

Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN30976923X

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN30976923X>

OPAC: <http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X>

LOG Id: LOG_0163

LOG Titel: X. Ueber die Composition der binären quadratischen Formen.

LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

X. Ueber die Composition der binären quadratischen Formen.

§. 145.

Den Ausgangspunct für unsere Darstellung der von *Gauss**) gegründeten Theorie der Composition bildet folgendes Lemma:

Ist

$$bb \equiv D \pmod{a}, \quad b'b' \equiv D \pmod{a'}, \quad (1)$$

und haben die drei Zahlen $a, a', b + b'$ keinen gemeinschaftlichen Theiler, so existirt in Bezug auf den Modulus aa' eine und nur eine Classe von Zahlen B , welche den drei Bedingungen

$$B \equiv b \pmod{a}, \quad B \equiv b' \pmod{a'}, \quad BB \equiv D \pmod{aa'} \quad (2)$$

genügen.

Dies leuchtet unmittelbar ein, falls a und a' relative Primzahlen sind (§§. 25, 37); unter der allgemeineren Voraussetzung aber, dass $a, a', b + b'$ keinen gemeinschaftlichen Theiler haben, bestimme man (nach §. 24) drei ganze Zahlen h, h', h'' , welche die Bedingung

$$ha + h'a' + h''(b + b') = 1 \quad (3)$$

befriedigen; dann werden alle durch die Congruenz

$$B \equiv hab' + h'a'b + h''(bb' + D) \pmod{aa'} \quad (4)$$

bestimmten Zahlen B und nur diese den Forderungen (2) genügen. Da nämlich

*) *D. A.* art. 234 seqq. — Vergl. *Lejeune Dirichlet: De formarum binariarum secundi gradus compositione.* 1851.

$$(B-b)(B-b') = BB - (b+b')B + bb'$$

ist, so folgt zunächst, dass die Forderungen (2) vollständig übereinstimmen mit den folgenden

$$a'B \equiv a'b, aB \equiv ab', (b+b')B \equiv bb' + D \pmod{aa'}, \quad (5)$$

welche, mit h', h, h'' multiplicirt und addirt, die Congruenz (4) nach sich ziehen. Dass umgekehrt jede durch die Congruenz (4) bestimmte Zahl B den Bedingungen (2) oder (5) genügt, ergibt sich leicht, wenn man aus (3) und (4) der Reihe nach h', h, h'' eliminirt und hierbei die Voraussetzungen (1) berücksichtigt.

Wir bemerken schliesslich, dass die Zahlen $a, a', 2B$ keinen gemeinschaftlichen Theiler haben; denn ist δ ein solcher, so folgt aus (2) auch $b \equiv b' \equiv B \pmod{\delta}$, also $b + b' \equiv 2B \equiv 0 \pmod{\delta}$; mithin ist δ gemeinschaftlicher Theiler von $a, a', b + b'$, und folglich $\delta = 1$.

§. 146.

Zwei binäre quadratische Formen $(a, b, c), (a', b', c')$ von gleicher Determinante D sollen *einig**) heissen, wenn die Zahlen $a, a', b + b'$ keinen gemeinschaftlichen Theiler haben. Da unter dieser Voraussetzung auch $bb \equiv D \pmod{a}, b'b' \equiv D \pmod{a'}$ ist, so folgt aus dem vorhergehenden Lemma unmittelbar die Existenz von unendlich vielen (nach §. 56 äquivalenten) Formen (aa', B, C) derselben Determinante D , deren mittlere Coefficienten B den Bedingungen $B \equiv b \pmod{a}, B \equiv b' \pmod{a'}$ genügen; jede solche Form (aa', B, C) heisse *zusammengesetzt****) (*composita*) aus (a, b, c) und (a', b', c') .

Wir bemerken zunächst, dass (nach §. 56) die Formen $(a, b, c), (a', b', c')$ resp. den Formen $(a, B, a' C), (a', B, a C)$ äquivalent sind; diese letzteren sind ebenfalls einig, weil die Zahlen $a, a', 2B$ keinen gemeinschaftlichen Theiler haben (§. 145), und aus ihnen ist ebenfalls die Form (aa', B, C) zusammengesetzt. Bedeuten nun x, y, x', y' variable Grössen, und setzt man

*) Diese Benennung soll an die *radices concordantes* von Dirichlet erinnern.

**) Vergl. Gauss: *D. A.* artt. 235, 242, 243, 244.

$$X = xx' - Cy'y', \quad Y = (ax + By)y' + (a'x' + B'y')y, \quad (1)$$

so wird

$$(ax + (B + \sqrt{D})y)(a'x' + (B + \sqrt{D})y') = aa'X + (B + \sqrt{D})Y; \quad (2)$$

ersetzt man hierin \sqrt{D} durch $-\sqrt{D}$ und multiplicirt die so entstehende Gleichung mit der vorstehenden, so ergiebt sich nach Wegwerfung des beiden Seiten gemeinschaftlichen Factors aa' die Gleichung

$$\begin{aligned} (ax^2 + 2Bxy + a'Cy^2)(a'x'^2 + 2B'x'y' + a'Cy'^2) \\ = aa'X^2 + 2BXY + CY^2, \end{aligned} \quad (3)$$

d. h. die Form (aa', B, C) geht durch die bilineare Substitution (1) in das Product aus den beiden Formen $(a, B, a' C)$, $(a', B, a C)$ über.

Auf dem vorstehenden Resultate beruht zugleich der Beweis des folgenden Fundamentalsatzes*):

Sind die beiden einigen Formen (a, b, c) , (a', b', c') resp. äquivalent den beiden einigen Formen (m, n, l) , (m', n', l') , so ist auch die aus den beiden ersteren zusammengesetzte Form (aa', B, C) äquivalent der aus den beiden letzteren zusammengesetzten Form (mm', N, L) .

Aus den Voraussetzungen folgt zunächst, dass die Formen $(a, B, a' C)$, $(a', B, a C)$ resp. den Formen $(m, N, m' L)$, $(m', N, m L)$ äquivalent sind, und hieraus (nach §. 60. Anmerkung) die Existenz von vier ganzen Zahlen x, y, x', y' , welche den folgenden Bedingungen genügen

$$ax^2 + 2Bxy + a'Cy^2 = m, \quad a'x'^2 + 2B'x'y' + a'Cy'^2 = m' \quad (4)$$

$$ax + (B + N)y \equiv 0, \quad (B - N)x + a'Cy \equiv 0 \pmod{m} \quad (5)$$

$$a'x' + (B + N)y' \equiv 0, \quad (B - N)x' + a'Cy' \equiv 0 \pmod{m'}, \quad (6)$$

und ebenso braucht man, um die Aequivalenz der beiden Formen (aa', B, C) , (mm', N, L) darzuthun, nur die Existenz von zwei ganzen Zahlen X, Y nachzuweisen, welche die Forderungen

$$aa'X^2 + 2BXY + CY^2 = mm' \quad (7)$$

$$aa'X + (B + N)Y \equiv 0 \pmod{mm'} \quad (8)$$

$$(B - N)X + CY \equiv 0 \pmod{mm'} \quad (9)$$

befriedigen. Es lässt sich nun leicht zeigen, dass die beiden (offenbar ganzen) Zahlen X, Y , welche nach (1) aus den vier ganzen

*) Gauss: D. A. art. 239. — Dirichlet a. a. O.

Zahlen x, y, x', y' gebildet sind, in der That den vorstehenden Bedingungen genügen. Zunächst folgt (7) unmittelbar aus (3) und (4). Da ferner aus jeder Gleichung von der Form

$$(t + u \vee D) (t' + u' \vee D) = (t'' + u'' \vee D) (t''' + u''' \vee D),$$

wo t, u, t' u. s. w. ganze Zahlen bedeuten, die in Bezug auf die Variable z identische Gleichung

$$(t + uz) (t' + u'z) = (t'' + u''z) (t''' + u'''z) + (uu' - u''u''') (zz - D),$$

und hieraus, da $NN \equiv D \pmod{mm'}$ ist, auch die Congruenz

$$(t + uN) (t' + u'N) \equiv (t'' + u''N) (t''' + u'''N) \pmod{mm'}$$

hervorgeht, so folgt (8) unmittelbar aus (2) unter Berücksichtigung von (5) und (6). Dieselbe Gleichung (2) lässt sich endlich durch Multiplication mit $B - \vee D$, oder mit C , und durch Division mit a oder mit a' auf die folgenden vier Formen bringen

$$((B - \vee D)x + a' Cy) (a' x' + (B + \vee D)y') = a' U$$

$$(ax + (B + \vee D)y) ((B - \vee D)x' + a Cy') = a U$$

$$((B - \vee D)x + a' Cy) ((B - \vee D)x' + a Cy') = (B - \vee D) U$$

$$C(ax + (B + \vee D)y) (a' x' + (B + \vee D)y') = (B + \vee D) U,$$

wo zur Abkürzung

$$(B - \vee D) X + C Y = U$$

gesetzt ist; ersetzt man überall $\vee D$ durch N , so gehen nach dem oben angeführten Princip diese Gleichungen wieder in Congruenzen nach dem Modulus mm' über; bezeichnet man den aus U hervorgehenden Ausdruck, d. h. die linke Seite der zu beweisenden Congruenz (9), mit V , so ergibt sich unter Berücksichtigung von (5) und (6), dass die Producte $a' V, a V, (B - N) V, (B + N) V$, mithin auch $2B V$ durch mm' theilbar sind; da aber die Factoren $a, a', 2B$ keinen gemeinschaftlichen Theiler haben, so muss der andere Factor V für sich allein durch mm' theilbar sein, also die Congruenz (9) wirklich Statt finden.

Mithin genügen die beiden ganzen Zahlen X, Y den Bedingungen (7), (8), (9), und hieraus folgt (nach §. 60. Anmerkung) die Aequivalenz der Formen $(aa', B, C), (mm', N, L)$; was zu beweisen war.

§. 147.

Um den Charakter des eben bewiesenen Fundamentalsatzes in das rechte Licht zu setzen, bemerken wir zunächst Folgendes: Sind (a, b, c) , (a', b', c') zwei einige Formen, so sind ihre Theiler σ , σ' (§. 61) relative Primzahlen, und $\sigma\sigma'$ ist der Theiler der aus ihnen zusammengesetzten Form $(aa' B, C)$. Denn da die Formen (a, b, c) , (a', b', c') resp. den Formen $(a, B, a' C)$, $(a', B, a C)$ äquivalent sind, so ist (nach §. 61) σ der grösste gemeinschaftliche Divisor von $a, 2B, a' C$, und σ' ist der grösste gemeinschaftliche Divisor von $a', 2B, a C$; da nun $a, a', 2B$ keinen gemeinschaftlichen Divisor haben, so muss die in a und $2B$ aufgehende Zahl σ relative Primzahl zu a' (und also auch zu der in a' aufgehenden Zahl σ') sein; und da σ in $a' C$ aufgeht, so muss σ auch in C aufgehen; ebenso muss σ' relative Primzahl zu a sein und folglich auch in C aufgehen. Da ferner schon gezeigt ist, dass σ und σ' relative Primzahlen sind, und da beide sowohl in $2B$, als auch in C aufgehen, so ist $\sigma\sigma'$ offenbar gemeinschaftlicher Divisor der drei Zahlen $aa', 2B, C$. Wollte man nun annehmen, $\sigma\sigma'$ wäre nicht ihr grösster gemeinschaftlicher Divisor, sondern sie liessen sich nach der Division mit $\sigma\sigma'$ noch durch eine Primzahl p theilen, so müsste p wenigstens in einer der beiden Zahlen $a:\sigma$ oder $a':\sigma'$ aufgehen; gesetzt aber, p ginge in $a:\sigma$ auf, so hätten die drei Zahlen $a, 2B, a' C$ den gemeinschaftlichen Divisor $p\sigma$, während doch σ ihr grösster gemeinschaftlicher Divisor ist. Ebenso wenig kann p in $a':\sigma'$ aufgehen, und folglich ist $\sigma\sigma'$ der grösste gemeinschaftliche Divisor der Zahlen $aa', 2B, C$, d. h. $\sigma\sigma'$ ist der Theiler der Form (aa', B, C) , was zu beweisen war.

Umgekehrt: hat man zwei Formenklassen K, K' von gleicher Determinante D , deren Theiler σ, σ' relative Primzahlen sind, so kann man stets zwei einige Formen (a, b, c) , (a', b', c') resp. aus den Classen K, K' auswählen. Denn man kann (nach §. 93) den Repräsentanten (a, b, c) der Classe K zunächst so wählen, dass a relative Primzahl zu σ' wird, worauf der Repräsentant (a', b', c') der Classe K' so gewählt werden kann, dass a' relative Primzahl zu a wird; dann sind aber (a, b, c) , (a', b', c') gewiss zwei einige Formen. Wie nun auch zwei einige Formen aus den Classen K, K'

ausgewählt sein mögen, so wird zufolge des bewiesenen Fundamentalsatzes die aus ihnen zusammengesetzte Form stets einer und derselben Formenklasse \mathfrak{R} von derselben Determinante D angehören, deren Theiler nach dem Obigen $= \sigma \sigma'$ ist. Wir werden daher sagen, dass diese Classe \mathfrak{R} aus den beiden einigen Classen K, K' zusammengesetzt ist, und werden dies durch die symbolische Gleichung*)

$$\mathfrak{R} = KK' = K'K$$

ausdrücken.

Sind ferner je zwei der drei Classen K, K', K'' einig, so lassen sie sich successive zu einer Classe zusammensetzen, und zwar wird diese resultirende Classe von der Anordnung der beiden successiven Compositionen völlig unabhängig sein**); d. h. symbolisch ausgedrückt, es wird

$$(KK')K'' = (KK'')K' = (K'K'')K$$

sein. Man kann nämlich die Repräsentanten $(a, b, c), (a', b', c'), (a'', b'', c'')$ der drei Classen K, K', K'' (nach §. 93) so wählen, dass a, a', a'' relative Primzahlen sind; bestimmt man nun (nach §. 25) B durch die Congruenzen

$$B \equiv b \pmod{a}, \quad B \equiv b' \pmod{a'}, \quad B \equiv b'' \pmod{a''},$$

so wird von selbst $BB \equiv D \pmod{a a' a''}$, also $D = BB - a a' a'' C$, wo C eine ganze Zahl bedeutet. Dann enthält

die Classe K	die Form $(a, B, a' a'' C)$
„ „ K'	„ „ $(a', B, a a'' C)$
„ „ K''	„ „ $(a'', B, a a' C)$
„ „ KK'	„ „ $(a a', B, a'' C)$
„ „ KK''	„ „ $(a a'', B, a' C)$
„ „ $K'K''$	„ „ $(a' a'', B, a C)$

und jede der Classen $(KK')K'', (KK'')K', (K'K'')K$ enthält folglich dieselbe Form $(a a' a'', B, C)$; mithin sind diese drei Classen identisch. Diese eine Classe kann daher einfach durch das Symbol $KK'K''$ bezeichnet werden, wobei die Stellung der drei Symbole K, K', K'' gleichgültig ist.

Wendet man nun dieselbe Schlussfolgerung an, wie in §. 2, so ergibt sich, dass auch für jede grössere Anzahl von Classen

*) Gauss bezeichnet die aus K und K' zusammengesetzte Classe mit $K + K'$ (D. A. art. 249).

***) Gauss: D. A. artt. 240, 241.

$K, K' \dots$ die durch ihre successive Composition entstehende Classe völlig bestimmt, und von der Anordnung der Composition gänzlich unabhängig ist. Erforderlich bleibt aber die Bedingung, dass diese Classen $K, K' \dots$ zu derselben Determinante gehören, und dass ihre Theiler $\sigma, \sigma' \dots$ relative Primzahlen sind, weil nur dann die Composition in der oben angegebenen Art ausgeführt werden kann; für unsere Zwecke reicht aber dieser specielle Fall der allgemeineren Theorie der Composition völlig aus.

§. 148.

Wir betrachten zunächst einige besonders wichtige specielle Fälle der Classencomposition*).

1. Die Hauptform $(1, 0, -D)$ ist offenbar einig mit jeder Form (a, b, c) derselben Determinante, und die Composition beider Formen giebt als Resultat dieselbe Form (a, b, c) , also: *Durch Composition irgend einer Classe K mit der Hauptclasse entsteht immer die Classe K .* Bezeichnet man daher die Hauptclasse durch das Symbol 1, so ist immer $1K = K$, wo K eine beliebige Classe bedeutet.

2. Ist (a, b, c) eine ursprüngliche Form der ersten Art, so ist sie einig mit der Form (c, b, a) , und aus beiden ist die Form $(ac, b, 1)$ zusammengesetzt. Da nun (c, b, a) mit $(a, -b, c)$, und ebenso $(ac, b, 1)$ mit $(1, -b, ac)$ und folglich auch mit der Hauptform $(1, 0, -D)$ äquivalent ist (§. 56), so kann man dies Resultat kurz so aussprechen: *Die Composition von zwei entgegengesetzten ursprünglichen Classen der ersten Art H, H' giebt stets die Hauptclasse $HH' = 1$.*

Hieraus ziehen wir eine wichtige Folgerung, von welcher sehr häufig Gebrauch gemacht wird: *Bedeutet H eine ursprüngliche Classe erster Art, so folgt aus $HK = HL$ auch stets $K = L$.* Ist nämlich H' der Classe H entgegengesetzt, also $HH' = 1$, so folgt aus $HK = HL$ zunächst $(HK)H' = (HL)H'$, und hieraus $(HH')K = (HH')L$, also $K = L$.

*) Gauss: D. A. artt. 243, 250.

3. Ist K eine Classe vom Theiler σ , so kann man (nach §. 93) ihren Repräsentanten $(a\sigma, b, c)$ so wählen, dass a relative Primzahl zu σ ist; dann ist diese Form offenbar zusammengesetzt aus den beiden einzigen Formen $(a, b, c\sigma)$ und (σ, b, ac) , deren letztere den Theiler σ hat und der einfachsten Classe dieses Theilers angehört (§. 61), woraus von selbst folgt, dass die erstere Form eine ursprüngliche Form der ersten Art sein muss, was sich auch leicht direct nachweisen liesse. Wir haben daher das Resultat: *Ist S die einfachste, und K irgend eine Classe vom Theiler σ , so giebt es immer mindestens eine ursprüngliche Classe erster Art H von der Beschaffenheit, dass $SH = K$ ist.*

Man überzeugt sich leicht mit Hülfe von 2., dass der Satz 3. auch dann noch gilt, wenn S und K irgend welche Classen desselben Theilers bedeuten; ebenso leuchtet ein, dass aus den einfachsten Classen der Theiler σ, σ' stets die einfachste Classe des Theilers $\sigma\sigma'$ zusammengesetzt ist, natürlich unter der Voraussetzung, dass σ und σ' relative Primzahlen sind. Wir verweilen aber nicht länger bei diesen und anderen ebenso leicht zu beweisenden Sätzen, weil sie für die nachfolgenden Untersuchungen völlig entbehrlich sind.

§. 149.

Durch Composition einer *ursprünglichen Classe der ersten Art A* mit sich selbst, oder kürzer, durch *Duplication**) der Classe A entsteht eine Classe AA , welche man auch durch A^2 bezeichnen kann; ähnlich ist die allgemeine Bezeichnung A^m zu verstehen, wo m irgend eine positive ganze Zahl bedeutet. Durch Anwendung derselben Schlüsse, wie in §. 28, findet man nun leicht, dass immer ein kleinster positiver Exponent δ existirt, welcher der Bedingung $A^\delta = 1$ genügt; dann sind die Classen

$$1, A, A^2 \dots A^{\delta-1},$$

welche die sogenannte *Periode****) der Classe A bilden, von einander verschieden; aus $A^r = A^s$ folgt $r \equiv s \pmod{\delta}$, und umgekehrt; verallgemeinert man hiernach die Bezeichnung A^m , in-

*) Gauss: D. A. art. 249.

**) Gauss: D. A. art. 306. II.

dem man sie auch auf negative Exponenten m (und auf $m = 0$) ausdehnt, so ist z. B. $A^{-1} = A^{d-1}$ das Symbol für die Classe, welche der Classe A entgegengesetzt ist (§. 148, 2.).

Eine solche Classenperiode bildet nur einen speciellen Fall des folgenden neuen Begriffs, welcher von der höchsten Wichtigkeit für die Gesetze der Composition ist: Ein System \mathfrak{A} von ursprünglichen Classen der ersten Art soll eine *Gruppe**) heissen, wenn die Composition von je zwei Classen des Systems \mathfrak{A} immer wieder eine Classe desselben Systems liefert; die Anzahl a der in \mathfrak{A} enthaltenen verschiedenen Classen heisse der *Grad* dieser Gruppe \mathfrak{A} .

Aus dieser Erklärung folgt sofort, dass, wenn die Classe A in einer Gruppe \mathfrak{A} enthalten ist, auch die ganze Periode der Classe A , also auch die entgegengesetzte Classe A^{-1} und die Hauptclasse sich in \mathfrak{A} vorfindet. Setzt man ferner jede in der Gruppe \mathfrak{A} enthaltene Classe $A_1, A_2 \dots A_a$ mit einer ursprünglichen Classe erster Art B zusammen, so sind die entstehenden Classen $A_1 B, A_2 B \dots A_a B$ von einander verschieden (§. 148, 2.) und bilden einen Complex, den wir kurz durch $\mathfrak{A}B$ bezeichnen können; zwei so gebildete Complexe $\mathfrak{A}B$ und $\mathfrak{A}B'$ sind nun entweder vollständig identisch (was wieder durch das Zeichen $=$ angedeutet werden soll), oder sie haben keine einzige gemeinschaftliche Classe; denn wenn sie eine gemeinschaftliche Classe $AB = A'B'$ haben, wo A und A' in \mathfrak{A} enthalten sind, so folgt $B = A^{-1}A'B' = A''B'$, wo $A'' = A^{-1}A'$ eine ebenfalls in \mathfrak{A} enthaltene Classe bedeutet, und hieraus $\mathfrak{A}B = \mathfrak{A}A''B' = \mathfrak{A}B'$, weil offenbar der Complex $\mathfrak{A}A''$ mit \mathfrak{A} selbst identisch ist.

Stützt man sich auf diese fundamentale Eigenschaft einer Gruppe und wendet dieselbe Schlussfolgerung an, wie in §. 127, so ergibt sich unmittelbar folgender Satz:

Sind alle a Classen einer Gruppe \mathfrak{A} zugleich in einer Gruppe \mathfrak{B} vom Grade b enthalten, so ist a ein Divisor von $b = \mu a$, und die Gruppe \mathfrak{B} besteht aus μ Complexen von der Form $\mathfrak{A}B$; die Gruppe \mathfrak{A} soll daher auch ein *Divisor* der Gruppe \mathfrak{B} , letztere ein *Multiplum* der ersteren heissen.

*) Ich wähle absichtlich diese von *Galois* in die Algebra eingeführte Benennung, weil seine Theorie und die obige, welche den sogenannten *Abel'schen* Gleichungen entspricht, gemeinschaftlich enthalten sind in der allgemeineren Theorie der Composition, in welcher $(KK')K'' = K(K'K'')$ ist, und ausserdem sowohl aus $KK' = KK''$, als auch aus $K'K = K''K$ stets $K' = K''$ folgt (vergl. §. 55).

Sind ferner \mathfrak{A} und \mathfrak{B} zwei beliebige Gruppen, so bildet das System \mathfrak{D} aller in \mathfrak{A} und \mathfrak{B} gemeinschaftlich enthaltenen Classen ebenfalls eine Gruppe, welche der grösste gemeinschaftliche Divisor von \mathfrak{A} und \mathfrak{B} heissen mag; sind a, b, d die Grade dieser drei Gruppen, so ist d ein gemeinschaftlicher Divisor von $a = \alpha d$ und $b = \beta d$; besteht ferner die Gruppe \mathfrak{B} aus den β Complexen $\mathfrak{D} B_1, \mathfrak{D} B_2 \dots \mathfrak{D} B_\beta$, so bilden, wie man leicht erkennt, auch die β Complexen $\mathfrak{A} B_1, \mathfrak{A} B_2 \dots \mathfrak{A} B_\beta$ eine Gruppe \mathfrak{M} vom Grade $m = a\beta = b\alpha = ab:d$, und zwar ist diese Gruppe \mathfrak{M} das kleinste gemeinschaftliche Multiplum der beiden Gruppen \mathfrak{A} und \mathfrak{B} *).

Die am leichtesten zu überblickenden Gruppen sind die oben erwähnten Perioden; jede solche Gruppe, deren Classen durch wiederholte Composition aus einer einzigen Classe entstehen, wollen wir eine *reguläre* Gruppe nennen; jede *irreguläre* Gruppe lässt sich als das kleinste Multiplum von gewissen regulären Gruppen darstellen, von denen je zwei nur die Hauptclasse gemeinschaftlich haben. Auf diese Darstellung und die damit zusammenhängenden Sätze von *Gauss***), deren Beweis leicht auf das Vorhergehende gegründet werden kann, wollen wir aber hier nicht mehr eingehen.

§. 150.

Eine der hauptsächlichsten Anwendungen, welche *Gauss* von der Theorie der Composition gemacht hat, besteht in der Vergleichung der Anzahl h' der Classen vom Theiler σ mit der Anzahl h der ursprünglichen Classen erster Art***); offenbar ist dies dieselbe Aufgabe, welche Dirichlet in der oben mitgetheilten Art (§§. 97, 99, 100) gelöst hat.

Bedeutet S die einfachste, und K irgend eine Classe vom Theiler σ , so existirt (nach §. 148, 3.) *mindestens* eine ursprüngliche Classe erster Art H , welche mit S componirt die Classe K

*) Dieser Satz verliert seine allgemeine Gültigkeit, wenn die *Ordnung* der zusammensetzenden Elemente einen Einfluss auf das Compositum hat.

**) *D. A.* artt. 305 — 307; ferner *Démonstration de quelques théorèmes concernant les périodes des classes des formes binaires du second degré* (*Gauss* Werke, Bd. II. p. 266. 1863). — Vergl. *Schering: Die Fundamental-Classen der zusammensetzbaren arithmetischen Formen.* Göttingen 1869.

***) *D. A.* artt. 253 — 256.

hervorbringt; durch Composition von S mit allen h Classen H müssen also jedenfalls alle Classen K vom Theiler σ , jede mindestens einmal erzeugt werden. Es seien nun $R_1, R_2 \dots R_r$ die sämmtlichen r von einander verschiedenen ursprünglichen Classen erster Art, welche mit S componirt die Classe S selbst hervorbringen; da aus $SR = S$ und $SR' = S$ auch $S(RR') = S$ folgt, so bilden diese r Classen eine Gruppe \mathfrak{R} vom Grade r ; und da das System aller h ursprünglichen Classen erster Art ebenfalls eine Gruppe \mathfrak{S} bildet, welche ein Multiplum der Gruppe \mathfrak{R} ist (§. 149), so ist $h = rk$, und die Gruppe \mathfrak{S} zerfällt in k Complexe von der Form $\mathfrak{R}H$; alle r Classen eines solchen Complexes $\mathfrak{R}H$ geben, mit S componirt, eine und dieselbe Classe SH vom Theiler σ ; und umgekehrt, wenn $SH' = SH$ ist, so folgt $SH'H^{-1} = S$, also ist $H'H^{-1} = R$ in \mathfrak{R} , mithin $H' = RH$ in dem Complex $\mathfrak{R}H$ enthalten. Die Anzahl h' der verschiedenen Classen vom Theiler σ ist daher $= k$, und wir sind also zu folgendem Resultate gelangt:

Die Anzahl h der ursprünglichen Classen der ersten Art ist r mal so gross als die Anzahl h' der Classen vom Theiler σ , wo r die Anzahl derjenigen ursprünglichen Classen der ersten Art bedeutet, welche mit der einfachsten Classe vom Theiler σ zusammengesetzt diese letztere wieder erzeugen.

Dies Resultat behält offenbar seine Gültigkeit für eine negative Determinante, auch wenn nicht alle, sondern nur die sogenannten positiven Classen gezählt werden (§. 64).

Es kommt jetzt offenbar nur noch darauf an, die Anzahl r zu bestimmen, und zu diesem Zwecke stellt Gauss folgenden schönen Satz auf:

Die r ursprünglichen Classen der ersten Art, welche mit der einfachsten Classe vom Theiler σ zusammengesetzt diese letztere wieder erzeugen, sind identisch mit denjenigen Classen, durch deren Formen das Quadrat des Theilers σ eigentlich oder uneigentlich dargestellt werden kann.

Um denselben zu beweisen, bemerken wir zunächst, dass man als Repräsentanten einer jeden ursprünglichen Classe H der ersten Art stets eine Form $(a, B, C\sigma)$ annehmen kann, in welcher a relative Primzahl zu σ ist, $2B$ und C aber durch σ theilbar sind; hat man nämlich (nach §. 93) als Repräsentanten zunächst eine Form (a, b, c) gewählt, in welcher a relative Primzahl zu σ ist, und componirt man dieselbe mit einer Form (σ, b', c') aus der einfachsten Classe S vom Theiler σ , so erhält man (§§. 146, 147) eine Form

($a\sigma, B, C$) vom Theiler σ , und zwar so, dass die Formen (a, b, c), (σ, b', c') resp. den Formen ($a, B, C\sigma$), (σ, B, aC) äquivalent sind; es kann daher ($a, B, C\sigma$) statt (a, b, c) als Repräsentant der Classe H gewählt werden.

