Ueber Zahlengruppen in algebraischen Körpern.

Von

H. Weber in Strassburg.

Der vorliegende Aufsatz bildet die Einleitung und nothwendige Grundlage zu einer eingehenden Untersuchung gewisser algebraischer Zahlkörper, deren Ergebnisse ich in einem folgenden Aufsatze ausführlich mitzutheilen hoffe, über die aber schon hier einige vorläufige Angaben Platz finden mögen.

Die Resultate beziehen sich zunächst auf einen imaginären quadratischen Körper, für den bis jetzt allein die nöthigen Hilfsmittel bereit sind, wiewohl es wahrscheinlich ist, dass die ganze Theorie einer wesentlichen Verallgemeinerung fähig ist.

Aus einem quadratischen Körper (mit negativer Grundzahl) lässt sich eine Kette höherer Körper ableiten, die gewissen Zahlengruppen in dem quadratischen Körper entsprechen. Der erste unter diesen Körpern ist der aus der complexen Multiplication der elliptischen Functionen bekannte *Classenkörper*, dessen Galois'sche Gruppe der Gruppe der Idealclassen im quadratischen Körper isomorph ist; daran schliessen sich die gleichfalls in der Theorie der complexen Multiplication vorkommenden Körper, die in gleicher Weise den Gruppen der Idealclassen in den verschiedenen Ordnungen des quadratischen Körpers entsprechen, die ich die *Ordnungskörper* nennen will. Diese sind relativ Abel'sche Körper in Bezug auf den gegebenen quadratischen Körper.

Ueber jedem dieser Körper giebt es dann wieder eine unendliche Zahl höherer Körper, die in Bezug auf einen dieser Ordnungskörper Abel'sche sind; diese Körper erhält man aus der *Theilung der elliptischen Functionen mit einem singulären Modul* und sie sollen daher *Theilungskörper* genannt werden. Der Theiler, den ich den *Modul* dieses Körpers nenne, kann dabei ein beliebiges *Ideal* des quadratischen Körpers sein.

Um die Entstehung und gegenseitige Beziehung dieser Körper deutlich darlegen zu können, sind die in der vorliegenden ersten Arbeit

gegebenen Ausführungen nothwendig, deren Bedeutung besser erkannt wird, wenn sie gleich allgemein, für beliebige Körper durchgeführt werden. Ich mache hier schon auf die allgemeine Definition der *Genera* oder *Geschlechter* (§ 6) aufmerksam, die eine weit tiefer gehende ist, als die in § 13 des zweiten Bandes meiner Algebra gegebene*).

Die erste und wichtigste Frage, der sich die weitere Untersuchung zuwenden muss, ist die Gradbestimmung dieser Körper oder die Irreducibilität der die Körper definirenden Gleichungen. Als Hilfsmittel für diese Untersuchung hat sich bis jetzt nur eines in allen Fällen als wirksam erwiesen, was bereits in der Kreistheilungstheorie gute Dienste thut, und das sich auf die Dirichlet'schen Formeln für Classenzahlen stützt**).

Mit jedem solchen Irreducibilitätsbeweis ist zugleich der Beweis eines Satzes über unendlich viele Primideale in einer gewissen Idealgruppe gegeben, wie mit dem entsprechenden Beweise der Irreducibilität der Kreistheilungsgleichung der Satz von den unendlich vielen Primzahlen in einer arithmetischen Progression***).

Der relative Grad eines Ordnungskörpers in Bezug auf den Körper, der ausser den rationalen Zahlen beliebige Einheitswurzeln enthält, ergiebt sich auf diesem Wege gleich der Anzahl der in dem Hauptgeschlecht enthaltenen Idealclassen, und daraus erhält man zugleich aufs Einfachste den Beweis des Dirichlet'schen Satzes, dass durch jede quadratische Form unendlich viele Primzahlen darstellbar sind, die zugleich in einer gegebenen mit den Charakteren der quadratischen Form verträglichen Linearform enthalten sind. (Freilich bis jetzt nur für negative Discriminanten.) Dieser tiefere Zusammenhang des Dirichlet'schen Satzes, der bisher ziemlich unvermittelt aufgetreten ist, mit der Theorie der quadratischen Körper und der von Kronecker entwickelten Zerfällung der Classengleichung in der complexen Multiplication durch Adjunction gewisser Quadratwurzeln, ist mir besonders überraschend und interessant gewesen. Es folgt daraus, dass eine weitere Zerfällung der Classengleichung, selbst nach Adjunction beliebiger Kreistheilungszahlen unmöglich ist.

Der Relativgrad eines Theilungskörpers in Bezug auf den zu Grunde gelegten Ordnungskörper, der einen realen oder idealen Modul $\mathfrak{m}$ hat, ist gleich der Anzahl zu $\mathfrak{m}$ theilerfremder, nach $\mathfrak{m}$ incongruenter Zahlen, getheilt durch die Anzahl der nach dem Modul $\mathfrak{m}$ incongruenten Einheiten des Körpers (die letztere Zahl ist beim imaginären quadra-

*) Weber, Lehrbuch der Algebra, Braunschweig 1894, 1896.

**) Wahrscheinlich hat Kronecker dies oder ein sehr verwandtes Beweismittel in der Theorie der complexen Multiplication angewandt (Monatsberichte der Berliner Academie 26. Juni 1862).

***) Vgl. Algebra, Bd. II, zweiter Nachtrag.

tischen Körper im allgemeinen $= 2$, in zwei bekannten speciellen Fällen $= 4$ oder $= 6$.)

Mit diesem Beweise ist der Beweis eines neuen Satzes über unendlich viele Primideale verbunden, der geradezu als eine Verallgemeinerung des Satzes von den unendlich vielen Primzahlen in arithmetischen Progressionen aufgefasst werden kann. Wenn man nämlich die Ideale des quadratischen Körpers in der Weise in Classen theilt, dass zwei Ideale nur dann in eine Classe aufgenommen werden, wenn ihr Quotient eine nach dem Modul $\mathfrak{m}$ mit einer Einheit congruente Zahl ist, so ergiebt sich, dass in jeder dieser Classen unendlich viele Primideale ersten Grades vorkommen; und darin ist als specieller Fall der Satz enthalten, dass durch eine Linearform $\alpha\xi + \beta$, in der α, β, feste ganze Zahlen ohne gemeinsame Theiler und ξ eine variable ganze Zahl des quadratischen Körpers bedeuten, unendlich viele complexe Primzahlen dargestellt werden können.

Die so gewonnenen Resultate bahnen den Weg zu einer genaueren Untersuchung der Grundzahl und des Grundideals des Classenkörpers, die ursprünglich das Ziel der ganzen Arbeit bildete, insbesondere zum Beweise des von Kronecker vermutheten Satzes, dass das Partialgrundideal des Classenkörpers in Bezug auf den gegebenen quadratischen Körper gleich 1 ist.

Ich stütze mich auf die Darstellung der Theorie der algebraischen Zahlen, die ich im zweiten Bande meines Lehrbuches der Algebra gegeben habe. Ausserdem ist aber noch eine Reihe von Sätzen über die Theilung der elliptischen Functionen erforderlich, die noch wenig oder gar nicht bekannt sind, die daher auch noch abgeleitet werden müssen. Dies aber muss auf eine spätere Abhandlung verspart werden.

§ 1.

Abel'sche Gruppen.

Es sei G ein System irgend welcher Elemente

$$\alpha, \beta, \gamma, \ldots (G),$$

die eine endliche oder unendliche *Abel'sche Gruppe* bilden, so dass sich aus zwei Elementen α, β des Systems ein bestimmtes drittes ableiten lässt, das mit $\alpha\beta$ bezeichnet wird, also etwa

$$\alpha\beta = \gamma, \tag{1}$$

dass bei dieser Zusammensetzung das associative und das commutative Gesetz

$$(\alpha\beta)\gamma = \alpha(\beta\gamma), \quad \alpha\beta = \beta\alpha \tag{2}$$

gilt, dass endlich, wenn α, γ gegeben sind, immer ein Element β

gefunden werden kann, was der Bedingung (1) genügt. Dies Element bezeichnen wir mit

$$\beta = \frac{\gamma}{\alpha} = \gamma : \alpha. \tag{3}$$

Es folgt dann, dass es ein Element 1 in G giebt, das für jedes α der Bedingung $1 . \alpha = \alpha . 1 = \alpha$ genügt, und dass die Regeln des Rechnens in dieser Gruppe genau übereinstimmen mit den Regeln der Multiplication und Division im Zahlenreich (ohne die Null). Demnach werden wir auch die Ausdrücke *Product* und *Quotient* für die Verbindungen $\alpha\beta$ und $\gamma : \alpha$ brauchen.

Wenn A, B irgend zwei Theile von G sind (Gruppen oder nicht) so verstehen wir unter dem *Product* AB das System der Elemente $\alpha\beta$, wenn α alle Elemente von A, β alle Elemente von B durchläuft, wobei ein Element, was mehrmals in der Form $\alpha\beta$ dargestellt werden kann, nur einmal in AB aufgenommen wird. (Composition der Theile, Algebra Bd. II, § 4). Ist A eine Gruppe, und B ein Theil von A, so ist hiernach $A = AB$. Sind A und B zwei Gruppen, so ist auch AB eine Gruppe, die das kleinste gemeinschaftliche Vielfache von A und B genannt wird. Aber auch der kürzere Ausdruck *„Product von A und B“* ist nicht misszuverstehen, und soll daher in der Folge gebraucht werden. Wenn die beiden Systeme A, B gemeinschaftliche Elemente haben, so bilden diese ein System D, das der *Durchschnitt**) von A und B heisst. Ein solcher Durchschnitt ist immer vorhanden, wenn A und B Gruppen sind, da sie ja dann wenigstens die 1 gemein haben, und D ist dann selbst wieder eine Gruppe. Zwei Gruppen, die *nur* das Element 1 gemein haben, heissen *theilerfremd* oder *relativ prim.*

Ist A eine Gruppe, und sind ϱ, σ irgend zwei Elemente aus G, so haben die beiden Systeme ϱA, σA entweder kein einziges Element gemein, oder sie sind ganz identisch.

Die Systeme ϱA heissen die *Nebengruppen zu A.* Zwei Elemente aus G, die in derselben Nebengruppe vorkommen, heissen *äquivalent nach A.* Aequivalente Elemente sind auch dadurch definirt, *dass ihr Quotient in A enthalten ist.*

Es seien jetzt A und B zwei Gruppen in G, von der Art, dass alle Elemente von B zugleich in A enthalten sind, wofür wir auch sagen, *dass B ein Theiler von A ist.*

Wählt man die Elemente α, α', α'', ... aus A so aus, dass unter den in A enthaltenen Nebengruppen

---

*) Indem ich den Ausdruck „*Durchschnitt*“ statt des längeren „grösster gemeinschaftlicher Theiler“ brauche, folge ich einem Vorschlag von Study.

(4) $$\alpha B,\ \alpha' B.\ \alpha'' B, \ldots$$

niemals zwei identisch sind, so sind zwei Fälle möglich:

1) Die Reihe (4) bricht nach einer endlichen Anzahl von Gliedern ab. Dann zerfällt A in eine endliche Anzahl von Nebengruppen αB, deren Zahl wir den *Index des Theilers B von A nennen* und mit

(5) $$j = (A, B)$$

bezeichnen. Wir setzen nach einer von Galois gebrauchten Bezeichnung

(6) $$A = \alpha B + \alpha' B + \alpha'' B + \cdots = \Sigma \alpha B$$

und nennen α, α', α'' ein *volles Repräsentantensystem von A nach B.* In diesem Falle heisst B ein Theiler von A von endlichem Index.

2) Die Reihe (4) bricht nicht ab. In diesem Falle geben wir dem Zeichen (A, B) die Bedeutung

(7) $$(A, B) = 0$$

und nennen *B einen Theiler von A ohne Index oder vom Index Null.*

Ist B ein Theiler von A von endlichem Index, so bilden die Nebengruppen (4) unter sich eine *endliche Abel'sche Gruppe,* wenn wir

$$\alpha B\, \alpha' B = \alpha \alpha' B$$

setzen, weil das System $\alpha \alpha' B$ ja auch unter den Nebengruppen (4) vorkommt. Diese Gruppe kann der Quotient von A durch B genannt und mit $A|B$ bezeichnet werden (Algebra, Bd. II, § 4). Der Grad dieser Gruppe ist gleich (A, B).

Wenn zwei solche Gruppen $A|B$ und $A'|B'$ isomorph sind (einstufig) so setzen wir auch kurz

$$A|B = A'|B',$$

was zur Folge hat, dass auch $(A, B) = (A', B')$ ist.

Wir beweisen zunächst eine Reihe von Sätzen über Gruppentheiler:

I. *Ist B ein Theiler von A und C ein Theiler von B so ist auch C ein Theiler von A und*

$$(A, C) = (A, B)\,(B, C).$$

Denn jede Nebengruppe αB zerfällt in ebenso viele Nebengruppen $\alpha \beta C = \alpha' C$ als B in Nebengruppen βC zerfällt.

Es ergiebt sich daraus, dass, wenn (A, C) von Null verschieden ist, keine der Zahlen (A, B), (B, C) gleich Null sein kann.

II. *Ist B ein Theiler von A, und C so beschaffen, dass B der Durchschnitt von A und BC ist, so ist*

$$(AC, BC) = (A, B).$$

Wenn nämlich αB und $\alpha' B$ zwei verschiedene Nebengruppen zu B sind, so können die Nebengruppen αBC, $\alpha' BC$ nur dann identisch sein, wenn $\alpha : \alpha'$ in BC enthalten ist. Wenn nun aber, wie vorausgesetzt, B der Durchschnitt von A und BC ist, so müsste hiernach

$\alpha:\alpha'$ in B enthalten, also αB und $\alpha' B$ nicht verschieden sein, wie doch angenommen war. Die Anzahl der von einander verschiedenen Nebengruppen αBC ist also gewiss nicht kleiner als die Anzahl der αB, und folglich ist $(AC, BC) = 0$, wenn $(A, B) = 0$ ist. Ist aber (A, B) von Null verschieden, so ist

$$A = \Sigma \alpha B, \quad AC = \Sigma \alpha BC,$$

woraus sich die Formel II ergiebt.

Die im Satze II über C gemachte Voraussetzung ist immer erfüllt, wenn *C ein Theiler von B ist, oder wenn C theilerfremd zu A ist.*

Daraus ergiebt sich leicht der Satz:

III. *Ist B ein Theiler von A und B_1 ein Theiler von A_1, und ist A_1 relativ prim zu A, so ist*

$$(AA_1, BB_1) = (A, B)(A_1, B_1).$$

Die Voraussetzung involvirt zugleich, dass B theilerfremd zu A_1 ist, und demnach ergiebt sich durch zweimalige Anwendung des Satzes II.

$$(AA_1, BA_1) = (A, B),$$
$$(BA_1, BB_1) = (A_1, B_1)$$

und daraus nach I die zu beweisende Formel.

IV. *Ist A' ein Theiler von A von der Art, dass*

$$A = A'B, \tag{8}$$

so ist, wenn B' der Durchschnitt von A' und B ist

$$(A, B) = (A', B').$$

Die Voraussetzung (8) besagt nämlich, dass in jeder Nebengruppe αB ein Element aus A' vorkommt, dass also, wenn αB eine beliebige Nebengruppe zu B in A ist, man immer eine α' in A' finden kann, so dass $\alpha B = \alpha' B$ wird. Sind dann $\alpha_1' B$, $\alpha_2' B$ verschiedene Nebengruppen zu B in A, so sind $\alpha_1' B'$, $\alpha_2' B'$ verschiedene Nebengruppen zu B' in A' und umgekehrt. Daraus ergiebt sich unmittelbar unsere Formel. Wir sprechen noch den folgenden, hieraus fliessenden Satz aus:

V. *Reducirt man G auf einen Theiler G' und sind A', B' die Durchschnitte von G' mit A und B, so ist unter der Voraussetzung, dass $A = A'B$ ist, d. h. dass in jeder Nebengruppe αB ein Element aus G' vorkommt,*

$$(A, B) = (A', B').$$

Ist $j = (A, B)$ von Null verschieden, so ist in der Gruppe $A|B$ die Gruppe B selbst das Einheitselement. Nach einem bekannten Satze der Gruppentheorie ist daher die j^{te} Potenz einer jeden Nebengruppe αB mit B selbst identisch. Wir formuliren dies als sechsten Satz:

VI. *Ist der Index j von B in Bezug auf A von Null verschieden, so ist die j^{te} Potenz eines jeden Elementes α von A in B enthalten.*

Wir machen noch den

Zusatz. *Wenn α^k die niedrigste Potenz von α mit positiven Exponenten ist, die in B enthalten ist, so ist k ein Theiler von j.*

§ 2.

