Ideale sind (nach § 1, 10°) identisch mit den sämtlichen Produkten $\mathfrak{a}\mathfrak{k}$, wo $\mathfrak{a}$ alle Ideale durchläuft. Dieses Ideal $\mathfrak{k}$ soll der Führer der Ordnung $\mathfrak{o}'$ heißen. Da das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{o}'$ und folglich auch durch $\mathfrak{k}$ teilbar ist, so ist k^n als Norm von $\mathfrak{o}k$ teilbar durch

$$N(\mathfrak{k}) = (\mathfrak{o}, \mathfrak{k}) = (\mathfrak{o}, \mathfrak{o}')(\mathfrak{o}', \mathfrak{k}) = k(\mathfrak{o}', \mathfrak{k}).$$

Ist der Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ und für jede der $(\mathfrak{o}', \mathfrak{k})$ Zahlklassen, aus denen $\mathfrak{o}'$ besteht, ein Repräsentant gegeben, so ist $\mathfrak{o}'$ vollständig definiert. Nicht jedes Ideal $\mathfrak{k}$ kann der Führer einer Ordnung sein, sondern hierzu ist eine gewisse Bedingung erforderlich, deren Auffindung keine großen Schwierigkeiten darbietet; doch würde die Ableitung derselben sowie ein näheres Eingehen auf die Konstitution der Ordnungen überhaupt, uns hier zu weit führen. Das Gebiet $\mathfrak{o}$ ist offenbar selbst eine Ordnung und auch zugleich der Führer derselben.

§ 4.

Ideale der Ordnung $\mathfrak{o}'$.

Es sei nun $\mathfrak{o}'$ eine bestimmte Ordnung im Körper Ω, und $\mathfrak{k}$ der Führer derselben, so wollen wir ein System $\mathfrak{a}'$ von unendlich vielen Zahlen ein Ideal der Ordnung $\mathfrak{o}'$ oder kürzer ein Ideal in $\mathfrak{o}'$ nennen, wenn es die folgenden drei Bedingungen erfüllt:

I. Die Summen und Differenzen von je zwei in $\mathfrak{a}'$ enthaltenen Zahlen gehören ebenfalls dem System $\mathfrak{a}'$ an, d. h. $\mathfrak{a}'$ ist ein Modul im allgemeinsten Sinne des Wortes.

II. Jedes Produkt aus einer Zahl des Systems $\mathfrak{a}'$ und aus einer Zahl der Ordnung $\mathfrak{o}'$ ist eine Zahl des Systems $\mathfrak{a}'$; d. h. $\mathfrak{o}'\mathfrak{a}'$ ist teilbar durch $\mathfrak{a}'$ und folglich auch $= \mathfrak{a}'$, weil $\mathfrak{o}'$ ein Teiler von [1] ist.

III. Der größte gemeinschaftliche Teiler $\mathfrak{a}' + \mathfrak{k}$ von $\mathfrak{a}'$ und $\mathfrak{k}$ ist $= \mathfrak{o}'$.

Für den Fall, daß die Ordnung $\mathfrak{o}'$ identisch mit $\mathfrak{o}$ ist, geht diese Definition eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ vollständig in die frühere Definition (§ 1, 1°) eines Ideals über, da die dritte Bedingung nur darauf hinauskommt, daß $\mathfrak{a}'$ durch $\mathfrak{o}$ teilbar ist. Wir werden daher diese Ideale künftig, wenn Mißverständnisse zu befürchten sind, Ideale in $\mathfrak{o}$ zu nennen haben. Im folgenden nehmen wir immer an, daß $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist.

Ist nun α' eine beliebige, aber von 0 verschiedene Zahl in $\mathfrak{a}'$, und bilden die n Zahlen $\omega_1', \omega_2' \cdots \omega_n'$ eine Basis der Ordnung $\mathfrak{o}'$, so sind die n Produkte $\alpha'\omega_1', \alpha'\omega_2', \cdots \alpha'\omega_n'$, welche (zufolge II) in $\mathfrak{a}'$ enthalten sind, voneinander unabhängig und bilden folglich eine Basis des Körpers Ω; mithin kann jede Zahl des Körpers durch Multiplikation mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Ideals $\mathfrak{a}'$ verwandelt werden, woraus wieder leicht folgt, daß $\mathfrak{a}'$ ein endlicher Modul $[\alpha_1', \alpha_2' \cdots \alpha_n']$, also ein Modul in dem Sinne des § 3 ist. Die Basiszahlen haben die Form

$$\begin{aligned}
\alpha_1' &= a_1'\omega_1' + a_2'\omega_2' + \cdots + a_n'\omega_n', \\
\alpha_2' &= a_1''\omega_1' + a_2''\omega_2' + \cdots + a_n''\omega_n', \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha_n' &= a_1^{(n)}\omega_1' + a_2^{(n)}\omega_2' + \cdots + a_n^{(n)}\omega_n',
\end{aligned}$$

wo die Koeffizienten ganze rationale Zahlen sind, deren Determinante

$$\sum \pm a_1' a_2'' \cdots a_n^{(n)} = (\mathfrak{o}', \mathfrak{a}')$$

die Norm des Ideals $\mathfrak{a}'$ heißen und mit $N'(\mathfrak{a}')$ bezeichnet werden soll.

Es ergibt sich ferner leicht, daß $\mathfrak{o}'$ auch die Ordnung des Ideals $\mathfrak{a}'$ ist; in der Tat besteht die letztere, die wir mit $\mathfrak{o}_1$ bezeichnen wollen, zufolge ihrer Definition (§ 2, 6°) aus allen Zahlen ω_1, für welche $\mathfrak{a}'\omega_1 > \mathfrak{a}'$ wird, und da (nach II) $\mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'$ ist, so ist jedenfalls $\mathfrak{o}' > \mathfrak{o}_1$, und es braucht nur noch bewiesen zu werden, daß umgekehrt auch $\mathfrak{o}_1 > \mathfrak{o}'$ ist. Da nun $\mathfrak{a}'$ ein endlicher Modul des Körpers, und folglich (nach § 3, 1° und 2°) $[1] > \mathfrak{o}_1 > \mathfrak{o}$ ist, so ergibt sich $\mathfrak{k}[1] > \mathfrak{k}\mathfrak{o}_1 > \mathfrak{k}\mathfrak{o}$, mithin $\mathfrak{k}\mathfrak{o}_1 = \mathfrak{k}$, weil $\mathfrak{k}[1] = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$ ist; da außerdem (nach § 2, 6°) $\mathfrak{a}'\mathfrak{o}_1 = \mathfrak{a}'$, und (nach III) $\mathfrak{o}' = \mathfrak{k} + \mathfrak{a}'$ ist, so folgt $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{k}\mathfrak{o}_1 + \mathfrak{a}'\mathfrak{o}_1 = \mathfrak{k} + \mathfrak{a}'$, also $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{o}'$; nun ist aber $[1] > \mathfrak{o}'$, also auch $[1]\mathfrak{o}_1 > \mathfrak{o}'\mathfrak{o}_1$, d. h. $\mathfrak{o}_1 > \mathfrak{o}'$, was zu beweisen war.

Sind ferner $\mathfrak{a}'$, $\mathfrak{b}'$ zwei beliebige Ideale in $\mathfrak{o}'$, so überzeugt man sich leicht, daß $\mathfrak{a}' - \mathfrak{b}'$, $\mathfrak{a}' + \mathfrak{b}'$, $\mathfrak{a}'\mathfrak{b}'$ ebenfalls Ideale in $\mathfrak{o}'$ sind, und daß $\mathfrak{a}'\mathfrak{b}'$ sowohl durch $\mathfrak{a}'$ als durch $\mathfrak{b}'$ teilbar ist. Der Kürze wegen beschränke ich mich auf die Betrachtung des Produkts. Da $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, so ergibt sich $\mathfrak{o}'(\mathfrak{a}'\mathfrak{b}') = (\mathfrak{o}'\mathfrak{a}')\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}'$, also besitzt $\mathfrak{a}'\mathfrak{b}'$ die Eigenschaft II. Da ferner $\mathfrak{b}' > \mathfrak{o}'$ und $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$ ist, so folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{a}'$; ebenso ist $\mathfrak{a}'\mathfrak{b}'$ durch $\mathfrak{b}'$ teilbar. Da endlich $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{k}$ ist, so folgt $\mathfrak{b}' = \mathfrak{o}'\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}'$, also $\mathfrak{o}' = \mathfrak{b}' + \mathfrak{k} = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}' + \mathfrak{k}$; da nun $\mathfrak{k} = \mathfrak{k}\mathfrak{o}$, und $\mathfrak{b}' > \mathfrak{o}$ ist, so folgt $\mathfrak{k}\mathfrak{b}' + \mathfrak{k} = \mathfrak{k}(\mathfrak{b}' + \mathfrak{o}) = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$, also $\mathfrak{o}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}$, womit auch die Eigenschaft III für $\mathfrak{a}'\mathfrak{b}'$ dargetan ist.

§ 5.

Korrespondenz zwischen den Idealen in $\mathfrak{o}'$ und $\mathfrak{o}$.

Man könnte nun eine Theorie der Ideale in $\mathfrak{o}'$ aufstellen, welche sowohl in den Sätzen wie in ihren Beweisen eine vollständige Analogie mit der früheren Theorie der Ideale in $\mathfrak{o}$ darbieten würde. Allein es ist viel bequemer, die neue Theorie auf die alte zurückzuführen. Dies geschieht durch die folgenden Sätze.

1°. Ist $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, so ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{f}$; zugleich ist $\mathfrak{a}'$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{o}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}'$ und $\mathfrak{o}\mathfrak{a}'$, und folglich $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. Ist ferner $\mathfrak{b}'$ ebenfalls ein Ideal in $\mathfrak{o}'$, und $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$, so ist $\mathfrak{a}' = \mathfrak{b}'$.

Beweis. Der Modul $\mathfrak{o}\mathfrak{a}'$ genügt der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{a}') = \mathfrak{o}\mathfrak{a}'$, weil $\mathfrak{o}^2 = \mathfrak{o}$ ist, und er ist teilbar durch $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $[1] > \mathfrak{o}' > \mathfrak{o}$ ist; also ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$. Aus $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{f}$ folgt durch Multiplikation mit $\mathfrak{o}$ ferner $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{f}$, also sind $\mathfrak{o}\mathfrak{a}'$ und $\mathfrak{f}$ relative Primideale. Hieraus ergibt sich ferner (entweder nach der bekannten Theorie der Ideale in $\mathfrak{o}$, oder auch unmittelbar), daß ihr kleinstes gemeinschaftliches Vielfaches $\mathfrak{f} - \mathfrak{o}\mathfrak{a}' = \mathfrak{f}\mathfrak{o}\mathfrak{a}' = \mathfrak{f}\mathfrak{a}'$ ist. Wendet man nun den allgemeinen Satz (§ 2, 1°)

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{a}'$, $\mathfrak{b} = \mathfrak{f}$, $\mathfrak{c} = \mathfrak{o}\mathfrak{a}'$ an, so ergibt sich, weil $\mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = (\mathfrak{o}' + \mathfrak{o})\mathfrak{a}' = \mathfrak{o}\mathfrak{a}'$ ist,

$$\begin{aligned}\mathfrak{o}' - \mathfrak{o}\mathfrak{a}' &= \mathfrak{a}' + (\mathfrak{f} - \mathfrak{o}\mathfrak{a}') = \mathfrak{a}' + \mathfrak{f}\mathfrak{a}' \\ &= \mathfrak{a}'(\mathfrak{o}' + \mathfrak{f}) = \mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'.\end{aligned}$$

Ferner ist

$$\mathfrak{o}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{f} + \mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{f} + \mathfrak{o}\mathfrak{a}' = \mathfrak{o}.$$

Hieraus ergibt sich (nach § 2, 2°)

$$(\mathfrak{o}', \mathfrak{o}\mathfrak{a}') = (\mathfrak{o}', \mathfrak{a}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{a}'),$$

also $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. Aus $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$ folgt endlich, weil $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{a}'$ und $\mathfrak{b}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{b}'$ ist, auch $\mathfrak{a}' = \mathfrak{b}'$, was zu beweisen war.

2°. Ist $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{f}$, so ist das kleinste gemeinschaftliche Vielfache $\mathfrak{a}'$ von $\mathfrak{o}'$, $\mathfrak{a}$ ein Ideal in $\mathfrak{o}'$, und zugleich ist $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$.

Beweis. Zunächst ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}\mathfrak{a} = \mathfrak{a}$, weil $\mathfrak{o}' > \mathfrak{o}$, $\mathfrak{a}' > \mathfrak{a}$ ist; außerdem ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}'$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $\mathfrak{o}'\mathfrak{o}' = \mathfrak{o}'$ ist; mithin ist

$\mathfrak{o}'\mathfrak{a}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$ und folglich auch teilbar durch $\mathfrak{a}'$, d. h. $\mathfrak{a}'$ genügt der Bedingung II. Nach einem für drei beliebige Moduln $\mathfrak{a}$, $\mathfrak{k}$, $\mathfrak{o}'$ geltenden Satze (§ 2, 1°) ist ferner

$$(\mathfrak{o}' - \mathfrak{a}) + (\mathfrak{o}' - \mathfrak{k}) = \mathfrak{o}' - (\mathfrak{a} + (\mathfrak{o}' - \mathfrak{k})),$$

und da in unserem Falle $\mathfrak{o}' - \mathfrak{a} = \mathfrak{a}'$, $\mathfrak{o}' - \mathfrak{k} = \mathfrak{k}$, $\mathfrak{a} + \mathfrak{k} = \mathfrak{o}$, $\mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$ ist, so ergibt sich $\mathfrak{a}' + \mathfrak{k} = \mathfrak{o}'$, also genügt $\mathfrak{a}'$ auch der Bedingung III und ist folglich ein Ideal in $\mathfrak{o}'$. Hieraus folgt (nach dem Satze 1°), daß $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und daß zugleich $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{k}$, also auch $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'\mathfrak{a} + \mathfrak{k}\mathfrak{a}$ ist; da nun $\mathfrak{a}$, $\mathfrak{k}$ Ideale in $\mathfrak{o}$ sind, so ist $\mathfrak{k}\mathfrak{a} > \mathfrak{k} > \mathfrak{o}'$ und $\mathfrak{k}\mathfrak{a} > \mathfrak{a}$, also muß $\mathfrak{k}\mathfrak{a}$, als gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$, durch $\mathfrak{a}'$ und folglich auch durch $\mathfrak{o}\mathfrak{a}'$ teilbar sein; da nun auch $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ durch $\mathfrak{o}\mathfrak{a}'$ teilbar, also $\mathfrak{o}\mathfrak{a}'$ ein gemeinschaftlicher Teiler von $\mathfrak{k}\mathfrak{a}$ und $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ ist, so folgt, daß $\mathfrak{a}$ als größter gemeinschaftlicher Teiler von $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ und $\mathfrak{k}\mathfrak{a}$ gewiß durch $\mathfrak{o}\mathfrak{a}'$ teilbar ist; umgekehrt ist aber auch $\mathfrak{o}\mathfrak{a}' > \mathfrak{a}$, weil $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ ist; mithin ist $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$, was zu beweisen war.