Ist nun $SH = S$, also H eine der r Classen aus der Gruppe \mathfrak{R} , so ist ($a\sigma, B, C$) äquivalent mit (σ, B, aC), und folglich existiren zwei ganze Zahlen x, y , welche der Bedingung

$$a\sigma x^2 + 2Bxy + Cy^2 = \sigma$$

genügen; hieraus folgt aber

$$a(\sigma x)^2 + 2B(\sigma x)y + C\sigma y^2 = \sigma^2,$$

d. h. σ^2 wird durch die Form ($a, B, C\sigma$) der Classe H dargestellt, wenn den Variabeln die Werthe $\sigma x, y$ beigelegt werden.

Umgekehrt, ist σ^2 durch die Formen der Classe H , also auch durch die Form ($a, B, C\sigma$) darstellbar, so existiren zwei ganze Zahlen x', y , welche der Bedingung

$$ax'^2 + 2Bx'y + C\sigma y^2 = \sigma^2$$

genügen. Zunächst ergibt sich hieraus, dass x' durch σ theilbar sein muss; denn da C und $2B$, also auch $2By = \beta\sigma$ durch σ theilbar ist, so folgt $ax'^2 + \beta\sigma x' \equiv 0 \pmod{\sigma^2}$; ist nun δ der grösste gemeinschaftliche Divisor von $x' = \delta x$ und $\sigma = \delta\varrho$, wo also x und ϱ relative Primzahlen bedeuten, so ergibt sich $ax^2 + \beta\varrho x \equiv 0 \pmod{\varrho^2}$, also muss ax^2 , folglich auch a durch ϱ theilbar sein; da aber a relative Primzahl zu $\sigma = \delta\varrho$, also auch zu ϱ ist, so muss $\varrho = 1$, $\delta = \sigma$, also $x' = \sigma x$ sein. Nachdem dies bewiesen ist, ergibt sich

$$a\sigma x^2 + 2Bxy + Cy^2 = \sigma;$$

da ferner $2B$ und C durch σ theilbar sind, so folgt, dass x und y relative Primzahlen sind; mithin ist σ eigentlich darstellbar durch die Form ($a\sigma, B, C$) vom Theiler σ , welche folglich (§.60) einer Form äquivalent sein muss, deren erster Coefficient = σ ist, und die also der einfachsten Classe S vom Theiler σ angehört. Da nun ($a\sigma, B, C$) auch der Classe SH angehört, so ist $SH = S$, d. h. H ist eine Classe aus der Gruppe \mathfrak{R} , was zu beweisen war.

Durch den hiermit bewiesenen obigen Satz sind wir nun in den Stand gesetzt, den Grad r der Gruppe \mathfrak{R} genau zu bestimmen. Ist R eine Classe aus dieser Gruppe, und wird σ^2 durch ihre Formen so dargestellt, dass die beiden darstellenden Zahlen (x, y) den grössten gemeinschaftlichen Theiler δ haben, so geht δ^2 in σ^2 , folg-

lich δ in $\sigma = \delta \rho$ auf; mithin ist (nach §. 60) ρ^2 eigentlich darstellbar durch die Formen der Classe R , und folglich kann man (nach §. 60) als Repräsentanten von R eine Form wählen, deren erster Coefficient $= \rho^2$ ist. Da umgekehrt durch jede solche Form auch σ^2 dargestellt wird, wenn den Variablen die Werthe $x = \delta$, $y = 0$ ertheilt werden, so gehört sie, wenn sie zugleich ursprünglich von der ersten Art ist, einer Classe R aus der Gruppe \mathfrak{R} an. Wir haben mithin folgenden Satz erhalten:

Der Grad r der Gruppe \mathfrak{R} ist gleich der Anzahl aller nicht äquivalenten ursprünglichen Formen der ersten Art, deren erster Coefficient ein quadratischer Divisor ρ^2 vom Quadrate des Theilers σ ist.

Wir bemerken schliesslich, dass für jeden solchen quadratischen Divisor ρ^2 (zufolge §. 56) nur alle diejenigen Formen zu untersuchen sind, deren mittlere Coefficienten ein vollständiges Restsystem nach dem Modulus ρ^2 bilden.

§. 151.

Nachdem im Vorhergehenden der Weg allgemein vorgezeichnet ist, auf welchem man zur Bestimmung des Verhältnisses der Classenzahlen h und h' gelangt, schreiten wir zur Betrachtung der speciellen Fälle, in welchen σ eine *Primzahl* ist, weil aus ihnen das allgemeine Resultat abgeleitet werden kann.

I. Ist die Determinante $D = 1 - 4n \equiv 1 \pmod{4}$, und $\sigma = 2$, so handelt es sich um die Vergleichung der Classenzahlen der ursprünglichen Formen der ersten und zweiten Art. Bezeichnet man dieselben wieder mit h und h' , so ist $h = rh'$, wo r die Anzahl der nicht äquivalenten ursprünglichen Formen erster Art bedeutet, deren erster Coefficient $= 1$ oder $= 4$ ist. Da im zweiten Fall der mittlere Coefficient ungerade sein muss, so sind nur die drei Formen

$$(1, 0, -D), (4, \pm 1, n)$$

in Betracht zu ziehen.

Ist $D \equiv 1 \pmod{8}$, also n gerade, so ist nur die erste dieser Formen ursprünglich von der ersten Art, folglich $r = 1$, und $h = h'$.

Ist aber $D \equiv 5 \pmod{8}$, also n ungerade, so sind alle drei Formen ursprünglich von der ersten Art, und es braucht nur noch untersucht zu werden, ob sie verschiedenen Classen angehören oder nicht. Zunächst lässt sich beweisen, dass sie entweder zu einer und derselben, oder zu drei verschiedenen Classen gehören. Gauss zeigt dies durch die Composition der ihnen entsprechenden Classen $1, P, Q$; da die Classen P, Q entgegengesetzt sind, so ist $PQ = 1$, und ferner lässt sich leicht zeigen, dass $PP = Q$ und $QQ = P$ ist (denn aus den beiden einigen, in P enthaltenen Formen $(4, 1, n)$, $(n, -1, 4)$ ist die Form $(4n, 2n - 1, n)$ zusammengesetzt, und da diese mit $(n, 1 - 2n, 4n)$, $(n, 1, 4)$, $(4, -1, n)$ äquivalent ist, so folgt $PP = Q$); nimmt man nun an, dass zwei der drei Classen $1, P, Q$ identisch sind, so ergiebt sich hieraus sofort, dass auch die dritte mit ihnen übereinstimmt. Dasselbe lässt sich auch durch die folgenden Sätze erweisen.

Sind irgend zwei der drei Formen $(1, 0, -D)$, $(4, \pm 1, n)$ äquivalent, so ist die Gleichung $t^2 - Du^2 = 4$ durch ungerade Zahlen t, u lösbar.

Ist nämlich die erste Form mit einer der beiden anderen äquivalent, so ist (nach §. 60) der erste Coefficient 4 dieser letztern eigentlich darstellbar durch die Form $(1, 0, -D)$, also giebt es zwei relative Primzahlen t, u , welche der Gleichung $t^2 - Du^2 = 4$ genügen, woraus folgt, dass t, u , da sie nicht beide gerade sein können, nothwendig beide ungerade sein müssen. Sind ferner die beiden letzten Formen äquivalent, so giebt es (nach §. 60. Anm.) zwei ganze Zahlen x, y , welche den Bedingungen

$$4x^2 + 2xy + ny^2 = 4, \quad -2x + ny \equiv 0 \pmod{4}$$

genügen; da n ungerade ist, so muss y gerade sein $= 2u$; setzt man dann $2x + u = t$, so gehen diese Bedingungen in die folgenden über

$$t^2 - Du^2 = 4, \quad t \equiv -u \pmod{4};$$

da aus der letztern $t^2 \equiv u^2 \pmod{8}$ folgt, und ausserdem $-D \equiv 3 \pmod{8}$ ist, so folgt aus der erstern $4u^2 \equiv 4 \pmod{8}$, mithin ist u , also auch t ungerade, was zu beweisen war.

Ist die Gleichung $t^2 - Du^2 = 4$ durch ungerade Zahlen t, u lösbar, so sind alle drei Formen $(1, 0, -D)$, $(4, \pm 1, n)$ äquivalent.

Denn wenn man t mit beliebigem Vorzeichen, dann aber $u \equiv -t \pmod{4}$ wählt, so geht die Form $(1, 0, -D)$ durch die Substitutionen

$$\begin{pmatrix} t, & \pm \frac{t + Du}{4} \\ \pm u, & \frac{t + u}{4} \end{pmatrix}$$

in die beiden Formen $(4, \pm 1, n)$ über. — Durch Verbindung der beiden vorstehenden Sätze ergibt sich:

Die drei obigen Formen sind äquivalent oder gehören drei verschiedenen Classen an, je nachdem die Gleichung $t^2 - Du^2 = 4$ durch ungerade Zahlen t, u lösbar ist oder nicht; im ersten Falle ist $h = h'$, im zweiten $h = 3h'$.

Ist nun D positiv, so tritt der erste Fall ein oder der zweite, je nachdem die kleinste Lösung $t = T', u = U'$ aus ungeraden oder geraden Zahlen besteht. Ist D negativ, so besitzt die Gleichung im Allgemeinen nur die beiden Auflösungen $t = \pm 2, u = 0$, und mithin ist $h = 3h'$; die einzige Ausnahme hiervon bildet die Determinante $D = -3$, weil die Gleichung ausser den beiden Lösungen $t^2 = 4, u = 0$ noch die vier Lösungen $t^2 = u^2 = 1$ besitzt, und folglich ist in diesem Falle wieder $h = h'$.

Diese Resultate stimmen vollkommen mit denjenigen überein, welche wir früher (§§. 97, '99) mit Hülfe ganz anderer Principien abgeleitet haben.

II. Ist $D = D' \sigma^2$, so leuchtet ein, dass h' zugleich die Anzahl der ursprünglichen Classen erster Art von der Determinante D' ist. Unter der Voraussetzung, dass σ eine Primzahl ist, haben wir, um das Verhältniss $r = h : h'$ zu bestimmen, nur die l Formen

$$(1, 0, -D) \quad \text{und} \quad (\sigma^2, B\sigma, BB - D') \quad (1)$$

zu betrachten, wo B ein vollständiges Restsystem (mod. σ) durchlaufen muss, mit Ausnahme derjenigen Werthe, für welche $BB \equiv D' \pmod{\sigma}$ wird, weil diesen keine ursprünglichen Formen entsprechen; die Anzahl der zu betrachtenden ursprünglichen Formen ist daher

$$l = 2 \quad \text{oder} \quad \sigma - \left(\frac{D'}{\sigma}\right) \quad (2)$$

je nachdem $\sigma = 2$ oder eine ungerade Primzahl ist. Zur Bestimmung der Anzahl r der verschiedenen Classen, welchen diese l Formen angehören, gelangen wir durch die folgenden Sätze.

Die beiden Formen $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen t', u' giebt, welche den Bedingungen

$$t't' - D'u'u' = 1, \quad t' + \beta u' \equiv 0 \pmod{\sigma} \quad (3)$$

genügen; zwei Formen $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen t', u' giebt, welche den Bedingungen

$$t't' - D'u'u' = 1, \quad (b - b')t' + (bb' - D')u' \equiv 0 \pmod{\sigma} \quad (4)$$

genügen.

Die Aequivalenz der Formen $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ ist (nach §. 60 Anmerkung) gleichbedeutend mit der Annahme der Existenz zweier ganzen Zahlen x, y , welche die Bedingungen

$$x^2 - D'\sigma^2y^2 = \sigma^2,$$

$$x + \beta\sigma y \equiv 0, \quad -\beta\sigma x - D'\sigma^2y \equiv 0 \pmod{\sigma^2}$$

erfüllen; da nun aus der ersten folgt, dass x durch σ theilbar ist, und da sie durch die Substitutionen $x = \sigma t', y = u'$ in die Bedingungen (3) übergehen, aus welchen sie umgekehrt folgen, so ist der erste Theil des Satzes erwiesen. Ebenso fällt die Annahme der Aequivalenz der Formen $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ zusammen mit der Annahme der Existenz zweier ganzen Zahlen x, y , welche die Bedingungen

$$\sigma^2x^2 + 2b\sigma xy + (bb - D')y^2 = \sigma^2,$$

$$\sigma^2x + (b + b')\sigma y \equiv 0, \quad (b - b')\sigma x + (bb - D')y \equiv 0 \pmod{\sigma^2}$$

befriedigen; da nun der Voraussetzung nach $bb - D'$ nicht durch σ theilbar ist, so muss y^2 und folglich auch y durch die Primzahl σ theilbar sein; da ferner die vorstehenden Bedingungen durch die Substitution $y = \sigma u', x = t' - bu'$ in die Bedingungen (4) übergehen, aus denen sie auch rückwärts folgen, so ist auch der zweite Theil des obigen Satzes bewiesen.

Bedeutet λ die Anzahl derjenigen Formen (1), welche der Hauptklasse angehören, so ist $l = r\lambda$.

Gehört die Form $(\sigma^2, \beta\sigma, \beta^2 - D')$ der Hauptklasse an, so existirt eine Lösung (t', u') der Gleichung

$$t't' - D'u'u' = 1 \quad (5)$$

welche der Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ genügt, und folglich kann u' nicht durch σ theilbar sein. Ist umgekehrt (t', u') eine Lösung der Gleichung (5), und u' nicht theilbar durch σ , so existirt

stets eine und nur eine Zahlklasse $\beta \pmod{\sigma}$, welche der Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ genügt, und ihr entspricht eine zur Hauptklasse gehörige Form $(\sigma^2, \beta\sigma, \beta^2 - D')$. Um also alle diese Formen zu erhalten, muss man alle Lösungen (t', u') der Gleichung (5) aufstellen, in welchen u' nicht durch σ theilbar ist, und jedesmal die entsprechende Zahlklasse $\beta \pmod{\sigma}$ durch die Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ bestimmen. Da ausserdem die Form $(1, 0, -D)$ zur Hauptklasse gehört, und λ die Anzahl aller zur Hauptklasse gehörenden Formen (1) bedeutet, so ist also $\lambda - 1$ die Anzahl der sämtlichen incongruenten Zahlklassen $\beta \pmod{\sigma}$, welche aus Lösungen (t', u') der Gleichung (5) vermöge der Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ erzeugt werden können.

Sind hierdurch schon alle Formen (1) erschöpft, so ist $l = \lambda$ und $r = 1$, also der Satz richtig. Giebt es aber eine nicht zur Hauptklasse gehörende ursprüngliche Form $(\sigma^2, b'\sigma, b'b' - D')$, d. h. giebt es eine von den $\lambda - 1$ Zahlklassen $\beta \pmod{\sigma}$ verschiedene Zahlklasse b' von der Beschaffenheit, dass $b'b' - D'$ nicht durch σ theilbar ist, so wollen wir zeigen, dass unter den l Formen (1) sich genau $(\lambda - 1)$ Formen $(\sigma^2, b\sigma, bb - D')$ finden, welche alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalent und von ihr verschieden sind. Ist nämlich $(\sigma^2, b\sigma, bb - D')$ eine solche Form, also $b - b'$ nicht durch σ theilbar, so giebt es, wie oben gezeigt ist, eine Lösung (t', u') der Gleichung (5), welche der Congruenz

$$(b - b')t' + (bb' - D')u' \equiv 0 \pmod{\sigma} \quad (4)$$

genügt, aus welcher zugleich folgt, dass u' nicht durch σ theilbar ist. Umgekehrt, ist (t', u') eine Lösung der Gleichung (5), in welcher u' nicht durch σ theilbar ist, und $t' + \beta u' \equiv 0 \pmod{\sigma}$, so existirt, weil $b' - \beta$ nicht durch σ theilbar ist, immer eine und nur eine Zahlklasse $b \pmod{\sigma}$, welche die Congruenz

$$(b' - \beta)b \equiv D' - b'\beta \pmod{\sigma} \quad (6)$$

befriedigt, und zwar kann b nicht $\equiv b' \pmod{\sigma}$ sein, weil hieraus $b'b' \equiv D' \pmod{\sigma}$ folgen würde; multiplicirt man nun (6) mit u' , so ergiebt sich (4), und folglich ist wirklich $(\sigma^2, b\sigma, bb - D')$ äquivalent mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ und zugleich verschieden von ihr, weil $b - b'$ nicht durch σ theilbar ist. Um also alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalenten und von ihr verschiedenen Formen $(\sigma^2, b\sigma, bb - D')$ zu erhalten, braucht man nur die sämtlichen $(\lambda - 1)$ Congruenzen (6) aufzustellen, welche den $(\lambda - 1)$ incongruenten Zahlklassen $\beta \pmod{\sigma}$ entsprechen, und für

jede die entsprechende Zahlclassen b zu bestimmen. Auf diese Weise entstehen aber wirklich auch $(\lambda - 1)$ verschiedene Zahlclassen $b \pmod{\sigma}$; denn wollte man annehmen, es könnte zwei verschiedenen Zahlclassen $\beta, \beta' \pmod{\sigma}$ eine und dieselbe Zahlclassen $b \pmod{\sigma}$ entsprechen, so wäre

$$(b' - \beta)b \equiv D' - b'\beta, (b' - \beta')b \equiv D' - b'\beta' \pmod{\sigma};$$

hieraus würde aber durch Subtraction $(\beta' - \beta)(b - b') \equiv 0 \pmod{\sigma}$ folgen, was unmöglich ist, da weder $\beta' - \beta$ noch $b - b'$ durch σ theilbar ist. Mithin giebt es wirklich genau $\lambda - 1$ verschiedene Formen $(\sigma^2, b\sigma, bb - D')$, welche mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalent und zugleich von ihr verschieden sind. Von den l Formen (1) gehören daher immer je λ , und nicht mehr, zu einer und derselben Classe, folglich ist $l = r\lambda$, was zu beweisen war.

Ist die Determinante $D = D' \sigma^2$ negativ, so ist h im Allgemeinen $= lh'$, und nur dann $= \frac{1}{2}lh'$, wenn $D' = -1$.

Denn die Gleichung (5) besitzt nur im letztern Falle Lösungen ($t' = 0, u' = \pm 1$), in welchen u' nicht durch σ theilbar ist; da denselben nur die eine Zahlclassen $\beta \equiv 0 \pmod{\sigma}$ entspricht, so ist $\lambda = 2$, also $r = \frac{1}{2}l$; in allen anderen Fällen ist $\lambda = 1$, also $r = l$.

Ist die Determinante $D = D' \sigma^2$ positiv, so ist $h \log(T + UVD) = l.h' \log(T' + U'VD')$, wo $(T, U), (T', U')$ resp. die kleinsten positiven Auflösungen der Gleichungen $T^2 - DU^2 = 1, T'^2 - D'U'^2 = 1$ bedeuten.

Um dies zu beweisen, schicken wir eine Bemerkung über die Lösungen der Gleichung (5) voraus. Wenn zwei solche Lösungen $(t', u'), (t'', u'')$ der Bedingung

$$t'u'' - u't'' \equiv 0 \pmod{\sigma} \tag{7}$$

genügen, so kann man, wenn $\sqrt{D'}$ und $\sqrt{D} = \sigma\sqrt{D'}$ immer positiv genommen werden,

$$t' + u'\sqrt{D'} = (t'' + u''\sqrt{D'}) (t + u\sqrt{D}), \tag{8}$$

setzen, wo die ganzen Zahlen t, u eine Lösung der Gleichung

$$t^2 - Du^2 = 1 \tag{9}$$

bilden. Umgekehrt, sind $(t'', u''), (t, u)$ resp. Lösungen der Gleichungen (5), (9), so liefert die Gleichung (8) stets eine Lösung (t', u') der Gleichung (5), welche zugleich der Bedingung (7) genügt. Je zwei solche Lösungen $(t', u'), (t'', u'')$ der Gleichung (5) wollen wir äquivalent nennen; dann leuchtet sofort ein, dass zwei Lö-

sungen, welche einer dritten äquivalent sind, auch einander äquivalent sein müssen. Man kann daher die sämmtlichen Lösungen der Gleichung (5) in Classen eintheilen, deren jede alle und nur solche Lösungen enthält, die unter einander äquivalent sind. Da nun die Gleichung (8) lehrt, aus einer gegebenen Lösung (t'', u'') alle ihr äquivalenten Lösungen (t', u') zu finden, und da $t + u\sqrt{D} = \pm (T + U\sqrt{D})^n$ ist, wo das Vorzeichen nach Belieben, und für n jede ganze Zahl gewählt werden darf (§. 85), so leuchtet ein (vergl. §. 87), dass aus jeder Classe von Lösungen ein und nur ein Repräsentant (t', u') so gewählt werden kann, dass

$$1 \leq t' + u'\sqrt{D}' < T + U\sqrt{D}$$

wird; da ferner $(T, U\sigma)$ ebenfalls eine Lösung der Gleichung (5), und folglich (§. 85)

$$T + U\sqrt{D} = (T' + U'\sqrt{D}')^{\lambda'}$$

ist, wo λ' eine bestimmte positive ganze Zahl bedeutet, so leuchtet ein, dass die ersten Factoren $t' + u'\sqrt{D}'$ der obigen Repräsentanten (t', u') von der Form $(T' + U'\sqrt{D}')^{n'}$ sind, wo n' die λ' Werthe 0, 1, 2 . . . $(\lambda' - 1)$ durchlaufen muss; dass also die Anzahl der Classen $= \lambda'$ ist.

Die erste von diesen Classen enthält also die Lösungen (t', u') und nur solche, deren zweite Elemente u' durch σ theilbar sind. Jede Lösung (t', u') aus einer der übrigen $\lambda' - 1$ Classen liefert aber durch die Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ eine zugehörige Zahlklasse $\beta \pmod{\sigma}$, und da unmittelbar einleuchtet, dass zwei solche Lösungen stets und nur dann zu derselben Zahlklasse $\beta \pmod{\sigma}$ führen, wenn sie derselben Classe von Lösungen angehören, so muss die Anzahl $\lambda - 1$ der Zahlklassen β mit der Anzahl $\lambda' - 1$ dieser Classen von Lösungen übereinstimmen; also ist $\lambda = \lambda'$, was zu beweisen war.

Offenbar lässt sich aus dem hier behandelten speciellen Fall ohne Schwierigkeit das in §. 100 erhaltene Resultat für den allgemeinen Fall ableiten, in welchem σ eine beliebige zusammengesetzte Zahl ist.

§. 152.

Wir beschränken uns nun im Folgenden auf die Composition von ursprünglichen Classen erster Art, und behalten ausserdem, wenn die Determinante D negativ ist, nur die positiven Classen bei, deren Zusammensetzung offenbar immer wieder zu positiven Classen führt. Diese h Classen, welche eine Gruppe \S bilden, zerfallen (§. 122) je nach dem Ausfall der λ Charaktere C , welche dieser Determinante D entsprechen, in Geschlechter, und es ist mit Hülfe des Reciprocitätssatzes gezeigt (§. 123), dass *höchstens* der Hälfte aller angebbaren Totalcharaktere wirklich existirende Classen entsprechen. Gauss*) leitet nun diesen letzteren Satz aus der Theorie der Composition ab, und er benutzt ihn, um darauf einen neuen, den *zweiten* Beweis des Reciprocitätssatzes zu gründen. Da diese tief sinnigen Principien sich auf die Beweise von höheren Reciprocitätsgesetzen übertragen lassen**), so theilen wir dieselben in diesem und den folgenden Paragraphen mit.

Sind $\varepsilon, \varepsilon'$ die Werthe eines Charakters C resp. für die Classen H, H' , so ist $C = \varepsilon \varepsilon'$ für die Classe HH' .

Man kann als Repräsentanten der Classen H, H' immer zwei einige Formen nehmen, deren erste Coefficienten a, a' relative Primzahlen zu $2D$ sind; da die aus ihnen zusammengesetzte, also der Classe HH' angehörende Form den ersten Coefficienten aa' hat, welcher ebenfalls relative Primzahl zu $2D$ ist, so ergibt sich der zu beweisende Satz unmittelbar, wenn man bedenkt, dass der Charakter C oder $C(n)$ ein Ausdruck von der Art

$$(-1)^{\frac{1}{2}(n-1)}, (-1)^{\frac{1}{6}(n^2-1)}, (-1)^{\frac{1}{2}(n-1) + \frac{1}{6}(n^2-1)}, \left(\frac{n}{l}\right) \dots$$

ist (§. 122), und dass folglich die drei Werthe $C(a), C(a'), C(aa')$, welche dieser Charakter resp. in den drei Classen H, H', HH' besitzt, der Bedingung $C(a)C(a') = C(aa')$ genügen.

Aus diesem Satze ergibt sich, dass, wenn die Classen K, K' resp. denselben Geschlechtern G, G' angehören, wie die Classen

*) D. A. artt. 257 — 262.

**) Kummer: Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. 1859. Vergl. Berliner Monatsbericht vom 18. Febr. 1858.

H, H' , dann auch die Classen KK' und HH' sich in einem und demselben Geschlechte finden, welches das *aus G, G' zusammengesetzte Geschlecht* heissen soll*). Sind ferner N, N' zwei Classen des *Hauptgeschlechtes*, d. h. desjenigen Geschlechtes, in welchem sich die Hauptform $(1, 0, -D)$ findet, und folglich alle Charaktere C den Werth $+1$ haben, so gehört die zusammengesetzte Classe NN' ebenfalls diesem Geschlechte an, mithin bilden alle n Classen des Hauptgeschlechtes eine Gruppe \mathfrak{N} vom Grade n (§. 149); zugleich zerfallen die sämtlichen h Classen in g Complexe $\mathfrak{N}H$ von je n Classen, welche jedesmal einem und demselben Geschlecht angehören; zwei verschiedene solche Complexe gehören, wie man leicht erkennt, auch zu verschiedenen Geschlechtern; mithin ist $h = ng$, und g die Anzahl der wirklich existirenden von einander verschiedenen Geschlechter**).

Die Determinante D heisst *regulär* oder *irregulär*, je nachdem die von den n Classen des Hauptgeschlechtes gebildete Gruppe regulär ist oder nicht (§. 149); bedeutet im letztern Falle δ den Grad der grössten in ihr enthaltenen regulären Gruppe, so heisst die ganze Zahl $n : \delta$ der *Irregularitätsexponent* der Determinante***).

Aus dem obigen Satze über den Charakter einer zusammengesetzten Classe ergibt sich ferner unmittelbar der folgende:

Jede Classe Q , welche durch Duplication einer Classe entsteht, gehört dem Hauptgeschlechte an.

Die Anzahl q der verschiedenen Classen Q , welche durch Duplication der sämtlichen h Classen entstehen, ist daher $\leq n$ (da diese Classen, wie leicht zu ersehen ist, eine Gruppe Ω bilden, so muss q gewiss ein Divisor von n sein). Um sie genauer zu bestimmen, nehmen wir an, Q entstehe durch Duplication der bestimmten Classe H , und fragen nach allen Classen H' , durch deren Duplication dieselbe Classe Q entsteht. Aus der Annahme $H'H' = Q = HH$ folgt nun, wenn man $H' = AH$ setzt, $AA = 1$, also $A = A^{-1}$, d. h. die Classe A ist identisch mit der ihr entgegengesetzten Classe, und folglich ist sie eine *ambige* Classe (§. 148, 2., §§. 56 — 58). Umgekehrt, ist $H' = AH$, und A eine ambige Classe, so ist auch $H'H' = HH$. Schreibt man daher alle α ambigen Classen A auf, welche offenbar eine Gruppe \mathfrak{A} bilden, so zerfallen alle h Classen

*) Gauss: D. A. artt. 246, 247.

**) Gauss: D. A. art. 252.

***) Gauss: D. A. art. 306. VII.

in q Complexe $\mathfrak{A}H$ von je α Classen, deren Duplication eine und dieselbe Classe HH hervorbringt, während zwei Classen, welche zwei verschiedenen solchen Complexen angehören, durch Duplication auch zwei verschiedene Classen hervorbringen; und endlich ist $h = \alpha q$.

Da nun h auch $= ng$, und ausserdem $q \leq n$ ist, so ergibt sich $g \leq \alpha$, d. h. der Satz: *Die Anzahl der wirklich existirenden verschiedenen Geschlechter ist höchstens gleich der Anzahl der ambigen Classen.*

§. 153.

Es kommt also jetzt darauf an, für eine gegebene Determinante D die Anzahl α aller ambigen Classen A genau zu bestimmen, welche ursprünglich von erster Art sind.

Da in jeder ambigen Classe $A = A^{-1}$ stets mindestens eine ambige Form (a, b, c) zu finden ist (§. 58), so bleibt gewiss keine jener α Classen unvertreten, wenn wir alle ambigen Formen aufschreiben. Da nun in einer solchen Form $2b$ durch a theilbar, folglich b entweder $\equiv 0$, oder $\equiv \frac{1}{2}a \pmod{a}$, also (a, b, c) selbst mit einer Form äquivalent ist (§. 56), deren mittlerer Coefficient entweder Null, oder die Hälfte des ersten Coefficienten ist, so genügt es, alle Formen

$$\left(a, 0, \frac{-D}{a}\right) \quad \text{und} \quad \left(2b, b, \frac{b^2 - D}{2b}\right)$$

zu betrachten, welche ursprünglich von erster Art sind.