Potenzgruppen.

Ein Element der Gruppe G, von dem eine Potenz mit endlichem Exponenten $=1$ wird, können wir eine *Einheitswurzel* (in G) nennen. Nehmen wir nun ein Element α_1 in G, welches keine Einheitswurzel ist, so bilden die Potenzen $\alpha_1^{x_1}$, wenn x_1 alle positiven und negativen ganzen Zahlen durchläuft, eine unendliche Abel'sche Gruppe A_1. Wir nehmen nun, wenn es möglich ist, ein zweites Element α_2 von der Art, dass $\alpha_2^{x_2}$ *nur* für $x_2 = 0$ in A_1 enthalten ist, und erhalten in der Gesammtheit der Elemente $\alpha_1^{x_1}\alpha_2^{x_2}$ eine neue Gruppe A_2. So fahren wir fort und bilden eine Gruppe A_m indem wir in

$$\alpha = \alpha_1^{x_1}\alpha_2^{x_2}\ldots\alpha_m^{x_m} \tag{1}$$

die Exponenten $x_1, x_2, \ldots, x_m$ alle ganzzahligen Werthe durchlaufen lassen. Es ist hierbei für jedes m vorausgesetzt, dass α nur dann in A_{m-1} enthalten ist, wenn $x_m = 0$ ist. Daraus folgt, dass zwei Elemente α mit verschiedenen Exponenten x niemals einander gleich sein können, und dass in allen Gruppen A_m keine Einheitswurzel ausser 1 vorkommt.

Die Gruppe A_m möge eine *Potenzgruppe* heissen.

Das System

$$\alpha_1, \alpha_2, \ldots, \alpha_m \tag{2}$$

heisst eine *Basis der Gruppe* A_m. Wenn nun

$$\beta_1, \beta_2, \ldots, \beta_n$$

gleichfalls eine Basis von A_m ist, so können wir ohne Beschränkung der Allgemeinheit $n \gtrless m$ annehmen, und da die β selbst der Gruppe A_m angehören, so lassen sich die Exponenten $a_{r,s}$ so bestimmen, dass

$$\beta_s = \alpha_1^{a_{1,s}}\alpha_2^{a_{2,s}}\ldots\alpha_m^{a_{m,s}}$$

wird, und dann ist, wenn $y_1, y_2, \ldots, y_n$ die Exponenten des Elementes α für die neue Basis bedeuten

$$x_r = a_{r,1}y_1 + \cdots + a_{r,n}y_n. \tag{3}$$

Nach dem Begriff der Basis müssen, wenn die $x_r = 0$ gesetzt werden auch die y_s sämmtlich verschwinden. Es muss also $n \lesseqgtr m$, und

folglich nach unserer Voraussetzung $n = m$ sein. Ausserdem muss die Determinante

$$|a_{r,s}| = \Sigma \pm a_{11} a_{22} \ldots a_{nn}$$

von Null verschieden sein. Da sich aber für ganzzahlige Werthe von x_r aus (3) immer ganzzahlige y_s ergeben müssen, so muss nach einen bekannten Determinantensatze

$$|a_{r,s}| = \pm 1$$

sein.

Die Zahl m ist also für die Potenzgruppe A_m invariant und soll der *Rang der Potenzgruppe* genannt werden.

Wir beweisen folgenden Satz:

VII. *Jeder Theiler B der Potenzgruppe A_m ist selbst Potenzgruppe von nicht höherem Rang als m. Sind die Durchschnitte*

(4) $$B_m,\ B_{m-1},\ B_{m-2}, \ldots 1$$

von B mit A_m, A_{m-1}, $A_{m-2}, \ldots 1$ alle von einander verschieden, so ist der Rang von B gleich m, und der Index (A_m, B_m) ist von Null verschieden.

Um diesen Satz zunächst für $m = 1$ zu beweisen, bezeichnen wir mit (α) die aus allen Potenzen irgend eines Elementes α bestehende Potenzgruppe ersten Ranges. Ist nun B ein von 1 verschiedener Theiler von (α), so giebt es eine gewisse kleinste positive Zahl b für die

$$\beta = \alpha^b$$

in B enthalten ist und dann ist B die Potenzgruppe (β). Zugleich ist

$$(\alpha) = (\beta) + \alpha(\beta) + \cdots + \alpha^{b-1}(\beta)$$

also der Index

(5) $$\big((\alpha), (\beta)\big) = b.$$

Nun können wir den allgemeinen Beweis unseres Satzes durch vollständige Induction führen.

Ist B ein Theiler von A_m, so können wir m so klein annehmen, dass $B = B_m$ nicht zugleich Theiler von A_{m-1} ist.

Es giebt dann eine gewisse kleinste positive Zahl b_m von der Beschaffenheit, dass $\alpha_m^{b_m}$ in der Gruppe $B_m A_{m-1}$ enthalten ist, und jeder andere Exponent x, für den α_m^x in dieser Gruppe enthalten ist, ist ein Vielfaches von b_m.

Setzen wir also

$$\alpha_m^{b_m} = \beta_m,$$

und bezeichnen mit β irgend ein Element aus B_m, so giebt es einen Exponenten y, so dass $\beta \beta_m^{-y}$ in A_{m-1} und folglich auch in B_{m-1} enthalten ist. Daraus folgt

(6) $$B_m = (\beta_m) B_{m-1}.$$

Da nun β_m^y nur für $y = 0$ in B_{m-1} enthalten ist, so folgt, wenn B_{m-1} bereits als Potenzgruppe nachgewiesen ist, dass auch B_m eine Potenzgruppe von einem an 1. höheren Rang als B_{m-1} ist.

Unter der in VII gemachten Voraussetzung ist B_{m-2} von B_{m-1} verschieden, und folglich B_{m-1} nicht in A_{m-2} enthalten. Wir nehmen demgemäss als bereits erwiesen an, dass (A_{m-1}, B_{m-1}) von Null verschieden ist.

Nun ist

$$A_m = (\alpha_m) A_{m-1} \tag{7}$$

und da (α_m) theilerfremd zu A_{m-1} ist, so ergiebt sich nach dem Satze III aus (6) und (7)

$$(A_m, B_m) = (A_{m-1}, B_{m-1}) \left((\alpha_m), (\beta_m)\right)$$

und folglich nach (5)

$$(A_m, B_m) = b_m (A_{m-1}, B_{m-1}), \tag{8}$$

wodurch das Theorem VII bewiesen ist.

Ueber die Bestimmung des Index können wir noch hinzufügen: Sind

$$b_m, b_{m-1}, \ldots, b_1$$

die kleinsten positiven Zahlen, für die die Potenzen

$$\alpha_m^{b_m}, \alpha_{m-1}^{b_{m-1}}, \ldots, \alpha_1^{b_1}$$

in

$$B_m A_{m-1}, B_{m-1} A_{m-2}, \ldots, B_1$$

enthalten sind, so ist

$$(A_m, B_m) = b_1 b_2 \ldots b_m. \tag{9}$$

§ 3.

Zahlengruppen und Idealgruppen in einem algebraischen Körper.

Die sämmtlichen Zahlen eines algebraischen Körpers Ω, mit Ausschluss der Null, bilden, wenn die wirkliche Multiplication und Division als Regel der Zusammensetzung gilt, eine Gruppe Ω_0 von der in § 1 betrachteten Art, die wir jetzt eine *Zahlengruppe* nennen wollen. Jede Zahlengruppe enthält die Zahl 1. Eine solche Zahlengruppe ist auch das System der in Ω enthaltenen Einheiten und diese Gruppe soll durchweg mit E bezeichnet werden.

Eine Gruppe wird auch noch gebildet von den sämmtlichen Einheitsfunctionalen*) des Körpers Ω, und diese Gruppe bezeichne ich mit $\overline{E}$. Ist dann φ irgend ein ganzes oder gebrochenes Functional in Körper Ω, so ist

$$\varphi \overline{E} = \mathfrak{a} \tag{1}$$

*) Algebra, Bd. II, § 138.

ein *Ideal* in Ω, und dies Ideal ändert sich nicht, wenn φ durch ein associirtes Functional ersetzt wird. Wir sagen, das Ideal $\mathfrak{a}$ wird durch das Functional φ *erzeugt*. Ist φ eine *Zahl*, so ist $\mathfrak{a}$ ein Hauptideal.

Die Ideale des Körpers Ω bilden eine Gruppe, wobei die Multiplication und Division der Ideale als Compositionsgesetz gilt. Eine solche Gruppe soll eine *Idealgruppe* heissen. Die aus allen Idealen von Ω gebildete Gruppe bezeichne ich mit $\overline{\Omega}_0$. Die *Hauptideale* in $\overline{\Omega}$ bilden gleichfalls eine Idealgruppe, die mit $\overline{E}\Omega_0$ zu bezeichnen ist. Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ sind nach $\overline{E}\Omega_0$ äquivalent, wenn der Quotient $\mathfrak{a} : \mathfrak{b}$ ein Hauptideal ist, oder, was dasselbe ist, wenn der Quotient der sie erzeugenden Functionale φ, ψ mit einer Zahl associirt ist. Die Nebengruppen zu $\overline{E}\Omega_0$ in $\overline{\Omega}_0$ sind die *Idealclassen*. Da nach einem Fundamentalsatz der Idealtheorie die Anzahl dieser Classen endlich ist, so ist der Index

$$h = (\overline{\Omega}_0, \overline{E}\Omega_0) \tag{2}$$

immer von Null verschieden. Er heisst die *Classenzahl des Körpers* Ω.

Man kann die Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ in Ω so auswählen, dass

$$\overline{\Omega}_0 = \mathfrak{a}_1\Omega_0 + \mathfrak{a}_2\Omega_0 + \cdots + \mathfrak{a}_h\Omega_0 \tag{3}$$

wird.

Ist $\overline{O}$ eine in $\overline{\Omega}_0$ enthaltene Idealgruppe und O der Inbegriff der Zahlen ω, deren Hauptideale $\overline{E}\omega$ in $\overline{O}$ enthalten sind, so ist $\overline{E}O$ die Gruppe der in $\overline{O}$ enthaltenen Hauptideale, und O ist eine in Ω_0 enthaltene Zahlengruppe. Wenn nun noch die Bedingung

$$\overline{\Omega}_0 = \overline{O}\Omega_0 \tag{4}$$

erfüllt ist, so ist nach dem Satze § 1, V

$$h = (\overline{\Omega}_0, \overline{E}\Omega_0) = (\overline{O}, \overline{E}O). \tag{5}$$

Die Bedingung (4) besagt, dass in jeder Idealclasse (3) ein Element aus $\overline{O}$ vorkommen muss, und diese Bedingung ist nach einem bekannten Satze der Idealtheorie z. B. dann erfüllt, wenn $\overline{O}$ die Gesammtheit der Ideale in $\overline{O}$ und folglich O die Gesammtheit der Zahlen in Ω bedeutet, *die zu einem gegebenen Ideal* $\mathfrak{a}$ *relativ prim sind**).

Ist O' ein Theiler der Zahlengruppe O, so ist $\overline{E}O'$ Theiler von $\overline{E}O$. Ist $\mathfrak{a}$ irgend ein Ideal in $\overline{O}$, so nennen wir das System $\mathfrak{a}O'$ eine *Idealclasse nach* O', und es ist eine wichtige Aufgabe, die Classenzahl nach O', d. h. die Zahl

*) Unter Zahlen oder Idealen, die zu einem gegebenen Ideal $\mathfrak{a}$ relativ prim sind, verstehe ich solche Zahlen oder Ideale, die, bei ihrer einfachsten Darstellung durch Idealbrüche, weder im Zähler, noch im Nenner mit $\mathfrak{a}$ einen gemeinschaftlichen Theiler haben.

(6) $$h' = (\bar{O}, \bar{E}O')$$

zu bestimmen. Diese Aufgabe lässt sich, wenn h bekannt ist, durch folgende Betrachtungen auf eine einfachere, nämlich auf die Bestimmung von Indices in Zahlengruppen zurückführen.

Nach § 1, I ist

(7) $$(\bar{O}, \bar{E}O') = (\bar{O}, \bar{E}O)\,(\bar{E}O, \bar{E}O')$$

und nach § 1, II

(8) $$(\bar{E}O, \bar{E}O') = (\bar{E}O, \bar{E}\bar{E}O') = (O, EO').$$

Ist nun ferner E' der Durchschnitt von E mit O', d. h. die Gruppe der in O' enthaltenen Einheiten, so ist nach § 1, I

(9) $$(O, EO')\,(EO', O') = (O, O')$$

und nach § 1, II

(10) $$(EO', O') = (EO', E'O') = (E, E').$$

Also nach (8), (9), (10)

$$(\bar{E}O, \bar{E}O')\,(E, E') = (O, O')$$

und nach (7)

$$(E, E')\,(\bar{O}, \bar{E}O') = (O, O')\,(\bar{O}, \bar{E}O)$$

oder endlich

(11) $$(E, E')\,h' = (O, O')\,h.$$

Wenn also (O, O') von Null verschieden ist, so ist auch (E, E') von Null verschieden, und es folgt

(12) $$(\bar{O}, \bar{E}O') = \frac{(O, O')}{(E, E')}\,(\bar{O}, \bar{E}O).$$

§ 4.

Normalordnungen.

Es sei jetzt Ω ein beliebiger algebraischer Zahlkörper, R der Körper der *rationalen Zahlen*, $\mathfrak{o}$ das System der *ganzen Zahlen* in Ω, $\mathfrak{r}$ das System der ganzen Zahlen in R.

1. *Wir nehmen irgend ein ganzes Ideal* $\mathfrak{k}$ *in* Ω *an und betrachten das System* $\mathfrak{o}'$ *aller Zahlen in* $\mathfrak{o}$, *die nach dem Modul* $\mathfrak{k}$ *mit einer rationalen Zahl congruent sind und nennen* $\mathfrak{o}'$ *durch das Ideal* $\mathfrak{k}$ *erzeugt.*

Das Zahlensystem $\mathfrak{o}'$ ist ein Specialfall der Zahlensysteme, die von Dedekind *Ordnungen**) genannt werden.

---

*) Vorlesungen über Zahlentheorie, 4. Auflage, § 170. „Ueber die Anzahl der Idealclassen in den verschiedenen Ordnungen eines endlichen Körpers", Festschrift zur Säcularfeier von Gauss Geburtstag (1877). „Ueber die Discriminanten endlicher Körper", Abhandlgn. der Ges. d. Wiss. zu Göttingen 1882.

2. *Es kann vorkommen, dass durch zwei verschiedene Moduln* $\mathfrak{k}$, $\mathfrak{k}'$ *dasselbe System* $\mathfrak{o}'$ *erzeugt wird. Wenn dies eintritt, so erzeugt auch der grösste gemeinschaftliche Theiler* $\mathfrak{k}_0$ *von* $\mathfrak{k}$ *und* $\mathfrak{k}'$ *dasselbe System* $\mathfrak{o}'$.