Durch diese beiden Sätze ist eine eindeutige, gegenseitige Korrespondenz zwischen allen Idealen $\mathfrak{a}'$ in $\mathfrak{o}'$ und allen denjenigen Idealen $\mathfrak{a}$ in $\mathfrak{o}$ begründet, welche relative Primideale zum Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ sind; die Korrespondenz zwischen $\mathfrak{a}$ und $\mathfrak{a}'$ besteht darin, daß gleichzeitig $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'$, und $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ ist. Offenbar entsprechen sich auf diese Weise die beiden Ideale $\mathfrak{o}$ und $\mathfrak{o}'$.

Es ist schon oben (§ 4) bewiesen, daß jedes Produkt $\mathfrak{a}'\mathfrak{b}'$ aus zwei Idealen $\mathfrak{a}'$, $\mathfrak{b}'$ in $\mathfrak{o}'$ wieder ein Ideal $\mathfrak{c}'$ in $\mathfrak{o}'$, und zwar durch $\mathfrak{a}'$ und durch $\mathfrak{b}'$ teilbar ist; da nun $\mathfrak{o}^2 = \mathfrak{o}$ ist, so ist gleichzeitig $\mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}' = \mathfrak{o}\mathfrak{c}'$, also (nach § 1, 9°) $N(\mathfrak{o}\mathfrak{a}'\mathfrak{b}') = N(\mathfrak{o}\mathfrak{a}')N(\mathfrak{o}\mathfrak{b}')$ und folglich auch

$$N'(\mathfrak{a}'\mathfrak{b}') = N'(\mathfrak{a}')N'(\mathfrak{b}').$$

Umgekehrt: wenn $\mathfrak{a}'$, $\mathfrak{c}'$ Ideale in $\mathfrak{o}'$ sind, und wenn $\mathfrak{c}'$ durch $\mathfrak{a}'$ teilbar ist, so ist auch $\mathfrak{o}\mathfrak{c}' > \mathfrak{o}\mathfrak{a}'$, und folglich (§ 1, 10°) gibt es ein und nur ein Ideal $\mathfrak{b}$ in $\mathfrak{o}$, für welches $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}$ wird; da nun $\mathfrak{o}\mathfrak{c}'$, also auch $\mathfrak{b}$, relatives Primideal zu $\mathfrak{k}$ ist, so gibt es (nach 2°) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$, für welches $\mathfrak{o}\mathfrak{b}' = \mathfrak{b}$ wird; es ist daher $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$, woraus (nach 1°) $\mathfrak{c}' = \mathfrak{a}'\mathfrak{b}'$ folgt; wäre nun zugleich $\mathfrak{c}' = \mathfrak{a}'\mathfrak{b}'$ und $\mathfrak{b}'$ ebenfalls ein Ideal in $\mathfrak{o}'$, so würde $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}'$, und hieraus (nach § 1, 10°) $\mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{b}'$, also auch $\mathfrak{b}' = \mathfrak{b}'$ folgen. Hiermit ist folgender Satz bewiesen:

3^0. Ist das Ideal $\mathfrak{c}'$ in $\mathfrak{o}'$ teilbar durch das Ideal $\mathfrak{a}'$ in $\mathfrak{o}'$, so gibt es ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{a}'\mathfrak{b}' = \mathfrak{c}'$ wird; außerdem ist immer $N'(\mathfrak{a}'\mathfrak{b}') = N'(\mathfrak{a}')N'(\mathfrak{b}')$.

Aus allem diesen ergibt sich ohne weiteres, daß die Gesetze der Teilbarkeit der Ideale in $\mathfrak{o}'$ und ihrer Multiplikation gänzlich mit den Gesetzen der Teilbarkeit derjenigen Ideale in $\mathfrak{o}$, welche relative Primideale zu $\mathfrak{k}$ sind, übereinstimmen und durch die genannte Korrespondenz aus den letzteren unmittelbar entnommen werden.

§ 6.

Hauptideale und Ideal-Klassen in $\mathfrak{o}'$.

Zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ des Körpers Ω, d. h. endliche Moduln, deren Basen zugleich Basen des Körpers sind (§ 3), sollen äquivalent heißen, wenn es eine Zahl μ von der Beschaffenheit gibt, daß $\mathfrak{a}\mu = \mathfrak{b}$, und folglich, da μ nicht verschwinden kann, auch $\mathfrak{b}\mu^{-1} = \mathfrak{a}$ wird. Offenbar muß μ eine Zahl des Körpers Ω sein, und wir wollen dem vorstehenden Begriff der Äquivalenz noch die Beschränkung hinzufügen, daß $\mathfrak{a}$, $\mathfrak{b}$ nur dann äquivalent heißen sollen, wenn eine Zahl μ von der genannten Beschaffenheit existiert, deren Norm zugleich positiv ist; wenn aber der Bedingung $\mathfrak{a}\mu = \mathfrak{b}$ nur durch solche Zahlen μ genügt werden kann, deren Normen negativ sind, so können $\mathfrak{a}$, $\mathfrak{b}$ halb-äquivalent genannt werden. Sind zwei Moduln $\mathfrak{b}$, $\mathfrak{c}$ mit einem dritten $\mathfrak{a}$ äquivalent, so sind $\mathfrak{b}$, $\mathfrak{c}$ offenbar auch miteinander äquivalent. Man kann daher die Moduln des Körpers Ω in Modul-Klassen einteilen, deren jede aus allen den Moduln besteht, welche mit einem bestimmten Modul, dem Repräsentanten der Klasse, äquivalent sind. Alle Moduln einer Klasse besitzen dieselbe Ordnung $\mathfrak{o}'$, welche die Ordnung der Klasse heißen soll; denn wenn $\mathfrak{a}\mu = \mathfrak{b}$, und ω' irgend eine Zahl ist, für welche $\mathfrak{a}\omega' > \mathfrak{a}$ wird, so folgt durch Multiplikation mit μ oder $[\mu]$, daß auch $\mathfrak{b}\omega' > \mathfrak{b}$ ist, und umgekehrt ergibt sich hieraus wieder $\mathfrak{a}\omega' > \mathfrak{a}$. Durchläuft $\mathfrak{a}$ alle Moduln einer Klasse A, ebenso $\mathfrak{b}$ alle Moduln einer Klasse B, so gehören offenbar alle Produkte $\mathfrak{a}\mathfrak{b}$ einer und derselben Klasse an, welche die aus A, B zusammengesetzte Klasse oder das Produkt aus A, B heißen und mit AB bezeichnet werden soll.

Wir beschränken uns aber hier auf die Betrachtung der Ideale und verstehen unter einer Ideal-Klasse der Ordnung $\mathfrak{o}'$ den Inbegriff A' aller Ideale in $\mathfrak{o}'$, welche mit einem bestimmten Ideal $\mathfrak{a}'$

in $\mathfrak{o}'$ äquivalent sind. Jedes mit $\mathfrak{o}'$ selbst äquivalente Ideal soll ein Hauptideal in $\mathfrak{o}'$, und der Inbegriff aller dieser Hauptideale soll die Hauptklasse in $\mathfrak{o}'$ heißen und mit O' bezeichnet werden. Ein solches Hauptideal ist daher von der Form $\mathfrak{o}'\mu$, wo μ in $\mathfrak{o}'$ enthalten ist, weil $\mathfrak{o}'\mu$ durch $\mathfrak{o}'$ teilbar sein muß; außerdem muß das zugehörige Ideal $\mathfrak{o}\mathfrak{o}'\mu = \mathfrak{o}\mu$ relatives Primideal zu $\mathfrak{k}$, d. h. μ muß relative Primzahl zu $\mathfrak{k}$ sein (D. § 163, 7.). Umgekehrt, ist die in $\mathfrak{o}'$ enthaltene Zahl μ relative Primzahl zu $\mathfrak{k}$, und ist $N(\mu) > 0$, so ist $\mathfrak{o}'\mu$ offenbar ein Hauptideal in $\mathfrak{o}'$. Nun besteht folgender Satz, von welchem wichtige Anwendungen zu machen sind:

1°. Ist $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, und $\mathfrak{n}'$ ein durch $\mathfrak{o}'$ teilbarer Modul, welcher der Bedingung $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$ genügt, so gibt es immer ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{a}'\mathfrak{b}'$ ein Hauptideal in $\mathfrak{o}'$, und $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ wird.

Beweis. Der Modul $\mathfrak{o}\mathfrak{n}'$ ist ein Ideal in $\mathfrak{o}$, weil er durch $\mathfrak{o}$ teilbar ist und der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{n}') = \mathfrak{o}\mathfrak{n}'$ genügt. Man zerlege nun $\mathfrak{o}\mathfrak{n}'$ in seine sämtlichen Primideal-Faktoren (§ 1, 12°) und bezeichne mit $\mathfrak{k}_1$ das Produkt aller derjenigen dieser Primideale, welche in $\mathfrak{k}$ aufgehen, mit $\mathfrak{n}_1$ das Produkt aller übrigen, so daß $\mathfrak{o}\mathfrak{n}' = \mathfrak{k}_1\mathfrak{n}_1$ wird. Nun gibt es (§ 1, 14° oder D. § 163, 7.) immer ein Ideal $\mathfrak{m}_1$ in $\mathfrak{o}$ von der Art, daß $\mathfrak{o}\mathfrak{a}'\mathfrak{m}_1 = \mathfrak{a}'\mathfrak{m}_1 = \mathfrak{o}\alpha$, d. h. ein Hauptideal in $\mathfrak{o}$, und daß zugleich $\mathfrak{m}_1 + \mathfrak{n}_1 = \mathfrak{o}$, also $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$ wird. Da ferner $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, also $\mathfrak{o}\mathfrak{a}'$ relatives Primideal zu $\mathfrak{k}$ ist, so sind auch $\mathfrak{o}\mathfrak{a}'\mathfrak{n}_1 = \mathfrak{a}'\mathfrak{n}_1$ und $\mathfrak{k}\mathfrak{k}_1$ relative Primideale, und folglich (§ 2, 2° oder D. § 163, 7.) gibt es Zahlen μ, welche den beiden gleichzeitigen Kongruenzen

$$\mu \equiv \alpha \pmod{\mathfrak{a}'\mathfrak{n}_1}, \quad \mu \equiv 1 \pmod{\mathfrak{k}\mathfrak{k}_1}$$

genügen; diese Zahlen μ bilden eine bestimmte Zahl-Klasse in bezug auf den Modul $\mathfrak{a}'\mathfrak{n}_1\mathfrak{k}\mathfrak{k}_1 = \mathfrak{k}\mathfrak{a}'\mathfrak{n}'$, und man kann, wie unten nachträglich bewiesen werden soll, die Zahl μ zugleich so wählen, daß $N(\mu) > 0$ wird. Aus der zweiten der beiden vorstehenden Kongruenzen folgt nun, daß μ relative Primzahl zu $\mathfrak{k}\mathfrak{k}_1$ und folglich auch zu $\mathfrak{k}$ ist; da ferner $\mathfrak{k}\mathfrak{k}_1 > \mathfrak{k} > \mathfrak{o}'$, und da die Zahl 1 in der Ordnung $\mathfrak{o}'$ enthalten ist, so ist zufolge der zweiten Kongruenz auch μ in $\mathfrak{o}'$ enthalten, und folglich ist $\mathfrak{o}'\mu$ ein Hauptideal in $\mathfrak{o}'$. Aus der ersten Kongruenz folgt ferner mit Rücksicht auf $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, daß auch $\mathfrak{o}\mu + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, und folglich $\mathfrak{o}\mu = \mathfrak{o}\mathfrak{a}'\mathfrak{b} = \mathfrak{a}'\mathfrak{b}$ ist, wo $\mathfrak{b}$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{n}_1$ ist. Da ferner $\mathfrak{o}\mu$, und

folglich auch $\mathfrak{b}$ relatives Primideal zu $\mathfrak{f}\mathfrak{f}_1$ ist, so ist $\mathfrak{b}$ auch relatives Primideal zu $\mathfrak{f}\mathfrak{f}_1\mathfrak{n}_1 = \mathfrak{f}\mathfrak{n}'$, also $\mathfrak{b} + \mathfrak{f}\mathfrak{n}' = \mathfrak{o}$. Bedeutet ferner $\mathfrak{b}'$ das dem Ideal $\mathfrak{b}$ entsprechende Ideal in $\mathfrak{o}'$ (§ 5), so ist $\mathfrak{b} = \mathfrak{o}\mathfrak{b}'$, und aus $\mathfrak{o}\mu = \mathfrak{a}'\mathfrak{b}$, d. h. aus $\mathfrak{o}(\mathfrak{o}'\mu) = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$ folgt $\mathfrak{o}'\mu = \mathfrak{a}'\mathfrak{b}'$. Nun ist $\mathfrak{f} > \mathfrak{o}'$ und nach Voraussetzung $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$, folglich $\mathfrak{f}\mathfrak{n}' > \mathfrak{n}'$, und da ebenfalls $\mathfrak{n}' > \mathfrak{o}'$ vorausgesetzt ist, so folgt $\mathfrak{f}\mathfrak{n}' > \mathfrak{o}'$, also $\mathfrak{o}' - \mathfrak{f}\mathfrak{n}' = \mathfrak{f}\mathfrak{n}'$; wendet man daher den allgemeinen Satz (§ 2, 1°)

$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{o}'$, $\mathfrak{c} = \mathfrak{f}\mathfrak{n}'$ an und berücksichtigt außerdem, daß $\mathfrak{o}' - \mathfrak{b} = \mathfrak{b}'$, und $\mathfrak{b} + \mathfrak{f}\mathfrak{n}' = \mathfrak{o}$ ist, so folgt $\mathfrak{b}' + \mathfrak{f}\mathfrak{n}' = \mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$, woraus mit Rücksicht auf $\mathfrak{f}\mathfrak{n}' > \mathfrak{n}' > \mathfrak{o}'$ sich endlich auch $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ ergibt, was zu beweisen war.