Bedeutet μ die Anzahl aller verschiedenen *ungeraden* Primzahlen, welche in D aufgehen, ist ferner $\nu = 0$ oder $= 1$, je nachdem D ungerade oder gerade, so ist $\mu + \nu$ die Anzahl *aller* verschiedenen in D aufgehenden Primzahlen. Dann leuchtet ein, dass die Anzahl aller ursprünglichen Formen vom Typus

$$(a, 0, a')$$

gleich $2^{\mu+\nu+1}$ ist; die eine Hälfte derselben hat positive erste Coefficienten, die andere Hälfte negative.

Betrachten wir nun die anderen ambigen ursprünglichen Formen erster Art, deren Typus

$$\left(2b, b, \frac{b^2 - D}{2b}\right)$$

ist, so muss b ein solcher Divisor von $D = -bb'$ sein, dass der dritte Coefficient $\frac{1}{2}(b + b')$ eine ganze Zahl und relative Primzahl zu $2b$ wird; mithin muss zunächst $b + b' \equiv 2 \pmod{4}$ sein, und ferner dürfen b und b' keinen gemeinschaftlichen ungeraden Divisor haben. Sind nun b und b' ungerade, so folgt $b' \equiv b$, $D \equiv -bb \equiv 3 \pmod{4}$; umgekehrt, wenn $D \equiv 3 \pmod{4}$, so kann b nur ungerade sein, und aus $bb' = -D \equiv 1 \pmod{4}$ folgt von selbst, dass $b \equiv b'$, also $b + b' \equiv 2 \pmod{4}$ wird; mithin kann b jeder Divisor von D sein, für welchen b und b' relative Primzahlen werden. Die Anzahl dieser Formen

$$(2b, b, \frac{1}{2}(b + b'))$$

ist daher $= 2^{\mu+1}$, unter welchen ebensoviele mit positiven, wie mit negativen ersten Coefficienten vorkommen. Sind aber b und b' gerade, so ist eine von ihnen $\equiv 0$, die andere $\equiv 2 \pmod{4}$, mithin $D \equiv 0 \pmod{8}$, und $\frac{1}{2}b$, $\frac{1}{2}b'$ sind relative Primzahlen. Umgekehrt, wenn $D \equiv 0 \pmod{8}$ ist, so muss b gerade sein, und man kann für $\frac{1}{2}b$ jeden Divisor von $\frac{1}{4}D = -\frac{1}{2}b \cdot \frac{1}{2}b'$ wählen, für welchen $\frac{1}{2}b$, $\frac{1}{2}b'$ relative Primzahlen werden; mithin ist die Anzahl dieser Formen, da $\frac{1}{4}D$ gerade ist, gleich $2^{\mu+2}$, und unter ihnen finden sich ebensoviele mit positiven wie mit negativen ersten Coefficienten.

Die Anzahl aller dieser ambigen ursprünglichen Formen erster Art ist daher gleich

$$\begin{array}{ll} 2^{\mu+1}, & \text{wenn } D \equiv 1 \pmod{4}, \\ 2^{\mu+2}, & \text{„ } D \equiv 2, 3, 4, 6, 7 \pmod{8}, \\ 2^{\mu+3}, & \text{„ } D \equiv 0 \pmod{8}; \end{array}$$

sie ist folglich in allen Fällen genau doppelt so gross, als die Anzahl $2^\lambda = 2^\tau$ aller angebbaren Totalcharaktere für die Determinante D (§. 122). Es kommt jetzt darauf an, die Anzahl der verschiedenen Classen zu bestimmen, welche durch diese Formen repräsentirt werden.

Sieht man von dem singulären Fall $D = -1$ vorläufig ganz ab, so erkennt man leicht, dass die Coefficienten α und α' , ebenso die Zahlen b und b' , selbst ihren absoluten Werthen nach, von einander verschieden sein müssen. Hätten nämlich die relativen Primzahlen α , α' denselben absoluten Werth 1, so wäre $D = \pm 1$; dasselbe würde sich ergeben, wenn man annehmen wollte, die unge-

raden Zahlen b und b' hätten denselben absoluten Werth; sind endlich b und b' gerade, so ist die eine der Zahlen $\frac{1}{2}b, \frac{1}{2}b'$ gerade, die andere ungerade, also haben sie verschiedene absolute Werthe. Hieraus folgt, dass die sämmtlichen obigen Formen immer in Paare von je zwei von einander verschiedenen Formen $(a, 0, a')$, $(a', 0, a)$, und $(2b, b, \frac{1}{2}(b + b'))$, $(2b', b', \frac{1}{2}(b + b'))$ zerfallen, und da die erste resp. durch die Substitutionen $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} -1 & -1 \\ +2 & +1 \end{pmatrix}$ in die zweite übergeht, so genügt es, diejenige von ihnen beizubehalten, deren erster Coefficient der kleinere ist; mithin haben wir nur noch 2τ Formen $(a, 0, a')$, $(2b, b, \frac{1}{2}(b + b'))$, in welchen die absoluten Werthe (a) und $(b) < \sqrt{D}$ sind; und unter diesen Formen giebt es wieder ebensoviele mit positiven ersten Coefficienten, wie mit negativen.

Ist nun D negativ, so behalten wir nur die τ Formen bei, deren äussere Coefficienten positiv sind, und wir wollen zeigen, dass sie die Repräsentanten von ebensovielen verschiedenen Classen sind. Zunächst sind alle Formen $(a, 0, a')$ und diejenigen Formen $(2b, b, \frac{1}{2}(b + b'))$, in welchen $3b \leq b'$ ist, *reducirt* (§. 64), und statt jeder nicht reducirten Form $(2b, b, \frac{1}{2}(b + b'))$, in welcher also $3b > b'$, können wir die ihr nach rechts benachbarte reducirt Form $(\frac{1}{2}(b + b'), \frac{1}{2}(b' - b), \frac{1}{2}(b + b'))$ substituiren. Man erkennt nun leicht, dass alle diese τ reducirten Formen von einander verschieden, und dass auch keine zwei einander entgegengesetzt sind, weil keiner der mittleren Coefficienten negativ ist; sie gehören daher (§. 65) ebensovielen verschiedenen Classen an. Wir haben daher das Resultat: *Die Anzahl α aller positiven ambigen ursprünglichen Classen erster Art von negativer Determinante D ist halb so gross wie die Anzahl 2τ aller angebbaren Totalcharaktere.* Dies gilt offenbar auch noch für den oben ausgeschlossenen singulären Fall $D = -1$, da die beiden Formen $(1, 0, 1)$, $(2, 1, 1)$ äquivalent sind.

Ist aber die Determinante D positiv, so entspricht jeder der obigen 2τ ambigen Formen (A, B, C) eine einzige ihr äquivalente ambige Form (A, B', C') , wo B' durch die Bedingungen

$$B' \equiv B \pmod{A}, \quad 0 < \sqrt{D} - B' < (A)$$

vollständig bestimmt ist; offenbar entstehen auf diese Weise wieder 2τ ambige und von einander verschiedene Formen (A, B', C') . Um nun zu zeigen, dass alle diese Formen zugleich *reducirt* sind (§. 74), braucht nur nachgewiesen zu werden, dass $(A) < \sqrt{D} + B'$ ist; wenn $(A) < \sqrt{D}$ ist, so folgt dies unmittelbar daraus, dass zufolge der obigen Grenzbedingungen B' positiv ist; wenn aber $(A) > \sqrt{D}$

ist, was nur bei den Formen des zweiten Typus eintreten kann, so ist $A = 2B$, und $(B) < \sqrt{D}$, folglich $B' = (B)$, weil dieser Werth allen an B' gestellten Forderungen genügt, und also wieder $(A) < \sqrt{D} + B'$. Endlich behaupten wir, dass jede ambige reducirte Form (a, b, c) , welche zugleich ursprünglich von erster Art ist, nothwendig mit einer dieser 2τ Formen (A, B', C') identisch sein muss; ist nämlich b theilbar durch a , so muss $(a) < \sqrt{D}$ sein, weil in einer reducirten Form $0 < b < \sqrt{D}$ ist, und die mit (a, b, c) äquivalente Form $(a, 0, a')$ ist eine der 2τ Formen (A, B, C) , woraus folgt, dass (a, b, c) selbst mit der entsprechenden Form (A, B', C') identisch sein muss, weil b als mittlerer Coefficient einer reducirten Form denselben charakteristischen Bedingungen genügt, wie B' ; ist aber b nicht theilbar durch a , so ist wenigstens $(a) < 2\sqrt{D}$, und folglich die mit (a, b, c) äquivalente Form $(a, \frac{1}{2}a, c')$ eine der Formen (A, B, C) , woraus wieder folgt, dass (a, b, c) mit der entsprechenden Form (A, B', C') identisch ist. Wir müssen aus dem Vorhergehenden schliessen, dass die Anzahl aller ambigen ursprünglichen Formen erster Art, welche zugleich reducirt sind, genau $= 2\tau$ ist; da nun in jeder ambigen Classe sich stets zwei und nur zwei solche Formen finden (§§. 78, 82), so erhalten wir dasselbe Resultat, wie für negative Determinanten: *Die Anzahl α aller ambigen ursprünglichen Classen erster Art von positiver Determinante D ist genau halb so gross wie die Anzahl 2τ aller angebbaren Totalcharaktere.*

Verbinden wir diese Resultate mit dem des vorigen Paragraphen, so ergibt sich folgender Satz*):

Die Anzahl der wirklich existirenden verschiedenen Geschlechter ist höchstens halb so gross wie die Anzahl der angebbaren Totalcharaktere.

§. 154.

Das soeben erhaltene Resultat führt nun zu einem neuen Beweise des Reciprocitätssatzes, sowie der Ergänzungssätze über den Charakter der Zahlen — 1 und 2. Wir machen zunächst die Be-

*) Vergl. §. 123.

merkung, dass in den Fällen $D = -1, \pm 2$, und wenn $D \equiv 1 \pmod{4}$ eine positive oder negative Primzahl ist, nur ein einziger Charakter C (§. 122), und folglich (§. 153) nur ein einziges Geschlecht vorhanden ist, welches kein anderes, als das durch die Form $(1, 0, -D)$ vertretene Hauptgeschlecht ($C = +1$) sein kann. Wir bezeichnen nun mit p, q immer positive, ungerade (von einander verschiedene) Primzahlen, und wenden uns zum Beweise der drei Sätze:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$$

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)}.$$

1. Ist zunächst $p \equiv 1 \pmod{4}$, so ist $(-1, 0, p)$ eine ursprüngliche Form erster Art von der Determinante $D = p \equiv 1 \pmod{4}$, für welche nur Formen existiren, die dem Hauptgeschlecht angehören; mithin muss der Coefficient -1 quadratischer Rest von p sein. Ist aber $p \equiv 3 \pmod{4}$, so ist -1 Nichtrest von p ; wäre nämlich $-1 = b^2 - cp$, so wäre (p, b, c) eine (positive) Form der Determinante $D = -1$, welche zufolge ihres Coefficienten p den Charakter $C = -1$ besäße, was unmöglich ist.

2. Ist $p \equiv 1 \pmod{8}$, so ist $(8, 1, \frac{1}{8}(1-p))$ oder $(8, 3, \frac{1}{8}(9-p))$, je nachdem $p \equiv 9$ oder $\equiv 1 \pmod{16}$ ist, eine ursprüngliche Form erster Art von der Determinante $D = p \equiv 1 \pmod{4}$, und muss deshalb dem Hauptgeschlecht angehören, woraus folgt, dass 8 und also auch 2 quadratischer Rest von p ist.

Ist ferner $p \equiv 7 \pmod{8}$, so ist 2 ebenfalls quadratischer Rest von p ; denn im entgegengesetzten Fall wäre (zufolge 1. und §. 33, III.) die Zahl -2 Rest von p , also $-2 = b^2 - cp$, und es existirte eine (positive) Form (p, b, c) der Determinante $D = -2$, für welche $C = -1$ wäre, was unmöglich ist.

Ist endlich $p \equiv 3$ oder $5 \pmod{8}$, so ist 2 Nichtrest von p ; wäre nämlich $2 = b^2 - cp$, so wäre (p, b, c) eine Form der Determinante $D = 2$, für welche $C = -1$ wäre, was unmöglich ist.

3. Ist wenigstens eine der beiden Primzahlen p, q , z. B. $p \equiv 1 \pmod{4}$, so ist

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

Ist nämlich q Rest von p , so gilt Dasselbe von $-q$ (zufolge 1. und §. 33, I.), mithin kann man, nachdem man das Vorzeichen \pm so gewählt hat, dass $\pm q \equiv 1 \pmod{4}$ wird, immer $\pm q = b^2 - cq$ setzen, und folglich ist (p, b, c) eine ursprüngliche Form erster Art von der Determinante $D = \pm q \equiv 1 \pmod{4}$, und zwar eine positive, wenn D negativ ist; sie gehört also dem Hauptgeschlechte an, und folglich ist p Rest von q . Ist aber q Nichtrest von p , so muss auch p Nichtrest von q sein, weil im entgegengesetzten Falle $p = b^2 - cq$ wäre, also eine ursprüngliche Form erster Art (q, b, c) der Determinante $D = p \equiv 1 \pmod{4}$ existirte, für welche $C = -1$ wäre, was unmöglich ist.

Sind aber beide Primzahlen $p, q \equiv 3 \pmod{4}$, so ist

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Dies ergibt sich am einfachsten durch die Betrachtung der Determinante $D = pq \equiv 1 \pmod{4}$, für welche zwei Charaktere C , also höchstens zwei verschiedene Geschlechter existiren. Da nun die beiden ursprünglichen Formen $(1, 0, -pq)$, $(-1, 0, pq)$ erster Art (zufolge 1.) wirklich zwei verschiedenen Geschlechtern angehören, so muss jede andere ursprüngliche Form erster Art von derselben Determinante, z. B. die Form $(p, 0, -q)$ einem der durch diese beiden Formen repräsentirten Geschlechter angehören. Gehört sie in das Hauptgeschlecht, so ist gleichzeitig p Rest von q , und $-q$ Rest von p , folglich (nach 1.) q Nichtrest von p ; gehört sie aber in dasselbe Geschlecht wie die Form $(-1, 0, pq)$, so ist gleichzeitig p Nichtrest von q , und $-q$ Nichtrest von p , folglich q Rest von p . Was zu beweisen war.

§. 155.

Mit Hülfe des so von Neuem bewiesenen Reciprocitätssatzes lässt sich nun wieder, wie in §. 123 geschehen ist, darthun, dass höchstens diejenigen τ Geschlechter existiren können, deren Totalcharaktere der dortigen Bedingung $II C' = +1$ genügen; dass aber alle diese τ Geschlechter wirklich existiren (§. 125), hat Gauss mit Hülfe der von ihm gegründeten Theorie der ternären quadratischen Formen

$$Ax^2 + By^2 + Cz^2 + 2A'yz + 2B'zx + 2C'xy$$

bewiesen*). Da oben (§. 152) gezeigt ist, dass $ng = \alpha q$ ist, wo g die Anzahl der wirklich existirenden Geschlechter, n die Anzahl der in jedem derselben enthaltenen Classen, $\alpha = \tau$ die Anzahl der ambigen Classen oder also die Anzahl der Totalcharaktere, welche der Bedingung $\Pi C' = +1$ genügen, und q die Anzahl der durch Duplication entstehenden Classen bedeutet, so leuchtet ein, dass der zu beweisende Satz $g = \alpha$ wesentlich identisch ist mit dem Satze $n = q$; da ferner n die Anzahl aller Classen des Hauptgeschlechtes ist, und jede der durch Duplication entstehenden q Classen gewiss dem Hauptgeschlechte angehört (§. 152), so ist der zu beweisende Satz wesentlich identisch mit dem folgenden**):

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Wir können hier unmöglich darauf eingehen, den Beweis mitzutheilen, welchen *Gauss* auf die Theorie der ternären Formen gestützt hat; da dieses tiefe Theorem aber den schönsten Abschluss der Lehre von der Composition bildet, so können wir es uns nicht versagen, dasselbe auch ohne Hülfe der Dirichlet'schen Principien auf einem Wege abzuleiten, der zugleich die Grundlage für andere wichtige Untersuchungen bildet.

Um einen bestimmten Boden für diese Untersuchung zu gewinnen, heben wir zunächst eine charakteristische Eigenschaft aller der Classen Q hervor, welche durch Duplication entstehen: *alle Formen dieser Classen und nur diese Formen sind fähig, Quadratzahlen darzustellen, welche relative Primzahlen zu $2D$ sind.* Entsteht nämlich Q durch Duplication einer Classe K , so kann man aus K immer eine solche Form auswählen, deren erster Coefficient x relative Primzahl zu $2D$ ist; da alsdann diese Form mit sich selbst einig ist, so entsteht durch Duplication eine der Classe Q angehörige Form, deren erster Coefficient $= x^2$ ist, und folglich ist diese Quadratzahl durch die Formen der Classe Q eigentlich darstellbar. Umgekehrt, ist Q eine Classe, durch deren Formen eine Quadratzahl dargestellt werden kann, welche relative Primzahl zu $2D$ ist, so giebt es auch eine solche Quadratzahl x^2 , welche durch diese Formen *eigentlich* darstellbar ist, und folglich findet sich in dieser Classe Q eine Form (x^2, x', x'') , welche offenbar

*) *D. A.* art. 287.

***) *Gauss: D. A.* art. 286.

durch Duplication der Form (x, x', xx'') entsteht; mithin ist $Q = K^2$, wo K die Classe bedeutet, welcher die Form (x, x', xx'') angehört. Das obige zu beweisende Theorem ist daher identisch mit dem folgenden:

Ist (A, B, C) eine Form des Hauptgeschlechtes der Determinante D , so ist die Gleichung

$$Az^2 + 2Bzy + Cy^2 = x^2$$

stets lösbar in ganzen Zahlen z, y, x , deren letzte relative Primzahl zu $2D$ ist.

§. 156.

Durch die vorstehende Betrachtung sind wir dahin geführt, die Lösbarkeit einer Gleichung von der Form

$$ax^2 + by^2 + cz^2 + 2a'yz + 2b'zx + 2c'xy = 0$$

in ganzen Zahlen x, y, z (oder was Dasselbe ist, die Lösbarkeit der allgemeinen Gleichung

$$au^2 + bv^2 + 2c'uv + 2b'u + 2a'v + c = 0$$

in rationalen Zahlen u, v) zu untersuchen. Dieselbe kann, allgemein zu reden, auf den speciellen Fall zurückgeführt werden, in welchem die Coefficienten $a', b', c' = 0$ sind*), und wir beschäftigen uns daher im Folgenden nur mit Gleichungen von der Form

$$ax^2 + by^2 + cz^2 = 0, \tag{1}$$

wo a, b, c drei gegebene, von Null verschiedene ganze Zahlen bedeuten, die wir ausserdem stets als *relative Primzahlen* annehmen, weil jeder andere Fall, wie man leicht erkennt, sich auf diesen zurückführen lässt**). Wir wollen nun eine Lösung x, y, z eine *eigentliche Lösung* nennen, wenn die drei Zahlen x, y, z *relative Primzahlen* sind; dann leuchtet ein, dass ax, by, cz ebenfalls relative Primzahlen sind; ginge nämlich eine Primzahl p in zweien von ihnen auf, so müsste p zufolge (1) auch in der dritten aufgehen; da aber höchstens einer der Coefficienten a, b, c durch p

*) Gauss: D. A. artt. 299, 300.

***) Gauss: D. A. art. 298.

theilbar sein kann, so wären wenigstens zwei der Zahlen x, y, z theilbar durch p , also keine relative Primzahlen.

Nach dieser Vorbemerkung beginnen wir unsere Untersuchung*), indem wir uns die folgende Aufgabe stellen:

I. Aus einer gegebenen eigentlichen Lösung $x = u, y = v, z = w$ der Gleichung (1) ihre sämtlichen Lösungen abzuleiten.

Da au, bv, cw relative Primzahlen sind, und eine von ihnen, z. B. au , zufolge der Gleichung

$$au^2 + bv^2 + cw^2 = 0 \quad (2)$$

gerade ist, so haben auch die Zahlen $2au, bv, cw$ keinen gemeinschaftlichen Theiler, und man kann daher (nach §. 24) die Gleichung

$$aul + bvm + cwn = 1$$

so lösen, dass l gerade, und folglich die eine der beiden Zahlen m, n gerade, die andere ungerade wird; setzt man nun

$$al^2 + bm^2 + cn^2 = h$$

und

$$u' = 2l - hu, v' = 2m - hv, w' = 2n - hw,$$

so wird h ungerade, und man erhält**)

$$au'^2 + bv'^2 + cw'^2 = 0 \quad (3)$$

$$auu' + bvv' + cww' = 2 \quad (4)$$

$$u \equiv u', v \equiv v', w \equiv w' \pmod{2}; \quad (5)$$

man kann daher

$$vw' - wv' = 2u'', wu' - uw' = 2v'', uv' - vu' = 2w'' \quad (6)$$

setzen, wo u'', v'', w'' ganze Zahlen bedeuten, welche mit den andern noch durch folgende Relationen***)) verbunden sind:

*) Sie ist der Kürze halber synthetisch geführt; derselbe Gegenstand ist auf andere Weise behandelt in der mir erst nachträglich bekannt gewordenen Abhandlung von G. Cantor: *De aequationibus secundi gradus indeterminatis*. 1867.

**) Umgekehrt lässt sich aus (2), (3), (4), (5) leicht beweisen, dass a, b, c relative Primzahlen sind, und dass sowohl u, v, w , als auch u', v', w' eigentliche Lösungen der Gleichung (1) bilden; doch ist dies für unsere Zwecke nicht nöthig.

***)) Man findet z. B. die erste der Gleichungen (7) aus der identischen Gleichung

$$(bv^2 + cw^2)(bv'^2 + cw'^2) = (bvv' + cww')^2 + bc(vw' - wv')^2$$

unter Berücksichtigung von (2), (3), (4), (6); die Gleichung (8) ergibt sich

$$\left. \begin{aligned} auu' &= 1 + bcu''^2 \\ bvv' &= 1 + cav''^2 \\ cww' &= 1 + abw''^2 \end{aligned} \right\} \quad (7)$$

$$bcu''^2 + cav''^2 + abw''^2 = -1 \quad (8)$$

$$\left. \begin{aligned} vw' + wv' &= 2av''w'' \\ wu' + uw' &= 2bw''u'' \\ uv' + vu' &= 2cu''v'' \end{aligned} \right\} \quad (9)$$

Mit Hülfe derselben ist es leicht, unsere Aufgabe allgemein zu lösen. Sind x, y, z drei beliebige ganze Zahlen, so werden auch

$$\left. \begin{aligned} t &= au'x + bv'y + cw'z \\ t' &= aux + byv + czw \\ t'' &= u''x + v''y + w''z \end{aligned} \right\} \quad (10)$$

ganze Zahlen, welche zufolge (5) der Bedingung

$$t \equiv t' \pmod{2} \quad (11)$$

genügen; umgekehrt, sind t, t', t'' drei beliebige ganze Zahlen, welche nur der Bedingung (11) unterworfen sind, so folgt aus (10) unter Berücksichtigung von (5), (7) und (9), dass

$$\left. \begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ 2y &= vt + v't' - 2cav''t'' \\ 2z &= wt + w't' - 2abw''t'' \end{aligned} \right\} \quad (12)$$

gerade, also x, y, z ganze Zahlen sind. Multiplicirt man diese letzten Gleichungen resp. mit ax, by, cz , und addirt mit Rücksicht auf (10), so folgt

$$ax^2 + by^2 + cz^2 = tt' - abct''^2;$$

mithin haben wir folgendes Resultat: *Bilden die ganzen Zahlen x, y, z eine Lösung der Gleichung (1), so werden t, t', t'' vermöge (10) ganze Zahlen, welche den Bedingungen (11) und*

$$tt' = abct''^2 \quad (13)$$

genügen; umgekehrt, befriedigen die ganzen Zahlen t, t', t'' die Be-

durch Addition aus (7) mit Rücksicht auf (4); und die erste der Gleichungen (9) folgt aus der Identität

$$\begin{aligned} (auu' + bvv' + cww')(vw' + wv') - a(wu' - uw')(uv' - vu') \\ = (au^2 + bv^2 + cw^2)v'w' + (au'^2 + bv'^2 + cw'^2)vw. \end{aligned}$$

dingungen (11) und (13), so werden x, y, z vermöge (12) ganze Zahlen, welche der Gleichung (1) genügen*).

Zur Vervollständigung fügen wir hinzu: *Damit die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1) bilden, ist ferner erforderlich und hinreichend, dass die Zahlen t, t' keinen ungeraden gemeinschaftlichen Theiler haben, und dass, wenn beide gerade sind,*

$$t + t' \equiv 2 \pmod{4} \quad (14)$$

ist.

Für unsern Zweck genügt es zu beweisen, dass die beiden angegebenen Bedingungen hinreichend sind. Gesetzt, es ginge eine Primzahl p in zweien der Zahlen ax, by, cz auf, so müsste sie zufolge (1) auch in der dritten aufgehen, mithin zufolge (10) auch in t und t' ; da aber t, t' der Annahme nach keinen ungeraden gemeinschaftlichen Theiler haben, so müsste $p = 2$ sein, und es wären also t, t', ax, by, cz gerade Zahlen; dann würde aber aus (10) mit Rücksicht auf (5) folgen, dass $t + t' \equiv 0 \pmod{4}$ wäre, während wir doch angenommen haben, dass $t + t' \equiv 2 \pmod{4}$ ist, sobald t und t' gerade Zahlen sind. Hieraus folgt also, dass ax, by, cz relative Primzahlen sind, was zu beweisen war**).

*) Die allgemeinste Lösung der Gleichung (13), deren wir zwar in der Folge nicht bedürfen, besteht, wie man sehr leicht findet, in den Gleichungen

$$t = \tau d \omega^2, \quad t' = \tau d' \omega'^2, \quad t'' = \tau \omega \omega',$$

wo $d, d', \tau, \omega, \omega'$ beliebige ganze Zahlen bedeuten, welche der einzigen Bedingung

$$d d' = a b c$$

unterworfen sind; man kann aber auch, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass τ der grösste gemeinschaftliche Theiler von t, t', t'' , und dass $\tau d, \tau d'$ die grössten Theiler sind, welche $\tau a b c$ resp. mit t, t' gemeinschaftlich hat. Führt man diese Ausdrücke in (12) ein, so erhält man die binären quadratischen Formen

$$\frac{2x}{\tau} = (du, -bcu'', d'u'), \quad \frac{2y}{\tau} = (dv, -cav'', d'v'),$$

$$\frac{2z}{\tau} = (dw, -abw'', d'w'),$$

deren Variablen ω, ω' , und deren Determinanten zufolge (7) die Zahlen $-bc, -ca, -ab$ sind. Transformirt man diejenige dieser Formen, deren Determinante negativ ist, in eine reducirte Form (§. 64), so erhält man die einfachsten Lösungen.

**) Es ist leicht, wenn auch für unsern Zweck nicht erforderlich, die beiden angegebenen Bedingungen auf die Zahlen $d, d', \tau, \omega, \omega'$ zu übertragen: die Zahlen d, d' müssen relative Primzahlen sein, und nur, wenn

II. Bilden die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1), so sind ax, by, cz relative Primzahlen, und man kann folglich drei Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ bestimmen, welche den Congruenzen

$$\mathfrak{A}z \equiv by \pmod{a}, \quad \mathfrak{B}x \equiv cz \pmod{b}, \quad \mathfrak{C}y \equiv ax \pmod{c} \quad (15)$$

genügen, woraus in Verbindung mit (1)

$$\mathfrak{A}^2 \equiv -bc \pmod{a}, \quad \mathfrak{B}^2 \equiv -ca \pmod{b}, \quad \mathfrak{C}^2 \equiv -ab \pmod{c} \quad (16)$$

folgt. Wir haben mithin folgenden Satz erhalten:

Ist die Gleichung (1) eigentlich lösbar, so sind die Zahlen $-bc, -ca, -ab$ resp. quadratische Reste der Zahlen a, b, c , und jede eigentliche Lösung x, y, z führt durch die Congruenzen (15) zu drei völlig bestimmten Zahlclassen $\mathfrak{A} \pmod{a}, \mathfrak{B} \pmod{b}, \mathfrak{C} \pmod{c}$, welche den Congruenzen (16) genügen).*

Von der grössten Wichtigkeit für unsere Untersuchungen ist es aber, dass dieser Satz sich in folgender Weise umkehren lässt:

Ist die Gleichung (1) eigentlich lösbar, und sind drei Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ gegeben, welche den Congruenzen (16) genügen, so kann man stets eigentliche Lösungen x, y, z finden, welche die Bedingungen (15) erfüllen.