Um dies nachzuweisen, bezeichnen wir für den Augenblick mit $\mathfrak{o}_0$ die durch $\mathfrak{k}_0$ erzeugte Ordnung $\mathfrak{o}'$, so dass zu zeigen ist, dass jede Zahl ω' aus $\mathfrak{o}'$ in $\mathfrak{o}_0$ vorkommt, und dass auch umgekehrt jede Zahl ω_0 aus $\mathfrak{o}_0$ in $\mathfrak{o}'$ enthalten ist.

Bezeichnen wir mit r, r', r_0 ganze rationale Zahlen, so sind die Zahlen ω' durch die Congruenzen

$$\omega' \equiv r \pmod{\mathfrak{k}}, \qquad \omega' \equiv r' \pmod{\mathfrak{k}'}$$

charakterisirt, und es muss also $r \equiv r' \equiv r_0 \pmod{\mathfrak{k}_0}$ sein. Es ist also auch

$$\omega' \equiv r_0 \pmod{\mathfrak{k}_0},$$

also ω' in $\mathfrak{o}_0$ enthalten.

Um auch das Umgekehrte nachzuweisen, sei ω_0 eine beliebige Zahl in $\mathfrak{o}_0$. Dann können wir, wenn mit μ irgend eine durch $\mathfrak{k}_0$ theilbare Zahl aus $\mathfrak{o}$ und mit r eine rationale Zahl bezeichnet wird

$$\omega_0 = r + \mu \tag{1}$$

setzen. Wir nehmen nun eine durch $\mathfrak{k}$ theilbare Zahl α und eine durch $\mathfrak{k}'$ theilbare Zahl α' in $\mathfrak{o}$ so an, dass $\mathfrak{k}_0$ der grösste gemeinschaftliche Theiler von α und α' ist, was nach einem bekannten Satze der Idealtheorie immer möglich ist; dann lassen sich, wie gleichfalls aus der Theorie der algebraischen Zahlen bekannt ist, die Zahlen ξ, ξ' in $\mathfrak{o}$ so bestimmen, dass

$$\mu = \alpha\xi + \alpha'\xi' \tag{2}$$

wird*), und daraus folgt dann nach (1)

$$\omega_0 \equiv r + \alpha\xi \pmod{\mathfrak{k}'}. \tag{3}$$

Nun ist $r + \alpha\xi \equiv r \pmod{\mathfrak{k}}$ und daher in $\mathfrak{o}'$ enthalten. Demnach ist nach unserer Voraussetzung $r + \alpha\xi \equiv r' \pmod{\mathfrak{k}'}$ und folglich nach (1) und (3)

$$\omega_0 \equiv r' \pmod{\mathfrak{k}'}$$

also ω_0 in $\mathfrak{o}'$ enthalten, wie bewiesen werden sollte. Daraus schliessen wir:

3. *Unter allen Moduln* $\mathfrak{k}$, *die dieselbe Ordnung* $\mathfrak{o}'$ *erzeugen, giebt es einen bestimmten von kleinster Norm; dieser wird der Führer der Ordnung genannt.*

Die Zahlen von $\mathfrak{o}$ bilden, wenn die *Addition* als Compositionsgesetz und die Null als Gruppeneinheit gilt, eine *Abel'sche Gruppe*. Die Zahlen $\mathfrak{o}$ zerfallen nach dem Modul $\mathfrak{k}$ in Classen, deren Anzahl

*) Lehrbuch der Algebra Bd. II, Seite 524, 3. Seite 543, 4.

gleich der Norm $N(\mathfrak{k})$ von $\mathfrak{k}$ ist, und wenn wir daher unter $\mathfrak{k}$ zugleich den Inbegriff aller durch $\mathfrak{k}$ theilbaren Zahlen in $\mathfrak{o}$ verstehen*), so ist

$$(\mathfrak{o}, \mathfrak{k}) = N(\mathfrak{k}). \tag{4}$$

Andererseits ist nach der Definition 1.

$$(\mathfrak{o}', \mathfrak{k}) = (\mathfrak{r}, \mathfrak{k}) = Q, \tag{5}$$

wenn Q die kleinste durch $\mathfrak{k}$ theilbare *natürliche Zahl* ist, und folglich ist nach § 1, I.

$$(\mathfrak{o}, \mathfrak{o}') = \frac{(\mathfrak{o}, \mathfrak{k})}{(\mathfrak{o}', \mathfrak{k})} = \frac{N(\mathfrak{k})}{Q}. \tag{6}$$

Diese Formel gilt, mag nun $\mathfrak{k}$ der Führer von $\mathfrak{o}'$ selbst sein, oder ein anderes die Ordnung $\mathfrak{o}'$ erzeugendes Ideal. Sie lässt sich aber verwenden, um den Führer einer Ordnung zu ermitteln. Wenn nämlich $\mathfrak{k}$ und $\mathfrak{k}_0$ dieselbe Ordnung $\mathfrak{o}'$ erzeugen, so wird $\mathfrak{o}'$ auch von jedem Theiler $\mathfrak{k}'$ von $\mathfrak{k}$, der durch $\mathfrak{k}_0$ theilbar ist, erzeugt. Denn die durch $\mathfrak{k}'$ erzeugte Ordnung ist, da $\mathfrak{k}'$ Theiler von $\mathfrak{k}$ ist, in $\mathfrak{o}'$ enthalten, und enthält $\mathfrak{o}'$, da $\mathfrak{k}_0$ Theiler von $\mathfrak{k}'$ ist.

Verstehen wir nun unter $\mathfrak{p}$ ein in $\mathfrak{k}$ aufgehendes Primideal und unter p die durch $\mathfrak{p}$ theilbare natürliche Primzahl und setzen $\mathfrak{k} = \mathfrak{p}\mathfrak{k}'$, so wird nur dann $\mathfrak{k}$ und $\mathfrak{k}'$ dieselbe Ordnung $\mathfrak{o}'$ erzeugen, wenn

$$\frac{N(\mathfrak{k})}{Q} = \frac{N(\mathfrak{k}')}{Q'}, \tag{7}$$

wenn Q' die kleinste durch $\mathfrak{k}'$ theilbare natürliche Zahl, also

$$Q = Q' \quad \text{oder} \quad Q = pQ';$$

nun ist $N(\mathfrak{k}) = N(\mathfrak{p})\, N(\mathfrak{k}')$, und wenn $\mathfrak{p}$ vom Grade f ist,

$$N(\mathfrak{p}) = p^f.$$

Also ergiebt sich aus (7)

$$Q = p^f Q',$$

und das ist nur dann möglich, wenn $f = 1$ und $Q = pQ'$ ist. Wir können das Resultat in folgendem Satze zusammenfassen:

> 4. *Das Ideal $\mathfrak{k}$ ist dann und nur dann der Führer der durch $\mathfrak{k}$ erzeugten Ordnung, wenn für jedes in $\mathfrak{k}$ aufgehendes Primideal ersten Grades die durch $\mathfrak{k} : \mathfrak{p}$ theilbare kleinste natürliche Zahl auch durch $\mathfrak{k}$ theilbar ist.*

Ist diese Bedingung nicht erfüllt, so erhält man den Führer der durch $\mathfrak{k}$ erzeugten Ordnung, wenn man, eins nach dem andern, die Primideale ersten Grades weglässt, die der Forderung des Satzes 3. nicht entsprechen**).

Wir wollen jetzt unter $\mathfrak{k}$ den *Führer* der Ordnung $\mathfrak{o}'$ selbst verstehen und noch folgenden Satz beweisen:

---

*) Dies ist nach Dedekind's Definition das Ideal $\mathfrak{k}$.

**) Dedekind, Discriminanten endlicher Körper Seite 28, Anmerkung.

5. *Ist* $\mathfrak{a}$ *ein zu* $\mathfrak{k}$ *theilerfremdes ganzes Ideal des Körpers* Ω, *so existirt in* $\mathfrak{o}'$ *eine durch* $\mathfrak{a}$ *theilbare Zahl* $\omega' = \mathfrak{a}\mathfrak{m}$ *von der Art, dass das Ideal* $\mathfrak{m}$ *relativ prim ist zu einem beliebig gegebenen Ideal* $\mathfrak{b}$ *in* Ω*).

Zum Beweise nehme man eine durch $\mathfrak{a}$ theilbare Zahl

$$\mu = \mathfrak{a}\mathfrak{n} \tag{4}$$

so in $\mathfrak{o}$ an, dass $\mathfrak{n}$ relativ prim zu $\mathfrak{k}$ und zu $\mathfrak{b}$ wird, und ferner eine durch $\mathfrak{k}$ theilbare Zahl α relativ prim zu μ. Dann kann man die Zahl ξ aus $\mathfrak{o}$ durch die Congruenz

$$1 + \xi\alpha \equiv 0 \pmod{\mu}$$

bestimmen**) und daher

$$1 + \xi\alpha = \mu\beta$$

setzen, worin β eine zu α theilerfremde Zahl in $\mathfrak{o}$ ist. Nehmen wir jetzt

$$\omega' = 1 + \xi\alpha + \alpha\mu\eta = \mu(\beta + \alpha\eta), \tag{5}$$

so genügt diese Zahl der Forderung unseres Satzes 3., wenn wir η in $\mathfrak{o}$ so bestimmen, dass jeder Primtheiler von $\mathfrak{b}$ in einer und nur in einer der beiden Zahlen β und η aufgeht. Denn dann ist nach der ersten Darstellung (5) $\omega' \equiv 1 \pmod{\mathfrak{k}}$, also in $\mathfrak{o}'$ enthalten; es ist ferner wegen (4) ω' durch $\mathfrak{a}$ theilbar, und

$$\mathfrak{m} = \mathfrak{n}(\beta + \alpha\eta)$$

ist relativ prim zu $\mathfrak{b}$.

6. *Ist* $\mathfrak{a}$ *ein zu* $\mathfrak{k}$ *theilerfremdes ganzes Ideal, und* α *eine beliebige Zahl in* $\mathfrak{o}$, *so kann man die Congruenz*

$$\omega \equiv \alpha \pmod{\mathfrak{a}}$$

durch eine Zahl ω *in* $\mathfrak{o}'$ *befriedigen.*

Man nehme nämlich eine durch $\mathfrak{a}$ theilbare, zu $\mathfrak{k}$ theilerfremde Zahl μ in $\mathfrak{o}$ beliebig an und bestimme ξ aus der Congruenz

$$\omega = \alpha + \mu\xi \equiv 1 \pmod{\mathfrak{k}},$$

dann erfüllt ω die gestellte Forderung.

Die Ordnungen $\mathfrak{o}'$ geben nun Anlass zu Zahlengruppen im Sinne von § 3. Es sei $\mathfrak{o}'$ eine solche Ordnung und $\mathfrak{k}$ ihr Führer. Wir entfernen zunächst aus $\mathfrak{o}$ alle Zahlen, die zu $\mathfrak{k}$ nicht relativ prim sind, und nehmen auch noch die Quotienten aller in $\mathfrak{o}$ übrig bleibenden Zahlen. Der Inbegriff der so entstandenen Zahlen ist nach der Definition von § 3 eine Zahlengruppe, die wir mit O bezeichnen. Ebenso verfahren wir mit $\mathfrak{o}'$, indem wir aus $\mathfrak{o}'$ alle Zahlen, die mit $\mathfrak{k}$ einen gemeinsamen Theiler haben, ausschliessen, und die Quotienten je

*) Dieser Satz ist eine Verallgemeinerung des oben angewandten Satzes (Algebra Bd. II, Seite 524, 3). Vgl. Dedekind, Gauss Festschrift Seite 28.

**) Algebra II, § 149, 1.

zweier der übrigen Zahlen nehmen. Das so entstandene System O' ist gleichfalls eine Gruppe und zwar ein Theiler von O.

O umfasst alle Zahlen ω des Körpers Ω die zu $\mathfrak{k}$ fremd sind in dem Sinne, dass in der einfachsten Darstellung von ω durch einen Idealbruch sowohl Zähler als Nenner relativ prim zu $\mathfrak{k}$ sind. Um den Index (O, O') zu ermitteln, betrachten wir noch die durch die symbolische Congruenz

$$O_0 \equiv 1 \pmod{\mathfrak{k}}$$

definirte Gruppe, die aus allen nach dem Modul $\mathfrak{k}$ mit 1 congruenten Zahlen ω besteht, und die, da ω mit rationalem zu $\mathfrak{k}$ theilerfremden Nenner dargestellt werden kann, in O' enthalten ist.

Bezeichnen wir nun mit $\psi(\mathfrak{k})$ und $\varphi(\mathfrak{k})$ die Anzahl der Zahlclassen nach dem Modul $\mathfrak{k}$, die in O und in O' enthalten sind, so ist, wenn Q wie oben die kleinste durch $\mathfrak{k}$ theilbare natürliche Zahl, und r die in Q aufgehenden natürlichen Primzahlen bedeuten,

$$\varphi(\mathfrak{k}) = \varphi(Q) = Q\prod\left(1 - \frac{1}{r}\right),$$

(6)
$$\psi(\mathfrak{k}) = N(\mathfrak{k})\prod\left(1 - \frac{1}{N(\mathfrak{p})}\right),^{*})$$

und es ergiebt sich

$$(O, O_0) = \psi(\mathfrak{k}), \quad (O', O_0) = \varphi(\mathfrak{k}),$$

und folglich

$$(O, O') = \frac{\psi(\mathfrak{k})}{\varphi(\mathfrak{k})}. \tag{7}$$

Daraus, dass (O', O_0) einen endlichen Werth hat, lässt sich leicht beweisen, dass jede *ganze Zahl* in O' in der Ordnung $\mathfrak{o}'$ enthalten ist, oder mit anderen Worten, dass, wenn eine Zahl in $\mathfrak{o}'$ durch eine andere theilbar ist, auch der Quotient in $\mathfrak{o}'$ enthalten sein muss.

Jede Zahl ω in O' lässt sich nach der Definition so darstellen:

$$\omega = \frac{\alpha}{\beta}$$

worin α, β zu $\mathfrak{k}$ theilerfremde Zahlen in $\mathfrak{o}'$ sind. Weil nun (O', O_0) endlich ist, so ist eine gewisse Potenz von β mit positivem Exponenten, β^m, in O_0 enthalten, also $\beta^m \equiv 1 \pmod{\mathfrak{k}}$. Hiernach wird

$$\omega = \frac{\alpha\beta^{m-1}}{\beta^m} \equiv \alpha\beta^{m-1} \pmod{\mathfrak{k}},$$

also ist ω nach dem Modul $\mathfrak{k}$ mit einer rationalen Zahl congruent, d. h. in $\mathfrak{o}'$ enthalten.

Auf die gleiche Weise lässt sich der folgende besonders hervorzuhebende Satz beweisen:

7. *Die Gruppe O' ist der Inbegriff aller zu $\mathfrak{k}$ theilerfremden, ganzen oder gebrochenen, Zahlen in Ω, die nach dem Modul k mit einer rationalen Zahl congruent sind.*

*) Dedekind, Vorlesungen über Zahlentheorie 4. Aufl., Seite 569.

Denn ist

$$\omega = \frac{\alpha}{\beta} \equiv r \pmod{\mathfrak{k}}$$

theilerfremd zu $\mathfrak{k}$, so kann man die ganzen Zahlen α, β selbst relativ prim zu $\mathfrak{k}$ annehmen. Dann muss eine gewisse Potenz β^m von β in $\mathfrak{o}'$ enthalten, also mit einer rationalen Zahl congruent sein, und es ist dann auch

$$\alpha\beta^{m-1} \equiv \beta^m r \equiv r', \pmod{\mathfrak{k}}.$$

Demnach ist $\omega = \alpha\beta^{m-1} : \beta^m$ als Quotient zweier Zahlen in $\mathfrak{o}'$ in O' enthalten.

Um nach der Formel § 3 (12) die Anzahl der Idealclassen $(\bar{O}, \bar{E}O')$ zu bestimmen, ist es noch nöthig, den Index (E, E') zu ermitteln. Diesen erhält man aber aus den Sätzen des § 2.