Es ist nun noch der oben vorläufig übergangene Beweis nachzuholen, daß man μ so wählen kann, daß $N(\mu)$ positiv wird. Dies geschieht offenbar durch den Beweis des folgenden allgemeineren Satzes:

2°. Ist $\mathfrak{m}$ ein Modul des Körpers Ω, und μ_0 eine bestimmte Zahl dieses Körpers, so gibt es unter den Zahlen μ, welche $\equiv \mu_0 \pmod{\mathfrak{m}}$ sind, unendlich viele, die eine positive Norm haben.

Beweis. Dieser Satz ist selbstverständlich, sobald die sämtlichen Wurzeln der Gleichung $f(\Theta) = 0$, aus welcher der Körper Ω abgeleitet ist, imaginär, und folglich die n Faktoren von $N(\mu) = \mu'\mu'' \cdots \mu^{(n)}$ aus $\frac{1}{2}n$ Paaren von zwei Zahlen $a + bi$, $a - bi$ bestehen; und wenn die Gleichung eine oder mehrere reelle Wurzeln hat, so braucht man offenbar nur die diesen Wurzeln entsprechenden Faktoren von $N(\mu)$ zu betrachten, weil das Produkt der übrigen gewiß positiv ist. Da nun nach Voraussetzung die Basiszahlen des endlichen Moduls $\mathfrak{m}$ zugleich eine Basis des Körpers Ω bilden, so kann die dem Körper angehörende Zahl 1 durch Multiplikation mit einer positiven rationalen Zahl m in eine Zahl m des Moduls $\mathfrak{m}$ verwandelt werden, und wenn h eine beliebige ganze rationale Zahl bedeutet, so wird $hm \equiv 0 \pmod{\mathfrak{m}}$, und folglich $\mu = \mu_0 + hm \equiv \mu_0 \pmod{\mathfrak{m}}$. Offenbar kann man nun die ganze rationale Zahl h positiv und so groß wählen, daß diejenigen Faktoren

$$\mu' = \mu_0' + hm, \quad \mu'' = \mu_0'' + hm \cdots \mu^{(n)} = \mu_0^{(n)} + hm,$$

welche den reellen Wurzeln der Gleichung $f(\Theta) = 0$ entsprechen, sämtlich positiv ausfallen, womit der Satz bewiesen ist.

§ 7.

Komposition der Ideal-Klassen.

Sind $\mathfrak{o}'$, $\mathfrak{o}''$ zwei beliebige Ordnungen des Körpers Ω, und $\mathfrak{f}'$, $\mathfrak{f}''$ ihre Führer, so ist offenbar ihr Produkt $\mathfrak{o}''' = \mathfrak{o}'\mathfrak{o}''$ ebenfalls eine Ordnung (§ 3), und da $\mathfrak{o}'''$ ein gemeinschaftlicher Teiler von $\mathfrak{o}'$, $\mathfrak{o}''$ ist, so muß der Führer $\mathfrak{f}'''$ der Ordnung $\mathfrak{o}'''$ auch ein gemeinschaftlicher Teiler von $\mathfrak{f}'$, $\mathfrak{f}''$ sein. Ist nun $\mathfrak{a}'$ ein beliebiges Ideal in $\mathfrak{o}'$, ebenso $\mathfrak{b}''$ ein beliebiges Ideal in $\mathfrak{o}''$, so wird $\mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$ ein Ideal in $\mathfrak{o}'''$; denn aus $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, $\mathfrak{o}''\mathfrak{b}'' = \mathfrak{b}''$ folgt $\mathfrak{o}'''\mathfrak{c}''' = \mathfrak{o}'\mathfrak{o}''\mathfrak{a}'\mathfrak{b}'' = \mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$; aus $\mathfrak{a}' + \mathfrak{f}' = \mathfrak{o}'$, $\mathfrak{b}'' + \mathfrak{f}'' = \mathfrak{o}''$ ergibt sich ferner durch Multiplikation

$$\mathfrak{a}'\mathfrak{b}'' + \mathfrak{a}'\mathfrak{f}'' + \mathfrak{f}'\mathfrak{b}'' + \mathfrak{f}'\mathfrak{f}'' = \mathfrak{o}'''$$

und hieraus, weil jedes der Ideale $\mathfrak{a}'\mathfrak{f}''$, $\mathfrak{f}'\mathfrak{b}''$, $\mathfrak{f}'\mathfrak{f}''$ durch $\mathfrak{f}'''$, und $\mathfrak{f}'''$ durch $\mathfrak{o}'''$ teilbar ist, $\mathfrak{a}'\mathfrak{b}'' + \mathfrak{f}''' = \mathfrak{o}'''$; also besitzt der Modul $\mathfrak{a}'\mathfrak{b}''$ die charakteristischen Eigenschaften eines Ideals in $\mathfrak{o}'''$ (§ 4), und da allgemein bewiesen ist, daß die Ordnung eines Ideals in $\mathfrak{o}'$ identisch mit $\mathfrak{o}'$ ist, so ergibt sich, daß die Ordnung eines Produkts von Idealen gleich dem Produkt aus den Ordnungen der Faktoren ist*).

Ist $\mathfrak{a}'$ ein Repräsentant der Ideal-Klasse A' in $\mathfrak{o}'$, und $\mathfrak{b}''$ ein Repräsentant der Ideal-Klasse B'' in $\mathfrak{o}''$, so ist jedes Produkt von zwei beliebigen Idealen in A', B'' von der Form $\mathfrak{a}'\mu \cdot \mathfrak{b}''\nu = \mathfrak{a}'\mathfrak{b}''(\mu\nu)$, also ein mit $\mathfrak{a}'\mathfrak{b}''$ äquivalentes Ideal; alle diese Produkte gehören daher einer und derselben Ideal-Klasse in $\mathfrak{o}'''$ an, welche (wie bei den Moduln) die aus A', B'' zusammengesetzte Klasse oder das Produkt aus A', B'' heißen und mit $A'B''$ bezeichnet werden soll. Bedeuten A, B, C beliebige Ideal-Klassen beliebiger Ordnungen, so ist offenbar $AB = BA$, $(AB)C = A(BC)$.

Von dieser allgemeinsten Komposition der Ideal-Klassen aller Ordnungen kehren wir zurück zu der Betrachtung der Ideal-Klassen einer einzigen Ordnung $\mathfrak{o}'$; jedes Produkt von solchen Klassen gehört derselben Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{o}'^2 = \mathfrak{o}'$ ist. Da das Produkt $\mathfrak{o}'\mu \cdot \mathfrak{a}' = \mu\mathfrak{a}'$ aus einem Hauptideal $\mathfrak{o}'\mu$ und einem beliebigen Ideal $\mathfrak{a}'$

*) Wenn, wie es bei den quadratischen Körpern der Fall ist, jede Modul-Klasse auch Ideale enthält, so gilt der obige Satz auch für Produkte aus Moduln; aber schon bei kubischen Körpern gibt es Moduln, welche keinem Ideale äquivalent sind, und der obige Satz darf nicht mehr auf alle Produkte von Moduln übertragen werden. Auf diese wichtige Frage werde ich bei einer anderen Gelegenheit zurückkommen.

mit diesem letzteren äquivalent ist, so folgt $O'A' = A'$, wo A' eine beliebige Ideal-Klasse in $\mathfrak{o}'$, und O' die Hauptklasse in $\mathfrak{o}'$ bedeutet. Da ferner, wenn $\mathfrak{a}'$ ein beliebiger Repräsentant der Ideal-Klasse A' in $\mathfrak{o}'$ ist, immer ein solches Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ existiert, daß $\mathfrak{a}'\mathfrak{b}'$ ein Hauptideal in $\mathfrak{o}'$ wird, so gibt es eine Ideal-Klasse B' in $\mathfrak{o}'$ von der Art, daß $A'B' = O'$ wird; und zwar gibt es nur eine einzige solche Klasse B'; denn wenn C' ebenfalls eine Ideal-Klasse in $\mathfrak{o}'$, und wenn $AC' = O'$ ist, so folgt $A'B'C' = O'B' = O'C' = B' = C'$. Diese Klasse B' soll die zu A' gehörende entgegengesetzte, oder die reziproke, oder inverse Klasse heißen und durch A'^{-1} bezeichnet werden; offenbar ist A' zugleich die inverse Klasse von A'^{-1}. Sind nun A', B', C' beliebige Ideal-Klassen derselben Ordnung $\mathfrak{o}'$, so folgt aus $A'B' = A'C'$ durch Multiplikation mit A'^{-1} stets $B' = C'$*). Sind ferner A', B' beliebige Ideal-Klassen derselben Ordnung $\mathfrak{o}'$, so gibt es immer eine und nur eine Ideal-Klasse $C' = A'^{-1}B'$ der Ordnung $\mathfrak{o}'$, welche der Bedingung $A'C' = B'$ genügt.

§ 8.

Korrespondenz zwischen den Ideal-Klassen in $\mathfrak{o}$ und $\mathfrak{o}'$.

Ist $\mathfrak{o}$ wieder die aus allen ganzen Zahlen des Körpers Ω bestehende Ordnung, O die Klasse der Hauptideale in $\mathfrak{o}$, und $\mathfrak{o}'$ eine beliebige Ordnung, so wird durch jede bestimmte Ideal-Klasse A' der Ordnung $\mathfrak{o}'$ eine bestimmte Ideal-Klasse $OA' = A$ der Ordnung $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$ erzeugt, z. B. O selbst durch die Hauptklasse O' der Ordnung $\mathfrak{o}'$. Umgekehrt, ist A eine Ideal-Klasse der Ordnung $\mathfrak{o}$, so gibt es in ihr immer einen Repräsentanten $\mathfrak{a}$, der relatives Primideal zum Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ ist (denn nach § 1, 14° oder § 6 oder D. § 163, 7. kann jedes Ideal der inversen Klasse A^{-1} durch Multiplikation mit einem solchen Ideal $\mathfrak{a}$ in ein Hauptideal verwandelt werden, und dies muß folglich in A enthalten sein); dann ist $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ das korrespondierende Ideal in $\mathfrak{o}'$, und $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$ (§ 5, 2°), und wenn A' die Ideal-Klasse in $\mathfrak{o}'$ ist, welcher $\mathfrak{a}'$ angehört, so ist $OA' = A$; also wird jede Ideal-Klasse A der Ordnung $\mathfrak{o}$ durch mindestens eine Ideal-Klasse A' der Ordnung $\mathfrak{o}'$ auf diese Weise erzeugt. Wir suchen nun zunächst alle Ideal-Klassen B' der Ordnung $\mathfrak{o}'$, welche dieselbe

*) Dieser Satz verliert, wie man leicht sieht, seine allgemeine Gültigkeit, wenn die Klassen A', B', C' nicht derselben Ordnung angehören.

Klasse A hervorbringen, so daß $OB' = OA'$ wird; hieraus folgt aber $OB'A'^{-1} = OO'$, also, wenn

$$B'A'^{-1} = M', \quad B' = M'A'$$

gesetzt wird,

$$OM' = O.$$

Umgekehrt, wenn M' eine der vorstehenden Bedingung genügende Ideal-Klasse der Ordnung $\mathfrak{o}'$, und wenn $B' = M'A'$ ist, so ist auch wirklich $OB' = OA'$.

Der Komplex $\mathfrak{M}'$ aller dieser Ideal-Klassen M', unter denen sich auch O' und jede inverse Klasse M'^{-1} befindet, besitzt den Charakter einer Gruppe, insofern das Produkt von je zwei solchen Klassen M' offenbar wieder demselben Komplex $\mathfrak{M}'$ angehört. In den folgenden Paragraphen wird gezeigt werden, daß die Anzahl dieser Klassen M' eine endliche ist; wir wollen dieselbe mit m bezeichnen und zunächst ihre Bedeutung für das Problem nachweisen, welches den Hauptgegenstand dieser Abhandlung bildet. Ist A' eine bestimmte Ideal-Klasse in $\mathfrak{o}'$, und durchläuft M' alle m Klassen der Gruppe $\mathfrak{M}'$, so bilden die sämtlichen Produkte $M'A'$ einen Komplex von Klassen der Ordnung $\mathfrak{o}'$, der mit $\mathfrak{M}'A'$ bezeichnet werden mag; da aus $M_1'A' = M_2'A'$ auch $M_1' = M_2'$ folgt (§ 7), so besteht ein solcher Komplex $\mathfrak{M}'A'$ aus m verschiedenen Klassen. Enthalten ferner zwei solche Komplexe $\mathfrak{M}'A'$, $\mathfrak{M}'B'$ eine und dieselbe Klasse $M_1'A' = M_2'B'$, so ist $B' = M_2'^{-1}M_1'A' = M_3'A'$, wo $M_3' = M_1'^{-1}M_1'$ ebenfalls in $\mathfrak{M}'$ enthalten ist, und hieraus folgt offenbar, daß die sämtlichen m Klassen des Komplexes $\mathfrak{M}'B'$ mit denen von $\mathfrak{M}'A'$ vollständig übereinstimmen. Man kann daher alle Ideal-Klassen der Ordnung $\mathfrak{o}'$ in lauter verschiedene solche Komplexe von der Form $\mathfrak{M}'A'$, $\mathfrak{M}'B'$ ··· einteilen. Nun ist oben gezeigt, daß jede bestimmte Ideal-Klasse A der Ordnung $\mathfrak{o}$ in der angegebenen Weise durch die sämtlichen m Klassen eines bestimmten solchen Komplexes $\mathfrak{M}'A'$, und durch keine andere Klasse der Ordnung $\mathfrak{o}'$ erzeugt wird, und daß umgekehrt alle m Klassen eines solchen Komplexes durch Multiplikation mit O eine und nur eine Klasse A der Ordnung $\mathfrak{o}$ erzeugen. Mithin ist die Anzahl aller dieser Komplexe identisch mit der Anzahl h der verschiedenen Ideal-Klassen der Ordnung $\mathfrak{o}$, deren Endlichkeit schon bewiesen ist (D. § 164, 2°), und zugleich ergibt sich, daß

$$h' = mh$$

die Anzahl aller verschiedenen Ideal-Klassen der Ordnung $\mathfrak{o}'$ ist.