Um dies zu beweisen, bestimmen wir zunächst drei Zahlen X, Y, Z durch die (nach §. 25) stets vereinbaren Congruenzpaare

$$\left. \begin{aligned} X &\equiv c \pmod{b}, & Y &\equiv a \pmod{c}, & Z &\equiv b \pmod{a} \\ X &\equiv \mathfrak{C} \pmod{c}, & Y &\equiv \mathfrak{A} \pmod{a}, & Z &\equiv \mathfrak{B} \pmod{b} \end{aligned} \right\} \quad (17)$$

aus welchen unter Berücksichtigung der Annahme (16) die der Gleichung (1) ähnliche Congruenz

$$aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{abc} \quad (1')$$

folgt, weil ihre linke Seite durch jede der drei relativen Primzahlen a, b, c theilbar ist. Da ferner die Existenz einer eigentlichen Lö-

$abc \equiv 0 \pmod{8}$), können sie auch den grössten gemeinschaftlichen Theiler 2 haben; umgekehrt, genügt die Zerlegung $abc = dd'$ diesen Bedingungen, so kann man τ, ω, ω' so wählen, dass x, y, z eine eigentliche Lösung der Gleichung (1) bilden.

*) Wirft man zwei eigentliche Lösungen in dieselbe oder in verschiedene Classen, je nachdem sie zu denselben drei Zahlclassen $\mathfrak{A} \pmod{a}, \mathfrak{B} \pmod{b}, \mathfrak{C} \pmod{c}$ führen oder nicht, so ist die Anzahl aller verschiedenen Classen höchstens gleich der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1 \pmod{abc}$, und der nachfolgende Satz behauptet die wirkliche Existenz aller dieser Classen von eigentlichen Lösungen.

sung u, v, w der Gleichung (1) angenommen ist, so behalten wir alle früheren Bezeichnungen bei und setzen

$$\left. \begin{aligned} T &\equiv au'X + bv'Y + cw'Z \\ T' &\equiv auX + bvY + cwZ \end{aligned} \right\} \pmod{2abc}, \quad (10')$$

woraus zufolge (5)

$$T \equiv T' \pmod{2} \quad (11')$$

und mit Rücksicht auf (7) und (9)

$$\left. \begin{aligned} 2X &\equiv uT + u'T' \pmod{2bc} \\ 2Y &\equiv vT + v'T' \pmod{2ca} \\ 2Z &\equiv wT + w'T' \pmod{2ab} \end{aligned} \right\} \quad (12')$$

folgt; multiplicirt man diese Congruenzen resp. mit aX, bY, cZ , wodurch sie in Congruenzen nach dem Modulus $2abc$ übergehen, so ergibt sich durch Addition unter Berücksichtigung von (1') und (10')

$$TT' \equiv 0 \pmod{abc}. \quad (13')$$

Wir behaupten nun, dass die drei Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Divisor haben, und dass, wenn abc gerade ist,

$$T + T' \equiv 2 \pmod{4} \quad (14')$$

ist. Ginge nämlich eine ungerade Primzahl p in T, T' und abc , also auch z. B. in c auf, so würde Y zufolge (12') durch p theilbar sein, und da $a \equiv Y \pmod{c}$ ist, so hätten a und c den gemeinschaftlichen Theiler p , was unmöglich ist. Wenn ferner abc , und also auch z. B. c gerade ist, so sind zufolge (11') und (13') auch T und T' gerade Zahlen; wäre nun die Congruenz (14') unrichtig, so wäre $T' \equiv T \pmod{4}$, und aus (12') würde folgen, dass $2Y \equiv (v + v')T \equiv 0 \pmod{4}$, also Y gerade wäre, was abermals gegen die Congruenz $a \equiv Y \pmod{c}$ streitet, weil a relative Primzahl zu c ist.

Nach diesen Vorbereitungen sind wir im Stande, eine eigentliche Lösung x, y, z nachzuweisen, welche den Bedingungen (15) genügt; diese letztern gehen vermöge der Definition (17) der Zahlen X, Y, Z in die folgenden über

$$Yz \equiv Zy \pmod{a}, \quad Zx \equiv Xz \pmod{b}, \quad Xy \equiv Yx \pmod{c};$$

da ferner aus den Definitionen (10) und (10') der Zahlen t, t', T, T' die Congruenz

$$T't - Tt \equiv$$

$$2bcu''(Yz - Zy) + 2cav''(Zx - Xz) + 2abw''(Xy - Yx) \Big\} \pmod{2abc}$$

folgt, und da u'', v'', w'' zufolge (7) resp. relative Primzahlen zu a, b, c sind, so fallen die von x, y, z zu erfüllenden Bedingungen (15) durchaus mit der einzigen Forderung

$$T't \equiv Tt \pmod{2abc}$$

zusammen, welcher die Zahlen t, t' genügen müssen; sollen ferner die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1) bilden, so haben t und t' ausserdem noch die früher erwähnten Bedingungen (11), (13), (14) zu erfüllen. Dies Alles lässt sich in der That auf folgende Weise erreichen.

Ist abc ungerade, so sei d der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$; da nun zufolge (13') TT' durch abc theilbar ist, so geht d' in T' auf, und da, wie oben gezeigt ist, die Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Theiler haben, so sind d und d' relative Primzahlen, und d' ist zugleich der grösste gemeinschaftliche Theiler der beiden Zahlen T' und abc . Dann leuchtet ein, dass man allen Forderungen genügt, wenn man z. B. $t = d, t' = d', t'' = 1$ nimmt; denn weil $t \equiv t' \equiv 1 \pmod{2}$, so werden x, y, z ganze Zahlen, die wegen $tt' = abct''^2$ eine Lösung der Gleichung (1) bilden; diese Lösung ist eine eigentliche, weil t, t' ungerade relative Primzahlen sind; da endlich $t \equiv t', T \equiv T' \pmod{2}$, und $T't \equiv Tt \equiv 0 \pmod{dd'}$ ist, so folgt auch $T't \equiv Tt \pmod{2abc}$ d. h. die eigentliche Lösung x, y, z genügt den vorgeschriebenen Congruenzen (15).

Ist aber abc , und folglich auch T, T' gerade, und zwar $T + T' \equiv 2 \pmod{4}$, so können wir der Symmetrie wegen annehmen, es sei $T \equiv 0, T' \equiv 2 \pmod{4}$; dann sei d wieder der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$, so wird d' in T' aufgehen. Ist nun d' ungerade, so genügt man allen Bedingungen, wenn man z. B. $t = 2d, t' = 2d', t'' = 2$ nimmt; denn es ist $t \equiv 0, t' \equiv 2 \pmod{4}$, $tt' = abct''^2$, $T't \equiv Tt \equiv 0 \pmod{2abc}$, und t, t' haben keinen ungeraden gemeinschaftlichen Theiler. Ist aber d' gerade, so kann man wieder durch $t = d, t' = d', t'' = 1$ allen Bedingungen genügen; da nämlich $T:d$ relative Primzahl zu d' und folglich ungerade ist, so muss, weil $T \equiv 0 \pmod{4}$, auch $d \equiv 0 \pmod{4}$ sein; da ferner d' in T' aufgeht, und $T' \equiv 2 \pmod{4}$ ist, so muss auch $d' \equiv 2 \pmod{4}$ sein; mithin ist $t \equiv 0, t' \equiv 2 \pmod{4}$; es ist ferner $tt' = abct''^2$, und

die Zahlen t, t' haben keinen ungeraden gemeinschaftlichen Theiler; da endlich die Quotienten $T:d$ und $T':d'$ ungerade sind, so ist ihre Differenz gerade, und folglich, wenn man mit $dd' = abc$ multiplicirt, $T'd' - T'd = Tt' - T't \equiv 0 \pmod{2abc}$, was zu beweisen war.

Es hat keine Schwierigkeit, ausser den eben angegebenen speciellen Lösungen, welche die vorgeschriebenen Congruenzen (15) erfüllen, alle andern zu bestimmen, und man findet namentlich leicht, dass zwei eigentliche Lösungen x, y, z und x_1, y_1, z_1 , welche resp. durch die Werthe t, t', t'' und t_1, t'_1, t''_1 hervorgebracht werden, stets und nur dann denselben Congruenzen (15) genügen, wenn $tt'_1 \equiv t't_1 \pmod{2abc}$ ist*); allein alle diese an sich interessanten Vervollständigungen sind für unsere Zwecke nicht erforderlich. Wir begnügen uns daher, aus den obigen Resultaten noch den Beweis des folgenden Satzes abzuleiten, dessen wir später durchaus bedürfen.

III. *Ist die Gleichung (1) eigentlich lösbar, und ist $-bc$ quadratischer Rest von ap^2 , wo p eine in bc nicht aufgehende Primzahl bedeutet, so besitzt die Gleichung (1) auch solche eigentliche Lösungen x, y, z , welche der Bedingung $x \equiv 0 \pmod{p}$ genügen.*

Der Annahme zufolge besitzt die Gleichung (1) eine eigentliche Lösung u, v, w , und wir können alle hieraus in I. gezogenen Folgerungen für uns in Anspruch nehmen; es versteht sich von selbst, dass wir den vorstehenden Satz nur für den Fall zu beweisen brauchen, dass keine der beiden Zahlen u, u' durch p theilbar ist.

Ist nun p ungerade, so kann man, da der Annahme nach $-bc \equiv \alpha^2 \pmod{p}$ ist, das Vorzeichen von α so wählen, dass $bcu'' + \alpha$ nicht theilbar durch p ist; wären nämlich beide Zahlen

*) Hieraus folgt, dass allen zu derselben Classe gehörigen eigentlichen Lösungen dieselbe Zerlegung $abc = dd'$ entspricht, mit einziger Ausnahme des Falles, wo $abc \equiv 2 \pmod{4}$, in welchem der Factor 2 nach Belieben in d oder in d' aufgenommen werden kann, ohne dass eine Aenderung der Classe eintritt. Auf diese Weise ergibt sich (vergl. die früheren Noten), dass die Anzahl der wesentlich verschiedenen Zerlegungen, und also auch die der wirklich existirenden Classen genau mit der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1 \pmod{abc}$ übereinstimmt; hierin liegt also ein neuer Beweis des obigen Satzes. Aber es schien angemessener, ihn so zu führen, dass zugleich eine Lösung gefunden wird, welche den vorgeschriebenen Congruenzen genügt.

$bcu'' + \alpha$ und $bcu'' - \alpha$ durch p theilbar, so müsste auch ihre Differenz 2α , also auch α durch die ungerade Primzahl p theilbar sein, was gegen $-bc \equiv \alpha^2 \pmod{p}$ und die Annahme streitet, dass p nicht in bc aufgeht. Da nun u ebenfalls nicht durch p theilbar ist, so kann man eine Zahl ω stets so bestimmen (§. 25), dass sie der Congruenz

$$u\omega \equiv bcu'' + \alpha \pmod{p}$$

genügt und ausserdem relative Primzahl zu $2abc$ wird, weil ω , falls p in $2abc$, also in a aufgehen sollte, schon vermöge dieser Congruenz relative Primzahl zu p wird. Setzt man nun

$$t = \tau\omega^2, \quad t' = \tau abc, \quad t'' = \tau\omega,$$

wo $\tau = 1$ oder $= 2$ zu nehmen ist, je nachdem abc ungerade oder gerade ist, so erhält man eine entsprechende eigentliche Lösung x, y, z , welche auch der Bedingung $x \equiv 0 \pmod{p}$ genügt. Ist nämlich abc ungerade, also $\tau = 1$, so ist $t \equiv t' \equiv 1 \pmod{2}$; ist aber abc gerade, also $\tau = 2$, so ist $t \equiv 2, t' \equiv 0 \pmod{4}$; da ferner ω relative Primzahl zu abc ist, so haben t, t' keinen ungeraden gemeinschaftlichen Divisor, und da $tt' = abct''^2$ ist, so bilden x, y, z eine eigentliche Lösung der Gleichung (1). Nun ist nach (12)

$$\begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ &= \tau(u\omega^2 - 2bcu''\omega + abc u') \end{aligned}$$

also mit Rücksicht auf (7)

$$2ux = \tau \{(u\omega - bcu'')^2 + bc\} \equiv 0 \pmod{p},$$

weil $u\omega - bcu'' \equiv \alpha, bc \equiv -\alpha^2$ ist; da endlich $2u$ nicht durch p theilbar ist, so folgt hieraus $x \equiv 0 \pmod{p}$.

Wir gehen jetzt zu dem Falle $p = 2$ über. Ist erstens a gerade, aber nicht $\equiv 0 \pmod{8}$, so ergibt sich leicht, da der Annahme nach $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1 \pmod{8}$ ist, dass u gar nicht ungerade sein kann; da nämlich a gerade, also bv, cw ungerade sind, und $b \equiv -c \pmod{8}$ ist, so folgt aus $au^2 + bv^2 + cw^2 = 0$, dass $au^2 \equiv 0 \pmod{8}$, und folglich, da a nicht $\equiv 0 \pmod{8}$ ist, jedenfalls u gerade sein muss; und offenbar haben dann alle anderen eigentlichen Auflösungen x, y, z dieselbe Eigenschaft $x \equiv 0 \pmod{2}$. Ist zweitens $a \equiv 0 \pmod{8}$, also $-bc \equiv 1 \pmod{8}$, so nehme man $t'' = 1$, und $tt' = abc$ der Art, dass einer der beiden Factoren, z. B. $t \equiv 2 \pmod{4}$, also der andere $t' \equiv 0 \pmod{4}$ wird, und dass sie keinen ungeraden gemeinschaftlichen Divisor erhalten, was sich stets erreichen lässt.

Hieraus folgt, dass die Zahlen x, y, z eine eigentliche Lösung bilden werden. Da nun der Voraussetzung nach u ungerade ist, und da aus $1 + bcu''^2 = auu' \equiv 0 \pmod{8}$ folgt, dass auch u'' ungerade ist, so ergibt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 2 + 0 - 2 \equiv 0 \pmod{4},$$

also ist $x \equiv 0 \pmod{2}$. Ist endlich drittens a ungerade, und $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1 \pmod{4}$, so nehme man $t'' = 1$, und nach Belieben $t't' = abc$, nur so, dass t und t' relative Primzahlen werden; dann bilden x, y, z eine eigentliche Lösung, weil ausserdem $t \equiv t' \equiv 1 \pmod{2}$ ist. Da nun der Voraussetzung nach keine der Zahlen u, u' gerade ist, so folgt aus $auu' = 1 + bcu''^2$, dass u'' gerade, und folglich $auu' \equiv 1 \pmod{4}$ ist; mithin ist $ut \cdot u't' = auu' \cdot bc \equiv -1 \pmod{4}$, also $ut \equiv -u't' \pmod{4}$, und hieraus ergibt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 0 \pmod{4},$$

also ist $x \equiv 0 \pmod{2}$.

Hiermit ist der obige Satz vollständig bewiesen, und dieser Beweis enthält offenbar eine Methode, aus einer eigentlichen Lösung u, v, w einer Gleichung, deren Coefficienten a, b, c sind, eine eigentliche Lösung $x:p, y, z$ derjenigen Gleichung abzuleiten, deren Coefficienten ap^2, b, c sind, vorausgesetzt, dass $-bc$ quadratischer Rest von ap^2 und nicht durch die Primzahl p theilbar ist. Durch wiederholte Anwendung desselben Satzes gelangt man offenbar zu folgendem Resultat:

Sind die Zahlen $A = aP^2, B = bQ^2, C = cR^2$ relative Primzahlen, und sind die Zahlen $-BC, -CA, -AB$ resp. quadratische Reste von A, B, C , so folgt aus der Existenz einer eigentlichen Lösung der Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

stets die Existenz einer eigentlichen Lösung der Gleichung

$$Ax^2 + By^2 + Cz^2 = 0.$$

§. 157.

Durch den zuletzt bewiesenen Satz ist offenbar die Frage nach der eigentlichen Lösbarkeit der Gleichung

$$ax^2 + by^2 + cz^2 = 0 \quad (1)$$

auf den Fall zurückgeführt, in welchem keine der relativen Primzahlen a, b, c durch ein Quadrat theilbar ist; als eine erforderliche Bedingung für die Lösbarkeit ist ferner im vorigen Paragraphen (II) erkannt, dass die Zahlen $-bc, -ca, -ab$ resp. quadratische Reste von den Zahlen a, b, c sein müssen, und ausserdem leuchtet ein, dass die letzteren unmöglich alle dasselbe Vorzeichen haben können. Mit Hülfe einer Reductionsmethode, welche im Wesentlichen von *Lagrange**) herrührt, lässt sich nun wirklich beweisen, dass diese Bedingungen auch die hinreichenden sind, dass also folgender Satz**) besteht:

Sind a, b, c drei von Null verschiedene und durch kein Quadrat theilbare relative Primzahlen, welche nicht alle dasselbe Vorzeichen haben, und sind die Zahlen $-bc, -ca, -ab$ resp. quadratische Reste der Zahlen a, b, c ; so ist die Gleichung (1) eigentlich lösbar.

Zunächst bemerken wir, dass der Satz in dem speciellen Falle richtig ist, wenn einer der Coefficienten, z. B. $a = +1$, ein anderer, z. B. $b = -1$ ist; denn man genügt der Gleichung (1) durch die relativen Primzahlen $x = y = 1, z = 0$.

Um uns nun bequemer ausdrücken zu können, nennen wir, indem wir den absoluten Werth einer Grösse k mit (k) bezeichnen, dasjenige der drei Producte $(bc), (ca), (ab)$, welches der Grösse nach zwischen den beiden anderen liegt, den *Index* der Gleichung (1), und wenn etwa zwei dieser Producte oder alle drei einander gleich sein sollten, so soll unter dem Index der gemeinschaftliche

*) *Sur la solution des problèmes indéterminés du second degré.* Mém. de l'Acad. de Berlin. T. XXIII. 1769. (Œuvres de L. T. II. 1868. p. 375.) — *Additions aux Éléments d'Algèbre par L. Euler.* §. V.

**) *Legendre: Théorie des Nombres*, 3^{me} éd. T. I. §§. III, IV. — *Gauss: D. A.* artt. 294, 295. — Der nachfolgende Beweis lässt sich auf den Fall ausdehnen, dass a, b, c quadratische Divisoren besitzen.

Werth dieser beiden oder aller Producte verstanden werden. Aus dieser Erklärung ergibt sich unmittelbar die Richtigkeit des Satzes für den Fall, dass ihr Index = 1 ist; denn dann muss, wie man leicht erkennt, $(a) = (b) = (c) = 1$ sein, und da die Coefficienten nicht alle dasselbe Vorzeichen haben, so ergibt sich die Lösbarkeit der Gleichung aus der vorausgeschickten Bemerkung.

Um nun den Beweis allgemein zu führen, nehmen wir an, er sei schon geleistet für alle Gleichungen, deren Index kleiner als eine bestimmte positive ganze Zahl J ist, und zeigen, dass der Satz dann auch für alle Gleichungen gelten muss, deren Index = J ist. Gelingt dies, so gilt der Satz allgemein, weil er für $J = 1$ richtig ist.

Es sei daher $J \geq 2$ der Index der Gleichung (1). Nehmen wir an, was der Symmetrie wegen erlaubt ist, es sei $(a) \leq (b) \leq (c)$, also auch $(ab) \leq (ac) \leq (bc)$, so ist $J = (ac)$; wäre nun $(b) = (c)$, so müsste, weil b und c relative Primzahlen sind, $(b) = (c) = 1$ sein, woraus auch $J = 1$ folgen würde, was mit unserer Annahme streitet; mithin ist

$$(a) \leq (b) < (c), (ab) < (ac) = J \leq (bc). \quad (2)$$

Der Annahme nach ist nun $-ab$ quadratischer Rest von c , und folglich kann man eine Zahl r so bestimmen, dass $ar^2 \equiv -b \pmod{c}$, und zugleich $(r) \leq \frac{1}{2}(c)$ wird; setzt man dann

$$ar^2 + b = cC, \quad (3)$$

so wird C eine ganze Zahl, deren absoluter Werth

$$(C) \leq \frac{(a)r^2 + (b)}{(c)} < \frac{1}{4}J + 1 < J \quad (4)$$

ist, weil $(r) \leq \frac{1}{2}(c)$, $(ac) = J \geq 2$, und $(b) < (c)$ ist.

Ist nun $C = 0$, so folgt $b = -ar^2$, also, da b relative Primzahl zu a und durch kein Quadrat theilbar ist, $(r) = 1$ und $b = -a = \pm 1$, und mithin besitzt die Gleichung (1) in diesem Fall wieder die eigentliche Lösung $x = y = 1, z = 0$.

Ist aber C von Null verschieden, so führen wir die Gleichung (1) folgendermaassen auf eine andere von kleinerem Index zurück. Es sei a' der grösste gemeinschaftliche Divisor der drei in der Gleichung (3) vorkommenden Glieder ar^2, b, cC , so ist a' zugleich der grösste gemeinschaftliche Divisor von je zweien dieser Zahlen, so dass die drei Glieder der Gleichung

$$\frac{ar^2}{a'} + \frac{b}{a'} = \frac{cC}{a'}$$

gewiss relative Primzahlen sind. Da nun a' in b aufgeht, also relative Primzahl zu c und zu a ist, so muss a' in C und in r^2 , also auch in r selbst aufgehen, weil a' als Divisor von b durch kein Quadrat theilbar ist. Man kann daher

$$r = a'\alpha, \quad b = a'\beta, \quad C = a'C' = a'c'\gamma^2 \quad (5)$$

setzen, wo γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat bedeutet; hierdurch geht die Gleichung (3) in die folgende über

$$aa'\alpha^2 + \beta = c'c'\gamma^2, \quad (6)$$

deren drei Glieder also relative Primzahlen sind; setzen wir endlich noch

$$b' = a\beta, \quad (7)$$

so sind hierdurch drei Zahlen a', b', c' definirt, welche, wie wir beweisen wollen, dieselben Eigenschaften besitzen, wie die gegebenen Zahlen a, b, c .

Dass erstens keine der Zahlen $a', b', c' = 0$ ist, leuchtet ein, weil $a'b' = a'a\beta = ab$ ist, und c' in C aufgeht. Aus $a'b' = ab$ folgt ferner, dass a', b' relative Primzahlen und durch kein Quadrat theilbar sind, weil a, b dieselben Eigenschaften haben; da ferner γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat ist, so kann c' durch kein Quadrat theilbar sein; und da die Glieder der Gleichung (6) relative Primzahlen sind, so ist c' auch relative Primzahl zu $aa'\beta = a'b'$.

Die Zahlen a', b', c' können auch nicht alle dasselbe Vorzeichen haben; ist nämlich $ab = a'b'$ negativ, so haben a', b' entgegengesetzte Zeichen; ist aber ab positiv, folglich ca und bc negativ, so ergibt sich aus der Gleichung $ar^2 + b = ca'c'\gamma^2$, dass $a'c'$ negativ ist, dass also a', c' entgegengesetzte Vorzeichen haben.

Da ferner zufolge der Gleichung (6), deren drei Glieder relative Primzahlen sind, die drei Zahlen $\beta cc', ac'a'c', -aa'\beta = -a'b'$ resp. quadratische Reste der drei Zahlen aa', β, c' sein müssen, und da nach Voraussetzung die beiden Zahlen $-bc = -\beta a'c', -ca$ resp. Reste von den beiden Zahlen $a, b = a'\beta$ sind, so ergibt sich hieraus leicht, dass die drei Zahlen $-b'c', -c'a', -a'b'$ resp. Reste der drei Zahlen a', b', c' sind.

Endlich ist $(a'b') = (ab) < J$ zufolge (2), und $(c'a') \leq (c'a')\gamma^2 = (C) < J$ zufolge (4); mithin ist der Index der Gleichung

$$a'x'^2 + b'y'^2 + c'z'^2 = 0$$

gewiss kleiner als J , und folglich ist sie nach unserer obigen Voraussetzung lösbar in relativen Primzahlen x', y', z' ; da nun die Zahlen $a' \alpha x' - \beta y', x' + a \alpha y'$ nicht beide verschwinden, weil sonst auch $x' = y' = 0$ wäre, so kann man

$$mx = a' \alpha x' - \beta y'; \quad my = x' + a \alpha y'; \quad mz = c' \gamma z'$$

setzen, wo m den grössten gemeinschaftlichen Theiler der drei Zahlen rechter Hand bedeutet; hieraus folgt aber mit Beachtung von (5), (6), (7)

$$m^2(ax^2 + by^2 + cz^2) = cc' \gamma^2 (a' x'^2 + b' y'^2 + c' z'^2) = 0,$$

also, da m nicht $= 0$ ist, auch

$$ax^2 + by^2 + cz^2 = 0;$$

da endlich die Zahlen x, y, z keinen gemeinschaftlichen Theiler haben, und keine der Zahlen a, b, c durch ein Quadrat theilbar ist, so sind x, y, z auch relative Primzahlen und bilden folglich eine eigentliche Lösung der Gleichung (1).

Hiermit ist der Schluss vollständig durchgeführt, und also auch der obige Satz allgemein bewiesen. Es leuchtet ferner ein, dass in der successiven Zurückführung der Gleichung (1) auf ähnliche Gleichungen von immer kleinerem Index und endlich auf eine Gleichung, in welcher ein Coefficient $= +1$, ein anderer $= -1$ ist, auch eine Methode liegt, eine Lösung derselben zu finden.

Nachdem für diejenigen Gleichungen, deren Coefficienten durch kein Quadrat theilbar sind, die oben genannten *erforderlichen* Bedingungen zugleich als *hinreichend* für die Existenz eigentlicher Lösungen erkannt sind, so geht aus dem Schlussätze des vorigen Paragraphen hervor, dass genau Dasselbe Statt findet für alle Gleichungen (1), deren Coefficienten von Null verschieden und relative Primzahlen sind. Wir können daher das Gesamtergebn unserer Untersuchungen in dem folgenden wichtigen Satze niederlegen:

Sind die Zahlen a, b, c relative Primzahlen und von Null verschieden, so ist die Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

stets und nur dann in relativen Primzahlen x, y, z lösbar, wenn die Zahlen $-bc, -ca, -ab$ resp. quadratische Reste von den Zahlen a, b, c sind, und diese letzteren nicht alle dasselbe Vorzeichen haben; ist ferner

$-bc \equiv \mathfrak{A}^2 \pmod{a}$, $-ca \equiv \mathfrak{B}^2 \pmod{b}$, $-ab \equiv \mathfrak{C}^2 \pmod{c}$,
 so ist die obige Gleichung in relativen Primzahlen x, y, z der Art
 lösbar, dass

$\mathfrak{A}z \equiv by \pmod{a}$, $\mathfrak{B}x \equiv cz \pmod{b}$, $\mathfrak{C}y \equiv ax \pmod{c}$
 wird.

§. 158.

Mit Hülfe dieses Satzes lässt sich nun das oben (§. 155) erwähnte grosse Theorem von *Gauss* leicht beweisen:

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Als Repräsentanten der dem Hauptgeschlechte der Determinante D angehörenden Classe wählen wir eine Form (A, B, C) , deren erster Coefficient A relative Primzahl zu $2D$ ist (§. 93). Da die Zahl A durch diese Form darstellbar ist, und alle Einzel-Charaktere derselben den Werth $+1$ haben, so ist A quadratischer Rest von jeder in D aufgehenden ungeraden Primzahl, und auch von 4 oder von 8, falls D durch 4 oder 8 theilbar ist (§. 122); mithin ist (nach §. 37) A quadratischer Rest von D selbst (umgekehrt ergibt sich leicht, zum Theil mit Hülfe des Reciprocitätssatzes, dass die Form (A, B, C) gewiss dem Hauptgeschlechte angehört, wenn A relative Primzahl zu $2D$, quadratischer Rest von D , und, falls D negativ sein sollte, positiv ist). Ja, man kann sogar voraussetzen, dass A quadratischer Rest von $4D$ ist, d. h. dass $A \equiv 1 \pmod{4}$, oder $A \equiv 1 \pmod{8}$ ist, je nachdem D ungerade oder gerade ist. Dies ist in der That von selbst der Fall, wenn $D \equiv 3 \pmod{4}$, oder $D \equiv 0 \pmod{8}$ ist; sollte ferner A in den übrigen Fällen dieser Bedingung nicht genügen, wäre also $A \equiv 3 \pmod{4}$, $\equiv 7 \pmod{8}$, $\equiv 3 \pmod{8}$, $\equiv 5 \pmod{8}$, je nachdem $D \equiv 1 \pmod{4}$, $\equiv 2 \pmod{8}$, $\equiv 6 \pmod{8}$, $\equiv 4 \pmod{8}$, so kann man die Form (A, B, C) durch eine Substitution $\begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}$ in eine Form transformiren, deren erster Coefficient $A' = A\alpha^2 + 2B\alpha + C$ relative Primzahl zu $2D$ ist und zugleich die verlangte Eigenschaft besitzt; da nämlich $AA' = (A\alpha + B)^2 - D$ ist, so braucht man α nur so zu wählen, dass $A\alpha + B$ im ersten Falle gerade, in den drei übrigen Fällen aber ungerade wird, was sich stets in der Art erreichen lässt, dass $A\alpha + B$ zugleich relative Primzahl zu D wird.

Wir setzen daher voraus, dass A quadratischer Rest von $4D$ und relative Primzahl zu $4D$ ist; da nun $4D \equiv (2B)^2 \pmod{A}$, also quadratischer Rest von A ist, und da die Zahlen $A, 4D$ nicht beide negativ sind, so besitzt die Gleichung

$$Ax^2 + 4Dy^2 - z^2 = 0$$

immer eigentliche Lösungen x, y, z , welche der Bedingung

$$2Bz \equiv 4Dy, \text{ also } z \equiv 2By \pmod{A}$$

genügen (§. 157); man kann daher $z = At + 2By$ setzen, wodurch die obige Gleichung in die folgende übergeht

$$At^2 + 2B(2y) + C(2y)^2 = x^2;$$

da $Ax, 2Dy, z$ relative Primzahlen sind, so sind auch $t, 2y$ relative Primzahlen, und folglich ist (A, B, C) einer Form äquivalent (§. 60), deren erster Coefficient x^2 eine Quadratzahl und relative Primzahl zu $2D$ ist, und welche folglich (nach §. 155) durch Duplication einer Form entsteht, deren erster Coefficient $\pm x$ ist. Was zu beweisen war*).