Das System E besteht nach dem Satze von Dirichlet aus den in Ω enthaltenen Einheitswurzeln, die durch die Potenzen von einer von ihnen

$$1, \varrho, \varrho^2, \ldots, \varrho^{w-1} \tag{8}$$

erschöpft werden können, und aus einer Potenzgruppe $E_{\nu-1}$ vom Range $\nu - 1$, wenn ν die Anzahl der reellen Körper, vermehrt um die Anzahl der imaginären Paare unter den mit Ω conjugirten Körpern bedeutet. Ein Element von $E_{\nu-1}$ möge in der Form dargestellt sein

$$\varepsilon = \varepsilon_1^{\lambda_1} \varepsilon_2^{\lambda_2} \ldots \varepsilon_{\nu-1}^{\lambda_{\nu-1}}. \tag{9}$$

Daneben betrachten wir noch die Potenzgruppen E_s mit der Basis

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s.$$

Wegen der Endlichkeit von (O, O') giebt es zu jeder Zahl ε in O einen positiven Exponenten λ, so dass ε^λ in O' enthalten ist, und daraus ergiebt sich, dass die Durchschnitte

$$E'_{\nu-1}, E'_{\nu-2} \ldots E'_1$$

von E' mit

$$E_{\nu-1}, E_{\nu-2} \ldots E_1$$

alle von einander verschieden sind. (Denn es giebt immer Zahlen in E_s, die zwar in O', also auch in E', aber nicht in E_{s-1} enthalten sind.)

Bezeichnen wir also mit λ_s den kleinsten positiven Exponenten für den $\varepsilon_s^{\lambda_s}$ in $O'E_{s-1}$ enthalten ist, ferner mit λ_0 den kleinsten positiven Exponenten, für den ϱ^{λ_0} in O' vorkommt, so ergiebt sich nach § 1 und § 2:

$$(E, E') = \lambda_0 \lambda_1 \lambda_2 \ldots \lambda_{\nu-1} \text{ *)}. \tag{10}$$

*) Nach der von Dedekind in § 4 der Gauss-Festschrift gegebenen Definition ist der Inbegriff aller Zahlen in $\mathfrak{o}'$, die durch irgend ein zu $\mathfrak{k}$ theilerfremdes Functional φ theilbar sind, ein „*Ideal in* $\mathfrak{o}'$“. Ich will es hier das durch φ er-

Wir wollen jetzt annehmen, es sei Ω ein *Normalkörper*. Wir bezeichnen seine Galois'sche Gruppe mit Φ und die Substitutionen dieser Gruppe mit φ und wir bedienen uns überhaupt hier der Bezeichnung wie in Bd. II, § 160 der Algebra, so dass $\omega \mid \varphi$ die Zahl bedeutet, die durch die Substitution φ aus der Zahl ω hervorgeht. Es sei $\mathfrak{o}'$ ferner eine der durch 1. definirten Ordnungen. Von dieser Ordnung wollen wir aber ausserdem voraussetzen, dass die Gesammtheit ihrer Zahlen durch die Substitutionen von Φ ungeändert bleibt, oder dass

$$\mathfrak{o}' \mid \varphi = \mathfrak{o}' \tag{11}$$

sei. Eine solche Ordnung können wir eine *Normalordnung* in Ω nennen. Wenn eine Normalordnung durch den Modul $\mathfrak{k}$ erzeugt wird, so wird durch $\mathfrak{k} \mid \varphi$ dieselbe Ordnung erzeugt, und nach 2. wird dann dieselbe Ordnung durch den grössten gemeinschaftlichen Theiler aller $\mathfrak{k} \mid \varphi$ erzeugt. Der Führer einer Normalordnung muss also ein *Normalideal* sein, wenn wir unter *Normalideal ein solches verstehen, was mit allen seinen conjugirten identisch ist*, was also der Bedingung

$$\mathfrak{k} \mid \varphi = \mathfrak{k} \tag{12}$$

genügt.

Umgekehrt erzeugt jedes Normalideal eine Normalordnung und um den Führer einer solchen Ordnung zu ermitteln, haben wir den Satz 4. anzuwenden. Ist n der Grad des Körpers Ω und $\mathfrak{p}$ ein Primfactor ersten Grades der natürlichen Primzahl p, sind ferner $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_e$ die mit $\mathfrak{p}$ conjugirten Primideale (einschliesslich $\mathfrak{p}$), so ist

$$p = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_e)^g, \qquad n = eg\ ^*). \tag{13}$$

Ist nun $\mathfrak{k} = \mathfrak{p}\mathfrak{k}'$, so ist $\mathfrak{k}$ als Normalideal auch durch $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_e$ theilbar, und die kleinste durch $\mathfrak{k}'$ theilbare natürliche Zahl Q' ist

---

zeugte Ideal in $\mathfrak{o}'$ nennen. Werden die Ideale $\mathfrak{a}'$, $\mathfrak{b}'$ in $\mathfrak{o}'$ durch die Functionale φ und ψ erzeugt, so wird $\mathfrak{a}\mathfrak{b}$ durch $\varphi\psi$ erzeugt.

Zwei Ideale $\mathfrak{a}'$, $\mathfrak{b}'$ in $\mathfrak{o}'$ heissen *äquivalent*, wenn es eine *Zahl* μ giebt, so dass im Sinne von Dedekind

$$\mathfrak{a}'\mu = \mathfrak{b}'$$

ist, d. h. so dass jedes Product von μ mit einer Zahl in $\mathfrak{a}'$ gleich einer Zahl in $\mathfrak{b}'$ ist. Die Zahl μ ist also darstellbar als Quotient zweier Zahlen in $\mathfrak{o}'$, und ist also, da sie zu $\mathfrak{k}$ theilerfremd ist, eine Zahl in O'. Sind $\mathfrak{a}'$ und $\mathfrak{b}'$ durch die Functionale φ und ψ erzeugt, so ist also $\psi : \varphi$ associirt mit μ, und φ und ψ sind daher äquivalent nach $\bar{E}O'$ (in dem in § 3 festgesetzten Sinne). Wenn umgekehrt φ und ψ nach $\bar{E}O'$ äquivalent sind, so sind auch die durch φ und ψ erzeugten Ideale $\mathfrak{a}'$, $\mathfrak{b}'$ äquivalent im Sinne von Dedekind, und daraus ergiebt sich, dass die Gruppe

$$\bar{O} \mid \bar{E}O'$$

isomorph ist mit der Gruppe der Idealclassen in $\mathfrak{o}'$.

*) Vgl. Algebra II, § 160.

daher gewiss immer dann durch $\mathfrak{k}$ theilbar, wenn $e > 1$ ist. Ist aber $e = 1$, also $g = n$, $p = \mathfrak{p}^n$, und $\mathfrak{p}^x$ die höchste in $\mathfrak{k}$ aufgehende Potenz von p, so ist Q' nur dann nicht durch $\mathfrak{k}$ theilbar, wenn $x \equiv 1 \pmod{n}$ ist, und wir erhalten also den Satz:

8. *Ist die Primzahl p die n^{te} Potenz eines Primideals $\mathfrak{p}$, so kann der Exponent der höchsten Potenz von $\mathfrak{p}$, die im Führer einer Normalordnung aufgeht, nicht congruent 1 nach dem Modul n sein.*

Oder auch:

9. *Ist $p = \mathfrak{p}^n$, und $\mathfrak{k} = p^\lambda \mathfrak{p} \mathfrak{k}'$ ein Normalideal, in dem λ eine positive ganze Zahl und $\mathfrak{k}'$ nicht mehr durch $\mathfrak{p}$ theilbar ist, so erzeugen $\mathfrak{k}$ und $p^\lambda \mathfrak{k}'$ dieselbe Normalordnung $\mathfrak{o}'$.*

Wenn in der Gruppe O' Zahlen mit negativer Norm vorkommen, so bilden die Zahlen mit positiver Norm einen Theiler O'_+ von O', dessen Index

$$(O', O'_+) = 2$$

ist. Bezeichnen wir mit E'_+ das System der in O' enthaltenen Einheiten mit positiver Norm, so ist $(E', E'_+) = 2$ oder $= 1$, je nachdem es in E' Einheiten mit negativer Norm giebt oder nicht giebt.

Wenden wir dann die Classenzahlformel § 3 (12) auf O'_+ an, so ergiebt sich

$$(\bar{O}, \bar{E} O'_+) = (\bar{O}, \bar{E} O') \quad \text{im Falle} \quad (E', E'_+) = 2$$

und

$$(\bar{O}, \bar{E} O'_+) = 2(\bar{O}, \bar{E} O') \quad \text{im Falle} \quad (E', E'_+) = 1.$$

Hierzu wollen wir noch bemerken, dass in dem Falle, wo Ω überhaupt nur Zahlen mit positiver Norm enthält, O'_+ mit O' übereinstimmt. Wenn aber in Ω auch Zahlen mit negativer Norm vorkommen, so giebt es auch in O' Zahlen mit negativer Norm; denn wenn α eine Zahl in Ω mit negativer Norm und x eine durch $\mathfrak{k}$ theilbare ganze rationale Zahl ist, so ist $1 + \alpha x$ in O' enthalten und die Zahl x lässt sich so gross annehmen, dass

$$N(1 + \alpha x) = N(\alpha)\, x^n + \cdots$$

im Vorzeichen mit $N(\alpha)$ übereinstimmt.

Dagegen kann es wohl vorkommen, dass es zwar in O, aber nicht in O' *Einheiten mit negativer Norm* giebt.

10. *In der Gruppe O'_+ giebt es eine durch ein beliebiges zu $\mathfrak{k}$ theilerfremdes Ideal $\mathfrak{a}$ theilbare ganze Zahl $\alpha = \mathfrak{a}\mathfrak{m}$, so dass das Ideal $\mathfrak{m}$ theilerfremd zu einem beliebigen Ideal $\mathfrak{b}$ ist.*

Denn nach dem Satz 5. giebt es zunächst eine solche Zahl in $\mathfrak{o}'$ und folglich auch in O'. Nun kann man aber die ganze rationale

Zahl x durch $\mathfrak{a}$ und durch $\mathfrak{b}$ theilbar und zugleich so gross annehmen, dass $N(\alpha + x)$ positiv wird, und dann genügt die Zahl $\alpha + x$ dem Satze 10.

§ 5.

Ordnungen im quadratischen Körper.

In einem quadratischen Körper Ω ist eine natürliche Primzahl entweder selbst noch Primzahl, oder sie zerfällt in zwei Primfactoren ersten Grades, und daraus ergiebt sich nach § 4, 4. und 8., dass jeder Führer einer Ordnung $\mathfrak{o}'$ eine *rationale Zahl* sein muss, und dass jede natürliche Zahl auch Führer einer Ordnung sein kann. Da ferner der quadratische Körper ein Normalkörper ist, so ist auch $\mathfrak{o}'$ eine *Normalordnung**).

Was uns hier noch interessirt, ist die Beziehung der Classen nach einer Gruppe O' (§ 3). Zu den Classen *der Irrationalzahlen zweiten Grades* (Algebra Bd. I, § 122 f.) und zu den Gauss'schen Classen der *quadratischen Formen.*

Bedeutet d eine feste positive oder negative ganze rationale Zahl *ohne quadratischen Theiler*, so haben alle Zahlen eines quadratischen Körpers Ω die Form

$$\omega = x + y\sqrt{d}, \tag{1}$$

wenn x und y *rationale Zahlen* sind. Die *ganzen Zahlen* des Körpers Ω sind immer in der Form enthalten

$$\omega = \frac{x + y\sqrt{d}}{2}, \tag{2}$$

worin x und y *ganze rationale Zahlen* sind.

Wir nehmen nun eine beliebige natürliche Zahl Q als Führer einer Ordnung $\mathfrak{o}'$ an, und suchen die Bedingung dafür, dass eine Zahl von der Form (2) mit einer rationalen Zahl nach Q congruent ist. Setzen wir

$$\omega' = \frac{x - y\sqrt{d}}{2},$$

so muss auch ω' derselben rationalen Zahl congruent sein, und folglich muss $\omega - \omega' = y\sqrt{d}$ durch Q theilbar sein. Dies ist aber, da d keinen quadratischen Theiler hat, nur dann möglich, wenn y durch Q theilbar ist. Demnach sind alle Zahlen von $\mathfrak{o}'$ in der Form

$$\omega = \frac{x + yQ\sqrt{d}}{2} \tag{3}$$

enthalten, worin x, y ganze rationale Zahlen sind. Es ist aber ausser-

*) Die Ordnungen im quadratischen Körper sind eingehend untersucht in § 187 der 4. Aufl. von Dirichlet-Dedekind, Zahlentheorie.

dem noch nöthig, dass ω selbst eine ganze Zahl sei, wofür die nothwendige und hinreichende Bedingung die ist, dass

$$\omega + \omega' = x, \qquad \omega\omega' = \frac{x^2 - y^2 Q^2 d}{4}$$

ganze rationale Zahlen sind. Hieraus ergeben sich folgende Bedingungen in drei Fällen:

$$(4)\qquad \begin{array}{ll} Q^2 d \equiv 0 \pmod 4, & x \equiv 0 \pmod 2, \\ Q^2 d \equiv 1 \pmod 4, & x \equiv y \pmod 2, \\ Q^2 d \equiv 2, 3 \pmod 4, & x \equiv y \equiv 0 \pmod 2. \end{array}$$

Diese Bedingungen sind zunächst nur nothwendig und hinreichend dafür, dass ω eine ganze Zahl sei. In den beiden letzten Fällen (4) ist Q ungerade, und es folgt $2\omega \equiv x \pmod Q$, woraus hervorgeht, dass ω auch zu $\mathfrak{o}'$ gehört. Im ersten Falle (4) aber ist Q gerade und, wenn wir daher $x = 2x_1$, $Q = 2Q_1$ setzen, so folgt nur $\omega \equiv x_1 \pmod{Q_1}$. Soll also ω zu $\mathfrak{o}'$ gehören, so muss es nach dem Modul Q mit einer rationalen Zahl von der Form $x_1 + Q_1 z$ congruent sein, d. h. es muss $y\sqrt{d}$ nach dem Modul 2 mit einer rationalen Zahl congruent sein. Ist nun $d \equiv 2, 3 \pmod 4$, so ist dies nur dann möglich, wenn y gerade ist. Ist aber $d \equiv 1 \pmod 4$, so ist $y\sqrt{d} \equiv y \pmod 2$ und y kann beliebig sein. Wir haben demnach vier Fälle zu unterscheiden, in denen wir als nothwendige und hinreichende Bedingung dafür, dass die durch (3) dargestellte Zahl ω zu $\mathfrak{o}'$ gehört, folgende erhalten:

$$(5)\qquad \begin{array}{lll} 1. & Q^2 d \equiv 0, \quad d \equiv 1 \pmod 4, & x \equiv 0 \pmod 2, \\ 2. & Q^2 d \equiv 0, \quad d \equiv 2, 3 \pmod 4, & x \equiv 0, \quad y \equiv 0 \pmod 2, \\ 3. & Q^2 d \equiv 1 \pmod 4, & x \equiv y \pmod 2, \\ 4. & Q^2 d \equiv 2, 3 \pmod 4, & x \equiv 0, \quad y \equiv 0 \pmod 2. \end{array}$$

Die Körperdiscriminante Δ ist in den Fällen 1., 3. $= d$, in den Fällen 2., 4 $= 4d$, und wenn wir daher $Q^2\Delta = D$ die *Discriminante der Ordnung* $\mathfrak{o}'$ nennen, so erhalten wir folgende Zusammenstellung:

$$(6)\qquad \begin{array}{lll} 1. & Q^2 d \equiv 0, \quad d \equiv 1 & \text{oder} \quad Q^2 d \equiv 1 \pmod 4, \\ & & D = Q^2 d, \quad \Theta = \frac{Q + \sqrt{D}}{2}, \\ 2. & Q^2 d \equiv 0, \quad d \equiv 2, 3 & \text{oder} \quad Q^2 d \equiv 2, 3 \pmod 4, \\ & & D = 4Q^2 d, \quad \Theta = \frac{1}{2}\sqrt{D}. \end{array}$$

Zur Bestimmung des Vorzeichens mag festgesetzt sein, dass $\sqrt{D}$ bei positivem D positiv, bei negativem D gleich i, multiplicirt mit einer positiven Zahl (positiv imaginär) sein soll, so dass Θ für die Ordnung $\mathfrak{o}'$ *eindeutig* bestimmt ist.