§ 9.

Bestimmung des Verhältnisses m der Klassen-Anzahlen h' und h.

Es sei M' eine bestimmte Klasse der Gruppe $\mathfrak{M}'$, und $\mathfrak{m}'$ ein bestimmter Repräsentant von M'. Da $OM' = O$ ist, so ist $\mathfrak{o}\mathfrak{m}'$ ein Hauptideal in $\mathfrak{o}$, also von der Form $\mathfrak{o}\mu$, wo μ eine ganze Zahl von positiver Norm, und zwar relative Primzahl zu $\mathfrak{f}$ ist, wo $\mathfrak{f}$ wieder den Führer der Ordnung $\mathfrak{o}'$ bedeutet. Umgekehrt, ist μ eine solche Zahl, so ist $\mathfrak{o}\mu$ ein Hauptideal in $\mathfrak{o}$ und relatives Primideal zu $\mathfrak{f}$, mithin gibt es (§ 5, 2°) ein und nur ein Ideal $\mathfrak{m}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, und wenn M' die durch $\mathfrak{m}'$ repräsentierte Ideal-Klasse in $\mathfrak{o}'$ bedeutet, so ist $OM' = O$; jeder bestimmten Zahl μ von der angegebenen Beschaffenheit entspricht daher auf diese Weise eine und nur eine Ideal-Klasse M', welche der Gruppe $\mathfrak{M}'$ angehört. Auf diese Korrespondenz bezieht sich der folgende Satz:

Sind μ, μ_1 ganze Zahlen von positiver Norm und relative Primzahlen zu $\mathfrak{f}$, so besteht die erforderliche und hinreichende Bedingung dafür, daß beiden Zahlen eine und dieselbe Klasse M' der Gruppe $\mathfrak{M}'$ entspreche, in der Kongruenz

$$\mu_1 \equiv \mu\varepsilon\omega' \pmod{\mathfrak{f}},$$

wo ε eine Einheit in $\mathfrak{o}$, und ω' eine in $\mathfrak{o}'$ enthaltene relative Primzahl zu $\mathfrak{f}$ bedeutet, deren Normen beide positiv sind.

Beweis. Ist $\mathfrak{m}' = \mathfrak{o}' - \mathfrak{o}\mu$ das Ideal in $\mathfrak{o}'$, welches dem Ideal $\mathfrak{o}\mu$ entspricht und folglich der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, so kann man, weil $\mathfrak{m}' + \mathfrak{f} = \mathfrak{o}'$ ist, eine Zahl μ' so wählen, daß $\mu' \equiv 0 \pmod{\mathfrak{m}'}$ und $\mu' \equiv 1 \pmod{\mathfrak{f}}$ wird (§ 2, 2°); auch leuchtet ein, daß zugleich die Bedingung $N(\mu') > 0$ erfüllt werden kann (§ 6, 2°). Dann ist $\mathfrak{o}'\mu'$ ein durch $\mathfrak{m}'$ teilbares Hauptideal in $\mathfrak{o}'$, weil $\mathfrak{o}'\mu' + \mathfrak{f} = \mathfrak{o}'$ ist, und folglich gibt es ein Ideal $\mathfrak{n}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{m}'\mathfrak{n}' = \mathfrak{o}'\mu'$ genügt und folglich der inversen Klasse M'^{-1} angehört. Hieraus folgt durch Multiplikation mit $\mathfrak{o}$, daß $\mathfrak{o}\mu' = \mathfrak{o}\mathfrak{n}'\mu$, also μ' durch μ teilbar ist; setzt man $\mu' = \mu\nu$, so ist ν eine ganze Zahl von positiver Norm und relative Primzahl zu $\mathfrak{f}$, weil $\mu\nu = \mu' \equiv 1 \pmod{\mathfrak{f}}$ ist; zugleich wird $\mathfrak{o}\mu\nu = \mathfrak{o}\mathfrak{n}'\mu$, und folglich $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$.

Wenn nun das dem Ideal $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}_1' = \mathfrak{o}' - \mathfrak{o}\mu_1$ derselben Klasse M' angehört, wie $\mathfrak{m}'$, so ist auch $\mathfrak{m}_1'\mathfrak{n}'$ ein Hauptideal in $\mathfrak{o}'$, also $\mathfrak{m}_1'\mathfrak{n}' = \mathfrak{o}'\omega'$, wo ω' eine Zahl in $\mathfrak{o}'$ von positiver Norm und relative Primzahl zu $\mathfrak{f}$ ist. Multipliziert man mit $\mathfrak{o}$ und berücksichtigt, daß $\mathfrak{o}\mathfrak{m}_1' = \mathfrak{o}\mu_1$ und $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$ ist, so folgt $\mathfrak{o}\mu_1\nu = \mathfrak{o}\omega'$, und hieraus $\mu_1\nu = \varepsilon\omega'$, wo ε eine Einheit in $\mathfrak{o}$ bedeutet, deren Norm $= +1$ sein muß, weil die Normen der Zahlen μ_1, ν, ω' positiv sind. Multipliziert man mit μ, so ergibt sich die zu beweisende Kongruenz, weil $\mu\nu = \mu' \equiv 1 \pmod{\mathfrak{f}}$ und $\mathfrak{o}\mathfrak{f} = \mathfrak{f}$ ist.

Umgekehrt, wenn diese Kongruenz, in welcher μ, μ_1, ε, ω' die in dem Satze angegebene Bedeutung haben, erfüllt ist, so folgt durch Multiplikation mit $\nu\varepsilon^{-1}$ die Kongruenz

$$\nu\mu_1\varepsilon^{-1} \equiv \omega' \pmod{\mathfrak{f}},$$

aus welcher hervorgeht, daß die ganze Zahl $\alpha' = \nu\mu_1\varepsilon^{-1}$, welche relative Primzahl zu $\mathfrak{f}$ ist und eine positive Norm besitzt, der Ordnung $\mathfrak{o}'$ angehört, und folglich ist $\mathfrak{o}'\alpha'$ ein Hauptideal in $\mathfrak{o}'$. Da nun $\mathfrak{o}\nu = \mathfrak{o}\mathfrak{n}'$ und $\mathfrak{o}\mu_1\varepsilon^{-1} = \mathfrak{o}\mu_1 = \mathfrak{o}\mathfrak{m}_1'$ ist, so folgt $\mathfrak{o}(\mathfrak{o}'\alpha') = \mathfrak{o}(\mathfrak{n}'\mathfrak{m}_1')$, also auch $\mathfrak{o}'\alpha' = \mathfrak{n}'\mathfrak{m}_1'$ (§ 5, 1°), mithin gehören die Ideale $\mathfrak{n}'$, $\mathfrak{m}_1'$ zu entgegengesetzten Klassen, d. h. das dem Ideal $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}_1'$ ist äquivalent mit $\mathfrak{m}'$, was zu beweisen war.

Mit Hilfe dieses Satzes ist es leicht, die Anzahl m der in der Gruppe $\mathfrak{M}'$ enthaltenen Klassen M' zu bestimmen. Wir bezeichnen mit $\psi(\mathfrak{f})$ die Anzahl aller der in $\mathfrak{o}$ enthaltenen Zahlen ω, welche inkongruent in bezug auf den Modul $\mathfrak{f}$ und zugleich relative Primzahlen zu $\mathfrak{f}$ sind; diese Anzahl ist (D. § 163, 7.)

$$\psi(\mathfrak{f}) = N(\mathfrak{f}) \prod \left(1 - \frac{1}{N(\mathfrak{q})}\right),$$

wo das Produktzeichen Π sich auf alle verschiedenen, in $\mathfrak{f}$ aufgehenden Primideale $\mathfrak{q}$ bezieht. Die Repräsentanten ω selbst können (nach § 6, 2°) immer so gewählt werden, daß sie positive Normen haben. Wenn eine dieser Zahlen (wie z. B. die Zahl 1) in $\mathfrak{o}'$ enthalten ist, so gehören auch alle mit ihr kongruenten Zahlen der Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{f}$ durch $\mathfrak{o}'$ teilbar ist; die Anzahl dieser nach $\mathfrak{f}$ inkongruenten Zahlen ω' oder der zugehörigen Zahlklassen ist ebenfalls als bekannt anzusehen, sobald $\mathfrak{o}'$ gegeben ist, und soll mit $\psi'(\mathfrak{f})$ bezeichnet werden. Da $\mathfrak{o}'^2 = \mathfrak{o}'$ ist, so ist das Produkt aus je zwei Repräsentanten dieser Zahlklassen immer wieder einem solchen Re-

präsentanten kongruent, und der Komplex dieser $\psi'(\mathfrak{f})$ Repräsentanten hat daher den Charakter einer Gruppe. Multipliziert man dieselben mit einer beliebigen in $\mathfrak{o}$ enthaltenen Zahl ω, welche relative Primzahl zu $\mathfrak{f}$ ist, so erhält man $\psi'(\mathfrak{f})$ inkongruente Zahlen, welche ebenfalls relative Primzahlen zu $\mathfrak{f}$ sind, und deren Komplex kurz mit (ω) bezeichnet werden soll; zwei solche Komplexe (α), (β) sind (nach der in § 8 angewendeten Schlußweise) entweder gänzlich verschieden, d. h. keine der in (α) enthaltenen Zahlen ist kongruent mit einer der in (β) enthaltenen Zahlen, oder sie sind völlig identisch, d. h. alle durch den einen Komplex vertretenen $\psi'(\mathfrak{f})$ Zahlklassen stimmen gänzlich mit den Zahlklassen des anderen Komplexes überein. Es wird daher auch das System aller $\psi(\mathfrak{f})$ Repräsentanten in eine Anzahl solcher Komplexe (ω) zerfallen, d. h. $\psi(\mathfrak{f})$ wird teilbar sein durch $\psi'(\mathfrak{f})$; wir betrachten zunächst aber nur alle diejenigen Komplexe (ε), welche entstehen, wenn ε alle Einheiten des Gebietes $\mathfrak{o}$ durchläuft, deren Normen $= +1$ sind. Es sei s die Anzahl aller verschiedenen Komplexe

$$(\varepsilon_1),\ (\varepsilon_2) \cdots (\varepsilon_s)$$

dieser Art, so bilden die in ihnen enthaltenen $s\psi'(\mathfrak{f})$ Repräsentanten offenbar wieder eine Gruppe im obigen Sinne; jede Zahl von der Form $\varepsilon\omega'$ ist einer und nur einer dieser Zahlen kongruent, welche umgekehrt selbst in dieser Form enthalten sind. Ist nun μ eine in $\mathfrak{o}$ enthaltene relative Primzahl zu $\mathfrak{f}$, deren Norm positiv ist, und bezeichnet man mit $((\mu))$ den Komplex der $s\psi'(\mathfrak{f})$ inkongruenten, in den s Komplexen $(\mu\varepsilon_1)$, $(\mu\varepsilon_2) \cdots (\mu\varepsilon_s)$ enthaltenen Zahlen, so sind wieder zwei solche Komplexe $((\mu))$ und $((\mu_1))$ entweder gänzlich verschieden, oder völlig identisch, und folglich besteht das System aller $\psi(\mathfrak{f})$ Repräsentanten ω aus einer Anzahl von solchen Komplexen $((\mu))$; diese Anzahl muß aber notwendig $= m$, d. h. gleich der Anzahl der verschiedenen, in der Gruppe $\mathfrak{M}'$ enthaltenen Idealklassen M' sein, weil nach dem obigen Satze je zwei Hauptidealen $\mathfrak{o}\mu$, $\mathfrak{o}\mu_1$ dieselbe Klasse M' oder zwei verschiedene solche Klassen entsprechen, je nachdem die beiden Komplexe $((\mu))$, $((\mu_1))$ identisch oder verschieden sind. Mithin ist

$$\psi(\mathfrak{f}) = m s \psi'(\mathfrak{f}),$$

also

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{f})}{s\psi'(\mathfrak{f})}.$$

§ 10.

Umformung des Resultates.