Die unendlich vielen eigentlichen Lösungen x, y, z der obigen Gleichung, welche der Bedingung $z \equiv 2By \pmod{A}$ genügen, zerfallen nun noch in verschiedene Classen in Bezug auf den Modul $4D$ (§. 156. II.); auf den Zusammenhang dieser Lösungen mit den verschiedenen Classen, durch deren Duplication dieselbe gegebene Classe des Hauptgeschlechtes entsteht, können wir aber hier nicht mehr eingehen.

§. 159.

Die Theorie der binären quadratischen Formen, ihrer Aequivalenz und Composition bildet nur einen speciellen Fall von der Theorie derjenigen homogenen Formen n ten Grades mit n Veränderlichen, welche sich in lineare Factoren mit algebraischen

*) Die Zurückführung dieses Satzes von *Gauss* auf den von *Lagrange* und *Legendre* ist, wie ich jetzt nachträglich bemerke, zuerst von *Arndt* ausgeführt (*Ueber die Anzahl der Genera der quadratischen Formen*; *Crelle's Journal* LVI), doch weicht die obige Darstellung in mehreren Punkten von der seinigen ab. In Wahrheit gehört der Satz von *Lagrange* nach Inhalt und Methode des Beweises in die Theorie der ternären Formen. — Man vergl. ferner *Kronecker*: *Ueber den Gebrauch der Dirichlet'schen Methoden in der Theorie der quadratischen Formen* (*Monatsber. d. Berliner Ak.* 12. Mai 1864).

Coefficienten zerlegen lassen. Diese Formen sind zuerst von *Lagrange* *) betrachtet; später hat *Dirichlet* **) sich vielfach mit diesem Gegenstande beschäftigt, aber er hat von seinen weit gehenden Untersuchungen nur diejenige veröffentlicht, welche die Transformationen solcher Formen in sich selbst (vergl. §§. 61, 62) oder, was dasselbe ist, die Theorie der Einheiten für die entsprechenden algebraischen Zahlen behandelt; endlich hat *Kummer* ***) durch die Schöpfung der idealen Zahlen einen neuen Weg betreten, welcher nicht nur zu einer sehr bequemen Ausdrucksweise, sondern auch zu einer tieferen Einsicht in die wahre Natur der algebraischen Zahlen führt. Indem wir versuchen, den Leser in diese neuen Ideen einzuführen, stellen wir uns auf einen etwas höheren Standpunkt und beginnen damit, einen Begriff einzuführen, welcher wohl geeignet scheint, als Grundlage für die höhere Algebra und die mit ihr zusammenhängenden Theile der Zahlentheorie zu dienen.

I. Unter einem *Körper* wollen wir jedes System von unendlich vielen reellen oder complexen Zahlen verstehen, welches in sich so abgeschlossen und vollständig ist, dass die Addition, Subtraction, Multiplication und Division von je zwei dieser Zahlen immer wieder eine Zahl desselben Systems hervorbringt. Der einfachste Körper wird durch alle rationalen, der grösste Körper durch alle Zahlen gebildet. Wir nennen einen Körper *A* einen *Divisor* des Körpers *M*, diesen ein *Multiplum* von jenem, wenn alle in *A* enthaltenen Zahlen sich auch in *M* vorfinden; man findet leicht, dass der Körper der rationalen Zahlen ein Divisor von jedem andern Körper ist. Der Inbegriff aller Zahlen, welche gleichzeitig in zwei Körpern *A*, *B* enthalten sind, bildet wieder einen Körper *D*, welcher der *grösste* gemeinschaftliche Divisor der beiden Körper *A*, *B* genannt werden kann, weil offenbar jeder gemeinschaftliche Divisor von *A* und *B* nothwendig ein Divisor von *D* ist; ebenso existirt immer ein Körper *M*, welcher das *kleinste* gemeinschaftliche Multiplum von *A* und *B* heissen soll, weil er ein Divisor von jedem andern gemeinschaftlichen Multiplum der beiden Körper ist. Entspricht ferner einer jeden Zahl *a* des Körpers *A* eine Zahl $b = \varphi(a)$

*) *Sur la solution des problèmes indéterminés du second degré.* §. VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. (Œuvres de L. T. II, 1868, p. 375.)
 — *Additions aux Éléments d'Algèbre par L. Euler.* §. IX.

**) Vergl. Anm. zu §. 141.

***) Vergl. Anm. zu §. 16.

in der Weise, dass $\varphi(a + a') = \varphi(a) + \varphi(a')$, und $\varphi(aa') = \varphi(a) \varphi(a')$ ist, so bilden die Zahlen b (falls sie nicht sämmtlich verschwinden) ebenfalls einen Körper $B = \varphi(A)$, welcher mit A conjugirt ist und durch die Substitution φ aus A hervorgeht; dann ist rückwärts auch $A = \psi(B)$ mit B conjugirt. Zwei mit einem dritten conjugirte Körper sind auch mit einander conjugirt, und jeder Körper ist mit sich selbst conjugirt. Correspondirende Zahlen in zwei conjugirten Körpern A und B , wie a und $b = \varphi(a)$, sollen *conjugirte Zahlen* heissen.

Die einfachsten Körper sind diejenigen, welche nur eine *endliche* Anzahl von Divisoren besitzen. Nennt man m bestimmte Zahlen $\alpha_1, \alpha_2 \dots \alpha_m$ von einander abhängig oder *unabhängig*, je nachdem die Gleichung $x_1 \alpha_1 + x_2 \alpha_2 + \dots + x_m \alpha_m = 0$ in rationalen Zahlen $x_1, x_2 \dots x_m$, die nicht sämmtlich verschwinden, lösbar ist oder nicht, so findet man durch sehr einfache Betrachtungen, auf die wir aber hier nicht eingehen wollen, dass aus einem Körper Ω von der angegebenen Art*) nur eine *endliche* Anzahl n von unabhängigen Zahlen $\omega_1, \omega_2 \dots \omega_n$ sich auswählen lässt, dass also jede Zahl ω des Körpers stets und nur auf eine einzige Art durch die Form

$$\omega = h_1 \omega_1 + h_2 \omega_2 + \dots + h_n \omega_n = \sum h_i \omega_i \quad (1)$$

darstellbar ist, wo $h_1, h_2 \dots h_n$ rationale Zahlen bedeuten. Wir wollen die Zahl n den *Grad*, ferner den Complex der n unabhängigen Zahlen ω_i eine *Basis des Körpers* Ω , und die n Zahlen h_i die dieser Basis entsprechenden *Coordinaten der Zahl* ω nennen; offenbar bilden je n Zahlen von der Form (1) wieder eine solche Basis, wenn die aus den entsprechenden n^2 Coordinaten gebildete Determinante von Null verschieden ist; einer solchen *Transformation* der Basis durch eine lineare Substitution entspricht eine Transformation der Coordinaten durch die sogenannte *transponirte* Substitution.

Die Forderung, dass die Zahlen ω des Körpers Ω durch Addition und Subtraction sich reproduciren sollen, wird durch ihre gemeinsame Form (1) schon erfüllt; für die Reproduction durch Multiplication ist ferner erforderlich und hinreichend, dass jedes

*) Ersetzt man die rationalen Zahlen überall durch Zahlen eines Körpers R , so gelten die nachfolgenden Betrachtungen auch für einen Körper Ω , welcher nur eine endliche Anzahl solcher Divisoren besitzt, die zugleich Multipla von R sind.

Product $\omega_i \omega_r$ wieder in der Form (1) enthalten ist; diese Bedingungen, deren Anzahl $= \frac{1}{2}n(n+1)$ ist, lassen sich am einfachsten zusammenfassen, indem man die Coordinaten h_i als *veränderlich* ansieht und

$$\omega^2 = 2 \sum H_i \omega_i \quad (2)$$

setzt, wo nun $H_1, H_2 \dots H_n$ bestimmte, mit *rationalen Coefficienten* behaftete, ganze homogene quadratische Functionen der Coordinaten bedeuten. Durch diese n Functionen H_i , auf deren analytische Eigenschaften wir unten zurückkommen werden, ist die Constitution des Körpers Ω vollständig bestimmt, und es lässt sich zunächst zeigen, dass die Zahlen von der Form (1) auch durch Division sich wieder erzeugen. Durch totale Differentiation von (2) erhält man

$$\omega d\omega = \sum dH_i \omega_i; \quad (3)$$

legt man den Coordinaten h_i und ihren Differentialen dh_i beliebige rationale Werthe bei, so ist durch die vorstehende Gleichung das Product aus zwei beliebigen Zahlen ω und $d\omega$ des Körpers Ω auf die Form (1) zurückgeführt. Speciell ergibt sich aus (3)

$$\omega \omega_r = \sum \frac{\partial H_i}{\partial h_r} \omega_i; \quad (4)$$

legt man nun den Coordinaten h_i beliebige rationale Werthe bei, welche aber nicht sämmtlich verschwinden, so kann auch der entsprechende Werth der Functional-Determinante

$$H = \sum \pm \frac{\partial H_1}{\partial h_1} \frac{\partial H_2}{\partial h_2} \dots \frac{\partial H_n}{\partial h_n} \quad (5)$$

nicht verschwinden; denn sonst liessen sich bekanntlich n rationale Zahlen dh_i , die nicht sämmtlich verschwinden, so bestimmen, dass für jeden Index r

$$dH_r = \sum \frac{\partial H_r}{\partial h_i} dh_i = 0,$$

und folglich auch $\omega d\omega = 0$ würde, während doch keine der beiden Zahlen ω und $d\omega$ verschwindet. Hieraus folgt weiter durch Umkehrung der n Gleichungen (4), dass die n Quotienten $\omega_i : \omega$ wieder Zahlen von der Form (1) sind; dasselbe gilt daher auch von jedem Quotienten $\alpha : \omega$, wo α irgend eine Zahl von der Form (1) bedeutet. Mithin bilden alle Zahlen von der Form (1) wirklich einen Körper.

Durch Elimination der n Zahlen ω_i aus den n Gleichungen (4) ergibt sich die Gleichung

$$\begin{vmatrix} \frac{\partial H_1}{\partial h_1} - \omega, & \frac{\partial H_2}{\partial h_1} & \dots & \frac{\partial H_n}{\partial h_1} \\ \frac{\partial H_1}{\partial h_2}, & \frac{\partial H_2}{\partial h_2} - \omega & \dots & \frac{\partial H_n}{\partial h_2} \\ \dots & \dots & \dots & \dots \\ \frac{\partial H_1}{\partial h_n}, & \frac{\partial H_2}{\partial h_n} & \dots & \frac{\partial H_n}{\partial h_n} - \omega \end{vmatrix} = 0 \quad (6)$$

mithin ist jede Zahl ω des Körpers Ω die Wurzel einer (von der Wahl der Basis unabhängigen) Gleichung n ten Grades mit rationalen Coefficienten, also eine *algebraische Zahl*, und es lässt sich leicht zeigen, dass in dem Körper Ω auch Zahlen existiren, welche keiner Gleichung mit rationalen Coefficienten von niedrigerem als dem n ten Grade genügen, für welche also die vorstehende Gleichung *irreductibel* ist*). Bedeutet θ eine solche Zahl, so bilden

*) Der Beweis dieser Behauptung kann z. B. auf das folgende Lemma gestützt werden:

Genügt eine homogene lineare Function $\omega = \sum h_i \omega_i$ der n Variablen h_i einer Identität von der Form

$$A \omega^m + A_1 \omega^{m-1} + \dots + A_m = 0, \quad (1)$$

wo $A, A_1 \dots A_m$ ganze Functionen der Variablen h_i mit *rationalen* Coefficienten bedeuten, die nicht sämmtlich identisch verschwinden, und ist der Grad m *kleiner* als die Anzahl n der Variablen, so sind die n Grössen ω_i von einander *abhängig*.

Durch totale Differentiation der Identität (1) ergibt sich zunächst

$$M d\omega + \omega^m dA + \omega^{m-1} dA_1 + \dots + dA_m = 0, \quad (2)$$

wo zur Abkürzung

$$M = m A \omega^{m-1} + (m-1) A_1 \omega^{m-2} + \dots + A_{m-1}$$

gesetzt ist. Man kann nun offenbar annehmen, dass keine solche Identität (1) von noch niedrigerem Grade als m existirt, dass also das Product AM nicht identisch verschwindet; nun lege man, was stets möglich ist, den Variablen h_i solche rationale Werthe bei, für welche AM einen von Null verschiedenen Werth erhält; hierauf kann man, weil $m < n$ ist, den n Differentialen dh_i solche rationale Werthe beilegen, welche den m homogenen linearen Gleichungen

$$A dA_1 = A_1 dA, A dA_2 = A_2 dA \dots A dA_m = A_m dA$$

genügen und nicht sämmtlich verschwinden; multiplicirt man nun (1) mit dA , (2) mit A , und subtrahirt, so folgt $AM d\omega = 0$, also auch $d\omega = \sum dh_i \omega_i = 0$, was zu beweisen war.

Hieraus folgt zunächst, dass, wenn die Grössen ω_i und ω wieder ihre alte Bedeutung erhalten, die aus den Coordinaten der n Grössen $1, \omega, \omega^2 \dots \omega^{n-1}$ gebildete Determinante D , welche eine homogene Function der

offenbar die Potenzen $1, \theta, \theta^2 \dots \theta^{n-1}$ ebenfalls eine Basis des Körpers Ω , und Ω ist das System aller Zahlen, welche sich durch beliebige Wiederholung der vier arithmetischen Grundoperationen aus θ ableiten lassen. Substituirt man nun für θ der Reihe nach alle Wurzeln derselben irreductibelen Gleichung, so entstehen ebensoviele entsprechende Körper welche offenbar mit Ω und folglich auch mit einander conjugirt sind, und es liesse sich leicht zeigen, dass ausser diesen Körpern kein anderer mit Ω conjugirt ist. Dabei bemerken wir aber, um Missverständnissen vorzubeugen, dass diese n Körper, was ihren gesammten Zahleninhalt anbetrifft, sehr wohl theilweise oder auch sämmtlich identisch sein können, obgleich sie durch n verschiedene Substitutionen aus einem von ihnen hervorgehen*).

Da nun vermöge des Begriffes conjugirter Körper die Gleichungen (4) gültig bleiben, wenn die Zahlen des Körpers Ω durch die entsprechenden Zahlen eines conjugirten Körpers ersetzt werden, so folgt leicht, dass die sämmtlichen Wurzeln der Gleichung (6) die mit ω conjugirten Zahlen sind. Bezeichnet man daher mit $N(\omega)$ die sogenannte Norm der Zahl ω , d. h. das Product aus allen n conjugirten Wurzeln, die auch gruppenweise einander gleich sein können, so ist zufolge (6)

$$N(\omega) = H, \quad (7)$$

d. h. die homogene Function H ist das Product aus n conjugirten Factoren ersten Grades mit algebraischen Coefficienten. Aus dieser

Variablen h_i vom Grade $\frac{1}{2}n(n-1)$ ist, nicht identisch verschwinden kann, weil sonst ω einer Identität von der obigen Form (1) und von niedrigerem Grade als n genüge, und folglich die Grössen ω_i von einander abhängig wären. Giebt man nun den Coordinaten h_i solche rationale Werthe, für welche D einen von Null verschiedenen Werth erhält, so folgt unmittelbar, dass die entsprechende Zahl ω des Körpers Ω die Wurzel einer irreductibelen Gleichung n ten Grades ist.

Jeder Lösung der Gleichung $D = 0$ in rationalen Zahlen h_i entspricht eine Zahl ω , welche einem Divisor des Körpers Ω von niedrigerem als dem n ten Grade angehört; der Grad eines solchen Divisors ist immer ein Divisor von n .

*) Durch die weitere Verfolgung dieses Gegenstandes gelangt man unmittelbar zu den von Galois in die Algebra eingeführten Principien (*Sur les conditions de résolubilité des équations par radicaux*; Journ. de Math. p. p. Liouville. T. XI. 1846); hierbei ist es zweckmässig, zunächst die einfachen Reciprocitätsgesetze aufzusuchen, welche zwischen irgend zwei solchen Körpern wie Ω , ihrem grössten gemeinschaftlichen Divisor und ihrem kleinsten gemeinschaftlichen Multiplum herrschen.

Definition geht unmittelbar der Satz hervor: *die Norm eines Productes ist immer gleich dem Product aus den Normen der Factoren.* Setzt man ferner

$$N(\omega) = \omega \omega', \quad (8)$$

so ist ω' , weil $N(\omega)$ als rationale Zahl in Ω enthalten ist, ebenfalls eine Zahl des Körpers Ω , was auch aus (6) hervorgeht, und zwar ist

$$N(\omega') = N(\omega)^{n-1}; \quad (9)$$

nennen wir ω' die *zu ω adjungirte Zahl**), so ist die zu ω' adjungirte Zahl $= \omega N(\omega)^{n-2}$.

Sind $\alpha_1, \alpha_2 \dots \alpha_n$ beliebige Zahlen des Körpers Ω , und bedeuten $\beta_i, \gamma_i \dots \lambda_i$ die übrigen $(n-1)$ mit α_i conjugirten Zahlen, so setzen wir zur Abkürzung

$$(\sum \pm \alpha_1 \beta_2 \dots \lambda_n)^2 = \Delta(\alpha_1, \alpha_2 \dots \alpha_n) \quad (10)$$

und nennen dieses Determinantenquadrat die *Discriminante* der n Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$; sie ist eine symmetrische Function der n mit θ conjugirten Zahlen und folglich eine *rationale* Zahl, und zwar ist

$$\Delta(\alpha_1, \alpha_2 \dots \alpha_n) = m^2 \Delta(\omega_1, \omega_2 \dots \omega_n), \quad (11)$$

wo m die aus den Coordinaten der Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$ gebildete Determinante bedeutet; da die Discriminante $\Delta(1, \theta, \theta^2 \dots \theta^{n-1})$ bekanntlich das Product aller Differenzen zwischen den mit θ conjugirten Zahlen und folglich von Null verschieden ist (weil eine irreductibele Gleichung nur ungleiche Wurzeln haben kann), so ist $\Delta(\alpha_1 \dots \alpha_n)$ stets und nur dann $= 0$, wenn die Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$ von einander abhängig sind. Endlich ist allgemein

$$\Delta(\omega \alpha_1, \omega \alpha_2 \dots \omega \alpha_n) = N(\omega)^2 \Delta(\alpha_1, \alpha_2 \dots \alpha_n). \quad (12)$$

II. Im Vorhergehenden sind die Begriffe und Sätze entwickelt, deren wir in der Folge bedürfen; zur Erläuterung mögen aber hier noch die wichtigsten und nächstliegenden Resultate aus dem grossen Reichthume analytischer Entwicklungen mitgetheilt werden, welche sich an die Betrachtung der Functionen H_i anknüpfen. Zwischen diesen n Functionen bestehen fundamentale Relationen, welche man erhält, wenn man das Product aus *drei* beliebigen Zahlen des Körpers Ω auf alle möglichen Arten bildet (vergl. §§. 1, 2). Bedeutet d' wieder eine beliebige Variation, so ist zufolge (4)

*) Dieser Ausdruck wird hier in ganz anderer Bedeutung gebraucht, wie von *Galois*.

$$d'\omega \omega_r = \Sigma d' \left(\frac{\partial H_i}{\partial h_r} \right) \omega_i;$$

multiplirt man nun (3) mit $d'\omega$, und ersetzt die Producte $d'\omega \omega_i$, der vorstehenden Gleichung gemäss durch Summen, so folgt

$$\omega d\omega d'\omega = \Sigma dH_i d' \left(\frac{\partial H_{i'}}{\partial h_i} \right) \omega_{i'};$$

da die linke Seite symmetrisch in Bezug auf d und d' ist, und da die n Zahlen $\omega_{i'}$ unabhängig sind, so ergibt sich, dass die Functionen H_i den n Differentialgleichungen

$$\Sigma dH_i d' \left(\frac{\partial H_r}{\partial h_i} \right) = \Sigma d'H_i d \left(\frac{\partial H_r}{\partial h_i} \right) \quad (13)$$

genügen, wo r irgend einen der Indices $1, 2 \dots n$ bedeutet. Um die Bedeutung dieser Relationen mehr hervortreten zu lassen, wollen wir sie den folgenden Entwicklungen zu Grunde legen, ohne den Zusammenhang der Functionen H_i mit dem Körper Ω zu benutzen.

Zunächst wollen wir zeigen, dass die Functionaldeterminante H , welche zufolge ihrer Definition (5) eine ganze homogene Function n ten Grades mit rationalen Coefficienten ist, sich durch Multiplication reproducirt; gehen die Formen K und L dadurch aus H hervor, dass die Coordinaten h_i resp. durch dh_i und durch dH_i ersetzt werden, so ist

$$L = HK; \quad (14)$$

denn wenn man die Coordinaten h_i durch dh_i ersetzt, so geht jede homogene lineare Function

$$\frac{\partial H_r}{\partial h_s} \text{ in } d \left(\frac{\partial H_r}{\partial h_s} \right),$$

und folglich H in

$$K = \Sigma \pm d \left(\frac{\partial H_1}{\partial h_1} \right) d \left(\frac{\partial H_2}{\partial h_2} \right) \dots d \left(\frac{\partial H_n}{\partial h_n} \right)$$

über; werden aber die Coordinaten h_i durch die bilinearen Functionen dH_i ersetzt, so geht zufolge (13)

$$\frac{\partial H_r}{\partial h_s} \text{ in } \Sigma \frac{\partial}{\partial h_s} \left(\frac{\partial H_r}{\partial h_i} \right) dH_i = \Sigma \frac{\partial H_i}{\partial h_s} d \left(\frac{\partial H_r}{\partial h_i} \right),$$

und folglich H in $L = HK$ über, was zu beweisen war. Dies ist der schon oben angeführte Satz über die Norm eines Productes.

Bedeutet φ eine willkürliche Function der Coordinaten h_i , und definiert man die Variation δ dadurch, dass

$$\delta \varphi = \Sigma \frac{\partial \varphi}{\partial H_i} h_i, \quad \text{also} \quad \delta H_i = h_i \quad (15)$$

wird, so ergibt sich aus (13), wenn man d' durch δ ersetzt,

$$\Sigma d H_i \delta \left(\frac{\partial H_r}{\partial h_i} \right) = \Sigma h_i d \left(\frac{\partial H_r}{\partial h_i} \right) = d H_r,$$

weil H_r eine homogene Function zweiten Grades ist, mithin

$$\delta \left(\frac{\partial H_r}{\partial h_s} \right) = 1 \quad \text{oder} \quad = 0 \quad (16)$$

je nachdem r und s gleich oder ungleich sind; hieraus folgt, dass die n Variationen δh_i *constante, rationale Zahlen* sind. Wird ferner die Variation δ' durch

$$\delta' \varphi = H \Sigma \frac{\partial \varphi}{\partial H_i} \delta h_i, \quad \text{also} \quad \delta' H_i = H \delta h_i \quad (17)$$

definiert, so ergibt sich, wenn man in (13) d' durch δ' ersetzt,

$$\begin{aligned} \Sigma d H_i \delta' \left(\frac{\partial H_r}{\partial h_i} \right) &= H \Sigma \delta h_i d \left(\frac{\partial H_r}{\partial h_i} \right) = H d \Sigma \frac{\partial H_r}{\partial h_i} \delta h_i \\ &= H d \delta H_r = H d h_r, \end{aligned}$$

folglich

$$\delta' \left(\frac{\partial H_r}{\partial h_s} \right) = H \frac{\partial h_r}{\partial H_s}; \quad (18)$$

da nun der Ausdruck rechter Hand der Coefficient des Elementes

$$\frac{\partial H_s}{\partial h_r}$$

in der Determinante H , also eine *ganze homogene Function* $(n - 1)$ ten Grades der Coordinaten h_i mit rationalen Coefficienten ist, so gilt dasselbe von den Grössen

$$h'_r = \delta' h_r = H \Sigma \frac{\partial h_r}{\partial H_i} \delta h_i, \quad (19)$$

und umgekehrt geht aus (18) hervor, dass die Coefficienten der einzelnen n^2 Elemente in der Determinante H sich als homogene lineare Functionen der soeben definirten n Grössen h'_i darstellen lassen. Wir wollen, wenn φ eine beliebige Function der Coordinaten h_i bedeutet, mit φ' dieselbe Function der Grössen h'_i bezeichnen; dann lautet die Gleichung (18)

$$\frac{\partial H'_r}{\partial h'_s} = H \frac{\partial h_r}{\partial H_s}, \quad (20)$$

und hieraus folgt zugleich

$$H' = H^{n-1}; \quad H \frac{\partial h'_s}{\partial H'_r} = \frac{\partial H_s}{\partial h_r}. \quad (21)$$

Da H eine Functionaldeterminante ist, so ist bekanntlich*)

$$d \log H = \sum \frac{\partial d H_i}{\partial H_i} - \sum \frac{\partial d h_i}{\partial h_i},$$

und folglich ergibt sich unter Berücksichtigung von (13)

$$\begin{aligned} \sum \frac{\partial \log H}{\partial h_i} d H_i &= \sum \frac{\partial}{\partial H_i} \left(\frac{\partial H_i}{\partial h_i} \right) d H_i \\ &= \sum d \left(\frac{\partial H_i}{\partial h_i} \right) \frac{\partial H_i}{\partial H_i} = d \sum \frac{\partial H_i}{\partial h_i}; \end{aligned}$$

führt man daher die *homogene lineare Function*

$$S = \sum \frac{\partial H_i}{\partial h_i} \quad (22)$$

ein, so ist

$$\sum \frac{\partial \log H}{\partial h_i} d H_i = d S; \quad \frac{\partial \log H}{\partial h_r} = \frac{\partial S}{\partial H_r}, \quad (23)$$

also mit Rücksicht auf (20)

$$\frac{\partial H}{\partial h_r} = H \sum \frac{\partial S}{\partial h_i} \frac{\partial h_i}{\partial H_r} = \sum \frac{\partial S}{\partial h_i} \frac{\partial H'_i}{\partial h'_r};$$

man führe daher die *ganze homogene Function zweiten Grades*

$$T = \sum \frac{\partial S}{\partial h_i} H_i \quad (24)$$

ein, so wird

$$\frac{\partial H}{\partial h_r} = \frac{\partial T}{\partial h'_r}; \quad d H = \sum \frac{\partial T}{\partial h'_i} d h_i, \quad (25)$$

mithin sind auch die Derivirten der Form H darstellbar als homogene lineare Functionen der in (19) definirten Grössen h'_i , und rückwärts diese durch jene. Da ferner zufolge (20)

*) *Jacobi: De determinantibus functionalibus* §. 9 (Crelle's Journal XXII); in der obigen Form ist auch der Fall berücksichtigt, dass die Differentiale $d h_i$ Functionen von den Veränderlichen h_i sind. Ersetzt man d durch d' , so folgt aus (17) und (19) unmittelbar

$$\sum \frac{\partial h'_i}{\partial h_i} = 0.$$

$$\sum \frac{\partial H'_i}{\partial h'_s} \frac{\partial H_r}{\partial h_s} = H \text{ oder } = 0$$

ist, je nachdem r und s gleich oder ungleich sind, so folgt durch Multiplication mit h'_s oder dh'_s und Summation in Bezug auf s

$$2 \sum H'_i \frac{\partial H_r}{\partial h_s} = H h'_r; \quad \sum dH'_i \frac{\partial H_r}{\partial h_s} = H dh'_r$$

und hieraus durch Differentiation

$$h'_r dH - H dh'_r = 2 \sum H'_i d \left(\frac{\partial H_r}{\partial h_s} \right). \quad (26)$$

Mit Hülfe von (25) und (26) ist man im Stande, auch die Differentiale höherer Ordnung von H zu bilden; auf diese Weise findet man

$$H d d' H - d H d' H = 2 H \sum \frac{\partial H}{\partial h_s} d d' h_s - 2 \sum \frac{\partial^2 T}{\partial h_s \partial h'_v} H'_i d d' H'_v; \quad (27)$$

ausserdem ergibt sich aus Gleichung (26), welcher man mit Hülfe von (13) auch die Form

$$h'_r dH - H dh'_r = \sum \frac{\partial H'_i}{\partial h'_v} \frac{\partial H'_r}{\partial h'_i} dh'_v$$

geben kann, die Functionaldeterminante

$$\sum \pm \frac{\partial h'_1}{\partial h_1} \frac{\partial h'_2}{\partial h_2} \dots \frac{\partial h'_n}{\partial h_n} = (-1)^{n-1} (n-1) H^{n-2} \quad (28)$$

und folglich aus (25) die Hesse'sche Determinante der Form H , nämlich

$$\sum \pm \frac{\partial^2 H}{\partial h_1^2} \dots \frac{\partial^2 H}{\partial h_n^2} = (-1)^{n-1} (n-1) H^{n-2} \sum \pm \frac{\partial^2 T}{\partial h_1^2} \dots \frac{\partial^2 T}{\partial h_n^2}. \quad (29)$$

Aus den Gleichungen (16), (22), (24), (25), (26), (27) ergeben sich unmittelbar folgende auf die Variation δ bezüglichen Resultate:

$$\begin{aligned} \delta S &= n; & \delta T &= S; & h'_r \delta H - H \delta h'_r &= 2 H'_r; \\ \delta H &= S'; & \delta' H &= \delta H^2 - H \delta^2 H &= 2 T'. \end{aligned} \quad (30)$$

III. Alle diese Sätze sind abgeleitet aus der Voraussetzung, dass das System der n ganzen homogenen Functionen H_i vom zweiten Grade den Bedingungen (13) genügt, und dass ihre Functionaldeterminante H nicht identisch verschwindet; fügt man noch die Voraussetzung hinzu, dass die Coefficienten dieser Functionen

rationale Zahlen sind, und dass die Form H *irreductibel*, d. h. nicht zerlegbar ist in Factoren niedrigeren Grades, deren Coefficienten ebenfalls rationale Zahlen sind, so lässt sich umgekehrt beweisen, dass zu diesem Functionensystem ein algebraischer Zahlkörper Ω von der oben betrachteten Art gehört. Der Kürze halber führen wir eine Charakteristik ε ein, welche folgenden Sinn hat: ist φ irgend eine Function der Coordinaten h_v , und ersetzt man die letzteren durch $h_v - \omega \delta h_v$, wo ω vorläufig eine *willkürliche* Function bedeutet, so geht φ in eine neue Function über, welche mit $\varepsilon(\varphi)$ bezeichnet werden soll. Aus dieser Definition folgt sofort

$$d \varepsilon(\varphi) = \varepsilon(d\varphi) - \varepsilon(\delta\varphi) d\omega; \quad (31)$$

unter der Voraussetzung, dass die Differentiale dh_v *constant* sind. Hierauf definire man die Function ω als Wurzel der Gleichung n ten Grades

$$\varepsilon(H) = 0, \quad (32)$$

welche zufolge (16) vollständig mit der Gleichung (6) übereinstimmt, so lässt sich beweisen, dass ω eine *ganze* (homogene) Function ersten Grades, d. h. dass $d d' \omega = 0$ ist, wenn die Differentiale dh_v , $d' h_v$ als constant vorausgesetzt werden. In der That ergibt sich durch successive Differentiation der Identität (32) nach der in (31) ausgesprochenen Regel

$$\varepsilon(\delta H) d\omega = \varepsilon(dH) \quad (33)$$

und

$$\varepsilon(\delta H)^3 d d' \omega = \varepsilon(R), \quad (34)$$

wo zur Abkürzung die homogene Function (3n - 4)ten Grades

$$\left\{ \begin{array}{l} \delta H^2 d d' H + \delta^2 H d H d' H \\ - \delta H d H d' \delta H - \delta H d' H d \delta H \end{array} \right\} = R$$

gesetzt ist. Dass diese Function R durch H theilbar, in Zeichen, dass $R \equiv 0$ ist*), ergibt sich auf folgende Weise.