Es ist dann die hierdurch eingeführte Zahl Θ eine durch Q theilbare ganze Zahl, und es ergiebt sich:

1. *Durch*

$$\omega = x + y\Theta \tag{7}$$

werden alle und nur Zahlen der Ordnung $\mathfrak{o}'$ dargestellt, wenn x, y ganze rationale Zahlen sind. Die Zahlen 1, Θ *bilden eine Basis von $\mathfrak{o}'$.*

2. *Aus dem Ausdruck $\omega = x + y\Theta$ erhält man alle Zahlen der Gruppe O', wenn man für x, y auch gebrochene rationale Zahlen setzt, von denen x im Zähler und Nenner, y im Nenner relativ prim zu Q ist.*

Ist der Körper Ω imaginär, so ist O' zugleich die Gruppe O'_+, während bei einem reellen Körper O' noch in zwei Nebengruppen O'_+ und O'_- zerfällt.

Es sei jetzt $\mathfrak{a}$ ein beliebiges *zu Q theilerfremdes Ideal* in Ω. Wir bestimmen ein dies Ideal repräsentirendes Functional in $\mathfrak{o}'$. Zu dem Ende bezeichne ich mit

$$\alpha_1 = a_{1,1} \equiv 0 \pmod{\mathfrak{a}} \tag{8}$$

die kleinste durch $\mathfrak{a}$ theilbare natürliche Zahl, und mit $a_{2,2}$ die kleinste natürliche Zahl, für die $a_{2,2}\Theta$ mit einer rationalen Zahl $-a_{1,2}$ congruent wird, und setze

$$\alpha_2 = a_{1,2} + a_{2,2}\Theta \equiv 0 \pmod{\mathfrak{a}}. \tag{9}$$

Jede durch $\mathfrak{a}$ theilbare ganze rationale Zahl ist dann durch $a_{1,1}$ theilbar, und wenn

$$\omega = x + y\Theta \tag{10}$$

eine durch $\mathfrak{a}$ theilbare Zahl in $\mathfrak{o}'$ ist, so muss y durch $a_{2,2}$ theilbar sein. Demnach ist auch $a_{1,1}$ durch $a_{2,2}$ theilbar. Hieraus aber ergiebt sich:

3. *Jede durch $\mathfrak{a}$ theilbare Zahl α in $\mathfrak{o}'$ lässt sich in der Form*

$$\alpha = x_1\alpha_1 + x_2\alpha_2 \tag{10}$$

darstellen, worin x_1, x_2 ganze rationale Zahlen sind.

Hieraus ergiebt sich nach § 4, 5., dass $\mathfrak{a}$ der grösste gemeinschaftliche Theiler von α_1 und α_2 ist, und dass also

$$\varphi = \alpha_1 t_1 + \alpha_2 t_2$$

ein das Ideal $\mathfrak{a}$ repräsentirendes Functional ist.

4. *Wir nennen φ eine Basisform von $\mathfrak{a}$ in $\mathfrak{o}'$, und verstehen darunter also eine Linearform, aus der sich alle durch $\mathfrak{a}$ theilbaren Zahlen in $\mathfrak{o}'$ und nur diese ergeben, wenn für die Variablen ganze rationale Zahlen gesetzt werden**).

*) Algebra Bd. II, § 166.

Wenn wir x und y volle Restsysteme nach den Moduln $a_{1,1}, a_{2,2}$ durchlaufen lassen, so erhalten wir aus (10) lauter nach dem Modul $\mathfrak{a}$ incongruente Zahlen, und nach § 4, 6. erhält man also auf diese Weise ein volles Repräsentantensystem von Zahlen in $\mathfrak{o}'$ nach dem Modul $\mathfrak{a}$. Daraus ergiebt sich

$$N(\mathfrak{a}) = a_{1,1}\, a_{2,2}, \tag{11}$$

woraus noch folgt, dass $a_{1,1}$ und $a_{2,2}$ relativ prim zu Q sind.

Die Discriminante des Zahlensystems α_1, α_2 ist

$$(\alpha_1 \alpha_2' - \alpha_2 \alpha_1')^2 = a_{11}^2 a_{22}^2 D.$$

Sind nun

$$\beta_1 = \alpha_1 x_1 + \alpha_2 x_2, \qquad \beta_2 = \alpha_1 y_1 + \alpha_2 y_2$$

zwei durch $\mathfrak{a}$ theilbare Zahlen in $\mathfrak{o}'$, so ist deren Discriminante gleich

$$a_{1,1}^2 a_{2,2}^2 D(x_1 y_2 - x_2 y_1)^2,$$

und daraus ergiebt sich der Satz (vgl. Algebra Bd. II, § 147, 2.):

5. *Sind β_1, β_2 zwei durch $\mathfrak{a}$ theilbare Zahlen in $\mathfrak{o}'$, deren Discriminante gleich dem Product*

$$D N(\mathfrak{a})^2$$

ist, so ist $\beta_1 t_1 + \beta_2 t_2$ eine Basisform von $\mathfrak{a}$ in $\mathfrak{o}'$.

Bildet man die Norm von φ, so folgt aus (11), dass $2a_{1,2}$ durch $a_{2,2}$ theilbar ist, und wenn wir noch zur Abkürzung

$$N(\alpha_2) = -a a_{1,1} a_{2,2}, \tag{12}$$

$$a_{2,2} = e, \qquad a_{1,1} = ec, \qquad 2a_{12} = e(b - \Theta - \Theta') \tag{13}$$

und

$$\omega = \frac{\alpha_2}{\alpha_1} = \frac{a_{2,2} + a_{1,2}\Theta}{a_{11}}, \tag{14}$$

$$\varphi = ec(t_1 + \omega t_2) \tag{15}$$

setzen, so erhalten wir

$$\omega = \frac{b + \Theta - \Theta'}{2c} = \frac{b + \sqrt{D}}{2c}. \tag{16}$$

Die Zahl ω genügt wegen (12) und (13) der quadratischen Gleichung

$$c\omega^2 = a + b\omega \tag{17}$$

und folglich ist, was sich leicht durch Rechnung aus den Formeln (13) bestätigen lässt

$$D = b^2 + 4ac. \tag{18}$$

Nach (16) ist ω eine bestimmte der beiden Wurzeln der Gleichung (17). Die Zahl c ist als die *kleinste natürliche Zahl bestimmt, die $c\omega$ zu einer ganzen Zahl macht.* Denn nach (16) müssen, wenn c_1 diese kleinste Zahl ist

$$c_1(\omega + \omega') = \frac{bc_1}{c}, \qquad c_1(\omega - \omega') = \frac{\sqrt{D}c_1}{c}$$

ganze Zahlen sein; und da c relativ prim zu Q ist, so muss c_1 durch c theilbar und also $= c$ sein.

Die Zahl ω ist nach der Algebra I, § 122 angewandten Ausdrucksweise eine *quadratische Irrationalzahl mit der Discriminante D*. Sie ist durch das Ideal $\mathfrak{a}$ vollkommen bestimmt bis auf eine willkürlich bleibende additive ganze rationale Zahl. Nennen wir also ein System von Zahlen, die sich durch additive willkürliche ganze rationale Zahlen von einander unterscheiden, eine Schaar, so können wir den Satz aussprechen:

6. *Zu einer Ordnung $\mathfrak{o}'$ des quadratischen Körpers Ω mit dem Führer Q und der Discriminante D und zu jedem zu Q theilerfremden Ideal $\mathfrak{a}$ in Ω lässt sich eine und nur eine Schaar von quadratischen Irrationalzahlen zweiten Grades mit der Discriminante D bestimmen. Ist ω eine Zahl dieser Schaar, c die kleinste natürliche Zahl, die $c\omega$ ganz macht, und ec die kleinste durch $\mathfrak{a}$ theilbare natürliche Zahl, so ist*

$$\varphi = ec(t_1 + \omega t_2) \tag{19}$$

eine Basisform in $\mathfrak{o}'$ des Ideals $\mathfrak{a}$.

Hier ist unter den beiden Wurzeln der Gleichung (17) für ω die zu wählen, bei der das Zeichen von $\sqrt{D}$ so wie in (6) bestimmt ist. Es ist aber zu bemerken, dass

$$\varphi_2' = ec(t_1 - \omega t_2)$$

gleichfalls eine Basisform von $\mathfrak{a}$ ist. Man erhält also Basisformen des mit $\mathfrak{a}$ conjugirten Ideals $\mathfrak{a}'$ in der Form $\varphi = ec(t_1 \pm \omega' t_2)$, wenn ω' die zweite Wurzel der Gleichung (17) ist.

Von der Zahl e ist die Zahl ω nicht abhängig, und wenn wir also das System der Formen φ, die sich nur durch die verschiedenen Werthe von e unterscheiden, eine Formenschaar, und die dadurch repräsentirten Ideale eine Idealschaar nennen, so führen alle Ideale einer Schaar zu derselben Zahl ω. Der Quotient zweier Ideale einer Schaar ist mit einer *rationalen* Zahl äquivalent, und folglich sind die Ideale einer Schaar äquivalent nach O', und sogar nach O'_+.

Es gilt nun auch der umgekehrte Satz:

7. *Ist ω eine zur Discriminante D gehörige quadratische Irrationalzahl und c die kleinste natürliche Zahl, für die $c\omega$ ganz wird, und c relativ prim zu Q, ferner e eine beliebige zu Q theilerfremde natürliche Zahl, so ist*

$$\varphi = ec(t_1 \pm \omega t_2)$$

Basisform in $\mathfrak{o}'$ eines zu Q theilerfremden Ideals $\mathfrak{a}$.

Damit ω eine zur Discriminante D gehörige quadratische Irrationalzahl sei ist nothwendig und hinreichend, dass es die Wurzel einer quadratischen Gleichung

(20) $$c\omega^2 = a + b\omega, \qquad b^2 + 4ac = D$$

sei, in der a, b, c ganze Zahlen ohne gemeinschaftlichen Theiler sind. Wir nehmen c positiv und relativ prim zu Q an; dann ist c die kleinste natürliche Zahl, für die $c\omega$ ganz wird. Es ist dann

$$\omega = \frac{b \pm \sqrt{D}}{2c}$$

und $\Theta \mp c\omega$ ist eine ganze rationale Zahl. Bezeichnen wir nun das durch das Functional

(21) $$\varphi = ec(t_1 \pm \omega t_2)$$

repräsentirte Ideal mit $\mathfrak{a}$, so ergiebt sich hieraus leicht dass e die kleinste natürliche Zahl ist, für die $e\Theta$ nach dem Modul $\mathfrak{a}$ mit einer rationalen Zahl congruent ist, und ec die kleinste durch $\mathfrak{a}$ theilbare natürliche Zahl, und dies besagt, (nach (8) und (9)), dass (21) eine Basisform von $\mathfrak{a}$ ist.

8) *Wenn wir daher die durch* (20) *definirten, zur Discriminante D gehörigen quadratischen Irrationalzahlen, in denen c relativ prim zu Q ist, in Doppelschaaren eintheilen*

$$\pm\omega + \mathfrak{r}$$

worin $\mathfrak{r}$ *das System der ganzen rationalen Zahlen bedeutet, so entspricht jeder solchen Doppelschaar nach den Sätzen* 6., 7. *eine Schaar zu Q theilerfremder Ideale in* Ω, *und umgekehrt auch jeder solchen Idealschaar eine Doppelschaar von Irrationalzahlen.*

Wir nehmen zwei von den in 8. charakterisirten Irrationalzahlen ω, ω_1 und bilden die ihnen entsprechenden Basisformen

(22) $$\begin{aligned} \varphi &= c\,(t_1 + \omega\ t_2), \\ \varphi_1 &= c_1(t_1 + \omega_1 t_2). \end{aligned}$$

Die Zahlen ω_1, ω heissen äquivalent, wenn es ganze rationale Zahlen p, q, r, s giebt, so dass

(23) $$\omega_1 = \frac{p\omega + q}{r\omega + s}, \qquad ps - qr = \pm 1.$$

Ich will sie *ganz äquivalent* nennen, wenn $N(r\omega + s)$ positiv, also

(24) $$0 < cN(r\omega + s) = -ar^2 + brs + cs^2 = c_1,$$

positiv ist. Aus der Zusammensetzung der linearen Substitutionen ergiebt sich dann leicht, dass, wenn zwei Zahlen ω_1 und ω_2 mit einer dritten *ganz äquivalent sind*, ω_1 *und* ω_2 *auch unter einander ganz äquivalent sind.* Ist $N(r\omega + s)$ negativ, so mögen ω und ω_2 halb äquivalent heissen. Wir beweisen den Satz:

9. *Wenn ω, ω_1 äquivalent sind, so sind φ und φ_1 äquivalent nach O' und wenn ω, ω_1 ganz äquivalent sind, so sind φ und φ_1 äquivalent nach O'_+.*

Machen wir nämlich die Substitution (23) in (22), so ergiebt sich

$$(r\omega+s)\varphi_1 = c_1(u_1+u_2\omega),$$

wenn

$$u_1 = st_1 + qt_2, \quad u_2 = rt_2 + pt_2$$

gesetzt ist. Da die Determinante dieser Substitutionen $= \pm 1$ ist, so ist $c(u_1+u_2\omega)$ mit φ associirt*) und folglich ist $\varphi:\varphi_1$ mit $c(r\omega+s):c_1$ associirt. Damit ist der Beweis des Satzes 9 geführt.

Wir beweisen nun noch die Umkehrung dieses Satzes; und nehmen zu diesem Zweck an, die beiden Functionale φ, φ_1 in (22) seien äquivalent (nach O' oder O'_+).

Wir nehmen ein Functional

$$\psi = c'(t_1+t_2\eta) \tag{25}$$

in der Classe, die zu der Classe von φ reciprok ist, und es soll darin c', η dieselbe Bedeutung für ψ haben, wie c und ω für φ, so dass also c' positiv und relativ prim zu Q ist. Dann giebt es eine *ganze Zahl* ξ in O' oder in O'_+ und eine Functionaleinheit ε, so dass

$$\psi\varphi = \varepsilon\xi \tag{26}$$

und c und c' sind die absoluten Normen von φ und ψ, d. h. die Normen der durch φ und ψ repräsentirten Ideale. Setzen wir

$$N(\psi) = \psi\psi' = \varepsilon_1 c',$$

so ist ε_1 eine Einheitsform, und aus (26) folgt durch Multiplication mit ψ'

$$\frac{c'\varphi}{\xi} = \varepsilon_2\psi',$$

worin ε_2 eine Einheit ist. Setzen wir daher

$$\frac{c'\varphi}{\xi} = \frac{cc'(t_1+\omega t_2)}{\xi} = \chi,$$

so ist χ ein mit ψ' associirtes ganzes Functional, und daraus folgt, dass

$$\beta_1 = \frac{cc'}{\xi}, \quad \beta_2 = \frac{cc'\omega}{\xi}$$

ganze durch ψ' theilbare Zahlen in $\mathfrak{o}'$ sind. Da die absolute Norm von $\xi = cc'$ ist, so ist die Discriminante dieses Zahlensystems

$$\Delta(\beta_1, \beta_2) = c'^2 D$$

und daher ist nach dem Satz 5

$$\beta_1 t_1 + \beta_2 t_2$$

eine Basisform von ψ'. Da nun andererseits $c'(t_1+\eta' t_2)$ gleichfalls

*) Algebra, Bd. II, § 147.

eine Basisform von ψ' ist, so folgt die Existenz einer linearen Substitution $\begin{pmatrix} p, & q \\ r, & s \end{pmatrix}$ mit der Determinante ± 1, so dass

$$\begin{aligned} \beta_1 &= \frac{cc'}{\xi} = c'(r\eta' + s), \\ \beta_2 &= \frac{cc'\omega}{\xi} = c'(p\eta' + q) \end{aligned} \tag{27}$$

und bei der Aequivalenz nach O'_+ ist $N(\xi)$ und damit $N(r\eta' + s)$ positiv. Aus (27) aber folgt

$$\omega = \frac{r\eta' + q}{r\eta' + s} \tag{28}$$

d. h. ω ist mit η' äquivalent und zwar, bei der Aequivalenz nach O'_+, ganz äquivalent.