Es ist nun noch von Wichtigkeit, die Anzahl s in bestimmter Weise darzustellen, und hierzu gelangt man mit Hilfe der in der Einleitung erwähnten Theorie der Einheiten von Dirichlet, welche ich zu diesem Zwecke in etwas verallgemeinerter Form dargestellt habe (D. § 166). Wir fragen zunächst: wie müssen zwei Einheiten ε, ε_0 von positiver Norm beschaffen sein, damit die oben mit (ε), (ε_0) bezeichneten Komplexe identisch ausfallen? Offenbar ist hierzu erforderlich, daß $\varepsilon \equiv \varepsilon_0 \omega' \pmod{\mathfrak{f}}$ sei, wo ω' eine der Ordnung $\mathfrak{o}'$ angehörende Zahl bedeutet; mithin muß $\varepsilon \varepsilon_0^{-1} \equiv \omega' \pmod{\mathfrak{f}}$, also $\varepsilon = \varepsilon' \varepsilon_0$ sein, wo $\varepsilon' = \varepsilon \varepsilon_0^{-1}$ eine der Ordnung $\mathfrak{o}'$ angehörende Einheit von positiver Norm bedeutet; und es leuchtet unmittelbar ein, daß diese Bedingung $\varepsilon = \varepsilon' \varepsilon_0$ auch hinreichend ist, daß sie also die Identität der Komplexe (ε), (ε_0) zur Folge hat. Bezeichnet man daher, wie oben, mit $(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$ die sämtlichen s verschiedenen Komplexe von der Form (ε), so ergibt sich, daß man alle Einheiten ε der Ordnung $\mathfrak{o}$, und jede nur ein einziges Mal erhält, wenn man jede der s partikulären Einheiten $\varepsilon_1, \varepsilon_2 \cdots \varepsilon_s$ mit allen Einheiten ε' der Ordnung $\mathfrak{o}'$ multipliziert. Hieraus folgt zunächst, daß die s-te Potenz ε^s einer jeden Einheit ε in $\mathfrak{o}$ immer eine Einheit ε' in $\mathfrak{o}'$ ist, weil die s Komplexe $(\varepsilon\varepsilon_1), (\varepsilon\varepsilon_2) \cdots (\varepsilon\varepsilon_s)$ notwendig mit den Komplexen $(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$, wenn auch in anderer Ordnung, übereinstimmen müssen, und weil folglich das Produkt

$$\varepsilon\varepsilon_1 \cdot \varepsilon\varepsilon_2 \cdots \varepsilon\varepsilon_s = \varepsilon^s \cdot \varepsilon_1\varepsilon_2 \cdots \varepsilon_s$$

von der Form $\varepsilon' . \varepsilon_1\varepsilon_2 \cdots \varepsilon_s$ ist, wo ε' eine Einheit der Ordnung $\mathfrak{o}'$ bedeutet.

Wir müssen nun das Hauptresultat der Theorie der Einheiten kurz in Erinnerung bringen. Es sei ν die Gesamtanzahl der $(2\nu - n)$ reellen Wurzeln und der $(n - \nu)$ Paare von je zwei konjugiert-imaginären Wurzeln $a \pm bi$ der irreduktiblen Gleichung $f(\Theta) = 0$, aus welcher der Körper Ω entsprungen ist (§ 1); behält man von jedem Paare imaginärer Wurzeln nur die eine bei, so bleiben ν Wurzeln übrig, die mit

$$\Theta', \Theta'' \cdots \Theta^{(\nu)}$$

bezeichnet werden mögen. Ist nun $\varepsilon = \varphi(\Theta)$ eine beliebige Einheit des Körpers Ω, so soll durch das Symbol $l'(\varepsilon)$ der reelle Teil des

Logarithmen von $\varphi(\Theta')$ oder das Doppelte dieses reellen Teils bezeichnet werden, je nachdem Θ' reell oder imaginär ist, und die Symbole $l''(\varepsilon), l'''(\varepsilon) \cdots l^{(\nu)}(\varepsilon)$ sollen die entsprechende Bedeutung in bezug auf die anderen Wurzeln $\Theta'', \Theta''' \cdots \Theta^{(\nu)}$ haben. Dann folgt aus $N(\varepsilon) = 1$, daß immer

$$l'(\varepsilon) + l''(\varepsilon) + \cdots + l^{(\nu)}(\varepsilon) = 0$$

ist. Es wird nun zunächst bewiesen (D. § 166, 5.), daß es in jeder Ordnung $\mathfrak{o}'$ immer $(\nu - 1)$ voneinander unabhängige, d. h. solche Einheiten $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ gibt, für welche die Determinante

$$\sum \pm l'(\varrho_1') l''(\varrho_2') \cdots l^{(\nu-1)}(\varrho_{\nu-1}'),$$

welche wir zur Abkürzung mit

$$L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$$

bezeichnen wollen, einen von 0 verschiedenen (positiven) Wert besitzt. Läßt man nun $u_1, u_2 \cdots u_{\nu-1}$ alle ganzen rationalen Zahlen durchlaufen, so erhält man eine Gruppe R' von unendlich vielen in $\mathfrak{o}'$ enthaltenen Einheiten

$$\varrho_1'^{u_1} \varrho_2'^{u_2} \cdots \varrho_{\nu-1}'^{u_{\nu-1}},$$

die sich durch Multiplikation und Division reproduzieren; je zwei verschiedenen Systemen von Exponenten entsprechen zwei verschiedene Individuen der Gruppe R'. Die Einheiten $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$, welche eine Basis der Gruppe R' bilden, können offenbar ohne Änderung von R' und $L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ durch je $(\nu - 1)$ Einheiten ersetzt werden, welche aus R' so ausgewählt sind, daß die aus den zugehörigen $(\nu - 1)^2$ Exponenten u gebildete Determinante $= 1$ wird. Bezeichnet man mit $R'\alpha$ den Inbegriff aller Produkte aus einer bestimmten Zahl α und jeder der in R' enthaltenen Einheiten, so sind zwei solche Komplexe entweder gänzlich identisch, oder sie haben keine einzige Zahl gemeinschaftlich; das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ besteht (D. § 166, 6.) aus einer endlichen, von R' abhängigen Anzahl r' solcher Komplexe, woraus leicht folgt, daß $\varepsilon'^{r'}$ stets der Gruppe R' angehört. Hieraus ergibt sich unmittelbar, daß unter allen Systemen von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ auch solche Systeme $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ existieren, für welche die Determinante $L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ einen Minimumwert erhält; dann besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus r' Komplexen von der Form

$$R', R'\varrho', R'\varrho'^2 \cdots R'\varrho'^{r'-1},$$

wo ϱ' eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$ bedeutet (D. § 166, 7.). Ein solches System von $(\nu - 1)$ unabhängigen Einheiten $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ heißt ein Fundamental-System der Ordnung $\mathfrak{o}'$, und wir wollen zur Abkürzung den durch die Ordnung $\mathfrak{o}'$ vollständig bestimmten Quotienten

$$\frac{L(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1})}{r'} = \mathrm{E}(\mathfrak{o}')$$

setzen*). Es würde sich, wie wir beiläufig bemerken, durch Betrachtungen, welche den gleich folgenden sehr ähnlich sind (vgl. D. § 161), auch leicht beweisen lassen, daß Zähler und Nenner dieses Quotienten sich mit einer und derselben ganzen rationalen Zahl multiplizieren, wenn das Fundamental-System $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ durch ein beliebiges System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ ersetzt wird. Wir wollen nun beweisen, daß die in dem Verhältnis $h' : h = m$ auftretende Anzahl s der Komplexe $\varepsilon' \varepsilon_1$, $\varepsilon' \varepsilon_2 \cdots \varepsilon' \varepsilon_s$, aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht,

$$= \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})}$$

ist.

Zu diesem Zwecke bezeichnen wir mit $\varrho_1, \varrho_2 \cdots \varrho_{\nu-1}$ ein Fundamental-System von Einheiten der Ordnung $\mathfrak{o}$, mit R die zugehörige Gruppe der aus ihnen durch Multiplikation und Division gebildeten Einheiten, und mit r die Anzahl der Komplexe

$$R, R\varrho, R\varrho^2 \cdots R\varrho^{r-1},$$

aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht, wo nun ϱ eine primitive Wurzel der Gleichung $\varrho^r = 1$ bedeutet. Unter diesen Einheiten ε befinden sich auch alle Einheiten ε' der Ordnung $\mathfrak{o}'$, weil $\mathfrak{o}'$ durch $\mathfrak{o}$ teilbar ist. Ist nun e ein bestimmter Index aus der Reihe 0, 1, 2 $\cdots$ $(\nu - 1)$, so gibt es unter allen denjenigen Einheiten von der Form

$$\sigma'_e = \varrho^u \varrho_1^{u_1} \varrho_2^{u_2} \cdots \varrho_e^{u_e},$$

welche, wie z. B. ϱ_e^s, auch der Ordnung $\mathfrak{o}'$ angehören, mindestens eine

$$\varrho'_e = \varrho^{a^{(e)}} \varrho_1^{a_1^{(e)}} \varrho_2^{a_2^{(e)}} \cdots \varrho_e^{a_e^{(e)}},$$

*) In dem singulären Falle eines imaginären quadratischen Körpers ($n = 2$, $\nu = 1$) besteht R' aus der einzigen Einheit 1, r' bedeutet die endliche Anzahl aller in $\mathfrak{o}'$ enthaltenen Einheiten, und die Determinante $L(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1})$ ist durch 1 zu ersetzen.

in welcher der letzte Exponent u_e seinen kleinsten positiven Wert $a_e^{(e)}$ erreicht, und es leuchtet ein, daß in jeder anderen Einheit σ_e' der letzte Exponent u_e notwendig durch $a_e^{(e)}$ teilbar, also von der Form $a_e^{(e)} x_e$ sein muß, wo x_e eine ganze rationale Zahl bedeutet; es wird daher

$$\sigma_e' \varrho_e'^{-x_e}$$

eine in $\mathfrak{o}'$ enthaltene Einheit von der Form σ_{e-1}', oder $= 1$ sein, wenn $e = 0$ ist. In diesem letzteren Falle ist

$$\varrho' = \varrho^a,$$

und da $\varrho^r = 1$ eine Einheit der Ordnung $\mathfrak{o}'$ ist, so muß r durch a teilbar, also

$$r = ar'$$

sein, und folglich ist ϱ' eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$. Hat man nun nach der obigen Vorschrift für jeden Index $e = 0, 1, 2 \cdots (\nu - 1)$ eine solche partikuläre Einheit ϱ', ϱ_1', $\varrho_2' \cdots \varrho_{\nu-1}'$ der Ordnung $\mathfrak{o}'$ aufgestellt, so ergibt sich, daß jede Einheit ε' der Ordnung $\mathfrak{o}'$, d. h. jede Einheit $\sigma_{\nu-1}'$, von der Form

$$\sigma_{\nu-2}' \varrho_{\nu-1}'^{x_{\nu-1}} = \sigma_{\nu-3}' \varrho_{\nu-2}'^{x_{\nu-2}} \varrho_{\nu-1}'^{x_{\nu-1}} = \text{usw.},$$

also schließlich von der Form

$$\varepsilon' = \varrho'^{x} \varrho_1'^{x_1} \varrho_2'^{x_2} \cdots \varrho_{\nu-1}'^{x_{\nu-1}}$$

ist, wo $x, x_1, x_2 \cdots x_{\nu-1}$ ganze rationale Zahlen bedeuten, deren erste x auf die r' Werte $0, 1, 2 \cdots (r' - 1)$ einzuschränken ist; umgekehrt leuchtet ein, daß alle Zahlen ε' von der vorstehenden Form auch wirklich Einheiten der Ordnung $\mathfrak{o}'$ sind. Da die Zahlen $a, a_1', a_2'' \cdots a_{\nu-1}^{(\nu-1)}$ sämtlich positiv sind, so ist auch ihr Produkt

$$A = a a_1' a_2'' \cdots a_{\nu-1}^{(\nu-1)}$$

positiv; nun ergibt sich aus der Bildung der Einheiten $\varrho_1', \varrho_2'' \cdots \varrho_{\nu-1}'$, daß

$$L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}') = \frac{A}{a} L(\varrho_1, \varrho_2 \cdots \varrho_{\nu-1})$$

einen von 0 verschiedenen, positiven Wert hat; mithin bilden dieselben ein System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$, ja sogar ein Fundamental-System, weil für jedes beliebige System von $(\nu - 1)$ Einheiten $\varepsilon_1', \varepsilon_2' \cdots \varepsilon_{\nu-1}'$ dieser Ordnung $\mathfrak{o}'$ offenbar $L(\varepsilon_1', \varepsilon_2' \cdots \varepsilon_{\nu-1}') = pL(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ wird, wo p eine ganze rationale Zahl bedeutet. Bezeichnet man wieder mit R' die Gruppe aller Einheiten, welche

aus $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ durch Multiplikation und Division gebildet werden können, so besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus den r' verschiedenen Komplexen

$$R', R'\varrho', R'\varrho'^2 \cdots R'\varrho'^{r'-1}.$$

Da ferner oben $r = ar'$ gefunden ist, so ergibt sich aus der vorhergehenden Gleichung

$$\mathrm{E}(\mathfrak{o}') = A\,\mathrm{E}(\mathfrak{o}).$$

Nun ist offenbar A die Anzahl aller derjenigen in $\mathfrak{o}$ enthaltenen Einheiten

$$\varepsilon_0 = \varrho^v \varrho_1^{v_1} \varrho_2^{v_2} \cdots \varrho_{\nu-1}^{v_{\nu-1}},$$

deren Exponenten den Bedingungen

$$0 \leqq v < a, \quad 0 \leqq v_1 < a_1' \cdots 0 \leqq v_{\nu-1} < a_{\nu-1}^{(\nu-1)}$$

genügen. Da ferner jede Einheit der Ordnung $\mathfrak{o}'$ die Form

$$\varepsilon' = \varrho'^x \varrho_1'^{x_1} \varrho_2'^{x_2} \cdots \varrho_{\nu-1}'^{x_{\nu-1}} = \varrho^w \varrho_1^{w_1} \varrho_2^{w_2} \cdots \varrho_{\nu-1}^{w_{\nu-1}}$$