Aus (30) folgt

$$h'_r \delta H = 2 H'_r + H \delta h'_r \equiv 2 H'_r$$

ferner

$$h'_r \delta^2 H = 2 \delta H'_r + H \delta^2 h'_r \equiv 2 \delta H'_r$$

und hieraus durch Elimination von h'_r

$$\delta^2 H H'_r - \delta H \delta H'_r \equiv 0;$$

*) Dies gilt allgemein von dem Ausdrücke

$$d' H d''' H d d'' H + d H d'' H d' d''' H - d''' H d H d' d'' H - d' H d'' H d d''' H.$$

da nun zufolge (27) $dHd'H - Hd'd'H$ eine homogene lineare Function der n Grössen H_i ist, so folgt auch, dass

$$\delta^2 H(dHd'H - Hd'd'H) - \delta H\delta(dHd'H - Hd'd'H) \equiv 0$$

ist; die linke Seite unterscheidet sich aber von R nur um Bestandtheile, welche durch H theilbar sind. Mithin ist $R = PH$, wo P eine ganze Function bedeutet, und folglich $\varepsilon(R) = \varepsilon(P)\varepsilon(H) = 0$. Da sich nun aus den Voraussetzungen über H beweisen lässt, dass $\varepsilon(\delta H)$ nicht identisch verschwindet, so folgt aus (34) $dd'\omega = 0$, d. h. die Wurzel ω der Gleichung (32) ist eine ganze Function ersten Grades; dass sie zugleich homogen ist, versteht sich von selbst, weil $H, \delta H \dots \delta^{n-1}H$ und folglich auch ω gleichzeitig mit den Coordinaten h_i verschwinden. Setzt man nun

$$\frac{\partial \omega}{\partial h_i} = \omega_i, \quad \omega = \sum h_i \omega_i, \quad (1)$$

so ergibt sich aus (33), dass

$$\sum \delta h_i \omega_i = \delta \omega = 1 \quad (35)$$

und

$$\varepsilon\left(\frac{\partial H}{\partial h_i}\right) = \varepsilon(\delta H)\omega_i \quad (36)$$

ist. Da ferner zufolge (23)

$$\sum \frac{\partial H}{\partial h_i} dH_i = HdS \equiv 0$$

und

$$\varepsilon(dH_i) = dH_i - \omega d\delta H_i = dH_i - \omega dh_i$$

ist, so folgt

$$\begin{aligned} 0 &= \varepsilon(H)dS = \sum \varepsilon\left(\frac{\partial H}{\partial h_i}\right)\varepsilon(dH_i) \\ &= \varepsilon(\delta H)\sum \omega_i(dH_i - \omega dh_i), \end{aligned}$$

mithin

$$\omega d\omega = \sum dH_i \omega_i, \quad (3)$$

also auch

$$\omega^2 = 2 \sum H_i \omega_i, \quad (2)$$

wodurch wir rückwärts zu unseren ursprünglichen Annahmen zurückgekehrt sind; und man kann auch beweisen — worauf wir hier nicht eingehen wollen — dass aus den Voraussetzungen über H die *Unabhängigkeit* der n Zahlen ω_i folgt.

Wir fügen diesen Entwicklungen endlich noch folgende leicht zu beweisende Bemerkungen hinzu. Die ausgeführte Form der Gleichung (32) oder (6) ist folgende

$$0 = H - \delta H \frac{\omega}{1} + \delta^2 H \frac{\omega^2}{1.2} - \delta^3 H \frac{\omega^3}{1.2.3} + \dots; \quad (37)$$

es ist ferner

$$H = \Pi \omega = N(\omega), \quad (7)$$

wo das Productzeichen Π sich auf alle n Wurzeln ω bezieht; ebenso findet man (wenn man in (3) d durch δ' ersetzt)

$$H = \omega \omega', \quad (8)$$

wo

$$\omega' = \delta' \omega = \sum h'_i \omega_i, \quad (38)$$

zu ω adjungirt ist, und

$$S = \sum \omega, \quad 2T = \sum \omega^2, \quad (39)$$

wo die Summenzeichen sich ebenfalls auf alle n Wurzeln beziehen. Die quadratische Form T ist charakteristisch für die Anzahl der reellen Wurzeln; bildet man ferner die Hesse'sche Determinante des Productes $H = \Pi \omega$, so ergibt sich durch Vergleichung mit (29) die Discriminante

$$\Delta(\omega_1, \omega_2 \dots \omega_n) = \sum \pm \frac{\partial^2 T}{\partial h_1^2} \dots \frac{\partial^2 T}{\partial h_n^2}, \quad (40)$$

was auch unmittelbar aus (39) folgt.

§. 160.

Der Inbegriff *aller* algebraischen Zahlen bildet offenbar ebenfalls einen Körper*). Wir wollen nun, indem wir unserem eigent-

*) Dass es ausser den algebraischen noch andere, sogenannte *transcendente* Zahlen giebt, ist meines Wissens zuerst von *Liouville* bewiesen (*Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques*; Journ. de Math. T. XVI. 1851). Man vermuthet, dass die Ludolph'sche Zahl π eine solche transcendente Zahl ist; allein selbst die als specieller Fall hierin enthaltene Behauptung, dass die Quadratur des Zirkels unmöglich sei, ist bis auf den heutigen Tag noch nicht erwiesen. (Vergl. *Euler: De relatione inter ternas pluresve quantitates instituenda*. §. 10. Opusc. anal. T. II. 1785.)

lichen Gegenstände näher treten, eine Zahl α eine *ganze algebraische Zahl* nennen, wenn sie die Wurzel einer Gleichung ist, deren Coefficienten rationale ganze Zahlen sind, wobei wir ein für allemal bemerken, dass wir unter den *Coefficienten* einer Function *nten Grades*

$$F(x) = cx^m + c_1x^{m-1} + c_2x^{m-2} + \dots + c_m$$

oder der Gleichung $F(x) = 0$ stets die m Quotienten

$$-\frac{c_1}{c}, +\frac{c_2}{c} \dots (-1)^m \frac{c_m}{c}$$

verstehen. Aus dieser Erklärung folgt zunächst, dass eine rationale Zahl stets und nur dann eine ganze algebraische Zahl ist, wenn sie eine ganze Zahl im gewöhnlichen Sinne des Wortes ist (vergl. §. 5, 4.); diese Zahlen wollen wir von jetzt ab *rationale ganze Zahlen*, alle algebraischen ganzen Zahlen aber kurz *ganze Zahlen* nennen. Dieses vorausgeschickt, schreiten wir zum Beweise der folgenden Fundamentalsätze.

1. *Die Summe, die Differenz und das Product zweier ganzen Zahlen α, β sind wieder ganze Zahlen.*

Sind a, b resp. die Grade der Gleichungen $\varphi(\alpha) = 0, \psi(\beta) = 0$, deren Coefficienten rationale ganze Zahlen sind, und bezeichnet man mit $\omega_1, \omega_2 \dots \omega_n$ die sämtlichen ab Producte von der Form $\alpha^{a'}\beta^{b'}$, wo a' irgend eine der Zahlen $0, 1, 2 \dots (a-1)$, und b' irgend eine der Zahlen $0, 1, 2 \dots (b-1)$ bedeutet, so wird, wenn $\omega = \alpha + \beta$, oder $= \alpha - \beta$, oder $= \alpha\beta$ ist, jedes der n Producte $\omega\omega_1, \omega\omega_2 \dots \omega\omega_n$ mit Zuziehung der Gleichungen $\varphi(\alpha) = 0, \psi(\beta) = 0$ auf die Form $r_1\omega_1 + r_2\omega_2 + \dots + r_n\omega_n$ gebracht werden können, wo $r_1, r_2 \dots r_n$ rationale ganze Zahlen sind. Eliminiert man die n Grössen $\omega_1, \omega_2 \dots \omega_n$ aus diesen n Gleichungen, so ergibt sich für ω eine Gleichung vom n ten Grade (wie (6) in §. 159), deren Coefficienten rationale ganze Zahlen sind, was zu beweisen war (vergl. §. 139).

2. Die ganze Zahl α heisst *theilbar* durch die ganze Zahl β , oder ein *Multiplum* von β , wenn der Quotient $\alpha:\beta$ ebenfalls eine ganze Zahl ist; umgekehrt heisst β ein *Divisor* oder *Theiler* von α (vergl. §. 3). Ebenso setzen wir $\alpha \equiv \beta \pmod{\gamma}$, wenn $\alpha - \beta$ durch γ theilbar ist, und nennen α, β *congruent nach dem Modul γ* (vergl. §. 17). Man erkennt sofort (zufolge 1.), dass die Sätze des §. 3 und auch die des §. 17 (mit *vorläufiger* Ausnahme von 6. und 8.; vergl. §. 164, 3.) ihre Gültigkeit behalten.

3. Jede Wurzel ω einer Gleichung, deren Coefficienten ganze Zahlen sind, ist ebenfalls eine ganze Zahl.

Ist ω die Wurzel einer Gleichung m ten Grades $F(\omega) = 0$, deren Coefficienten $\alpha, \beta \dots$ ganze Zahlen sind, sind ferner $a, b \dots$ resp. die Grade der mit rationalen ganzen Coefficienten behafteten Gleichungen $\varphi(\alpha) = 0, \psi(\beta) = 0 \dots$, so führe man die sämtlichen $mab \dots$ Producte $\omega_1, \omega_2 \dots \omega_n$ von der Form $\omega^{m'} \alpha^{a'} \beta^{b'} \dots$ ein, wo die ganzen rationalen Exponenten den Bedingungen $0 \leq m' < m, 0 \leq a' < a, 0 \leq b' < b \dots$ genügen; dann lässt sich vermöge der Gleichungen $F(\omega) = 0, \varphi(\alpha) = 0, \psi(\beta) = 0 \dots$ jedes der n Producte $\omega \omega_1, \omega \omega_2 \dots \omega \omega_n$ wieder in die Form $r_1 \omega_1 + r_2 \omega_2 + \dots + r_n \omega_n$ bringen, wo $r_1, r_2 \dots r_n$ rationale ganze Zahlen bedeuten, und hieraus folgt unmittelbar die Richtigkeit des Satzes.

Ist daher z. B. α eine ganze Zahl, und r eine beliebige (ganze oder gebrochene) positive rationale Zahl, so ist auch α^r eine ganze Zahl (vergl. §. 5, 4.).

4. Bekanntlich lassen sich die Begriffe der Theilbarkeit und des Vielfachen von den ganzen rationalen Zahlen unmittelbar auf die ganzen rationalen Functionen übertragen, und es giebt einen Algorithmus zur Auffindung des grössten gemeinschaftlichen Divisors $\varphi(x)$ zweier gegebenen Functionen $F(x), f(x)$, welcher demjenigen der Zahlentheorie (§. 4) vollständig analog ist. Sind die Coefficienten von $F(x)$ und $f(x)$ sämtlich in einem Körper K enthalten, so werden auch die Coefficienten von $\varphi(x)$ Zahlen des Körpers K sein, weil sie durch Addition, Multiplication, Subtraction und Division aus den Coefficienten von $F(x)$ und $f(x)$ entstehen. Hieraus folgt leicht, dass, wenn α die Wurzel einer solchen Gleichung $F(\alpha) = 0$ ist, deren Coefficienten Zahlen des Körpers K sind, nothwendig auch eine solche Gleichung $\varphi(\alpha) = 0$ von *niedrigstem Grade* existiren muss, welche *irreductibel in K* heissen soll und welche offenbar keine anderen Wurzeln besitzen, kann als die Gleichung $F(\alpha) = 0$. Hieraus folgt der Satz:

Ist α eine ganze Zahl, und K ein bestimmter Körper, so sind alle Coefficienten der in K irreductibelen Gleichung $\varphi(\alpha) = 0$ ganze Zahlen.

Denn weil α eine ganze Zahl, also die Wurzel einer Gleichung $F(\alpha) = 0$ ist, deren Coefficienten rationale ganze Zahlen und folg-

lich auch Zahlen des Körpers K sind (§. 159), so kann die in K irreductibele Gleichung $\varphi(\alpha) = 0$, welcher α genügt, nur ganze Zahlen zu Wurzeln haben; da aber die Coefficienten einer Gleichung durch Addition und Multiplication aus ihren Wurzeln entstehen, so sind (zufolge 1.) auch die Coefficienten der Gleichung $\varphi(\alpha) = 0$ ganze Zahlen, was zu beweisen war.

Der einfachste Fall, in welchem K der Körper der rationalen Zahlen ist, findet sich bei *Gauss**).

5. Ist ϱ irgend eine algebraische Zahl, so giebt es immer unendlich viele (von Null verschiedene) rationale ganze Zahlen h von der Beschaffenheit, dass $h\varrho$ eine ganze Zahl wird, und zwar stimmen diese sämtlichen Zahlen h mit den sämtlichen rationalen Vielfachen der kleinsten unter ihnen überein.

Da ϱ eine algebraische Zahl, also die Wurzel einer Gleichung von der Form

$$c\varrho^m + c_1\varrho^{m-1} + c_2\varrho^{m-2} + \dots + c_m = 0$$

ist, wo $c, c_1, c_2 \dots c_m$ rationale ganze Zahlen bedeuten, so ergibt sich durch Multiplication mit c^{m-1} , dass $c\varrho$ eine ganze Zahl ist. Sind ferner $a\varrho, b\varrho$ ganze Zahlen, wo a, b rationale ganze Zahlen bedeuten, deren grösster gemeinschaftlicher Theiler $= h$ ist, so folgt leicht (aus 1. und §. 4), dass auch $h\varrho$ eine ganze Zahl ist. Hieraus ergibt sich unmittelbar der zu beweisende Satz.

6. Versteht man unter einer *Einheit* eine ganze Zahl ε , welche in allen ganzen Zahlen aufgeht, so ist zunächst erforderlich, dass sie auch in 1 aufgeht, dass also $1 = \varepsilon\varepsilon'$, und ε' eine ganze Zahl ist; wenn nun

$$\varepsilon^m + c_1\varepsilon^{m-1} + \dots + c_m = 0$$

die im Körper der rationalen Zahlen irreductibele Gleichung ist, welcher ε genügt, so muss (zufolge 4.) $c_m = \pm 1$ sein, weil ε' der ebenfalls irreductibelen Gleichung

$$c_m\varepsilon'^m + c_{m-1}\varepsilon'^{m-1} + \dots + c_1\varepsilon' + 1 = 0$$

genügt; umgekehrt, ist dies der Fall, so geht ε in 1 und folglich in allen ganzen Zahlen auf, ist also eine Einheit. Die Anzahl der Einheiten ist offenbar unbegrenzt.

Ist α theilbar durch α' , und sind $\varepsilon, \varepsilon'$ irgend welche Einheiten, so ist offenbar auch $\varepsilon\alpha$ durch $\varepsilon'\alpha'$ theilbar; hinsichtlich der Theilbarkeit verhalten sich daher alle Zahlen $\varepsilon\alpha$, welche den sämt-

*) *D. A.* art. 42.

lichen Einheiten ε entsprechen, genau wie α . Zwei ganze Zahlen, deren Quotient keine Einheit ist, wollen wir *wesentlich verschieden* nennen.

7. Will man nun den Begriff der *Primzahl* so fassen, dass sie ausser sich selbst und den Einheiten keine wesentlich verschiedene Theiler besitzt und auch selbst keine Einheit ist, so erkennt man sofort, dass gar keine solche Zahl existirt; ist nämlich α eine ganze Zahl, aber keine Einheit, so besitzt sie immer unendlich viele wesentlich verschiedene Divisoren, z. B. die Zahlen $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$, $\sqrt[4]{\alpha}$ u. s. f., welche (zufolge 3.) ganze Zahlen sind.

Dagegen lässt sich der Begriff von *relativen Primzahlen* vollständig definiren, und diese Frage wird uns überhaupt auf den richtigen Weg leiten, welcher bei den ferneren Untersuchungen einzuschlagen ist. Da von einem grössten gemeinschaftlichen Theiler zweier ganzen Zahlen *vorläufig* (vergl. §. 164, 3.) nicht gesprochen werden kann, so ist es auch unmöglich, die Definition von relativen Primzahlen so zu fassen, wie sie in der Theorie der rationalen Zahlen aufgestellt wird (§. 5); aber aus dieser Definition ergaben sich mehrere Sätze, deren jeder umgekehrt das Verhalten zweier relativen Primzahlen vollständig charakterisirt, ohne die Kenntniss ihrer sämtlichen Divisoren vorauszusetzen. Ein solcher Satz ist z. B. der folgende (§. 7): Sind a, b relative Primzahlen, so ist jede durch a und b theilbare Zahl auch durch ab theilbar. Dieser Satz lässt sich in der That umkehren: Ist jede durch a und b theilbare Zahl auch durch ab theilbar, so sind a, b relative Primzahlen. Hätten nämlich die beiden Zahlen $a = ha', b = hb'$ einen gemeinschaftlichen Theiler $h > 1$, so wäre $ha'b'$ eine durch a und b , aber nicht durch ab theilbare Zahl.

Diese Betrachtung veranlasst uns, folgende für das Gebiet aller ganzen algebraischen Zahlen gültige Erklärung aufzustellen:

Zwei von Null verschiedene ganze Zahlen α, β heissen relative Primzahlen, wenn jede durch α und β theilbare Zahl auch durch $\alpha\beta$ theilbar ist.

Vor Allem bemerken wir, dass zwei relative Primzahlen im alten Sinne des Wortes, d. h. zwei rationale ganze Zahlen a, b , deren grösster gemeinschaftlicher Divisor $= 1$ ist, auch im neuen Sinne relative Primzahlen bleiben; ist nämlich eine ganze algebraische Zahl γ theilbar durch a und b , so ist der Quotient $\varrho = \gamma : ab$ eine algebraische Zahl der Art, dass $a\varrho$ und $b\varrho$ ganze Zahlen sind; mithin muss (zufolge 5.) auch ϱ eine ganze Zahl, also γ theilbar durch

ab sein, was zu beweisen war. Dass ferner umgekehrt zwei relative Primzahlen im neuen Sinne des Wortes, welche zugleich rational sind, auch relative Primzahlen im alten Sinne sind, versteht sich zufolge der der neuen Erklärung vorausgeschickten Erörterung von selbst.

Wir nennen ferner die ganzen Zahlen $\alpha, \beta, \gamma, \delta \dots$ kurz relative Primzahlen, wenn jede von ihnen relative Primzahl zu jeder der andern ist (vergl. §. 6); ist dann eine ganze Zahl ω durch jede von ihnen theilbar, so ist sie auch durch ihr Product theilbar (vergl. §. 7), weil, wie man leicht findet, auch der folgende Satz (§. 5, 3.) seine Gültigkeit behält: Ist jede der Zahlen $\alpha', \beta', \gamma' \dots$ relative Primzahl zu jeder der Zahlen $\alpha'', \beta'', \gamma'', \delta'' \dots$, so sind auch die Producte $\alpha' \beta' \gamma' \dots$ und $\alpha'' \beta'' \gamma'' \delta'' \dots$ relative Primzahlen und umgekehrt.

Aber wie soll man definitiv entscheiden, ob zwei gegebene ganze Zahlen α, β relative Primzahlen sind? Man könnte versuchen, folgenden Weg einzuschlagen. Da α^{-1} und β^{-1} algebraische Zahlen sind, so giebt es (zufolge 5.) immer zwei kleinste positive ganze rationale Zahlen a, b von der Art, dass $a\alpha^{-1}$ und $b\beta^{-1}$ ganze Zahlen, d. h. dass a, b resp. durch α, β theilbar werden; zeigt sich nun, dass a, b relative Primzahlen sind, so sind auch α, β gewiss relative Primzahlen. Aber man muss sich hüten zu glauben, dass auch das Umgekehrte Statt findet, dass also die *kleinsten rationalen Multipla* a, b von zwei relativen Primzahlen α, β nothwendig selbst relative Primzahlen sein müssen. So z. B. sind in der That die beiden conjugirten Zahlen $\alpha = 2 + i$ und $\beta = 2 - i$ relative Primzahlen, und doch ist $a = b = 5$. Eine wesentliche Reduction unserer Aufgabe wird aber durch den folgenden Satz bewirkt:

Wenn zwei ganze Zahlen α, β sich in einem Körper K , dem sie selbst angehören, als relative Primzahlen bewähren, d. h. wenn jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist; so sind α, β wirklich relative Primzahlen.

Ist nämlich ω irgend eine durch α und durch β theilbare ganze Zahl, und ist

$$\omega^m + \gamma_1 \omega^{m-1} + \gamma_2 \omega^{m-2} + \dots + \gamma_m = 0$$

die in K irreductibele Gleichung, welcher ω genügt, so sind (zufolge 4.) die Zahlen $\gamma_1, \gamma_2 \dots \gamma_m$ ganze Zahlen des Körpers K ; da ferner

die ganzen Zahlen $\alpha' = \omega : \alpha$ und $\beta' = \omega : \beta$ resp. den in K irreductibelen Gleichungen

$$(\alpha \alpha')^m + \gamma_1 (\alpha \alpha')^{m-1} + \dots + \gamma_m = 0$$

$$(\beta \beta')^m + \gamma_1 (\beta \beta')^{m-1} + \dots + \gamma_m = 0$$

genügen, so sind (zufolge 4.) auch die Quotienten $\gamma_n : \alpha^n$ und $\gamma_n : \beta^n$ ganze Zahlen des Körpers K ; da ferner nach Voraussetzung jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist, so ergibt sich leicht, dass auch jede durch α^n und β^n theilbare Zahl γ_n des Körpers K durch $\alpha^n \beta^n$ theilbar, also von der Form $\alpha^n \beta^n \gamma'_n$ ist, wo γ'_n eine ganze Zahl bedeutet; setzt man nun $\omega = \alpha \beta \omega'$, so genügt ω' der Gleichung

$$\omega'^m + \gamma'_1 \omega'^{m-1} + \dots + \gamma'_m = 0,$$

deren Coefficienten ganze Zahlen sind; mithin ist ω' (zufolge 3.) eine ganze Zahl, d. h. ω ist auch theilbar durch $\alpha\beta$, was zu beweisen war.

Hieraus geht hervor, dass man, um das gegenseitige Verhalten zweier ganzen Zahlen α , β zu untersuchen, nur den kleinsten Körper K zu bilden braucht, welchem sie beide angehören; und dieser Körper ist, wie man leicht erkennt, immer von der im vorigen Paragraphen betrachteten Beschaffenheit.

§. 161.

Um den späteren Verlauf der Darstellung nicht zu unterbrechen, schalten wir hier eine sehr allgemeine Betrachtung ein, welche für die nachfolgenden, sowie für viele andere, unserem Gegenstande fremde Untersuchungen von grossem Nutzen ist.

1. Ein System a von reellen oder complexen Zahlen α , deren *Summen* und *Differenzen* demselben System a angehören, soll ein *Modul* heissen; wenn die Differenz zweier Zahlen ω , ω' in a enthalten ist, so wollen wir sie *congruent nach* a nennen und dies durch die Congruenz

$$\omega \equiv \omega' \pmod{a}$$

andeuten. Solche Congruenzen können addirt, subtrahirt und folglich auch mit beliebigen ganzen rationalen Zahlen multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen

auch einander congruent sind, so kann man alle existirenden Zahlen in *Classen* (mod. a) eintheilen, indem man je zwei congruente Zahlen in dieselbe Classe, je zwei incongruente in zwei verschiedene Classen aufnimmt.

2. Wenn alle Zahlen eines Moduls a auch Zahlen eines Moduls b sind, so heisse a ein *Vielfaches* von b , und b ein *Theiler* von a ; oder wir sagen auch, b gehe in a auf, a sei theilbar durch b . Aus jeder Congruenz $\omega \equiv \omega' \pmod{a}$ folgt auch $\omega \equiv \omega' \pmod{b}$. Offenbar besteht b aus einer endlichen oder unendlichen Anzahl von Classen (mod. a).

Sind a, b irgend zwei Moduln, so bilden alle die Zahlen, welche gleichzeitig in a und in b enthalten sind, das *kleinste* gemeinschaftliche Vielfache m von a und b , weil jedes gemeinschaftliche Vielfache von a und b auch durch den Modul m theilbar ist. Durchläuft α alle Zahlen des Moduls a , β alle Zahlen des Moduls b , so bilden die Zahlen $\alpha + \beta$ den *grössten* gemeinschaftlichen Theiler von a und b , weil jeder gemeinschaftliche Theiler von a und b auch in dem Modul b aufgeht.

3. Sind $\omega_1, \omega_2 \dots \omega_n$ gegebene Zahlen, so bilden alle Zahlen von der Form

$$\omega = h_1 \omega_1 + h_2 \omega_2 + \dots + h_n \omega_n, \quad (1)$$

wo $h_1, h_2 \dots h_n$ alle ganzen rationalen Zahlen durchlaufen, einen *endlichen* Modul v , und wir wollen den Complex der n Zahlen $\omega_1, \omega_2 \dots \omega_n$, mögen sie abhängig oder unabhängig von einander sein, eine *Basis* des Moduls v nennen. Dann besteht folgender Satz:

Wenn alle Zahlen ω eines endlichen Moduls v durch Multiplication mit rationalen, von Null verschiedenen Zahlen in Zahlen eines Moduls m verwandelt werden können, so enthält v nur eine endliche Anzahl incongruenter Zahlen (mod. m).

Da es nämlich n rationale, von Null verschiedene Zahlen $r_1, r_2 \dots r_n$ der Art giebt, dass die Producte $r_1 \omega_1, r_2 \omega_2 \dots r_n \omega_n$ in m enthalten sind, so giebt es auch eine ganze rationale, von Null verschiedene Zahl s der Art, dass alle Producte $s \omega \equiv 0 \pmod{m}$ sind. Lässt man daher jede der n ganzen rationalen Zahlen $h_1, h_2 \dots h_n$ ein vollständiges Restsystem (mod. s) durchlaufen, so entstehen s^n Zahlen ω von der Form (1), und jede Zahl des Moduls v ist wenigstens einer derselben congruent (mod. m); mithin ist die Anzahl der in v enthaltenen, nach m incongruenten Zahlen *höchstens* $= s^n$, was zu beweisen war.