Lassen wir nun φ_1 an Stelle des äquivalenten Functionales φ treten, so kann ψ und daher auch ψ' ungeändert bleiben, und es folgt, dass auch ω_1 mit η' und folglich auch ω mit ω_1 äquivalent ist, und zwar (bei der Aequivalenz nach O'_+) ganz äquivalent.

Da nun zwei in derselben Doppelschaar vorkommende Zahlen ω ganz äquivalent, und zwei in derselben Schaar vorkommende Ideale äquivalent nach O'_+ sind, so ergiebt sich

> 10. *Die Classen der zu Q theilerfremden Ideale in* Ω *nach* O'_+ *und die Classen der ganz äquivalenten zur Discriminante D gehörigen Irrationalzahlen zweiten Grades lassen sich gegenseitig eindeutig einander so zuordnen, dass die Beziehung zwischen je einem Repräsentanten einer Classe der einen und der anderen Art durch die Formel* (15) *gegeben ist. Die Anzahlen beider Arten von Classen stimmen überein.*

Hierzu ist noch zu bemerken, dass bei negativer Discriminante die Normen aller Zahlen positiv sind, dass daher O'_+ von O' nicht verschieden ist, und dass ebenso die ganze Aequivalenz mit der Aequivalenz überhaupt zusammenfällt.

Bei positiver Discriminante giebt es immer Zahlen mit negativer Norm und es sind zwei Fälle zu unterscheiden.

1) Wenn die Gliederzahl einer Periode der Kettenbruch-Entwickelung von ω ungerade ist, wenn also die Pell'sche Gleichung $T^2 - DU^2 = -4$ lösbar ist, so giebt es auch Einheiten mit negativer Norm. Daher ist zwar O'_+ von O' verschieden, aber die Aequivalenz von O'_+ ist mit der Aequivalenz nach O' identisch. Ebenso ist auch bei den Zahlen ω die ganze Aequivalenz mit der Aequivalenz schlechtweg gleichbedeutend, und die Anzahl der Idealclassen nach O' oder nach O'_+ ist gleich der Anzahl der verschiedenen zu der Discriminante D gehörigen Kettenbruchperioden.

2) Ist aber die Gliederzahl der Kettenbruchperiode gerade, so haben alle Einheiten positive Norm. Die Zahlen einer Kettenbruchperiode zerfallen bei der ganzen Aequivalenz in zwei Classen und die Aequivalenz nach O'_+ ist von der Aequivalenz nach O' verschieden. Die Anzahl der Idealclassen nach O' ist also gleich der Anzahl der Kettenbruchperioden, und die Anzahl der Idealclassen nach O'_+ ist doppelt so gross.

Diese Betrachtungen geben nun auch Aufschluss über die Beziehung der Zahl der Idealclassen zu der Classenzahl quadratischer Formen von gegebener Determinante nach Gauss.

Jeder zur Discriminante D gehörigen Irrationalzahl ω entsprechen nach der Gauss'schen Bezeichnung zwei primitive quadratische Formen der Determinante D,

$$\pm\psi = \pm(A, B, C)$$

so dass ω eine Wurzel von $\psi = 0$ ist.

Zwei conjugirte Zahlen ω, ω' entsprechen denselben Formen $\pm\psi$. Sonst aber gehören zu verschiedenen Zahlen ω auch verschiedene Formen ψ. Aequivalenten Zahlen ω entsprechen eigentlich oder uneigentlich äquivalente Formen ψ.

Da nun zwei Zahlen $\omega, -\omega$ uneigentlich und zugleich ganz äquivalent sind, so können wir in jeder Classe der Zahlen ω einen Repräsentanten auswählen, in dem der irrationale Theil ein bestimmtes Vorzeichen hat, so dass von zwei conjugirten Zahlen nur die eine zur Verwendung kommt. Es ergiebt sich nun für die drei Fälle Folgendes.

1. Wenn die Discriminante negativ ist, so sind zwei Formen $+\psi, -\psi$ nicht äquivalent. Wir beschränken uns auf die Formen mit positiven äusseren Coefficienten. Zwei Zahlen ω mit positivem imaginärem Bestandtheil können niemals uneigentlich äquivalent sein, und wenn wir uns also auf Zahlen ω mit positivem imaginärem Bestandtheil beschränken, so entsprechen sich die Zahlen ω und die Form ψ gegenseitig eindeutig. Aequivalente Zahlen ω entsprechen eigentlich äquivalenten Formen ψ und umgekehrt. Es ist also die Anzahl der Classen positiver Formen gleich der Anzahl der Classen der Form ω.

2. Wenn die Discriminante positiv ist und die Periode der Kettenbruchentwickelung von ω aus einer ungeraden Gliederzahl besteht, so ist die Form (A, B, C) mit $(-A, B, -C)$ eigentlich äquivalent, und da $(-A, B, -C)$ mit $(-A, -B, -C)$ uneigentlich äquivalent ist, so ist in diesem Fall ψ mit $-\psi$ uneigentlich äquivalent. Ist daher $C = \omega, \omega_1, , \ldots$ eine Classe äquivalenter quadratischer Irrationalzahlen, so erhalten wir entsprechend ein System von Formen $F = \pm\psi, \pm\psi_1, \ldots$

die mit einander eigentlich oder uneigentlich äquivalent sind; und die also eine oder zwei Gauss'sche Classen vertreten, je nachdem ψ zu einer Anceps-Classe gehört oder nicht. Die zu C conjugirte Classe C' ergiebt nun dasselbe System S; und da die Formen der Anceps-Classe dadurch charakterisirt sind, dass bei ihnen ω und ω' uneigentlich äquivalent sind, so folgt, dass C' mit C identisch ist, oder nicht, je nachdem F eine oder zwei Gauss'sche Classen umfasst. Es stimmt also auch hier die Anzahl der Gauss'schen Classen mit der Anzahl der Classen C überein. Einer Anceps-Classe entspricht eine Classe C, und einem Paar entgegengesetzter Formenclassen ψ, ψ' ein Paar conjugirter Classen, C, C'. Es ist jedoch hierdurch trotz der Uebereinstimmung der Anzahl, keine *eindeutige* Zuordnung der Formenclassen zu den Zahlenclassen (oder Idealclassen) gegeben.

3. Der dritte Fall unterscheidet sich von dem zweiten dadurch, dass ψ und $-\psi$ *nicht äquivalent* sind. Daher entsprechen jedem conjugirten Classenpaar C, C' vier Gauss'sche Formenclassen, oder, wenn C mit C' identisch ist, zwei Anceps-Classen. Die Gauss'sche Classenzahl stimmt mit der Anzahl der Classen der Ganz-Aequivalenz überein. Wir erhalten daher das Ergebniss.

Die Gauss'sche Classenzahl primitiver quadratischer Formen stimmt in allen Fällen überein mit der Anzahl der Idealclassen in der Ordnung $\mathfrak{o}'$ bei der Aequivalenz nach O'_+.

Dabei ist noch zu bemerken, dass die eigentlich primitiven Formen (Formen erster Art) dann auftreten, wenn b gerade, also $D \equiv 0 \pmod 4$ und die Gauss'sche Determinante $\frac{1}{4}D$ ist, die uneigentich primitiven Formen oder Formen zweiter Art, wenn b ungerade, also $D \equiv 1 \pmod 4$, und D selbst die Gauss'sche Determinante ist.

Um eine eindeutige Zuordnung der Idealclassen zu den Formenclassen zu erhalten, schlagen wir folgenden Weg ein.

Wir betrachten die Ideale $\mathfrak{a}$, die relativ prim zu Q sind, und wollen auch (zur Vereinfachung) annehmen, dass $\mathfrak{a}$ keinen rationalen Factor hat, dass also die oben mit e bezeichnete Zahl $= 1$ sei; dies ist genügend, da durch Wegnahme eines rationalen Factors die Classeneintheilung, auch bei der Aequivalenz nach O'_+, nicht geändert wird. Dann ist c die kleinste durch $\mathfrak{a}$ theilbare natürliche Zahl, und die rationale Zahl b wird durch die Bedingung, dass $\frac{1}{2}(b + \sqrt{D})$ eine durch $\mathfrak{a}$ theilbare ganze Zahl sein soll, nach den Modul $2c$ bestimmt. Hierbei ist $\sqrt{D}$ in der früher festgesetzten Weise bestimmt. Es ergiebt sich dann eine Irrationalzahl

$$\omega = \frac{b + \sqrt{D}}{2c}$$

die die Wurzel einer Form

$$\psi = (c, -b, -a)$$

ist, in der der erste Coefficient c *positiv* ist.

Hierdurch ist eine bestimmte Form ψ (genauer eine Schaar paralleler Formen) dem Ideal $\mathfrak{a}$ eindeutig zugeordnet.

Wir nehmen nun ein volles Repräsentantensystem der Idealclasse nach O'_+

$$\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$$

und wollen noch, zur Vereinfachung des Folgenden, annehmen, was gestattet ist, dass von den Zahlen

$$c_1, c_2, \ldots, c_h$$

keine zwei einen gemeinschaftlichen Theiler haben. Daraus leiten wir ein volles Repräsentantensystem von Zahlen ω her

$$\omega_1, \omega_2, \ldots, \omega_h$$

von denen keine zwei äquivalent sind. Diese Zahlen sind Wurzeln der Formen

$$\psi_1, \psi_2, \ldots, \psi_h,$$

und diese Formen sind inäquivalent nach der Gauss'schen Definition. Denn zwei dieser Formen ψ_1, ψ_2 könnten nur dann äquivalent sein, wenn die entsprechenden Zahlen ω_1, ω_2 halbäquivalent wären, was im Falle 3 möglich ist. Ist aber ω_1 mit ω_2 halbäquivalent, so kann die Aequivalenz nur eine uneigentliche sein (wegen des Vorzeichens von c_1, c_2 und $\sqrt{D}$) und es ist ψ_1 mit $-\psi_2$ uneigentlich äquivalent. Wären also ψ_1 und ψ_2 eigentlich äquivalent, so wäre ψ_2 mit $-\psi_2$ uneigentlich äquivalent, und daraus könnte man eine Lösung der Pell'schen Gleichung $T^2 - Du^2 = -4$ ableiten*), die im Falle 3 nicht existirt.

Setzen wir

$$\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2,$$

so ist nach unserer Voraussetzung, dass c_1, c_2 ohne gemeinsamen Theiler sind

$$c = c_1 c_2$$

die kleinste durch $\mathfrak{a}$ theilbare natürliche Zahl, und wenn wir b aus den Congruenzen

$$b \equiv b_1 \pmod{2c_1}, \quad b \equiv b_2 \pmod{2c_2}$$

bestimmen, so ist

$$\omega = \frac{b + \sqrt{D}}{2c}$$

eine durch $\mathfrak{a}$ theilbare ganze Zahl. Die Form ψ, deren Wurzel ω ist,

*) Ebenso wie bei Dirichlet-Dedekind, Zahlentheorie 4. Aufl. § 62.

ist dann aus den *beiden* Formen ψ_1, ψ_2 *componirt* und *die Composition der Formen und Formenclassen entspricht daher der Multiplication der Ideale und der Composition der Idealclassen.*

§ 6.

Genera in den Ordnungen.

Wir kehren nun wieder zu allgemeineren Betrachtungen zurück, indem wir unter Ω einen beliebigen Normalkörper, unter $\mathfrak{o}'$ eine darin enthaltene Normalordnung von der in § 4 betrachteten Art mit dem Führer $\mathfrak{k}$, und unter Q die kleinste durch $\mathfrak{k}$ theilbare natürliche Zahl verstehen. Aus $\mathfrak{o}'$ leiten wir die Gruppe O'_+ her, und bezeichnen mit $\overline{O}$ die Gruppe aller zu $\mathfrak{k}$ theilerfremden (ganzen und gebrochenen) Ideale des Körpers Ω. Unter Aequivalenz soll in diesem Paragraphen immer die Aequivalenz nach O'_+ verstanden sein.

Wir nehmen irgend eine natürliche Zahl m, und bezeichnen die endliche Gruppe vom Grade $\varphi(m) = \mu$ der nach dem Modul m genommenen rationalen Zahlclassen, die nur *relative Primzahlen zu m* enthalten, mit M.

Alle Zahlclassen der Gruppe M, deren Zahlen mit *Normen von Zahlen* ω' *aus* $\mathfrak{o}'$ nach dem Modul m congruent sein können, bilden eine in M enthaltene Gruppe M', deren Grad μ' sei, und wir bezeichnen die Gruppe M' durch die symbolische Congruenz

$$N(\omega') \equiv M' \pmod{m}. \tag{1}$$

Unter den Idealen der Gruppe $\overline{O}$ werden nun solche enthalten sein, deren Normen in M' enthalten sind, für die also, wenn $\mathfrak{a}$ ein solches Ideal ist, eine Zahl ω' in O'_+ existirt, die der Bedingung

$$N(\mathfrak{a}) \equiv N(\omega') \pmod{m} \tag{2}$$

genügt.

Diese Ideale $\mathfrak{a}$ bilden eine in $\overline{O}$ enthaltene Gruppe $\mathfrak{A}_m$, die wir das *Hauptgeschlecht für den Modul m* nennen wollen.

In der Gruppe $\mathfrak{A}_m$ ist die Gruppe der Hauptideale $\overline{E}\,O'_+$ enthalten, und wenn $\mathfrak{a}$ in $\mathfrak{A}_m$ enthalten ist, so sind auch alle mit $\mathfrak{a}$ nach O'_+ äquivalenten Ideale zugleich darin enthalten. Das Hauptgeschlecht $\mathfrak{A}_m$ enthält also nur vollständige Idealclassen nach O'_+, und wir fassen daher $\mathfrak{A}_m$ jetzt nicht mehr als Gruppen von Idealen, sondern als *Gruppen von Idealclassen* auf, die in der Gesammtgruppe der Idealclassen

$$\mathfrak{G} = \overline{O} \,|\, \overline{E}\,O'_+ \tag{3}$$

enthalten ist*). Da $\mathfrak{a}\omega'^{-1}$ mit $\mathfrak{a}$ äquivalent ist, so können wir die Definition nach (2) so fassen:

*) Die Unterscheidung von O'_+ und O' ist, wie schon oben bemerkt, nur in dem Falle nöthig, wo es Zahlen, aber darunter keine Einheiten, mit negativer

1. *Eine Idealclasse A der Gruppe $\mathfrak{G}$ gehört der Gruppe $\mathfrak{A}_m$, oder dem Hauptgeschlecht für den Modul m an, wenn in A ein Repräsentant $\mathfrak{a}$ existirt, der der Bedingung*

$$N(\mathfrak{a}) \equiv 1 \pmod{m} \tag{4}$$

genügt.

Setzen wir nun

$$h = (\bar{O},\ \bar{E}\,O'_+),\quad k_m = (\bar{O},\ \mathfrak{A}_m),\quad h_m = (\mathfrak{A}_m,\ \bar{E}\,O'_+),$$

so ist

$$h = h_m k_m, \tag{5}$$

und k_m ist die *Anzahl der Geschlechter* für den Modul m, h_m die Anzahl der in jedem Geschlechte enthaltenen Classen.