hat, wo

$$\begin{aligned}
w_{\nu-1} &= a_{\nu-1}^{(\nu-1)} x_{\nu-1} \\
w_{\nu-2} &= a_{\nu-2}^{(\nu-1)} x_{\nu-1} + a_{\nu-2}^{(\nu-2)} x_{\nu-2} \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
w_1 &= a_1^{(\nu-1)} x_{\nu-1} + a_1^{(\nu-2)} x_{\nu-2} + \cdots + a_1' x_1 \\
w &= a^{(\nu-1)} x_{\nu-1} + a^{(\nu-2)} x_{\nu-2} + \cdots + a' x_1 + a x
\end{aligned}$$

ist, so kann man, wenn eine beliebige Einheit

$$\varepsilon = \varrho^u \varrho_1^{u_1} \varrho_2^{u_2} \cdots \varrho_{\nu-1}^{u_{\nu-1}}$$

der Ordnung $\mathfrak{o}$ gegeben ist, die Einheit ε', d. h. die Exponenten $x_{\nu-1}, x_{\nu-2} \cdots x_1, x$ stets und nur auf einzige Weise so wählen, daß die Zahlen

$$v = u - w, \quad v_1 = u_1 - w_1 \cdots v_{\nu-1} = u_{\nu-1} - w_{\nu-1}$$

den obigen Bedingungen genügen, daß also $\varepsilon\varepsilon'^{-1}$ eine der A Einheiten ε_0 wird; jede Einheit ε der Ordnung $\mathfrak{o}$ läßt sich daher stets und nur auf eine einzige Weise in die Form $\varepsilon'\varepsilon_0$ setzen, wo ε' eine Einheit in $\mathfrak{o}'$, ε_0 eine der obigen A Einheiten in $\mathfrak{o}$ bedeutet. Durchläuft ε' alle Einheiten der Ordnung $\mathfrak{o}'$, während ε_0 konstant bleibt, so erhält man einen Komplex von unendlich vielen Einheiten $\varepsilon = \varepsilon'\varepsilon_0$, und zwei solche Komplexe, welche zwei verschiedenen Werten von ε_0 entsprechen, sind gänzlich verschieden voneinander; mithin besteht

das System aller Einheiten ε der Ordnung $\mathfrak{o}$ aus A solchen Komplexen. Aber es ist oben gezeigt, daß die Anzahl dieser Komplexe $= s$ ist; mithin ist $s = A$, d. h.

$$s = \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})},$$

was zu beweisen war.

Hiernach nimmt das frühere Resultat für das Verhältnis der Klassenanzahlen die folgende Form an

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{f})}{\psi'(\mathfrak{f})} \cdot \frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')},$$

in welcher die Lösung unseres Problems nach der Methode von Gauß enthalten ist.

§ 11.

Zerlegbare Formen, welche den Idealen von beliebiger Ordnung entsprechen.

Bevor wir zu der Ableitung desselben Resultates nach der Methode von Dirichlet übergehen, wird es zweckmäßig sein, mit einigen Worten den Zusammenhang zwischen den Idealen von beliebiger Ordnung und den zerlegbaren Formen des Körpers Ω zu besprechen.

Bilden die Zahlen $\omega_1, \omega_2 \cdots \omega_n$ eine bestimmte Basis der aus allen ganzen Zahlen des Körpers bestehenden Ordnung $\mathfrak{o}$, so wollen wir die n Basiszahlen

$$\omega_\iota' = k_1^{(\iota)} \omega_1 + k_2^{(\iota)} \omega_2 + \cdots + k_n^{(\iota)} \omega_n$$

der Ordnung $\mathfrak{o}'$ (§ 3) und die n Basiszahlen

$$\alpha_\iota' = a_1^{(\iota)} \omega_1' + a_2^{(\iota)} \omega_2' + \cdots + a_n^{(\iota)} \omega_n'$$

eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ (§ 4) immer so wählen, daß die Determinanten

$$\sum \pm k_1' k_2'' \cdots k_n^{(n)} = (\mathfrak{o}, \mathfrak{o}') = k,$$
$$\sum \pm a_1' a_2'' \cdots a_n^{(n)} = (\mathfrak{o}', \mathfrak{a}') = N'(\mathfrak{a}')$$

werden, also positive Werte erhalten.

Die sämtlichen Zahlen des Ideals $\mathfrak{a}'$ sind von der Form

$$\alpha' = x_1 \alpha_1' + x_2 \alpha_2' + \cdots + x_n \alpha_n',$$

wo die Variablen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, und es ergibt sich, genau wie für die Ideale in $\mathfrak{o}$ (D. § 165), daß

$$N(\alpha') = N'(\mathfrak{a}') X$$

ist, wo X eine homogene Funktion n-ten Grades der n Variablen $x_1, x_2 \cdots x_n$ mit ganzen rationalen Koeffizienten bedeutet, welche, wie aus § 6 folgt, keinen gemeinschaftlichen Teiler haben; die Determinante dieser Form X (§ 1) ist

$$= D(\mathfrak{o}, \mathfrak{o}')^2 = Dk^2,$$

wo $D = \Delta(\Omega)$ wieder die Grundzahl des Körpers Ω bedeutet. Alle Formen X, welche allen verschiedenen Basen aller mit $\mathfrak{a}'$ äquivalenten Ideale entsprechen, sind äquivalent, d. h. sie gehen durch lineare Substitutionen mit ganzen rationalen Koeffizienten, deren Determinanten $= +1$ sind, ineinander über; jeder Idealklasse entspricht also eine bestimmte Formenklasse. Der Multiplikation zweier Ideale $\mathfrak{a}'$, $\mathfrak{b}''$ der Ordnungen $\mathfrak{o}'$, $\mathfrak{o}''$ oder der Komposition der sie enthaltenden Idealklassen A', B'' entspricht die Komposition der zu den Idealen $\mathfrak{a}'\,\mathfrak{b}''$ gehörigen Formen X, Y zu einer dem Ideal $\mathfrak{a}'\,\mathfrak{b}''$ entsprechenden Form Z, deren Determinante

$$= D(\mathfrak{o}, \mathfrak{o}'\,\mathfrak{o}'')^2$$

ist, und zugleich folgt hieraus die Komposition der Formenklassen*).

Um die Rückkehr von diesen allgemeinen Untersuchungen zu dem Falle der quadratischen Körper und Formen zu erleichtern, füge ich noch folgende Bemerkungen hinzu, von deren Richtigkeit man sich leicht überzeugen wird (vgl. D. §§ 168 bis 170). Jede Wurzel einer irreduktiblen quadratischen Gleichung ist von der Form $a + b\sqrt{c}$, wo c eine ganze rationale Zahl bedeutet, welche keine Quadratzahl und auch durch keine Quadratzahl außer 1 teilbar ist; a und b sind rationale Zahlen, und b ist von 0 verschieden. Die Grundzahl D des quadratischen Körpers Ω, welcher aus der Zahl $a + b\sqrt{c}$ entspringt, ist $= c$ oder $= 4c$, je nachdem $c \equiv 1$, oder $c \equiv 2, 3 \pmod 4$ ist; setzt man

$$\Theta = \frac{D + \sqrt{D}}{2},$$

so bilden die Zahlen 1, Θ eine Basis der Ordnung $\mathfrak{o}$, welche aus allen ganzen Zahlen

$$\omega = \frac{t + u\sqrt{D}}{2}$$

*) Da, wie schon oben (§ 7, Anmerkung) bemerkt ist, Moduln existieren, welche keinem Ideal äquivalent sind, so ist, was ich hervorheben zu müssen glaube, in dem Obigen noch nicht die Theorie aller zerlegbaren Formen enthalten, welche den sämtlichen Moduln eines Körpers Ω entsprechen.

des Körpers besteht, wo t, u alle, der Bedingung $t \equiv Du \pmod 2$ genügenden Paare von ganzen rationalen Zahlen zu durchlaufen haben. Jede Ordnung $\mathfrak{o}'$ ist dann von der Form $[1, k\Theta]$, wo $k = (\mathfrak{o}, \mathfrak{o}')$ eine beliebige positive ganze rationale Zahl bedeutet; der Führer k einer solchen Ordnung ist das Hauptideal $\mathfrak{o}k = [k, k\Theta]$, und es ist $N(\mathfrak{k}) = k^2$. Setzt man, wenn p eine positive rationale Primzahl bedeutet,

$$(D, p) = 0, \ +1 \text{ oder } -1,$$

je nachdem $\mathfrak{o}p$ das Quadrat eines Primideals, das Produkt aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist (vgl. D. § 168), so ist

$$\psi(\mathfrak{o}k) = k^2 \prod \left(1 - \frac{1}{p}\right)\left(1 - \frac{(D, p)}{p}\right),$$

wo p alle verschiedenen in k aufgehenden Primzahlen durchläuft; da ferner jede Zahl der Ordnung $\mathfrak{o}'$ mit einer rationalen Zahl kongruent ist in bezug auf $\mathfrak{o}k$, so ist

$$\psi'(\mathfrak{o}k) = \varphi(k) = k \prod \left(1 - \frac{1}{p}\right),$$

und folglich

$$\frac{\psi(\mathfrak{o}k)}{\psi'(\mathfrak{o}k)} = k \prod \left(1 - \frac{(D, p)}{p}\right).$$

Ist nun der Körper Ω imaginär, also D negativ, so ist (vgl. § 10 Anmerkung)

$$\frac{E(\mathfrak{o})}{E(\mathfrak{o}')} = \frac{r'}{r},$$

wo r die Anzahl aller Einheiten in $\mathfrak{o}$, und r' die Anzahl aller Einheiten in $\mathfrak{o}'$ bedeutet. Die letztere Anzahl r' ist (wenn $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist) immer $= 2$, und ebenso ist r immer $= 2$, ausgenommen die beiden Fälle $D = -3$, wo $r = 6$, und $D = -4$, wo $r = 4$ ist. Es ist daher im allgemeinen

$$\frac{h'}{h} = m = k \prod \left(1 - \frac{(D, p)}{p}\right),$$

aber dieses Produkt ist im Falle $D = -3$ durch 3, im Falle $D = -4$ durch 2 zu dividieren. Ist der Körper Ω reell, also D positiv, so ist $r = r' = 2$, und folglich

$$\frac{E(\mathfrak{o})}{E(\mathfrak{o}')} = \frac{\log \varepsilon}{\log \varepsilon'},$$

wo, wenn $k\sqrt{D} = \sqrt{D'}$ gesetzt wird,

$$\varepsilon = \frac{T + U\sqrt{D}}{2}, \quad \varepsilon' = \frac{T' + U'\sqrt{D'}}{2}$$

die Fundamentaleinheiten der Ordnungen $\mathfrak{o}$, $\mathfrak{o}'$ bedeuten, und man erhält

$$\frac{h'}{h} = \frac{\log \varepsilon}{\log \varepsilon'} \cdot k \prod \left(1 - \frac{(D, p)}{p}\right).$$

Was das Zeichen (D, p) betrifft, so ist sein Wert $= 0$, wenn p in D aufgeht; ist $p = 2$ und D ungerade, also $D \equiv 1 \pmod 4$, so ist $(D, p) = +1$ oder $= -1$, je nachdem $D \equiv 1 \pmod 8$ oder $D \equiv 5 \pmod 8$; ist endlich p ungerade, und D nicht teilbar durch p, so ist unter Anwendung der Bezeichnung von Legendre

$$(D, p) = \left(\frac{D}{p}\right).$$

Jeder Idealklasse in $\mathfrak{o}'$ entspricht nach den obigen Festsetzungen eine Klasse von äquivalenten quadratischen Formen $ax^2 + bxy + cy^2$, deren konstante Koeffizienten a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Teiler sind, und die gemeinschaftliche Determinante*) dieser Formen ist $D' = b^2 - 4ac = Dk^2$; wenn D negativ ist, so treten nur sogenannte positive, d. h. solche Formen auf, deren äußere Koeffizienten a, c positiv sind. Umgekehrt entspricht eine bestimmte Klasse von äquivalenten quadratischen Formen, deren Determinante D' keine Quadratzahl ist, immer einer und nur einer Idealklasse eines quadratischen Körpers Ω, und wenn $\mathfrak{o}'$ die Ordnung dieser Idealklasse bedeutet, so ist $D' = D(\mathfrak{o}, \mathfrak{o}')^2 = Dk^2$, wo D die Grundzahl von Ω ist. Mithin sind in den obigen Formeln die verschiedenen Sätze enthalten, welche sich auf die Anzahl der quadratischen Formen in verschiedenen Ordnungen und auf die Unterscheidung der eigentlich und uneigentlich primitiven Formen beziehen.

§ 12.

Methode von Dirichlet.

Wir wenden uns nun der zweiten Lösung desselben allgemeinen Problems zu, welche auf den von Dirichlet eingeführten Prinzipien

*) Es ist wohl darauf zu achten, daß die hier im Sinne von § 1 definierte Determinante das Vierfache der Zahl ist, welche von Gauß die Determinante der Form genannt wird, während der Begriff der (eigentlichen) Äquivalenz der Formen derselbe bleibt.

beruht. Durchläuft $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so konvergiert die Reihe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s}$$

für alle positiven Werte von $(s-1)$; denn weil $N'(\mathfrak{a}') = N(\mathfrak{o}\,\mathfrak{a}')$ ist (§ 5, 1°), so bilden die Glieder dieser Reihe nur einen Teil der gleichfalls aus lauter positiven Gliedern bestehenden Reihe

$$S = \sum \frac{s-1}{N(\mathfrak{a})^s},$$

in welcher $\mathfrak{a}$ alle Ideale der Ordnung $\mathfrak{o}$ durchläuft, und deren Konvergenz schon früher bewiesen ist (D. § 167); übrigens ergibt sich die Konvergenz der Reihe S' auch aus den weiter unten folgenden Untersuchungen.

Unsere Hauptaufgabe besteht darin, den Grenzwert zu ermitteln, welchem die Summe S' sich für unendlich kleine positive Werte von $(s-1)$ annähert. Zu diesem Zwecke betrachten wir aber zunächst nur denjenigen Teil S'' der Reihe S', welcher allen, durch ein gegebenes Ideal $\mathfrak{m}'$ der Ordnung $\mathfrak{o}'$ teilbaren Hauptidealen $\mathfrak{a}'$ entspricht. Die allgemeine Form dieser Ideale $\mathfrak{a}'$ ergibt sich auf die folgende Weise.