Allein es ist wichtig, die Anzahl dieser incongruenten Zahlen *genau* zu bestimmen. Zu diesem Zweck betrachten wir das kleinste gemeinschaftliche Vielfache a der beiden Moduln ν und m ; da je zwei nach m congruente Zahlen ω, ω' des Modul ν auch nach a congruent sind, und umgekehrt, so ist unsere Aufgabe die, die Anzahl der Classen (mod. a) zu bestimmen, aus welchen ν besteht. Wir suchen daher zunächst die allgemeine Form aller in a enthaltenen Zahlen

$$\alpha = k_1 \omega_1 + k_2 \omega_2 + \dots + k_n \omega_n \quad (2)$$

aufzustellen, wo $k_1, k_2 \dots k_n$ jedenfalls ganze rationale Zahlen bedeuten. Ist nun r ein bestimmter Index aus der Reihe $1, 2 \dots n$, so giebt es unter allen den Zahlen $\alpha = \theta_r$, in welchen $k_{r+1} = 0, k_{r+2} = 0 \dots k_n = 0$ ist, auch solche, in denen k_r von Null verschieden ist (z. B. $s \omega_r$), und unter diesen sei

$$\alpha_r = a_1^{(r)} \omega_1 + a_2^{(r)} \omega_2 + \dots + a_r^{(r)} \omega_r \quad (3)$$

eine solche, in welcher k_r den *kleinsten* positiven Werth $a_r^{(r)}$ besitzt. Dann leuchtet ein, dass der Werth von k_r in jeder Zahl θ_r durch $a_r^{(r)}$ theilbar, also von der Form $a_r^{(r)} x_r$ ist, wo x_r eine ganze rationale Zahl bedeutet, und dass folglich $\theta_r - x_r \alpha_r = \theta_{r-1}$ eine Zahl α ist, in welcher $k_r, k_{r+1} \dots k_n$ verschwinden. Hieraus folgt sofort, dass, nachdem man für jeden Index r eine solche particuläre Zahl α_r des Moduls a aufgestellt hat*), jede Zahl α gewiss in die Form

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \dots + x_n \alpha_n \quad (4)$$

gebracht werden kann, wo $x_1, x_2 \dots x_n$ ganze rationale Zahlen bedeuten, aus welchen die in der Form (2) vorkommenden Zahlen $k_1, k_2 \dots k_n$ durch die Gleichungen

$$k_r = a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \dots + a_r^{(n)} x_n \quad (5)$$

abgeleitet werden; und umgekehrt sind alle Zahlen α von der Form (4) in a enthalten.

Ist nun eine Zahl ω von der Form (1) gegeben, sind also $h_1, h_2 \dots h_n$ gegebene rationale ganze Zahlen, so sind *alle* Zahlen ω' des Moduls ν , welche ihr nach m congruent sind, welche also eine Classe (mod. a) bilden, von der Form

$$\omega' = \omega + \alpha = h'_1 \omega_1 + h'_2 \omega_2 + \dots + h'_n \omega_n, \quad (6)$$

*) Das System dieser n particulären Zahlen wird ein vollständig bestimmtes, wenn man die Bedingung hinzufügt, dass $0 \leq a_r^{(r')} < a_r^{(r)}$ sein soll, wenn $r' > r$ ist.

wo zufolge (5)

$$h'_r = h_r + a_r^{(r)}x_r + a_r^{(r+1)}x_{r+1} + \dots + a_r^{(n)}x_n$$

ist, und hieraus folgt, dass man successive die willkürlichen rationalen ganzen Zahlen $x_n, x_{n-1} \dots x_2, x_1$ stets und nur auf eine einzige Art so bestimmen kann, dass die n Zahlen h'_r den Bedingungen

$$0 \leq h'_r < a_r^{(r)} \quad (7)$$

genügen. In jeder Classe existirt daher ein und nur ein *Repräsentant* ω' von der Form (6), welcher diesen Bedingungen (7) genügt; mithin ist die *Anzahl* der verschiedenen Classen (mod. \mathfrak{a}), aus welchen der Modul \mathfrak{o} besteht, gleich dem Producte $a'_1 a''_2 \dots a_n^{(n)}$, d. h. gleich der *Determinante* des Coefficientensystems in den n particulären Zahlen α_r von der Form (3), welche eine Basis von \mathfrak{a} bilden *).

§. 162.

Wir beschränken uns von jetzt an auf die Untersuchung der ganzen Zahlen, welche in einem endlichen Körper Ω (§. 159) enthalten sind.

1. Da jede algebraische Zahl (zufolge §. 160, 5.) durch Multiplication mit einer rationalen ganzen von Null verschiedenen Zahl in eine ganze Zahl verwandelt werden kann, so dürfen wir annehmen, dass die Zahlen $\omega_1, \omega_2 \dots \omega_n$, welche eine Basis des Körpers Ω bilden, sämmtlich *ganze* Zahlen sind, und es wird dann (zufolge §. 160, 1.) jede Zahl

$$\omega = \sum h_i \omega_i \quad (1)$$

gewiss eine ganze Zahl sein, wenn ihre Coordinaten h_i rationale ganze Zahlen sind; aber dies lässt sich im Allgemeinen nicht umkehren, d. h. es kann ω sehr wohl eine ganze Zahl sein, auch wenn ihre Coordinaten theilweise oder sämmtlich gebrochene Zahlen

*) Die weitere Entwicklung der allgemeinen Theorie der Moduln würde uns hier zu weit führen (vergl. §. 163); wir erwähnen nur noch folgenden Satz: Sind die Basiszahlen eines endlichen Moduls von einander abhängig, so giebt es immer eine aus unabhängigen Zahlen bestehende Basis desselben Moduls. Die eleganteste Methode, die neue Basis aufzufinden, besteht in einer Verallgemeinerung der von *Gauss* angewandten Behandlung der partialen Determinanten (*D. A. artt. 234, 236, 279*).

sind. Dies ist einer der wichtigsten Punkte der Theorie und muss deshalb vor Allem aufgeklärt werden.

Wir schicken zunächst die einleuchtende Bemerkung voraus, dass die Discriminante (§. 159, (10)) eines jeden Systems von n unabhängigen ganzen Zahlen gewiss eine von Null verschiedene rationale und zwar *ganze* Zahl ist, weil sie durch Addition, Subtraction und Multiplication aus lauter ganzen Zahlen gebildet ist. Giebt es nun wirklich in Ω eine *ganze* Zahl

$$\beta = \frac{\sum k_i \omega_i}{s} \quad (2)$$

wo $s, k_1, k_2 \dots k_n$ ganze rationale Zahlen ohne gemeinschaftlichen Theiler bedeuten, deren erste $s \geq 1$ ist, so behaupten wir, dass s^2 in der Discriminante $\Delta(\omega_1, \omega_2 \dots \omega_n)$ aufgeht, und dass man eine neue Basis von ganzen Zahlen $\beta_1, \beta_2 \dots \beta_n$ aufstellen kann, deren Discriminante absolut genommen $< \Delta(\omega_1, \omega_2 \dots \omega_n)$ ist.

Um dies zu beweisen, bezeichnen wir mit \mathfrak{o} den aus allen durch s theilbaren ganzen Zahlen bestehenden Modul, ebenso mit \mathfrak{o} das System aller Zahlen ω von der Form (1), deren Coordinaten h_i ganze Zahlen sind; da jedes Product $s\omega$ eine Zahl des Moduls \mathfrak{o} ist, so können wir die allgemeine Untersuchung des vorigen Paragraphen auf unsern Fall anwenden. Alle durch s theilbaren Zahlen α des Systems \mathfrak{o} sind daher von der Form

$$\alpha = \sum x_i \alpha_i = s \sum x_i \beta_i,$$

wo die n Zahlen $\alpha_i = s\beta_i$ particuläre Zahlen α , also die β_i ganze Zahlen des Körpers Ω , und die x_i willkürliche rationale ganze Zahlen bedeuten.

Da nun alle Zahlen $s\omega$ auch solche Zahlen α sind, so kann man

$$\omega_r = \sum b_i^{(r)} \beta_i, \quad \Delta(\omega_1, \omega_2 \dots \omega_n) = b^2 \Delta(\beta_1, \beta_2 \dots \beta_n)$$

setzen, wo die Coefficienten $b_i^{(r)}$ rationale ganze Zahlen sind, und b die aus ihnen gebildete Determinante bedeutet; durch Umkehrung ergibt sich, dass die n Producte $b\beta_i$, mithin auch alle Quotienten $b\alpha : s$ Zahlen des Systems \mathfrak{o} sind.

Wenden wir dies Resultat auf die obige Voraussetzung (2) an, dass die Zahl β eine ganze Zahl, ihr Zähler $\sum k_i \omega_i$ also eine Zahl α ist, obgleich die Zahlen $s, k_1, k_2 \dots k_n$ keinen gemeinschaftlichen Theiler haben, so folgt unmittelbar, dass b durch s theilbar ist, wodurch zugleich die obigen Behauptungen erwiesen sind. •

Da nun die Discriminante eines jeden Systems von n unabhängigen ganzen Zahlen des Körpers Ω eine von Null verschiedene ganze rationale Zahl ist, so giebt es unter allen diesen Discriminanten eine solche, deren Werth — abgesehen vom Vorzeichen — ein *Minimum* ist, und aus der vorstehenden Untersuchung folgt unmittelbar, dass, wenn eine Basis aus solchen ganzen Zahlen $\omega_1, \omega_2 \dots \omega_n$ besteht, deren Discriminante diesen Minimumwerth besitzt, die entsprechenden Coordinaten h_i einer jeden *ganzen Zahl* ω des Körpers nothwendig *ganze rationale Zahlen* sein müssen. Eine solche Basis $\omega_1, \omega_2 \dots \omega_n$ wollen wir eine *Grundreihe* des Körpers Ω nennen; aus ihr ergeben sich alle anderen Grundreihen desselben Körpers, wenn man n ganze Zahlen ω von der Form (1) so wählt, dass die aus den n^2 zugehörigen Coordinaten gebildete Determinante $= \pm 1$ wird.

Die wichtigste Rolle spielt aber die Minimaldiscriminante selbst, sowohl hinsichtlich der inneren*) Constitution des Körpers Ω , als auch hinsichtlich seiner Verwandtschaft mit anderen Körpern**); wir wollen daher diese positive oder negative ganze rationale Zahl die *Grundzahl* oder die *Discriminante des Körpers* Ω nennen und mit $\Delta(\Omega)$ bezeichnen; sie ist offenbar zugleich die Grundzahl eines jeden mit Ω conjugirten Körpers.

Die Zahlen eines quadratischen Körpers sind z. B. von der Form $t + u\sqrt{D}$, wo t, u alle rationalen Zahlen durchlaufen, und D eine ganze rationale Zahl bedeutet, welche kein Quadrat und auch durch kein Quadrat ausser 1 theilbar ist. Ist $D \equiv 1 \pmod{4}$, so bilden die Zahlen 1 und $\frac{1}{2}(1 + \sqrt{D})$ eine Grundreihe des Körpers, und seine Grundzahl ist $= D$; ist dagegen $D \equiv 2$ oder $\equiv 3 \pmod{4}$, so bilden die Zahlen 1 und \sqrt{D} eine Grundreihe des Körpers, und seine Grundzahl ist $= 4D$.

*) Vergl. *Kronecker: Ueber die algebraisch auflösbaren Gleichungen* (Monatsbericht der Berliner Ak. 14. April 1856).

***) Die erste Spur dieser Beziehungen hat sich bei einer schönen Untersuchung von *Kronecker* gezeigt (*Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$* ; Journ. de Math., p. p. Liouville; T. XIX. 1854). Um den Charakter dieser Gesetze, deren Entwicklung ich mir auf eine andere Gelegenheit verspare, näher anzudeuten, führe ich nur das einfachste Beispiel an: das kleinste gemeinschaftliche Multiplum zweier von einander verschiedenen quadratischen Körper A, B ist ein biquadratischer Körper K , der noch einen dritten quadratischen Körper C zum Divisor hat; die Grundzahl von K ist gleich dem Product aus den Grundzahlen von A, B, C , und zwar eine Quadratzahl.

Ist ferner θ eine primitive Wurzel der Gleichung $\theta^m = 1$ (§. 139), wo $m > 2$, so bilden die Zahlen $1, \theta, \theta^2 \dots \theta^{m-1}$ die Grundreihe eines Körpers vom Grade $n = \varphi(m)$, dessen Grundzahl

$$\left(\frac{m \sqrt{-1}}{\sqrt{a} \sqrt{b} \sqrt{c} \dots} \right)^n$$

ist, wo $a, b, c \dots$ alle verschiedenen in m aufgehenden Primzahlen bedeuten. Ist $m = 3$ (oder $= 6$), so ist dieser Körper ein quadratischer, seine Grundzahl $= -3$; ist $m = 4$, so ist die Grundzahl des quadratischen Körpers $= -4$.

2. Aus den vorstehenden Principien ergibt sich leicht der folgende Fundamentalsatz:

Ist μ eine von Null verschiedene ganze Zahl des Körpers Ω , so ist die Anzahl der nach dem Modul μ incongruenten ganzen Zahlen des Körpers gleich dem absoluten Werth der Norm des Moduls μ .

Es sei \mathfrak{o} das System aller durch μ theilbaren ganzen Zahlen (welche sich durch Addition und Subtraction reproduciren), und \mathfrak{o} das System *aller* ganzen Zahlen des Körpers Ω , d. h. aller Zahlen ω von der Form (1), wo die Zahlen ω_i eine Grundreihe des Körpers bilden, und die Coordinaten h_i beliebige ganze rationale Zahlen bedeuten; da jeder Quotient $\omega : \mu$ (zufolge §. 160, 5.) durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl in eine ganze Zahl verwandelt werden kann, so ist die Untersuchung des vorigen Paragraphen auf unsern Fall anwendbar. Mithin sind alle durch μ theilbaren Zahlen α des Systems \mathfrak{o} von der Form

$$\alpha = \sum x_i \alpha_i = \mu \sum x_i \beta_i,$$

wo die n Zahlen $\alpha_i = \mu \beta_i$ particuläre Zahlen α bedeuten, also die Zahlen β_i in \mathfrak{o} enthalten sind, und die Grössen x_i alle rationalen ganzen Zahlwerthe annehmen dürfen; die Anzahl der *Classen*, in welche das System \mathfrak{o} in Bezug auf den Modul μ zerfällt, ist ferner gleich der aus den Coordinaten der n Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$ gebildeten Determinante a . Zugleich ist (nach §. 159, (11), (12))

$$\Delta(\alpha_1 \dots \alpha_n) = a^2 \Delta(\Omega) = N(\mu)^2 \Delta(\beta_1 \dots \beta_n);$$

da nun jede durch μ theilbare Zahl $\alpha = \mu \omega$ des Systems \mathfrak{o} die Form $\mu \sum x_i \beta_i$ besitzt, so ist jede Zahl ω des Systems \mathfrak{o} auch von der Form $\sum x_i \beta_i$; mithin bilden die Zahlen β_i ebenfalls eine Grund-

reihe des Körpers, und folglich ist $\Delta(\beta_1 \dots \beta_n) = \Delta(\Omega)$, also $a = \pm N(\mu)$, was zu beweisen war.

Zugleich leuchtet ein, dass nach der Methode des vorigen Paragraphen ein System von a incongruenten Repräsentanten der verschiedenen Classen, also ein *vollständiges Restsystem für den Modul μ* aufgestellt werden kann*).

3. Will man jetzt zwei gegebene ganze Zahlen θ, μ darauf prüfen, ob sie relative Primzahlen sind, so braucht man offenbar ω nur ein vollständiges Restsystem (mod. μ) durchlaufen zu lassen und nachzusehen, wie oft $\theta\omega \equiv 0 \pmod{\mu}$ wird; zeigt sich, dass dies nur dann eintritt, wenn $\omega \equiv 0 \pmod{\mu}$ ist, so ist also jede durch θ und μ theilbare ganze Zahl $\theta\omega$ auch theilbar durch $\theta\mu$, mithin sind θ, μ relative Primzahlen; besitzt aber die Congruenz $\theta\omega \equiv 0 \pmod{\mu}$ auch eine Wurzel ω , welche nicht $\equiv 0 \pmod{\mu}$ ist, so ist die entsprechende Zahl $\theta\omega$ durch θ und μ , aber nicht durch $\theta\mu$ theilbar, mithin sind θ, μ keine relative Primzahlen.

Ist θ relative Primzahl zu μ (z. B. $\theta = 1$), so durchläuft $\theta\omega$ gleichzeitig mit ω ein vollständiges Restsystem (mod. μ); folglich hat jede Congruenz $\theta\omega \equiv \theta' \pmod{\mu}$ immer eine und nur eine Wurzel ω (vergl. §. 22); ist ferner $\psi(\mu)$ die Anzahl aller Classen, deren Zahlen relative Primzahlen zum Modul μ sind, so durchläuft $\theta\omega$ gleichzeitig mit ω die Repräsentanten aller dieser Classen, und da das Product dieser Zahlen ω auch relative Primzahl zu μ ist, so ergibt sich der Satz

$$\theta^{\psi(\mu)} \equiv 1 \pmod{\mu},$$

welcher dem Fermat'schen Satze (§. 19) entspricht.

4. Verfolgt man diese Analogie mit der rationalen Zahlentheorie weiter, so drängt sich immer wieder die Frage nach der Zusammensetzung der Zahlen des Systems \mathfrak{o} (d. h. der ganzen Zahlen des Körpers Ω) aus Factoren auf, welche demselben System \mathfrak{o} an-

*) Bilden die n Zahlen ω_i irgend eine Basis des Körpers Ω , und ist \mathfrak{o} das System aller der Zahlen ω von der Form (1), deren Coordinaten ganze Zahlen sind, so reproduciren sich die Zahlen des Systems \mathfrak{o} durch Addition und Subtraction; nimmt man ferner an, dass sie sich auch durch Multiplication reproduciren, woraus zugleich folgt, dass sie ganze Zahlen sind, und nennt man zwei solche Zahlen ω, ω' stets und nur dann congruent in Bezug auf eine dritte solche Zahl μ , wenn der Quotient $(\omega - \omega') : \mu$ wieder eine Zahl des Systems \mathfrak{o} ist, so ist die Anzahl der in \mathfrak{o} enthaltenen, nach μ incongruenten Zahlen ebenfalls $= \pm N(\mu)$. Vergl. §. 165, 4.

gehören, und es zeigt sich zunächst, dass die unbegrenzte Zerlegbarkeit der ganzen Zahlen, wie sie in dem unendlichen Körper *aller* algebraischen Zahlen auftrat (§. 160, 7.), in einem endlichen Körper Ω wieder verschwindet. Dafür tritt aber bei unendlich vielen solchen Körpern Ω ein höchst eigenthümliches Phänomen auf, das schon früher (§. 16) gelegentlich erwähnt ist*). Nennt man eine Zahl in \mathfrak{o} *zerlegbar*, wenn sie das Product aus zwei Zahlen in \mathfrak{o} ist, welche beide keine Einheiten sind, dagegen *unzerlegbar*, wenn dies nicht der Fall ist, so ist offenbar jede zerlegbare Zahl μ darstellbar als Product aus einer *endlichen* Anzahl von unzerlegbaren Zahlen (vergl. §. 8), weil die Norm von μ gleich dem Producte aus den Normen der einzelnen Factoren ist (§. 159); aber es zeigt sich häufig, dass diese Zerlegung nicht eine vollkommen bestimmte ist, sondern dass mehrere *wesentlich verschiedene* Zerlegungen derselben Zahl in unzerlegbare Factoren existiren (§. 160, 6.). Dies widerspricht so sehr dem in der rationalen Zahlentheorie herrschenden Begriffe des Primzahlcharakters (§. 8), dass wir deshalb eine unzerlegbare Zahl als solche noch nicht als Primzahl anerkennen wollen; wir suchen daher für den wahren Primzahlcharakter ein kräftigeres Kriterium als diese unzulängliche Unzerlegbarkeit aufzustellen, ähnlich wie früher bei dem Begriffe der relativen Primzahl (§. 160, 7.), indem wir die zu untersuchende Zahl μ nicht zerlegen, sondern ihr Verhalten als *Modul*-betrachten:

Eine ganze Zahl μ , welche keine Einheit ist, soll eine Primzahl heißen, wenn jedes durch μ theilbare Product $\eta\varrho$ wenigstens einen durch μ theilbaren Factor η oder ϱ besitzt.

Es ergibt sich dann sofort, dass die höchste in einem Producte aufgehende Potenz einer Primzahl μ das Product aus den höchsten in den einzelnen Factoren aufgehenden Potenzen von μ ,

*) Das dortige Beispiel passt freilich nicht ganz hierher, insofern die ganzen Zahlen des der Gleichung $\varrho^2 = -11$ entsprechenden quadratischen Körpers nicht durch die Form $t + u\varrho$, wohl aber durch die Form $t + u\theta$ erschöpft werden, wo $2\theta = 1 + \varrho$ ist; die Zahlen 3, 5, $2 + \varrho$, $2 - \varrho$ sind in der That zerlegbar: $3 = \theta(1 - \theta)$, $5 = (1 + \theta)(2 - \theta)$, $2 - \varrho = -\theta(1 + \theta)$, $2 + \varrho = -(1 - \theta)(2 - \theta)$; die vier Zahlen θ , $1 - \theta$, $1 + \theta$, $2 - \theta$ sind Primzahlen in diesem Körper. Die in Rede stehende Erscheinung tritt aber in dem der Gleichung $\alpha^2 = -5$ entsprechenden quadratischen Körper an dem Beispiel $3 \cdot 7 = (1 + 2\alpha)(1 - 2\alpha)$ wirklich auf (vergl. §. 71; die beiden Zahlen 3, 7 sind durch die Hauptform der Determinante -5 nicht darstellbar).

und dass jede durch μ nicht theilbare Zahl relative Primzahl zu μ ist. Man erkennt ferner leicht, dass die kleinste durch μ theilbare rationale ganze Zahl p nothwendig eine Primzahl (im Körper der rationalen Zahlen), und folglich die Norm von μ eine Potenz von p , nämlich ein rationaler Divisor von $N(\mu) = p^n$ sein muss. Es werden daher gewiss alle Primzahlen μ des Körpers Ω entdeckt, wenn die Divisoren aller rationalen Primzahlen p aufgesucht werden.

5. Ist aber μ keine Primzahl (und auch keine Einheit), existiren also zwei durch μ nicht theilbare Zahlen η , ϱ , deren Product $\eta\varrho$ durch μ theilbar ist, so schreiten wir zu einer Zerlegung von μ in wirkliche oder *ideale*, d. h. fingirte Factoren. Giebt es nämlich in \mathfrak{o} einen grössten gemeinschaftlichen Theiler ν der beiden Zahlen η und $\mu = \nu\mu'$, der Art, dass die Quotienten $\eta:\nu$ und $\mu:\nu$ relative Primzahlen sind, so ist μ in die beiden Factoren ν und μ' zerlegt, von denen keiner eine Einheit ist, weil weder ϱ noch η durch μ theilbar ist. Der Factor μ' ist wesentlich dadurch bestimmt, dass alle Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ durch μ' theilbar sind (z. B. auch $\alpha' = \varrho$), und dass ebenso jede durch μ' theilbare Zahl α' auch der vorstehenden Congruenz genügt. Umgekehrt, giebt es in \mathfrak{o} eine Zahl μ' , welche in allen Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ und nur in diesen aufgeht, so ist auch μ theilbar durch μ' , und der Quotient $\nu = \mu:\mu'$ ist der grösste gemeinschaftliche Theiler der beiden Zahlen η und μ .

Aber es kann sehr wohl der Fall eintreten, dass in \mathfrak{o} keine solche Zahl μ' zu finden ist; als nun diese Erscheinung (bei den aus Einheitswurzeln gebildeten Zahlen) *Kummer* entgegentrat, so kam er auf den glücklichen Gedanken, trotzdem eine solche Zahl μ' zu fingiren und dieselbe als *ideale Zahl* einzuführen; die *Theilbarkeit* einer Zahl α' durch diese ideale Zahl μ' besteht lediglich darin, dass α' eine Wurzel der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ ist, und da diese idealen Zahlen in der Folge immer nur als Theiler oder Moduln auftreten, so hat diese Art ihrer Einführung durchaus keine Bedenken. Allein die Befürchtung, dass die unmittelbare Uebertragung der bei den *wirklichen* Zahlen üblichen Benennungen auf die idealen Zahlen im Anfang leicht Misstrauen gegen die Sicherheit der Beweisführung einflössen könnte, veranlasst uns, die Untersuchung dadurch in ein anderes Gewand einzukleiden, dass wir immer ganze *Systeme* von wirklichen Zahlen betrachten.

§. 163.

Wir gründen die Theorie der in \mathfrak{o} enthaltenen Zahlen, d. h. aller ganzen Zahlen des Körpers Ω , auf den folgenden neuen Begriff.

1. Ein System \mathfrak{a} von unendlich vielen in \mathfrak{o} enthaltenen Zahlen soll ein *Ideal* heissen, wenn es den beiden Bedingungen genügt;

I. Die Summe und die Differenz je zweier Zahlen in \mathfrak{a} sind wieder Zahlen in \mathfrak{a} .

II. Jedes Product aus einer Zahl in \mathfrak{a} und einer Zahl in \mathfrak{o} ist wieder eine Zahl in \mathfrak{a} .

Ist α in \mathfrak{a} enthalten, so sagen wir, α sei *theilbar durch* \mathfrak{a} , \mathfrak{a} *gehe in* α *auf*, weil die Ausdrucksweise hierdurch an Leichtigkeit gewinnt. Wir nennen ferner zwei in \mathfrak{o} enthaltene Zahlen ω, ω' , deren Differenz durch \mathfrak{a} theilbar ist, *congruent nach* \mathfrak{a} (vergl. §. 161), und bezeichnen dies durch die Congruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$; solche Congruenzen dürfen (zufolge I.) addirt, subtrahirt und (zufolge II.) multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen auch einander congruent sind, so kann man alle Zahlen in *Classen* $\pmod{\mathfrak{a}}$ eintheilen, indem man je zwei congruente Zahlen in dieselbe, je zwei incongruente Zahlen in zwei verschiedene Classen wirft; da nun, wenn μ eine von Null verschiedene Zahl in \mathfrak{a} bedeutet, je zwei nach μ congruente Zahlen (zufolge II.) auch nach \mathfrak{a} congruent sind — woraus zugleich folgt, dass \mathfrak{a} aus einer oder mehreren Classen $\pmod{\mu}$ besteht — so ist (zufolge §. 162, 2.) die Anzahl der Classen $\pmod{\mathfrak{a}}$, in welche \mathfrak{o} zerfällt, *endlich**). Wählt man aus jeder Classe ein Individuum als Repräsentanten, so bilden dieselben ein *vollständiges Restsystem* $\pmod{\mathfrak{a}}$; die Anzahl dieser Classen oder incongruenten Zahlen soll die *Norm* von \mathfrak{a} heissen und mit $N(\mathfrak{a})$ bezeichnet werden.

Ist η eine von Null verschiedene Zahl in \mathfrak{o} , so bilden alle durch η theilbaren Zahlen in \mathfrak{o} ein Ideal, welches mit $i(\eta)$ bezeichnet werden soll; solche Ideale sind besonders ausgezeichnet und sollen

*) Dasselbe ergibt sich unmittelbar aus §. 161; ist nämlich ω irgend eine Zahl in \mathfrak{o} , so kann durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl der Quotient $\omega : \mu$ in eine ganze Zahl, also ω (zufolge II.) in eine Zahl des Ideals \mathfrak{a} verwandelt werden.

Hauptideale heissen; die Norm von $i(\eta)$ ist $= \pm N(\eta)$; ist η eine Einheit, so ist $i(\eta) = \mathfrak{o}$, und umgekehrt.

2. Wenn alle Zahlen eines Ideals \mathfrak{a} auch in einem Ideal \mathfrak{b} enthalten sind, so besteht offenbar \mathfrak{b} aus einer oder mehreren Classen (mod. \mathfrak{a}), und wir wollen sagen, \mathfrak{a} sei ein *Multiplum* von \mathfrak{b} oder *theilbar durch* \mathfrak{b} , \mathfrak{b} sei ein *Theiler* von \mathfrak{a} oder *gehe in* \mathfrak{a} auf.

Besteht \mathfrak{b} aus r Classen (mod. \mathfrak{a}), so ist $N(\mathfrak{a}) = rN(\mathfrak{b})$. Durchläuft nämlich δ die Repräsentanten dieser r Classen, und γ ein vollständiges Restsystem (mod. \mathfrak{b}), so bilden die $rN(\mathfrak{b})$ Zahlen $\gamma + \delta$ ein vollständiges Restsystem (mod. \mathfrak{a}); denn erstens ist jede Zahl in \mathfrak{o} congruent einer Zahl γ (mod. \mathfrak{b}), also $\equiv \gamma + \delta$ (mod. \mathfrak{a}), und zweitens folgt aus $\gamma + \delta \equiv \gamma' + \delta'$ (mod. \mathfrak{a}), wo γ', δ' ähnliche Bedeutung haben wie γ, δ , successivè $\gamma + \delta \equiv \gamma' + \delta'$ (mod. \mathfrak{b}), $\gamma \equiv \gamma'$ (mod. \mathfrak{b}), $\gamma = \gamma'$, also $\delta \equiv \delta'$ (mod. \mathfrak{a}), $\delta = \delta'$, d. h. die sämtlichen Zahlen $\gamma + \delta$ sind incongruent (mod. \mathfrak{a}).