Bezeichnen wir mit M'' die Gruppe der zu m theilerfremden, nach dem Modul m genommenen Zahlclassen, deren Zahlen mit *Normen von Idealen aus* $\bar{O}$ nach dem Modul m congruent sind, so ist M'' ein Theiler von M und M' ein Theiler von M'', und es ist

$$k_m = (M'', M') = \frac{(M, M')}{(M, M'')}. \tag{6}$$

Da eine Congruenz (4) nach dem Modul m die gleiche Congruenz für jeden Theiler von m zur Folge hat, so gilt der Satz:

2. *Ist m_1 ein Theiler von m, so ist $\mathfrak{A}_m$ ein Theiler von $\mathfrak{A}_{m_1}$.*

Daraus ziehen wir noch weitere Schlüsse.

3. *In der Gruppe $\mathfrak{G}$ der Idealclassen ist eine Gruppe $\mathfrak{A}$ enthalten, die aus allen Idealclassen A von $\mathfrak{G}$ besteht, die die Eigenschaft haben, dass für jeden beliebigen Modul m ein der Bedingung*

$$N(\mathfrak{a}) \equiv 1 \pmod{m} \tag{7}$$

genügender Repräsentant $\mathfrak{a}$ von A existirt.

Dass eine solche Gruppe $\mathfrak{A}$ immer existirt, ist von vorn herein klar, da ja die Hauptclasse $\bar{E}\,O'_+$ gewiss diese Eigenschaft hat.

Diese Gruppe $\mathfrak{A}$ nennen wir das *absolute Hauptgeschlecht* und die Nebengruppen zu $\mathfrak{A}$ die *absoluten Geschlechter*. Aus der Definition ergiebt sich unmittelbar, dass $\mathfrak{A}$ in jeder Gruppe $\mathfrak{A}_m$ enthalten ist,

---

Norm giebt. Wollte man die Unterscheidung nicht machen, so würde $\bar{E}\,O'$ nicht immer in $\mathfrak{A}_m$ enthalten sein, und es würden dann durch die Geschlechtereintheilung die Classen nach O' von selbst in zwei Theile zerlegt werden. Wollte man das vermeiden, so müsste man die Gruppe M' durch die Congruenz

$$N_a(\omega') \equiv M' \pmod{m}$$

definiren, wenn N_a die absolute Norm bedeutet, erhielte aber dann eine minder scharfe Eintheilung.

und dass umgekehrt jede Classe, die in allen $\mathfrak{A}_m$ vorkommt, auch in $\mathfrak{A}$ enthalten ist.

4. *Das absolute Hauptgeschlecht ist daher der Durchschnitt aller relativen Hauptgeschlechter.*

Wenn wir m durch Hinzufügung eines Factors zu m_1 erweitern, so verengert sich die Gruppe $\mathfrak{A}_m$, wenn nicht $\mathfrak{A}_m = \mathfrak{A}_{m_1}$ ist. Schliesslich müssen wir also zu einem Modul m_0 kommen, so dass durch weitere Hinzufügung von Factoren zu m_0 die Gruppe $\mathfrak{A}_{m_0}$ nicht mehr eingeengt werden kann. Dann ist $\mathfrak{A}_{m_0} = \mathfrak{A}$. Es giebt also gewisse Moduln m_0 für die das *relative* Hauptgeschlecht mit dem *absoluten* übereinstimmt, und wenn m_0 ein solcher Modul ist, so hat jedes Vielfache von m_0 die gleiche Eigenschaft. Man könnte einen, etwa den kleinsten unter diesen Moduln m_0 vor den andern auszeichnen, jedoch spricht dafür kein innerer Grund, da es z. B. vorkommen kann, dass $\mathfrak{A}_p = \mathfrak{A}_q = \mathfrak{A}$ ist, wenn p und q zwei verschiedene völlig gleichberechtigte Primzahlen sind.

Es gilt aber auch der folgende Satz:

5. *Sind m_1, m_2 relativ prim, so ist $\mathfrak{A}_{m_1 m_2}$ der grösste gemeinschaftliche Theiler von $\mathfrak{A}_{m_1}$ und $\mathfrak{A}_{m_2}$.*

Nach 2. ist zunächst $\mathfrak{A}_{m_1 m_2}$ ein Theiler, sowohl von $\mathfrak{A}_{m_1}$ als von $\mathfrak{A}_{m_2}$. Es ist also noch zu zeigen, dass eine Idealclasse A, die sowohl in $\mathfrak{A}_{m_1}$ als in $\mathfrak{A}_{m_2}$ vorkommt, auch in $\mathfrak{A}_{m_1 m_2}$ enthalten sein muss, oder dass, wenn es in A zwei Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ giebt, die den Bedingungen

$$N(\mathfrak{a}_1) \equiv 1 \pmod{m_1}, \qquad N(\mathfrak{a}_2) \equiv 1 \pmod{m_2} \tag{7}$$

genügen, in A auch ein Ideal $\mathfrak{a}$ existirt, so dass

$$N(\mathfrak{a}) \equiv 1 \pmod{m_1 m_2} \tag{8}$$

ist. Da $\mathfrak{a}_1$ und $\mathfrak{a}_2$ äquivalent sind, so giebt es eine *Zahl* ω' in O'_+ so dass

$$\mathfrak{a}_2 = \mathfrak{a}_1 \omega'$$

ist. Bestimmen wir nun die ganzen rationalen Zahlen x_1, x_2 so dass

$$\begin{aligned} x_1 &\equiv 1 \pmod{m_1}, & x_2 &\equiv 0 \pmod{m_1}, \\ &\equiv 0 \pmod{m_2}, & &\equiv 1 \pmod{m_2} \end{aligned} \tag{9}$$

und dass $N(x_1 + x_2\omega')$ positiv wird, und setzen

$$\mathfrak{a} = \mathfrak{a}_1 (x_1 + x_2 \omega'),$$

so ist $\mathfrak{a}$ in der Classe A enthalten, und

$$N(\mathfrak{a}) \equiv N(\mathfrak{a}_1) \pmod{m_1}, \quad N(\mathfrak{a}) \equiv N(\mathfrak{a}_2) \pmod{m_2}$$

also ist auch, wie verlangt, die Congruenz (8) befriedigt und das Theorem 5. bewiesen.

Um über die Anzahl der Genera näheren Aufschluss zu erhalten, betrachten wir zunächst die Gruppen der Zahlclassen M, M' nach einen beliebigen Modul m.

Es sei

$$m = m_1 m_2$$

und m_1, m_2 relative Primzahlen. Es mögen ferner M_1, M_1'; M_2, M_2' dieselbe Bedeutung für m_1, m_2 haben, wie M, M' für m. Dann ist der Grad von M gleich dem Product der Grade von M_1 und M_2 und dasselbe gilt von den Gruppen M', M_1', M_2'. Das erstere ist bekannt; um auch das zweite einzusehen, braucht man nur zu erwägen, dass eine Zahl a, die zu M' gehört auch in M_1' und in M_2' enthalten ist, dass aber auch umgekehrt eine Zahl a, die zugleich zu M_1' und zu M_2' gehört, in M' enthalten sein muss. Denn ist

$$N(\omega_1) \equiv a \pmod{m_1}. \quad N(\omega_2) \equiv a \pmod{m_2}$$

so ist, wenn wir x_1, x_2 durch (9) bestimmen,

$$N(x_1\omega_1 + x_2\omega_2) \equiv a \pmod{m},$$

also a auch in M enthalten. Hieraus folgt (§ 1, III)

$$(M, M') = (M_1, M_1')\,(M_2, M_2'). \tag{10}$$

Ist nun $m = p^\lambda$ eine Primzahlpotenz, so bezeichnen wir die entsprechenden Gruppen M, M' mit P_λ, P_λ' und ihre Grade mit π_λ, π_λ'. Dann ist bekanntlich, so lange $\lambda > 1$ ist, $\pi_\lambda = p\pi_{\lambda-1}$. Ferner ist jede Zahl a, die in P_λ' enthalten ist, auch in $P_{\lambda-1}'$ enthalten. Ist nun a eine Zahl aus $P_{\lambda-1}'$, so giebt es eine Zahl ω, die der Bedingung

$$N(\omega) \equiv a \pmod{p^{\lambda-1}}$$

genügt. Wenn nun für jedes a aus dieser Congruenz auch die Möglichkeit der Congruenz

$$N(\omega) \equiv a \pmod{p^\lambda}$$

folgt, so ergeben sich zu jedem a nach dem Modul $p^{\lambda-1}$ p verschiedene Zahlen nach dem Modul p^λ, d. h. es ist in diesem Fall

$$\pi_\lambda' = p\pi_{\lambda-1}'$$

in den anderen Fällen ist π_λ' kleiner als $p\pi_{\lambda-1}'$, und da $\pi_{\lambda-1}'$ ein Theiler von π_λ' sein muss, so ist in diesen Fällen $\pi_\lambda' = \pi_{\lambda-1}'$. Hieraus ergiebt sich im ersten Fall

$$(P_\lambda, P_\lambda') = (P_{\lambda-1}, P_{\lambda-1}'),$$

im anderen Falle

$$(P_\lambda, P_\lambda') = p\,(P_{\lambda-1}, P_{\lambda-1}').$$

6. Definition. *Wir nennen eine Primzahl p, bei der für irgend eine Potenz p^λ die Gruppe P_λ' von P_λ verschieden ist, eine charakteristische Primzahl der Ordnung $\mathfrak{o}'$, und die höchste Potenz p^λ, bei der (P_λ, P_λ') noch von $(P_{\lambda-1}, P_{\lambda-1}')$ verschieden ist, die charakteristische Potenz von p.*

Nehmen wir einen Modul m, der alle charakteristischen Primzahlpotenzen (deren Anzahl, wie sich gleich zeigen wird, endlich ist) als Theiler enthält, so ist

(11) $$(M, M') = \prod (P_i, P_i'),$$

das Product Π ausgedehnt über alle charakteristischen Primzahlpotenzen von $\mathfrak{o}'$. Dieser Ausdruck ist aber unabhängig von der sonstigen Beschaffenheit von m und ist der Zähler in dem Ausdruck für die Anzahl der absoluten Geschlechter. Der Nenner dieses Ausdrucks (M, M'') ist daher in demselben Umfang von m unabhängig.

§ 7.

Die charakteristischen Primzahlen.

Zur näheren Bestimmung der charakteristischen Primzahlen und ihrer Potenzen führen die folgenden Sätze, in denen der Grad des Körpers Ω immer mit n bezeichnet ist.

Es handelt sich zunächst darum, zu entscheiden, wenn p eine natürliche Primzahl und a eine durch p nicht theilbare rationale Zahl ist, unter welchen Umständen die Congruenz

(1) $$N(\omega) \equiv a \pmod{p}$$

durch eine Zahl ω in $\mathfrak{o}'$ lösbar ist.

1. *Wenn p in Q aufgeht, so kann die Congruenz* (1) *dann und nur dann durch eine Zahl in $\mathfrak{o}'$ gelöst werden, wenn a mit der n^{ten} Potenz einer andern rationalen Zahl b congruent ist:*

(2) $$a \equiv b^n \pmod{p}$$

oder was dasselbe ist, wenn δ den grössten gemeinschaftlichen Theiler von $p-1$ und n bedeutet unter der Bedingung

(3) $$a^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}.$$

Denn ist erstens die Bedingung (2) erfüllt, so wird (1) durch die in $\mathfrak{o}'$ enthaltene Zahl $\omega = b$ befriedigt. Ist umgekehrt (1) befriedigt, und $\mathfrak{f}$ der Führer von $\mathfrak{o}'$, so giebt es nach der Definition von $\mathfrak{o}'$ ein rationales b, so dass

$$\omega \equiv b \pmod{\mathfrak{f}},$$

also auch, wenn ω_i die mit ω conjugirten Zahlen sind

$$\omega_i \equiv b \pmod{\mathfrak{f}},$$

Also, indem man hiervon das Product nimmt

$$N(\omega_i) \equiv b^n \pmod{\mathfrak{f}}$$

und diese Congruenz besteht auch nach den Modul p.

Wenn zweitens p nicht in Q aufgeht, also relativ prim zu $\mathfrak{f}$ ist, so ist jede Zahl in $\mathfrak{o}$ nach den Modul p mit einer Zahl in $\mathfrak{o}'$ congruent. Denn wir können dann die Congruenz

$$Q\xi \equiv \omega \pmod{p}$$

durch eine Zahl ξ in $\mathfrak{o}$ befriedigen und $Q\xi$ ist in $\mathfrak{o}'$ enthalten. Ist also die Congruenz (1) in $\mathfrak{o}$ zu befriedigen, so kann sie auch in $\mathfrak{o}'$ befriedigt werden. Wir zerlegen p in seine Primideale

$$p = (\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_e)^g, \quad efg = n^*) \tag{4}$$

worin $\mathfrak{p}_1, \mathfrak{p}_2, , \ldots, \mathfrak{p}_e$ von einander verschiedene Primideale f^{ten} Grades sind, *und worin g ein Theiler von n ist, der nur dann grösser als* 1 *ist, wenn p in der Grundzahl Δ des Körpers Ω aufgeht.*

In der Gruppe Φ des Körpers Ω ist eine Gruppe X vom Grade g enthalten, deren Substitutionen χ für jede Zahl ω in $\mathfrak{o}$ der Bedingung

$$\omega|\chi \equiv \omega \pmod{\mathfrak{p}} \tag{5}$$

genügen, wenn $\mathfrak{p}$ irgend einer der Primfactoren von p ist. Ausserdem giebt es eine Substitution f^{ten} Grades, ψ_0, für die

$$\omega|\psi_0 \equiv \omega^p \pmod{\mathfrak{p}},$$

also für jeden Exponenten λ

$$\omega|\psi_0^{\lambda} \equiv \omega^{p^{\lambda}} \pmod{\mathfrak{p}}. \tag{6}$$

Die Gruppe gf^{ten} Grades

$$\Psi = \mathsf{X} + \mathsf{X}\psi_0 + \cdots + \mathsf{X}\psi_0^{f-1}$$

ist dann die Gruppe des Primideals $\mathfrak{p}$; ihre Substitutionen werden mit ψ bezeichnet. Aus (5) und (6) aber folgt für jedes ω

$$\prod^{\psi} \omega|\psi \equiv \omega^{g(1+p+\cdots+p^{f-1})} \pmod{\mathfrak{p}},$$

und wenn wir

$$\eta = \omega^{1+p+\cdots+p^{f-1}}$$

setzen, so ist

$$\eta^p \equiv \eta \pmod{\mathfrak{p}}.$$

Das ist aber (vgl. Algebra Bd. II, § 150) die nothwendige und hinreichende Bedingung dafür, dass η mit einer rationalen Zahl c congruent ist. Also:

$$\prod^{\psi} \omega|\psi \equiv c^g \pmod{\mathfrak{p}}, \tag{7}$$

Eine solche Congruenz gilt für jedes ω, und wenn daher φ eine nicht in Ψ enthaltene Substitution von ω ist, so ist auch

$$\prod^{\psi} \omega|\varphi\psi \equiv c_1^g \pmod{\mathfrak{p}}.$$

Multiplicirt man alle diese Congruenzen mit einander, und bezeichnet mit b eine rationale Zahl, so folgt für jede Zahl in $\mathfrak{o}$

*) Algebra, Bd. II, § 160, 168.

$$N(\omega) \equiv b^g \pmod{\mathfrak{p}}, \tag{9}$$

und diese Congruenz besteht daher auch für den Modul p.

Aber es gilt auch umgekehrt, dass eine Congruenz (9), wenn b eine beliebige rationale Zahl ist, immer in $\mathfrak{o}$ lösbar ist. Wenn nämlich b durch p nicht theilbar ist und γ eine primitive Wurzel von $\mathfrak{p}_1$ bedeutet, so kann man den Exponenten x immer so bestimmen, dass

$$b \equiv \gamma^{x(1+p+\cdots+p^{f-1})} \pmod{\mathfrak{p}_1}$$

wird. Nun nehmen wir eine Zahl ω an, die den Congruenzbedingungen

$$\omega \equiv \gamma^x \pmod{\mathfrak{p}_1},$$
$$\omega \equiv 1 \pmodd{\mathfrak{p}_2, \mathfrak{p}_3 \ldots, \mathfrak{p}_e}$$

genügt.