1. Jedes Ideal $\mathfrak{a}'$ ist von der Form $\mu\,\mathfrak{o}'$, wo μ eine in $\mathfrak{o}'$ enthaltene Zahl bedeutet, welche relative Primzahl zu dem Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ ist.

2. Die Zahl μ muß in dem gegebenen Ideal $\mathfrak{m}'$ enthalten sein.

3. Die Norm der Zahl μ muß positiv sein.

Umgekehrt, wenn μ diese drei Bedingungen erfüllt, so ist $\mu\,\mathfrak{o}'$ jedenfalls eins von den Idealen $\mathfrak{a}'$, auf welche sich die Summe S'' erstreckt.

Bilden nun die Zahlen $\mu_1, \mu_2 \cdots \mu_n$ eine Basis des gegebenen Ideals $\mathfrak{m}'$, so ist zur Erfüllung der Bedingung 2 erforderlich und hinreichend, daß

$$\mu = m_1\mu_1 + m_2\mu_2 + \cdots + m_n\mu_n$$

sei, wo $m_1, m_2 \cdots m_n$ ganze rationale Zahlen bedeuten, und da $\mathfrak{m}'$ durch $\mathfrak{o}'$ teilbar ist, so ist jede solche Zahl μ auch in $\mathfrak{o}'$ enthalten. Aber sie soll zufolge 1. auch relative Primzahl zu $\mathfrak{f}$ sein. Bezeichnen wir nun wieder (wie in § 9) mit $\psi'(\mathfrak{f})$ die Anzahl aller in $\mathfrak{o}'$ ent-

haltenen Zahlen ω', welche inkongruent in bezug auf $\mathfrak{k}$ und zugleich relative Primzahlen zu $\mathfrak{k}$ sind, so muß gleichzeitig

$$\mu \equiv \omega' \pmod{\mathfrak{k}}, \quad \mu \equiv 0 \pmod{\mathfrak{m}'}$$

sein; da $\mathfrak{k} + \mathfrak{m}' = \mathfrak{o}'$ ist, so gibt es (nach § 2, 2^0) immer Zahlen μ, welche einem solchen Kongruenzpaar genügen, und sie bilden eine bestimmte Zahlklasse in bezug auf den Modul $\mathfrak{k} - \mathfrak{m}'$, welcher offenbar $= \mathfrak{k}\mathfrak{m}'$ ist; denn da $\mathfrak{m}' > \mathfrak{o}\mathfrak{m}'$ ist, so ist $\mathfrak{k} - \mathfrak{m}'$ ein gemeinschaftliches Vielfaches der beiden relativen Primideale $\mathfrak{k}, \mathfrak{o}\mathfrak{m}'$, also auch ein Vielfaches ihres Produkts $\mathfrak{k}\mathfrak{o}\mathfrak{m}' = \mathfrak{k}\mathfrak{m}'$, und umgekehrt ist $\mathfrak{k}\mathfrak{m}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{k}$ und $\mathfrak{m}'$, weil $\mathfrak{m}' > \mathfrak{o}$, $\mathfrak{k} > \mathfrak{o}'$ und $\mathfrak{k}\mathfrak{o} = \mathfrak{k}$, $\mathfrak{o}'\mathfrak{m}' = \mathfrak{m}'$ ist. Die sämtlichen Zahlen μ, welche den Bedingungen 1 und 2 genügen, bilden daher $\psi'(\mathfrak{k})$ verschiedene Zahlklassen (mod. $\mathfrak{k}\mathfrak{m}'$). Jede solche Zahlklasse besteht aber, weil $k\mathfrak{m}' > \mathfrak{k}\mathfrak{m}''$ ist, aus $(\mathfrak{k}\mathfrak{m}, k\mathfrak{m}')$ verschiedenen Zahlklassen (mod. $k\mathfrak{m}'$), und folglich ist

$$c = \psi'(\mathfrak{k})\,(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}')$$

die Anzahl der Zahlklassen (mod. $k\mathfrak{m}'$), aus welchen das System aller dieser Zahlen μ besteht. Es läßt sich leicht zeigen, daß diese Anzahl c von $\mathfrak{m}'$ unabhängig ist. In der Tat, aus

$$(\mathfrak{o}, \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}')\,(\mathfrak{o}', \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{m}')\,(\mathfrak{o}\mathfrak{m}', \mathfrak{m}')$$

folgt

$$kN'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')\,(\mathfrak{o}\mathfrak{m}', \mathfrak{m}'),$$

mithin, weil $N'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')$ ist (§ 5, 1^0), $(\mathfrak{o}\mathfrak{m}', \mathfrak{m}') = k$, also auch

$$(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = k,$$

weil offenbar für je zwei Moduln $\mathfrak{a}, \mathfrak{b}$ der Satz $(\eta\mathfrak{a}, \eta\mathfrak{b}) = (\mathfrak{a}, \mathfrak{b})$ gilt, sobald η eine von 0 verschiedene Zahl ist. Da ferner

$$(\mathfrak{o}, k\mathfrak{o}\mathfrak{m}') = (\mathfrak{o}, \mathfrak{k}\mathfrak{m}')\,(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}'),$$

also

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}') = \frac{N(k\mathfrak{o}\mathfrak{m}')}{N(\mathfrak{k}\mathfrak{m}')} = \frac{N(k\mathfrak{o})}{N(\mathfrak{k})} = \frac{k^n}{N(\mathfrak{k})}$$

ist, so ergibt sich

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}') = (\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}')\,(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = \frac{k^{n+1}}{N(\mathfrak{k})},$$

und folglich ist

$$c = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})}\,k^{n+1}$$

die Anzahl der fraglichen Zahlklassen in bezug auf den Modul

$$k\mathfrak{m}' = [k\mu_1, k\mu_2 \cdots k\mu_n].$$

Wählt man aus jeder dieser Klassen einen bestimmten Repräsentanten

$$a_1\mu_1 + a_2\mu_2 + \cdots + a_n\mu_n,$$

so werden alle Zahlen μ derselben Klasse durch die Form

(I) $$\mu = (a_1 + kz_1)\mu_1 + (a_2 + kz_2)\mu_2 + \cdots + (a_n + kz_n)\mu_n$$

erzeugt, wenn $z_1, z_2 \cdots z_n$ alle ganzen rationalen Zahlen durchlaufen; und die sämtlichen Zahlen μ, welche den Bedingungen 1 und 2 genügen, werden durch c solche lineare Formen erzeugt, und zwar jede nur einmal.

Von diesen Zahlen μ sind aber nur diejenigen beizubehalten, welche auch der dritten Bedingung

(II) $$N(\mu) > 0$$

genügen. Umgekehrt erzeugt jede solche Zahl μ ein Hauptideal $\mu\mathfrak{o}'$ in $\mathfrak{o}'$, welches durch das gegebene Ideal $\mathfrak{m}'$ teilbar ist.

Aber es leuchtet ein, daß, wenn μ alle diese Zahlen durchläuft, jedes bestimmte, durch $\mathfrak{m}'$ teilbare Hauptideal $\mathfrak{a}'$ unendlich oft erzeugt wird. Ist nämlich μ_0 eine bestimmte von diesen Zahlen μ, so wird dasselbe Hauptideal $\mathfrak{o}'\mu_0$ offenbar durch alle, und nur durch die Zahlen μ erzeugt, welche von der Form $\mu = \varepsilon'\mu_0$ sind, wo ε' eine beliebige in $\mathfrak{o}'$ enthaltene Einheit (von positiver Norm) bedeutet. Um dies zu vermeiden, muß man den Zahlen μ neue Beschränkungen auferlegen. Zu diesem Zwecke kehren wir zu den Betrachtungen und Bezeichnungen des § 10 zurück und erweitern die Bedeutung der dort erklärten ν Symbole $l', l'' \cdots l^{(\nu)}$. Ist $\omega = \varphi(\Theta)$ eine beliebige von 0 verschiedene Zahl des Körpers Ω, und $\omega' = \varphi(\Theta')$, so verstehen wir unter $l'(\omega)$ den reellen Teil des Logarithmen von

$$\frac{\omega'}{\sqrt[n]{N(\omega)}}$$

oder das Doppelte dieses reellen Teiles, je nachdem Θ' eine reelle oder imaginäre Wurzel der irreduktiblen Gleichung $f(\Theta') = 0$ ist; legt man ferner den Symbolen $l''(\omega), l'''(\omega) \cdots l^{(\nu)}(\omega)$ die entsprechende Bedeutung in bezug auf die Wurzeln $\Theta'', \Theta''' \cdots \Theta^{(\nu)}$ bei, so ist offenbar

$$l'(\omega) + l''(\omega) + \cdots + l^{(\nu)}(\omega) = 0.$$

Bilden nun $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ ein bestimmtes Fundamentalsystem $\mathfrak{R}$ von Einheiten der Ordnung $\mathfrak{o}'$, so wollen wir unter den Exponenten

der Zahl ω in bezug auf $\mathfrak{R}$ diejenigen völlig bestimmten reellen Werte $x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$ verstehen, welche den ν Gleichungen

$$l'(\varrho_1')x_1(\omega) + l'(\varrho_2')x_2(\omega) + \cdots + l'(\varrho_{\nu-1}')x_{\nu-1}(\omega) = l'(\omega)$$
$$l''(\varrho_1')x_1(\omega) + l''(\varrho_2')x_2(\omega) + \cdots + l''(\varrho_{\nu-1}')x_{\nu-1}(\omega) = l''(\omega)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$l^{(\nu)}(\varrho_1')x_1(\omega) + l^{(\nu)}(\varrho_2')x_2(\omega) + \cdots + l^{(\nu)}(\varrho_{\nu-1}')x_{\nu-1}(\omega) = l^{(\nu)}(\omega)$$

genügen, deren letzte eine Folge der übrigen ist. Da $l'(\alpha\beta) = l'(\alpha) + l'(\beta)$ ist, und dasselbe für die anderen Symbole $l'', l''' \cdots l^{(\nu)}$ gilt, so ist auch $x_1(\alpha\beta) = x_1(\alpha) + x_1(\beta)$, und dasselbe gilt auch für die anderen Exponenten $x_2, x_3 \ldots x_{\nu-1}$. Die Exponenten der Einheit

$$\varepsilon' = \varrho'^{u}\varrho_1'^{u_1}\varrho_2'^{u_2}\cdots\varrho'^{u_{\nu-1}}_{\nu-1},$$

wo ϱ' wieder eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$ bedeutet, sind offenbar die ganzen rationalen Zahlen $u_1, u_2 \cdots u_{\nu-1}$.

Ist nun μ_0 eine bestimmte der oben definierten Zahlen μ, d. h. eine Zahl, welche in einer der c linearen Formen (I) enthalten ist und zugleich der Bedingung (II) genügt, so sind die sämtlichen Produkte $\mu = \varepsilon'\mu_0$, welche den sämtlichen Einheiten ε' der Ordnung $\mathfrak{o}'$ entsprechen, eben solche Zahlen, und alle diese Zahlen μ und keine anderen liefern, wie oben bemerkt, ein und dasselbe durch $\mathfrak{m}'$ teilbare Hauptideal $\mathfrak{a}' = \mathfrak{o}'\mu_0 = \mathfrak{o}'\mu$ der Ordnung $\mathfrak{o}'$. Da nun

$$x_1(\mu) = x_1(\mu_0) + u_1 \cdots x_{\nu-1}(\mu) = x_{\nu-1}(\mu_0) + u_{\nu-1}$$

ist, so kann man die ganzen rationalen Zahlen $u_1, u_2 \cdots u_{\nu-1}$ offenbar stets und nur auf eine einzige Art so wählen, daß

(III) $$0 \leqq x_1(\mu) < 1 \cdots 0 \leqq x_{\nu-1}(\mu) < 1$$

wird, und da hierbei der in ε' auftretende Faktor ϱ'^{u} seine sämtlichen r' Werte

$$1, \varrho', \varrho'^{2} \cdots \varrho'^{r'-1}$$

durchlaufen darf, so werden durch diese Bedingungen (III) aus dem System aller mit μ_0 assoziierten Zahlen $\mu = \varepsilon'\mu_0$ genau r' Zahlen μ herausgehoben, während alle übrigen ausgeschlossen werden. Läßt man daher μ alle diejenigen Zahlen durchlaufen, welche in den c linearen Formen (I) enthalten sind und zugleich den Bedingungen (II) und (III) genügen, so wird jedes durch $\mathfrak{m}'$ teilbare Hauptideal $\mathfrak{a}' = \mathfrak{o}'\mu$ der Ordnung $\mathfrak{o}'$ genau r'-mal erzeugt, und folglich ist der von uns betrachtete Teil S'' der Summe S' identisch mit

$$\frac{1}{r'}\sum\frac{s-1}{N'(\mathfrak{o}'\mu)^s} = \frac{1}{r'}\sum\frac{s-1}{N(\mu)^s}.$$