Um eine solche Zahl zu finden, nehme man eine Zahl α, die durch $\mathfrak{p}_1$ theilbar, durch $\mathfrak{p}_2, \ldots, \mathfrak{p}_e$ nicht theilbar ist, und bestimme die Zahl ξ aus

$$\omega = \alpha\xi + \gamma^x \equiv 1 \pmodd{\mathfrak{p}_2, \ldots, \mathfrak{p}_e}.$$

Dann ist

$$\omega \,|\, \chi\psi_0{}^\lambda \equiv \gamma^{xp^\lambda} \pmod{\mathfrak{p}_1},$$

und für jede nicht in Ψ enthaltene Substitution φ

$$\omega \,|\, \varphi \equiv 1 \pmod{\mathfrak{p}_1},$$

folglich

$$N(\omega) \equiv \gamma^{gx(1+p+\cdots+p^{f-1})} \equiv b^g \pmod{\mathfrak{p}_1}.$$

Wir haben also

2. Wenn p nicht in Q aufgeht, so ist die nothwendige und hinreichende Bedingung für die Lösbarkeit der Congruenz (1) *in* $\mathfrak{o}'$ *die, dass*

$$a \equiv b^g \pmod{p}$$

oder also, wenn δ *der grösste gemeinschaftliche Theiler von* g *und* $p-1$ *ist*

$$a^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}.$$

Wenn die Congruenz

$$N(\omega') \equiv a \pmod{p^\lambda} \tag{10}$$

für irgend einen positiven Exponenten λ durch eine Zahl in $\mathfrak{o}'$ lösbar ist, so setzen wir

$$N(\omega') = a + p^\lambda a'$$

und bilden eine Zahl

$$\eta = \omega'(p^\lambda x\xi + 1),$$

worin x rational, und ξ eine Zahl in $\mathfrak{o}$ sein soll, deren Spur $S(\xi)$ nicht durch p theilbar ist (wenn eine solche Zahl existirt). Dann ist

$$N(\eta) \equiv a + p^\lambda \left(a' + xS(\xi)\right) \pmod{p^{\lambda+1}}$$

und daher, wenn x der Congruenz

(11) $$x S(\xi) + a' \equiv 0 \pmod{p}$$

genügt,

$$N(\eta) \equiv a \pmod{p^{\lambda+1}}.$$

Wenn sich also ξ und x so bestimmen lassen, dass $1 + p^\lambda x\xi$ zu $\mathfrak{o}'$ gehört, so folgt, dass wenn die Congruenz (10) in $\mathfrak{o}'$ lösbar ist, auch

(12) $$N(\omega') \equiv a \pmod{p^{\lambda+1}}$$

lösbar ist.

Die Zahlen ξ, x, wie sie hier vorausgesetzt sind, existiren immer, wenn p theilerfremd zum Führer $\mathfrak{k}$ von $\mathfrak{o}'$ und zur Grundzahl Δ des Körpers ist, oder wenn p nicht im Grade n des Körpers Ω aufgeht.

Denn die Grundzahl Δ ist, wenn $\omega_1, \omega_2, \ldots, \omega_n$ eine Basis der ganzen Zahlen von Ω bedeutet, gleich der Determinante

$$\Delta = |S(\omega_\iota \omega_\varkappa)|,$$

und wenn also alle Spuren durch p theilbar sind, so ist auch Δ durch p theilbar. Folglich giebt es, wenn p nicht in Δ aufgeht, eine Zahl ξ in Ω, deren Spur nicht durch p theilbar ist. Geht dann aber auch p nicht in Q auf, so kann man x aus

$$x \equiv 0 \pmod{Q}, \quad x S(\xi) + a' \equiv 0 \pmod{p}$$

bestimmen, und dann ist $1 + p^\lambda x\xi$ in $\mathfrak{o}'$ enthalten.

Geht aber p nicht im Körpergrad n auf, so kann man $\xi = 1$, also $S(\xi) = n$ annehmen, und hat x aus der Congruenz

$$nx \equiv a' \pmod{p}$$

zu bestimmen, und $1 + p^\lambda x$ ist als rationale Zahl immer in $\mathfrak{o}'$ enthalten. Wir sprechen also den Satz aus:

5. *Geht p nicht in $Q\Delta$ oder nicht in n auf, und ist die Congruenz*

$$N(\omega') \equiv a \pmod{p}$$

lösbar, so ist auch

$$N(\omega') \equiv a \pmod{p^\lambda}$$

für jedes positive λ lösbar.

Wir haben daher den folgenden Satz:

6. *Die Primzahlen, die nicht in $Q\Delta$ aufgehen, kommen nicht unter den charakteristischen Primzahlen der Ordnung $\mathfrak{o}'$ vor. Ein Primfactor p, der in Q oder in Δ aber nicht in n aufgeht, kommt nur dann unter den charakteristischen Primzahlen vor, wenn $p - 1$ und n oder $p - 1$ und g nicht relativ prim sind, und von diesen Primzahlen ist die erste Potenz die charakteristische Potenz. Es ist, wenn δ der grösste gemeinschaftliche Theiler von $p - 1$ und n oder von $p - 1$ und g ist*

(13) $$(P, P') = \delta.$$

Wenn aber p in $Q\Delta$ und zugleich in n aufgeht, so können wir für die charakteristische Potenz von p im Allgemeinen eine obere Grenze angeben. Es sei

$$n = p^{\varkappa} n' \tag{14}$$

und n' nicht durch p theilbar. Die Aufgabe ist dann die, den niedrigsten Exponenten λ zu bestimmen, so dass aus der Congruenz

$$N(\omega) \equiv a \pmod{p^{\lambda}} \tag{15}$$

die Möglichkeit derselben Congruenz für jede höhere Potenz von p als Modul folgt.

Ist ω' eine Lösung von (15) in $\mathfrak{o}'$, so setzen wir

$$\eta = \omega'(1 + p^{\lambda-\varkappa} x),$$

worin x eine rationale Zahl bedeutet. Wenn ω' in $\mathfrak{o}'$ enthalten ist, so ist auch η darin enthalten. Ist nun

$$N(\omega') = a + a' p^{\lambda},$$

so folgt

$$N(\eta) = (a + a' p^{\lambda})(1 + p^{\lambda-\varkappa} x)^n,$$

und wenn wir λ so annehmen, dass $2(\lambda - \varkappa) > \lambda$, also

$$\lambda > 2\varkappa \tag{16}$$

ist, so folgt

$$N(\eta) = a + (n' a x + a') p^{\lambda} \pmod{p^{\lambda+1}}. \tag{17}$$

Wenn also x aus

$$n' a x + a' \equiv 0 \pmod{p}$$

bestimmt wird, so folgt

$$N(\eta) \equiv a \pmod{p^{\lambda+1}}.$$

Hiervon ist (16) die einzige Bedingung, und es ergiebt sich:

> 7. *Ist p in n und in $Q\Delta$ enthalten, und ist n durch $p^{\varkappa}$, aber durch keine höhere Potenz von p theilbar, so ist der Exponent der charakteristischen Potenz p^{λ} höchstens gleich $2\varkappa + 1$.*

Die Grenze für λ lässt sich unter Umständen noch etwas weiter herunterdrücken. Bemerkt man nämlich, dass in der Entwickelung der n^{ten} Potenz des Binoms $1 + p^{\lambda-\varkappa} x$ alle auf den ersten folgenden Binomialcoefficienten bis zum p^{ten} einschliesslich durch $p^{\varkappa}$ theilbar sind, so erkennt man, dass die Congruenz (17) auch noch unter der Voraussetzung

$$p(\lambda - \varkappa) > \lambda$$

gilt.

Es ist also λ *höchstens* gleich der zunächst über

$$\frac{p\varkappa}{p-1} \tag{18}$$

gelegenen ganzen Zahl. Dies ist für $\varkappa = 1$, $p = 2$, in Uebereinstimmung

stimmung mit dem Satze 7 die Zahl 3; dagegen für $\varkappa = 1$, $p > 2$ die Zahl 2.

Aber auch für $p = 2$ lässt sich in manchen Fällen die Grenze für λ noch erniedrigen. Für $p = 2$ giebt der Ausdruck (18) $2\varkappa + 1$ als obere Grenze für λ. Wir wollen untersuchen, ob nicht $\lambda = 2\varkappa$ schon genügen kann.

Da Ω ein Normalkörper ist, so gehört die Quadratwurzel aus der Grundzahl, $\sqrt{\Delta}$, dem Körper selbst an. Diese Wurzel kann rational sein, und muss es immer sein, wenn n ungerade ist. Bei geradem n kann $\sqrt{\Delta}$ auch irrational sein, und dann hat die Gruppe Φ einen Theiler Φ' vom Grade $\frac{1}{2}n$, durch deren Substitutionen $\sqrt{\Delta}$ ungeändert bleibt, während es durch die andere Hälfte der Substitutionen Φ sein Zeichen ändert. Es sei unter dieser Voraussetzung

$$n = 2^{\varkappa} n', \quad Q = 2^{\varkappa_1} Q', \quad \Delta = 2^{\varkappa_1} \Delta' \tag{19}$$

worin n', Q', Δ' ungerade sind.

Es handelt sich also noch um die Frage, unter welchen Voraussetzungen aus der Congruenz

$$N(\omega') \equiv a \pmod{2^{2\varkappa}}$$

die Möglichkeit derselben Congruenz für den Modul $2^{2\varkappa+\iota}$ folgt. Hierin bedeutet ω' eine Zahl in $\mathfrak{o}'$, und wir setzen

$$N(\omega') = a + 2^{2\varkappa} a', \tag{20}$$

$$\eta = \omega'(1 + 2^{\frac{\varkappa - \varkappa_2 + 1}{2}} Q' \sqrt{\Delta}\, x). \tag{21}$$

Diese Zahl gehört für jedes rationale x dem Körper Ω an, wenn $(\varkappa - \varkappa_2 + 1) : 2$ eine ganze Zahl, also

$$\varkappa_2 \equiv \varkappa + 1 \pmod{2} \tag{22}$$

vorausgesetzt wird. Die Zahl η wird aber auch der Ordnung $\mathfrak{o}'$ angehören, wenn

$$2^{\frac{\varkappa - \varkappa_2 + 1}{2}} Q' \sqrt{\Delta} = 2^{\frac{\varkappa + 1}{2}} Q' \sqrt{\Delta'}$$

eine nach den Modul Q mit einer rationalen Zahl congruente ganze Zahl ist, oder wenn

$$2^{\frac{\varkappa+1}{2}} \sqrt{\Delta'}$$

nach dem Modul $2^{\varkappa_1}$ mit einer rationalen Zahl congruent ist. Es ist hierbei zu unterscheiden, ob $\Delta' \equiv 1$ oder $\equiv 3 \pmod 4$ ist; denn im ersten Fall ist $\frac{1}{2}(\sqrt{\Delta'} - 1)$ eine ganze Zahl, im zweiten Falle nicht.

Es muss daher im ersten Fall

$$2^{\frac{\varkappa+3}{2}}\frac{\sqrt{\Delta'}-1}{2}$$

nach dem Modul $2^{\varkappa_1}$ mit einer rationalen Zahl congruent sein, was nur möglich ist, wenn

$$\frac{\varkappa+3}{2} \geqq \varkappa_1$$

und im zweiten muss

$$\frac{\varkappa+1}{2} \geqq \varkappa_1$$

sein. Man hat also zwei Fälle

(23)
$$\begin{aligned} &\text{a)}\quad \Delta' \equiv 1 \pmod 4, \quad \varkappa_2 \equiv \varkappa+1 \pmod 2, \quad \varkappa_1 \leqq \tfrac{\varkappa+3}{2}, \\ &\text{b)}\quad \Delta' \equiv 3 \pmod 4, \quad \varkappa_2 \equiv \varkappa+1 \pmod 2, \quad \varkappa_1 \leqq \tfrac{\varkappa+1}{2}, \end{aligned}$$

In beiden Fällen ist nach (21)

$$\begin{aligned} N(\eta) &= N(\omega')(1-2^{\varkappa+1}Q'^2\Delta' x^2)^{\frac{n}{2}}, \\ N(\eta) &\equiv (a+2^{\frac{1}{2}\varkappa}a')\,(1-2^{2\varkappa}Q'^2\Delta' n' x^2) \pmod{2^{2\varkappa+1}} \\ &\equiv a+2^{2\varkappa}(a'-aQ'^2\Delta' n' x^2) \pmod{2^{2\varkappa+1}} \end{aligned}$$

und es wird also, wenn $x \equiv a' \pmod 2$ angenommen wird,

$$N(\eta) \equiv a \pmod{2^{2\varkappa+1}}.$$

In diesen Fällen ist also die charakteristische Potenz von 2 höchstens $2^{2\varkappa}$.

Nehmen wir $\varkappa = 1$ an, so ergeben sich folgende Fälle, in denen die charakteristische Potenz von 2 höchstens $= 4$ ist.

(24)
$$\begin{aligned} &\text{a)}\quad \Delta' \equiv 1 \pmod 4, \quad \varkappa_2 \equiv 0 \pmod 2, \quad \varkappa_1 = 0, 1, 2, \\ &\text{b)}\quad \Delta' \equiv 3 \pmod 4, \quad \varkappa_2 \equiv 0 \pmod 2, \quad \varkappa_1 = 0, 1. \end{aligned}$$

Im Falle a) scheiden aber noch die Werthe $\varkappa_1 = 0, 1$ aus, in denen 2 überhaupt nicht unter den charakteristischen Primzahlen vorkommt. Denn in diesen Fällen ist

$$\omega = x + yQ'\sqrt{\Delta'}$$

für jedes ganze rationale x, y eine Zahl in $\mathfrak{o}'$ und es ist

$$N(\omega) = (x^2 - y^2 Q'^2 \Delta')^{n'}.$$

Je nachdem man nun x gerade und y ungerade oder x ungerade und y gerade annimmt, ist

$$N(\omega) \equiv -1 \quad \text{oder} \quad \equiv +1 \pmod 4.$$

Folglich ist die Congruenz

$$N(\omega) \equiv a \pmod 4$$

für jedes ungerade a in $\mathfrak{o}'$ lösbar.

Für einen *quadratischen Körper* Ω ist im Falle a) $\varkappa_2 = 0$, im Falle b) $\varkappa_2 = 2$, und es ergeben sich folgende drei Fälle, in denen 4 die charakteristische Potenz von 2 ist.

1) $\Delta' \equiv 1, \quad \Delta = \Delta', \quad Q = 4Q', \quad D = Q^2\Delta = 16Q'^2\Delta',$
2) $\Delta' \equiv 3, \quad \Delta = 4\Delta', \quad Q = Q', \quad D = Q^2\Delta = 4Q'^2\Delta',$
3) $\Delta' \equiv 3, \quad \Delta = 4\Delta', \quad Q = 2Q', \quad D = Q^2\Delta = 16Q'^2\Delta'.$

Die Gauss'sche Determinante ∇ der entsprechenden quadratischen Formen ist in diesen Fällen, wo D und also auch b gerade ist, gleich $\frac{1}{4}D$ (§ 5), und wir bekommen also

im Falle 1. $\nabla = 4Q'^2\Delta' \equiv 4 \pmod{16}$,
im Falle 2. $\nabla = Q'^2\Delta' \equiv 3 \pmod{4}$,
im Falle 3. $\nabla = 4Q'^2\Delta' \equiv 12 \pmod{16}$,

in denen 4 die charakteristische Potenz von 2 ist (in vollkommener Uebereinstimmung mit den Sätzen von Gauss über die Classencharaktere. Disq. ar. art. 228 f., Dirichlet-Dedekind, Zahlentheorie, 4. Auflage § 121).

Strassburg, 31. August 1896.