Nun zerlegen wir diese Summe abermals in c Partialsummen, indem wir jedesmal die Beiträge derjenigen Zahlen μ zu einer Partialsumme sammeln, welche in einer und derselben Linearform (I) enthalten sind und außerdem den Bedingungen (II) und (III) genügen. Es sei t eine beliebige positive Größe, und T die entsprechende Anzahl dieser Zahlen μ, für welche zugleich

$$N(\mu) \leqq t \tag{IV}$$

wird, so wollen wir beweisen, daß der Quotient $T:t$ mit unendlich wachsendem t sich einem endlichen Grenzwerte nähert. Zu diesem Zwecke bezeichnen wir mit

$$h_1, h_2 \cdots h_n$$

ein System von reellen, stetig veränderlichen Größen und betrachten die n homogenen linearen Funktionen $\omega', \omega'' \cdots \omega^{(n)}$, welche aus

$$\omega = h_1\mu_1 + h_2\mu_2 + \cdots + h_n\mu_n$$

dadurch hervorgehen, daß die dem Körper Ω angehörigen Konstanten $\mu_1, \mu_2 \cdots \mu_n$ durch die mit ihnen konjugierten Zahlen ersetzt werden, welche der Reihe nach den Wurzeln $\Theta', \Theta'' \cdots \Theta^{(n)}$ der Gleichung $f(\Theta) = 0$ entsprechen. Setzen wir auch in allen Fällen, wo die Werte der Variablen $h_1, h_2 \cdots h_n$ nicht sämtlich rational sind, der Kürze wegen

$$\omega'\omega'' \cdots \omega^{(n)} = N(\omega),$$

so ist $N(\omega)$ eine homogene Funktion n-ten Grades von den Variabeln $h_1, h_2 \cdots h_n$. Wir beschränken nun zunächst die Variabilität dieser Größen durch die Bedingung

$$0 < N(\omega) \leqq 1 \tag{V}$$

und definieren hierauf ein System von ν Funktionen

$$l'(\omega), l''(\omega) \cdots l^{(\nu)}(\omega)$$

und aus diesem ein System von $(\nu - 1)$ Funktionen

$$x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$$

genau nach denselben Regeln, wie dies oben für den Fall geschehen ist, daß die sämtlichen Variablen $h_1, h_2 \cdots h_n$ rationale Werte haben, und folglich ω eine Zahl des Körpers Ω ist. Hierauf beschränken

wir die Variabilität der Größen $h_1, h_2 \cdots h_n$ ferner durch die $(\nu - 1)$ Bedingungen

$$\text{(VI)} \qquad 0 \leqq x_1(\omega) < 1 \cdots 0 \leqq x_{\nu-1}(\omega) < 1.$$

Hierdurch, sowie durch die Bedingung (V), ist den Variablen $h_1, h_2 \cdots h_n$ ein bestimmtes Gebiet G angewiesen, und zwar ist (vgl. D. § 167) das über dieses Gebiet G ausgedehnte n-fache Integral

$$g = \int dh_1\, dh_2 \cdots dh_n = \frac{\sigma L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')}{\sqrt{\pm \Delta(\mu_1, \mu_2 \cdots \mu_n)}} = \frac{\sigma r' \mathrm{E}(\mathfrak{o}')}{k N'(\mathfrak{m}') \sqrt{\pm D}},$$

wo $\sigma = 2^{\nu-1}\pi^{n-\nu}$, im Falle $n = 2\nu$ aber $= (2\pi)^\nu$ ist; $\sqrt{\pm D}$ bedeutet die positive Quadratwurzel aus dem absoluten Werte der Grundzahl D des Körpers Ω.

Die oben mit T bezeichnete Anzahl der in einer bestimmten Linearform (I) erhaltenen Zahlen μ, welche außerdem den Bedingungen (II), (III), (IV) genügen, besitzt nun die folgende Bedeutung für das eben definierte Gebiet G. Setzt man

$$h_1 = \frac{a_1 + kz_1}{\sqrt[n]{t}}, \quad h_2 = \frac{a_2 + kz_2}{\sqrt[n]{t}} \cdots h_n = \frac{a_n + kz_n}{\sqrt[n]{t}},$$

so bringt jedes System von n ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$, welchem eine solche Zahl μ entspricht, ein System von n reellen Werten $h_1, h_2 \cdots h_n$ hervor, welches dem Gebiete G angehört; denn da $N(\omega)$ eine homogene Funktion n-ten Grades, jede der Funktionen $x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$ aber eine homogene Funktion 0-ten Grades von den Variablen $h_1, h_2 \cdots h_n$ ist, so gehen die Bedingungen (II) und (IV) in die Bedingung (V), und die Bedingungen (III) in die Bedingungen (VI) über. Setzt man ferner

$$\frac{k}{\sqrt[n]{t}} = \delta; \quad \frac{a_1}{\sqrt[n]{t}} = h_1^0, \quad \frac{a_2}{\sqrt[n]{t}} = h_2^0 \cdots \frac{a_n}{\sqrt[n]{t}} = h_n^0,$$

so ist das durch $z_1, z_2 \cdots z_n$ hervorgebrachte, dem Gebiet G angehörende Wertsystem $h_1, h_2 \cdots h_n$ von der Beschaffenheit, daß die Größen

$$\frac{h_1 - h_1^0}{\delta} = z_1, \quad \frac{h_2 - h_2^0}{\delta} = z_2 \cdots \frac{h_n - h_n^0}{\delta} = z_n$$

ganze rationale Zahlen werden; und umgekehrt leuchtet ein, daß jedes dem Gebiet G angehörende Wertsystem $h_1, h_2 \cdots h_n$, welches dieser letzten Bedingung genügt, rückwärts ein System von ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$ und dadurch eine Zahl μ der Linearform (I) hervorbringt, welche auch den Bedingungen (II), (III), (IV) genügt. Mithin ist T die Anzahl derjenigen dem Gebiet G angehörenden Wertsysteme $h_1, h_2 \cdots h_n$, für welche die Quotienten

$$\frac{h_1 - h_1^0}{\delta}, \frac{h_2 - h_2^0}{\delta} \cdots \frac{h_n - h_n^0}{\delta}$$

ganze rationale Zahlen werden. Wächst nun t über alle Grenzen, so wird δ unendlich klein, und aus dem Begriffe eines n-fachen bestimmten Integrals ergibt sich, daß

$$\lim (T\delta^n) = k^n \lim \left(\frac{T}{t}\right) = \int dh_1 dh_2 \cdots dh_n = g$$

ist, mögen die Größen $h_1^0, h_2^0 \cdots h_n^0$ von δ unabhängig sein oder nicht. Nach einem Fundamentalsatze von Dirichlet (D. § 118) folgt hieraus, daß die auf alle Zahlen μ der einen Linearform (I) ausgedehnte Partialsumme

$$\frac{1}{r'} \sum \frac{s-1}{N(\mu)^s}$$

für alle positiven Werte von $(s-1)$ konvergiert und für unendlich kleine Werte von $(s-1)$ sich dem Grenzwerte

$$\frac{1}{r'} \lim \left(\frac{T}{t}\right) = \frac{g}{k^n r'} = \frac{\sigma \mathrm{E}(\mathfrak{o}')}{k^{n+1} N'(\mathfrak{m}') \sqrt{\pm D}}$$

nähert. Da derselbe von den Zahlen $a_1, a_2 \cdots a_n$, welche diese eine Linearform charakterisieren, gänzlich unabhängig ist, und da die Anzahl der Partialsummen, aus welchen die bis jetzt von uns betrachtete Summe S'' besteht,

$$= c = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} k^{n+1}$$

ist, so erhalten wir das Resultat

$$\lim S'' = \lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma \mathrm{E}(\mathfrak{o}')}{N'(\mathfrak{m}') \sqrt{\pm D}},$$

wo links die Summe über alle durch $\mathfrak{m}'$ teilbaren Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnt ist.

§ 13.

Resultat dieser Methode.

Mit Hilfe des eben bewiesenen Satzes ist es leicht, unsere Aufgabe zu lösen. Nimmt man $\mathfrak{m}' = \mathfrak{o}'$, also $N'(\mathfrak{m}') = 1$, so ergibt sich

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}},$$

wo die Summe links über alle Ideale $\mathfrak{a}'$ ausgedehnt ist, welche der Hauptklasse O' der Ordnung $\mathfrak{o}'$ angehören.

Nun sei B' eine beliebige Ideal-Klasse der Ordnung $\mathfrak{o}'$, und $\mathfrak{m}'$ ein bestimmtes Ideal der inversen Klasse B'^{-1}. Durchläuft $\mathfrak{b}'$ alle Ideale der Klasse B', während $\mathfrak{m}'$ unverändert bleibt, so werden die Produkte $\mathfrak{b}'\mathfrak{m}'$ lauter Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$, welche durch $\mathfrak{m}'$ teilbar sind; und umgekehrt, ist $\mathfrak{a}'$ ein durch $\mathfrak{m}'$ teilbares Hauptideal der Ordnung $\mathfrak{o}'$, so gibt es (nach § 5, 3°) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{b}'\mathfrak{m}' = \mathfrak{a}'$ wird, und $\mathfrak{b}'$ muß notwendig der Klasse B' angehören, weil $\mathfrak{m}'$ ein Ideal der inversen Klasse ist. Da außerdem $N'(\mathfrak{b}'\mathfrak{m}') = N'(\mathfrak{b}')N'(\mathfrak{m}')$ ist, so ist die über alle Ideale $\mathfrak{b}'$ der Klasse B' ausgedehnte Summe

$$\sum \frac{s-1}{N'(\mathfrak{b}')^s} = N'(\mathfrak{m}')^s \sum \frac{s-1}{N'(\mathfrak{a}')^s},$$

wo $\mathfrak{a}'$ alle durch $\mathfrak{m}'$ teilbaren Hauptideale der Ordnung $\mathfrak{o}'$ durchläuft. Hieraus ergibt sich nach dem Schlußsatz des vorigen Paragraphen für unendlich kleine positive Werte von $(s-1)$

$$\lim \sum \frac{s-1}{N'(\mathfrak{b}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}},$$

d. h. der Grenzwert der über alle Ideale einer beliebigen Klasse in $\mathfrak{o}'$ ausgedehnten Summe ist für jede Klasse derselbe, und zwar offenbar von 0 verschieden.

Für den Spezialfall, in welchem $\mathfrak{o}'$ das Gebiet $\mathfrak{o}$ aller ganzen Zahlen des Körpers Ω ist, ergibt sich hieraus, weil

$$\mathfrak{f} = \mathfrak{o}, \quad N(\mathfrak{f}) = \psi'(\mathfrak{f}) = 1$$

wird, und weil die Anzahl h aller Ideal-Klassen der Ordnung $\mathfrak{o}$ endlich ist (D. § 164), das Resultat

$$\lim S = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = h \frac{\sigma E(\mathfrak{o})}{\sqrt{\pm D}},$$

wo die Summe über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ auszudehnen ist.

Durchläuft nun $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so durchläuft $\mathfrak{o}\mathfrak{a}'$ alle diejenigen Ideale der Ordnung $\mathfrak{o}$, welche relative Primideale zu dem Führer $\mathfrak{f}$ sind, und jedes nur ein einziges Mal. Da zugleich $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$ ist, so ist die über alle Ideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnte Summe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \sum \frac{s-1}{N(\mathfrak{o}\mathfrak{a}')^s};$$

durchläuft aber $\mathfrak{p}$ alle verschiedenen in $\mathfrak{f}$ aufgehenden Primideale in $\mathfrak{o}$, so ist nach den allgemeinen Gesetzen der Teilbarkeit die über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ ausgedehnte Summe

$$\sum \frac{1}{N(\mathfrak{a})^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N(\mathfrak{o}\mathfrak{a}')^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N'(\mathfrak{a}')^s},$$

und folglich, weil

$$\prod \left(1-\frac{1}{N(\mathfrak{p})}\right) = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})}$$

ist,

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim \sum \frac{s-1}{N(\mathfrak{a})^s},$$

d. h.

$$\lim S' = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim S.$$

Da die rechte Seite einen endlichen Wert hat, so folgt zunächst, daß die Anzahl h' der Ideal-Klassen in $\mathfrak{o}'$ endlich sein muß, weil oben für jeden Bestandteil der linken Seite, welcher einer einzelnen Klasse entspricht, ein und derselbe von 0 verschiedene Grenzwert gefunden ist. Setzt man diesen Wert und ebenso den Grenzwert der rechten Seite ein, so ergibt sich

$$h' \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}} = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \cdot h \frac{\sigma E(\mathfrak{o})}{\sqrt{\pm D}},$$

und hieraus

$$\frac{h'}{h} = \frac{\psi(\mathfrak{f})}{\psi'(\mathfrak{f})} \cdot \frac{E(\mathfrak{o})}{E(\mathfrak{o}')},$$

was mit dem in § 10 nach der Methode von Gauß gefundenen Resultat übereinstimmt.

Erläuterungen zur vorstehenden Abhandlung.

Diese Abhandlung findet ihre Ergänzung in dem im Nachlaß veröffentlichten Überblick über die allgemeine Modultheorie (Brief an Frobenius von 1883); beides war — wie dort und an anderen Stellen ausgesprochen ist — gedacht als Grundlage für die allgemeinen Reziprozitätsgesetze.

In der Tat ist die in der Abhandlung behandelte Klasseneinteilung eine Strahlklasseneinteilung, wie sie der Klassenkörpertheorie zugrunde liegt, wenn auch noch nicht die allgemeinste. Der Ausdruck für das Verhältnis der Klassenanzahlen (§ 10, Schluß) findet sich genau in der allgemeingültigen Form; auch die gruppentheoretischen Beweismethoden sind ähnlich, wenn auch noch etwas komplizierter, als in der späteren allgemeinen Theorie (H. Weber, Math. Ann., Bd. 48, S. 433 ff.). In § 12 werden die transzendenten Methoden zum ersten Male auf solche allgemeineren Klasseneinteilungen übertragen, was später viel weitergehend von H. Weber im allgemeinsten Falle entwickelt wurde (Math. Ann., Bd. 49, S. 83 ff.). Auf Weber aber baut Takagi auf.

Idealtheoretisch liegt die Bedeutung der Abhandlung darin, daß zum ersten Male die Beziehung zwischen Idealen verschiedener Ringe vermöge Zuordnung von Durchschnitts- und Erweiterungsideal behandelt wird. Die hier entwickelten Begriffe lassen sich auf beliebige Ringe ausdehnen und führen zu einer Zuordnung von Klassen von Idealen im Unter- und Oberring, wobei wieder Durchschnitts-(Verengungs-)Ideal und Erweiterungsideal eine ausgezeichnete Rolle spielen (vgl. H. Grell, Beziehungen zwischen den Idealen verschiedener Ringe, Math. Ann., Bd. 97, 1927).

Noether.