Ein Ideal besitzt folglich nur eine *endliche* Anzahl von Theilern. Ist \mathfrak{m} theilbar durch \mathfrak{a} , \mathfrak{a} durch \mathfrak{b} , so ist auch \mathfrak{m} durch \mathfrak{b} theilbar. Das Hauptideal \mathfrak{o} selbst geht in jedem Ideal auf und ist zugleich das *einzig*e Ideal, welches die Zahl 1 oder überhaupt Einheiten enthält, und dessen Norm $= 1$ ist.

Das System aller derjenigen Zahlen, welche gleichzeitig in zwei Idealen $\mathfrak{a}, \mathfrak{b}$ enthalten sind, ist das *kleinste gemeinschaftliche Multiplum* \mathfrak{m} von $\mathfrak{a}, \mathfrak{b}$, insofern jedes gemeinschaftliche Multiplum von $\mathfrak{a}, \mathfrak{b}$ durch das Ideal \mathfrak{m} theilbar ist. Durchläuft α alle Zahlen in \mathfrak{a} , β alle Zahlen in \mathfrak{b} , so ist das System aller Zahlen $\alpha + \beta$ der *grösste gemeinschaftliche Theiler* \mathfrak{d} der Ideale $\mathfrak{a}, \mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}, \mathfrak{b}$ in dem Ideale \mathfrak{d} aufgeht*).

Ist r die Anzahl der in \mathfrak{b} enthaltenen Zahlen, welche (mod. \mathfrak{a}) incongruent sind, so besteht \mathfrak{b} aus r Classen (mod. \mathfrak{m}), und \mathfrak{b} aus r Classen (mod. \mathfrak{a}); also ist $N(\mathfrak{m}) = rN(\mathfrak{b})$, $N(\mathfrak{a}) = rN(\mathfrak{b})$, und $N(\mathfrak{m})N(\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Ist \mathfrak{b} ein Hauptideal $= i(\eta)$, so ist die Anzahl r der in \mathfrak{b} enthaltenen Zahlen $\beta = \eta\omega$, welche (mod. \mathfrak{a}) incongruent sind, zugleich die Norm des aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. \mathfrak{a}) bestehenden Ideals \mathfrak{r} , weil zwei Zahlen ω, ω' stets und nur dann congruent (mod. \mathfrak{r}) sind, wenn $\eta\omega \equiv \eta\omega'$ (mod. \mathfrak{a}) ist. Mithin ist in diesem Falle $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{b})$.

*) Die Erweiterung dieser Definitionen von \mathfrak{m} und \mathfrak{d} für mehr als zwei Ideale $\mathfrak{a}, \mathfrak{b} \dots$ liegt auf der Hand.

3. Ein von \mathfrak{o} verschiedenes Ideal \mathfrak{p} , welches keinen von \mathfrak{o} und \mathfrak{p} verschiedenen Theiler besitzt, soll ein *Primideal* heissen. Dann gilt folgender Satz:

Ist $\eta\mathfrak{q} \equiv 0 \pmod{\mathfrak{p}}$, so ist wenigstens eine der beiden Zahlen η , \mathfrak{q} durch \mathfrak{p} theilbar. Ist nämlich η nicht $\equiv 0 \pmod{\mathfrak{p}}$, so bilden die sämtlichen Wurzeln \mathfrak{q} der Congruenz $\eta\mathfrak{q} \equiv 0 \pmod{\mathfrak{p}}$ offenbar ein in \mathfrak{p} aufgehendes Ideal, welches, da es die Zahl 1 nicht enthält, von \mathfrak{o} verschieden und folglich mit \mathfrak{p} identisch ist, was zu beweisen war.

Dieser Satz ist charakteristisch für ein Primideal, da er sich folgendermaassen umkehren lässt: *Enthält jedes durch ein (von \mathfrak{o} verschiedenes) Ideal \mathfrak{p} theilbare Product mindestens einen durch \mathfrak{p} theilbaren Factor, so ist \mathfrak{p} ein Primideal.* Ist nämlich \mathfrak{q} ein Theiler des Ideals \mathfrak{p} , aber verschieden von \mathfrak{p} , so giebt es in \mathfrak{q} eine nicht in \mathfrak{p} enthaltene Zahl ω ; dann ist (zufolge der Annahme) auch keine der Potenzen $\omega^2, \omega^3 \dots$ durch \mathfrak{p} theilbar; da aber nur eine endliche Anzahl von incongruenten Zahlen $\pmod{\mathfrak{p}}$ existirt, so muss einmal für zwei verschiedene Exponenten m und $m + s > m$ nothwendig $\omega^{m+s} \equiv \omega^m \pmod{\mathfrak{p}}$, also das Product $\omega^m(\omega^s - 1)$ durch \mathfrak{p} theilbar sein; da nun ω^m nicht durch \mathfrak{p} theilbar ist, so muss (zufolge der Annahme) der andere Factor $\omega^s - 1$ durch \mathfrak{p} , und folglich auch durch \mathfrak{q} theilbar sein; nun ist ω und, weil $s > 0$ ist, auch $\omega^s \equiv 0 \pmod{\mathfrak{q}}$, mithin ist auch die Zahl 1 in \mathfrak{q} enthalten, also $\mathfrak{q} = \mathfrak{o}$, was zu beweisen war.

Nennt man ein von \mathfrak{o} verschiedenes Ideal *zusammengesetzt*, wenn es kein Primideal ist, so lässt sich dieser Satz auch so aussprechen: *Ist \mathfrak{a} ein zusammengesetztes Ideal, so giebt es zwei durch \mathfrak{a} nicht theilbare Zahlen η , \mathfrak{q} , deren Product $\eta\mathfrak{q}$ durch \mathfrak{a} theilbar ist.* Wir beweisen ihn zum zweiten Male auf folgende Art. Es sei \mathfrak{e} ein von \mathfrak{a} und \mathfrak{o} verschiedener Theiler von \mathfrak{a} , so giebt es in \mathfrak{e} eine durch \mathfrak{a} nicht theilbare Zahl η , und der grösste gemeinschaftliche Theiler \mathfrak{b} von \mathfrak{a} und $i(\eta)$ ist theilbar durch \mathfrak{e} , also von \mathfrak{o} verschieden, mithin ist $N(\mathfrak{b}) > 1$. Das aus allen Wurzeln \mathfrak{q} der Congruenz $\eta\mathfrak{q} \equiv 0 \pmod{\mathfrak{a}}$ bestehende Ideal \mathfrak{r} ist ein Theiler von \mathfrak{a} , und da (zufolge 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{b}) > N(\mathfrak{r})$ ist, so ist \mathfrak{r} verschieden von \mathfrak{a} und enthält folglich eine durch \mathfrak{a} nicht theilbare Zahl \mathfrak{q} , was zu beweisen war.

Es leuchtet nun ein, dass die kleinste (von Null verschiedene) rationale Zahl \mathfrak{p} , welche in einem Primideale \mathfrak{p} enthalten ist, nothwendig eine *Primzahl* (im rationalen Zahlkörper) sein muss; da

ferner p in $i(p)$ aufgeht, so ist $N(p)$ ein Theiler von $N(p) = p^n$, also ebenfalls eine Potenz p^f der rationalen Primzahl p , und man findet leicht (vergl. §. 162, 3.), dass jede in \mathfrak{o} enthaltene Zahl ω der Congruenz

$$\omega^{p^f} \equiv \omega \pmod{p}$$

genügt*). Auch hat es keine Schwierigkeit, die allgemeinen Sätze der §§. 26, 27, 29, 30, 31 auf Congruenzen in Bezug auf den Modul p zu übertragen.

Ist das kleinste gemeinschaftliche Multipulum m der Ideale $a, b, c \dots$ durch das Primideal p theilbar, so geht p wenigstens in einem der Ideale $a, b, c \dots$ auf. Ist nämlich keins dieser Ideale durch p theilbar, giebt es also in $a, b, c \dots$ resp. Zahlen $\alpha, \beta, \gamma \dots$, die nicht durch p theilbar sind, so ist das in $a, b, c \dots$, also auch in

*) Hierauf beruht das Eingreifen der *Theorie der höheren Congruenzen* (vergl. §. 26), welche zur Bestimmung der Primideale dient. Für die Körper vom Grade $n = \varphi(m)$, welche aus den primitiven Wurzeln θ der Gleichung $\theta^m = 1$ entspringen, ist dieselbe zuerst ausgeführt, und zwar von *Kummer*, dem Schöpfer der Theorie der idealen Zahlen; den hierauf bezüglichen Theil seiner Untersuchungen findet man am vollständigsten zusammengestellt in den Abhandlungen: *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers* (Journ. de Math. p. p. Liouville, T. XVI. 1851). — *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist* (Abh. der Berliner Ak. 1856). Das Hauptresultat ergibt sich mit grösster Leichtigkeit aus unserer Theorie und lautet in unserer Ausdrucksweise folgendermassen: Ist p eine rationale Primzahl und m' der grösste durch p nicht theilbare Divisor von $m = p^f m'$, gehört ferner p zum Exponenten $f \pmod{m'}$, wo $\varphi(m') = ef$ (§. 28), so ist $i(p) = (\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e)^{\varphi(p^f)}$, wo $\mathfrak{p}_1, \mathfrak{p}_2 \dots \mathfrak{p}_e$ von einander verschiedene Primideale bedeuten, deren Normen $= p^f$ sind; wenn $p^f > 1$, so ist $i(1 - \theta^{m'}) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e$. — Für complexe Zahlen einer höheren Stufe vergl. *Kummer: Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist* (Abh. der Berliner Ak. 1859). — Für diejenigen Körper Ω , deren conjugirte Körper mit Ω identisch sind, und welche ich *Galois'sche Körper* nennen möchte, vergl. *Selwing: Ueber die idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln einer beliebigen irreductibelen Gleichung rational gebildet sind* (Schlömilch's Zeitschr. für Math. u. Phys. Bd. 10. 1865). — Ein specieller Fall biquadratischer Körper ist vollständig durchgeführt von *Bachmann: Die Theorie der complexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind*. 1867. — Für eine gewisse Classe cubischer Körper vergl. *Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken* (Crelle's Journ. XXVIII).

m enthaltene Product $\alpha\beta\gamma \dots$ nicht theilbar durch das Primideal \mathfrak{p} , und folglich geht \mathfrak{p} nicht in m auf, was zu beweisen war.

Ist die Zahl η nicht theilbar durch das Ideal \mathfrak{a} , so giebt es immer eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ ein Primideal bilden. Alle Wurzeln β der Congruenz $\eta\beta \equiv 0 \pmod{\mathfrak{a}}$ bilden ein in \mathfrak{a} aufgehendes Ideal \mathfrak{b} , welches von \mathfrak{o} verschieden ist, weil es die Zahl 1 nicht enthält; ist \mathfrak{b} ein Primideal, so ist der Satz bewiesen. Ist \mathfrak{b} kein Primideal, giebt es also zwei durch \mathfrak{b} nicht theilbare Zahlen η', ϱ' , deren Product $\eta'\varrho' \equiv 0 \pmod{\mathfrak{b}}$ ist, so bilden alle Wurzeln γ der Congruenz $\eta'\gamma \equiv 0 \pmod{\mathfrak{b}}$, d. h. der Congruenz $\eta\eta'\gamma \equiv 0 \pmod{\mathfrak{a}}$, ein in \mathfrak{b} aufgehendes Ideal \mathfrak{c} , und zwar ist (zufolge 2.) $N(\mathfrak{c}) < N(\mathfrak{b})$, weil ϱ' in \mathfrak{c} , aber nicht in \mathfrak{b} enthalten ist; ausserdem ist \mathfrak{c} von \mathfrak{o} verschieden, weil η' nicht in \mathfrak{b} , und folglich die Zahl 1 nicht in \mathfrak{c} enthalten ist; ist \mathfrak{c} ein Primideal, so ist der Satz bewiesen. Ist aber \mathfrak{c} kein Primideal, so kann man in derselben Weise fortfahren; endlich muss in der Reihe der Ideale $\mathfrak{b}, \mathfrak{c}, \mathfrak{d} \dots$, deren Normen immer kleiner werden, aber stets > 1 bleiben, ein Primideal \mathfrak{p} auftreten, welches aus allen Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ besteht, wo $\nu = \eta\eta'\eta'' \dots$ durch η theilbar ist.

4. Ist μ eine von Null verschiedene Zahl in \mathfrak{o} und keine Einheit, so existirt zufolge des zuletzt bewiesenen Satzes (in welchem man $\eta = 1$ nehmen kann) jedenfalls eine Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein Primideal \mathfrak{p} bilden; Primideale, welche aus den sämtlichen Wurzeln einer solchen Congruenz bestehen, wollen wir vorläufig *einfache* Ideale nennen. Ist nun r irgend ein ganzer rationaler, nicht negativer Exponent, so bilden alle Wurzeln ϱ der Congruenz $\varrho\nu^r \equiv 0 \pmod{\mu^r}$ ein Ideal, welches die r te Potenz von \mathfrak{p} heissen und mit \mathfrak{p}^r bezeichnet werden soll. Diese Definition ist unabhängig von dem zur Definition von \mathfrak{p} benutzten Zahlenpaar μ, ν ; ist nämlich μ' irgend eine von Null verschiedene, durch \mathfrak{p} theilbare Zahl, also $\nu\mu' = \mu\nu'$, so folgt aus $\varrho\nu^r \equiv 0 \pmod{\mu^r}$ durch Multiplication mit μ'^r und Division durch μ^r auch $\varrho\nu'^r \equiv 0 \pmod{\mu'^r}$, und umgekehrt. Von der grössten Wichtigkeit sind aber die folgenden Sätze über einfache Ideale \mathfrak{p} :

Ist $s \geq r$, so ist \mathfrak{p}^s theilbar durch \mathfrak{p}^r . Ist nämlich σ in \mathfrak{p}^s enthalten, also $\sigma\nu^s = \tau\mu^s$, so folgt, dass

$$\left(\frac{\sigma\nu^r}{\mu^r}\right)^s = \tau^s \mu^{s-r}$$

eine ganze Zahl ist; mithin ist (nach §. 160, 3.) der jedenfalls dem Körper Ω angehörige Quotient $\sigma v^r : \mu^r$ ebenfalls eine *ganze* Zahl, also in \mathfrak{o} enthalten, weil \mathfrak{o} *alle* ganzen Zahlen des Körpers Ω umfasst*); also ist jede Zahl σ des Ideals \mathfrak{p}^s auch in \mathfrak{p}^r enthalten.

Ist \mathfrak{q} eine von Null verschiedene Zahl in \mathfrak{o} , so giebt es immer eine höchste in \mathfrak{q} aufgehende Potenz von \mathfrak{p} . Wäre nämlich für unendlich viele Exponenten r das Product $\mathfrak{q} v^r$ theilbar durch μ^r , so müsste, da nur eine endliche Anzahl incongruenter Zahlen (mod. \mathfrak{q}) existirt, für zwei verschiedene solche Exponenten r, s nothwendig einmal

$$\frac{\mathfrak{q} v^r}{\mu^r} \equiv \frac{\mathfrak{q} v^s}{\mu^s} \pmod{\mathfrak{q}}, \quad \left(\frac{v}{\mu}\right)^r = \left(\frac{v}{\mu}\right)^s + \omega$$

werden, wo ω eine ganze Zahl; hieraus würde aber (nach §. 160, 3.) folgen, dass v durch μ theilbar wäre, was nicht der Fall ist, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre.

Sind $\mathfrak{p}^r, \mathfrak{p}^s$ resp. die höchsten in \mathfrak{q}, σ aufgehenden Potenzen, so ist \mathfrak{p}^{r+s} die höchste in $\mathfrak{q}\sigma$ aufgehende Potenz von \mathfrak{p} . Denn da $\mathfrak{q} v^r = \mathfrak{q}' \mu^r, \sigma v^s = \sigma' \mu^s$, und keins der Producte $v \mathfrak{q}', v \sigma'$ durch μ theilbar ist, so folgt $\mathfrak{q}\sigma v^{r+s} = \mathfrak{q}'\sigma' \mu^{r+s}$, und $v \mathfrak{q}'\sigma'$ kann nicht durch μ theilbar sein, weil \mathfrak{p} ein Primideal ist.

Ist $e \geq 1$ der Exponent der höchsten in μ selbst aufgehenden Potenz von \mathfrak{p} , also $\mu v^e = \kappa \mu^e$, wo $v \kappa$ nicht theilbar durch μ , so folgt $v^e = \kappa \mu^{e-1}$, d. h. der Exponent der höchsten in v aufgehenden Potenz von \mathfrak{p} ist $= e - 1$. Das Ideal \mathfrak{p}^e besteht aus den sämtlichen Wurzeln θ der Congruenz $\kappa \theta \equiv 0 \pmod{\mu}$. Die ganze Zahl $\lambda = \kappa \mu : v = \sqrt[e]{\mu \kappa^{e-1}}$ ist durch \mathfrak{p} , aber nicht durch \mathfrak{p}^2 theilbar; mithin ist λ^r durch \mathfrak{p}^r , aber nicht durch \mathfrak{p}^{r+1} theilbar, woraus beiläufig folgt, dass die Ideale \mathfrak{p}^r und \mathfrak{p}^{r+1} wirklich *verschieden* sind. Endlich leuchtet folgender Satz ein:

Jede Potenz \mathfrak{p}^r eines einfachen Ideals \mathfrak{p} ist durch kein von \mathfrak{p} verschiedenes Primideal theilbar. Ist nämlich π irgend eine Zahl in \mathfrak{p} , so muss ein in \mathfrak{p}^r aufgehendes Primideal in π^r , also (zufolge 3.) in π selbst, d. h. in \mathfrak{p} aufgehen und folglich mit \mathfrak{p} identisch sein.

5. Die Wichtigkeit der einfachen Ideale und ihre Analogie mit den rationalen Primzahlen tritt unmittelbar hervor in dem folgenden Hauptsatz:

*) Sobald diese Bedingung nicht erfüllt ist, verlieren auch die obigen Sätze ihre *allgemeine* Gültigkeit; dies ist von Wichtigkeit für die Erweiterung der Definition der Ideale (vergl. §. 165, 4.).

Wenn alle in einer von Null verschiedenen Zahl μ aufgehenden Potenzen einfacher Ideale auch in einer Zahl η aufgehen, so ist η durch μ theilbar. Ist η nicht theilbar durch μ , so giebt es (zufolge 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein in μ aufgehendes einfaches Ideal \mathfrak{p} bilden; ist \mathfrak{p}^e die höchste in μ aufgehende Potenz, so ist (nach 4.) \mathfrak{p}^{e-1} die höchste in ν aufgehende Potenz, und da ν durch η theilbar ist, so kann η nicht durch \mathfrak{p}^e theilbar sein, was zu beweisen war. Derselbe Satz lässt sich offenbar auch so aussprechen: *Jedes Hauptideal $i(\mu)$ ist das kleinste gemeinschaftliche Multiplum aller in μ aufgehenden Potenzen von einfachen Idealen.* Es folgt zunächst:

Jedes Primideal \mathfrak{p} ist ein einfaches Ideal. Es sei μ irgend eine von Null verschiedene Zahl in \mathfrak{p} , so muss \mathfrak{p} (zufolge 3.) in einer der Potenzen einfacher Ideale aufgehen, deren kleinstes gemeinschaftliches Multiplum $i(\mu)$ ist; mithin ist \mathfrak{p} selbst (zufolge 4.) ein einfaches Ideal. — Wir sprechen daher künftig nur noch von Primidealen, nicht mehr von einfachen Idealen.

Wenn alle in einem Ideal m aufgehenden Potenzen von Primidealen auch in einer Zahl η aufgehen, so ist η theilbar durch m . Ist η nicht theilbar durch m , so giebt es (nach 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{m}$ ein Primideal \mathfrak{p} bilden; ist \mathfrak{p}^e die höchste in m aufgehende Potenz von \mathfrak{p} , so giebt es in m eine nicht durch \mathfrak{p}^{e+1} theilbare Zahl μ , und das aus allen Wurzeln ϱ der Congruenz $\nu\varrho \equiv 0 \pmod{\mu}$ bestehende Ideal r ist theilbar durch \mathfrak{p} , weil $\nu\varrho \equiv 0 \pmod{m}$ ist. Sind nun $\mathfrak{p}^e, \mathfrak{p}'^e, \mathfrak{p}''^e \dots$ die sämtlichen höchsten in μ aufgehenden Potenzen verschiedener Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \dots$, so besteht r zufolge des obigen Hauptsatzes aus allen gemeinschaftlichen Wurzeln ϱ der Congruenzen $\nu\varrho \equiv 0 \pmod{\mathfrak{p}^e}, \nu\varrho \equiv 0 \pmod{\mathfrak{p}'^e}, \nu\varrho \equiv 0 \pmod{\mathfrak{p}''^e} \dots$ u. s. w., d. h. r ist das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{q}, \mathfrak{q}', \mathfrak{q}'' \dots$, welche resp. aus den Wurzeln jeder einzelnen dieser Congruenzen bestehen; da nun die Ideale $\mathfrak{q}', \mathfrak{q}'' \dots$ als Theiler von $\mathfrak{p}'^e, \mathfrak{p}''^e \dots$ nicht durch \mathfrak{p} theilbar sind, so muss, weil r durch \mathfrak{p} theilbar ist, auch \mathfrak{q} (zufolge 3.) durch \mathfrak{p} theilbar sein; es kann folglich \mathfrak{p}^e nicht in ν aufgehen (weil sonst $\mathfrak{q} = \mathfrak{o}$, also nicht durch \mathfrak{p} theilbar wäre), und da ν durch η theilbar ist, so kann \mathfrak{p}^e auch nicht in η aufgehen, was zu beweisen war.

Dieser *Fundamentalsatz* lässt sich offenbar auch so aussprechen: *Jedes Ideal ist das kleinste gemeinschaftliche Multiplum aller in ihm aufgehenden Potenzen von Primidealen.* Er entspricht durchaus

dem Fundamentalsatze der rationalen Zahlentheorie über die Zusammensetzung der Zahlen aus Primzahlen (§. 8); denn ihm zufolge ist jedes Ideal m *vollständig bestimmt*, sobald die höchsten in m aufgehenden Potenzen $p^e, p'^e, p''^e \dots$ von Primidealen gegeben sind; aus ihm ergiebt sich auch ohne Weiteres der folgende Satz: *Ein Ideal m ist stets und nur dann durch ein Ideal δ theilbar, wenn alle in δ aufgehenden Potenzen von Primidealen auch in m aufgehen.* Dies folgt unmittelbar aus dem Begriffe des kleinsten gemeinschaftlichen Multiplums.

Ist m das kleinste gemeinschaftliche Multiplum von $p^e, p'^e, p''^e \dots$, wo $p, p', p'' \dots$ von einander verschiedene Primideale bedeuten, so ist $N(m) = N(p)^e N(p')^e N(p'')^e \dots$. Es giebt immer (zufolge 4.) eine durch p^{e-1} , aber nicht durch $a = p^e$ theilbare Zahl η ; das aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0 \pmod{a}$ bestehende Ideal r ist verschieden von δ (weil es die Zahl 1 nicht enthält) und ein Theiler von p (zufolge 4.), folglich identisch mit p ; da ferner der grösste gemeinschaftliche Theiler δ der Ideale $a = p^e$ und $i(\eta)$ zufolge des eben bewiesenen Fundamentalsatzes $= p^{e-1}$ ist, so folgt (aus 2.) $N(a) = N(r) N(\delta)$, d. h. $N(p^e) = N(p) N(p^{e-1})$, und hieraus allgemein $N(p^e) = N(p)^e$. — Nun ist (zufolge der Definition 2.) das kleinste gemeinschaftliche Multiplum m der Ideale $p^e, p'^e, p''^e \dots$ zugleich auch das der Ideale $a = p^e$ und b , wo b das kleinste gemeinschaftliche Multiplum der Ideale $p'^e, p''^e \dots$ bedeutet; da ferner (zufolge des Fundamentalsatzes) δ der grösste gemeinschaftliche Theiler von a und b ist, so folgt (aus 2.) $N(m) = N(a) N(b)$, d. h. $N(m) = N(p)^e N(b)$ und hieraus ergiebt sich offenbar der zu beweisende Satz.

6. Multiplicirt man alle Zahlen eines Ideals a mit allen Zahlen eines Ideals b , so bilden diese Producte und deren Summen ein durch a und b theilbares Ideal, welches das *Product aus den Factoren a und b* heissen und mit ab bezeichnet werden soll. Aus dieser Erklärung leuchtet sofort ein, dass $a\delta = a, a\delta = \delta a$, ferner $(ab)c = a(\delta c)$ ist (vergl. §§. 1, 2, 147). Zugleich gilt folgender Satz:

Sind p^a, p^b resp. die höchsten in a, b aufgehenden Potenzen des Primideals p , so ist p^{a+b} die höchste in ab aufgehende Potenz von p ; und es ist $N(ab) = N(a) N(b)$.

Aus der Erklärung folgt nämlich unmittelbar (mit Rücksicht auf 4.), dass ab durch p^{a+b} theilbar ist; da ferner in a eine durch p^{a+1} nicht theilbare Zahl α , in b eine durch p^{b+1} nicht theilbare

Zahl β existirt, so giebt es in $a\ b$ eine durch p^{a+b+1} nicht theilbare Zahl $\alpha\beta$, womit der erste Theil des Satzes bewiesen ist. Ist also a das kleinste gemeinschaftliche Multiplum der Potenzen $p^a, p'^a, p''^a \dots$ der von einander verschiedenen Primideale $p, p', p'' \dots$, und b das kleinste gemeinschaftliche Multiplum der Potenzen $p^b, p'^b, p''^b \dots$, so ist $a\ b$ dasjenige der Potenzen $p^{a+b}, p'^{a+b}, p''^{a+b} \dots$, woraus (mit Rücksicht auf 5.) auch der zweite Theil des Satzes folgt.

Da aus diesem Satze auch $p^a p^b = p^{a+b}$ folgt, so ist die oben (in 4.) gewählte Ausdrucks- und Bezeichnungsweise gerechtfertigt. Sind ferner $p, p', p'' \dots$ von einander verschiedene Primideale, so ist $p^a p'^a p''^a \dots$ das kleinste gemeinschaftliche Multiplum der Potenzen $p^a, p'^a, p''^a \dots$. Auch leuchtet ein, dass der Begriff der Potenz durch die Definition $a^{r+1} = a a^r$ auf jedes Ideal a ausgedehnt werden kann. Ist endlich a *theilbar* durch b , so giebt es immer ein und nur ein Ideal r der Art, dass $a = r b$ wird; sind nämlich p^a, p^d die höchsten resp. in a, b aufgehenden Potenzen eines Primideals p , so ist $d \leq a$, und r ist das Product aus allen Potenzen p^{a-d} . Mit Rücksicht hierauf erkennt man leicht, dass die früheren Sätze (in 2.) sich jetzt einfacher aussprechen lassen.

7. Wir nennen nun a und b *relative Primideale*, wenn ihr grösster gemeinschaftlicher Theiler $= v$ ist; ebenso soll η *relative Primzahl zum Ideal* a heissen, wenn a und $i(\eta)$ relative Primideale sind. Es leuchtet dann ein, dass die Sätze der rationalen Zahlentheorie über relative Primzahlen sich leicht auf die Theorie der Ideale übertragen lassen; wir begnügen uns aber hier, folgenden wichtigen Satz zu beweisen (vergl. §. 25):

Sind a, b *relative Primideale, und* μ, ν *zwei gegebene Zahlen, so giebt es immer eine und nur eine Classe von Zahlen* η *(mod. ab), welche den Bedingungen* $\eta \equiv \mu$ *(mod. a),* $\eta \equiv \nu$ *(mod. b) genügen. Durchlaufen nämlich* μ, ν, η *vollständige Restsysteme resp. für die drei Moduln* $a, b, a\ b$, *so entspricht jeder Zahl* η *eine und nur eine Combination* μ, ν *der Art, dass* $\mu \equiv \eta$ *(mod. a),* $\nu \equiv \eta$ *(mod. b) ist; entspräche ferner zwei verschiedenen Zahlen* η, η' *des Restsystems für den Modul* $a\ b$ *eine und dieselbe Combination* μ, ν , *so wäre* $\eta - \eta'$ *theilbar sowohl durch* a *als durch* b , *also auch durch* $a\ b$ *(weil* a, b *relative Primideale sind), mithin wäre* $\eta \equiv \eta'$ *(mod. ab), was gegen die Voraussetzung streitet. Durchläuft daher* η *alle seine Werthe, deren Anzahl* $= N(a\ b) = N(a) N(b)$ *ist, so entstehen ebensoviele verschiedene Combinationen* μ, ν ; *und da genau ebensoviele ver-*

schiedene Combinationen μ, ν wirklich existiren, so muss auch umgekehrt jede Combination μ, ν einer Zahl η entsprechen, was zu beweisen war.

Bedeutet $\psi(a)$ die Anzahl der (mod. a) incongruenten relativen Primzahlen zu a , so ist $\psi(ab) = \psi(a)\psi(b)$, wenn a, b relative Primideale bedeuten. Ist ferner p ein Primideal, und $e \geq 1$, so ist $\psi(p^e) = N(p^e) - N(p^{e-1}) = N(p)^{e-1}(N(p) - 1)$; denn, wenn δ alle r durch p theilbaren und nach dem Modul p^e incongruenten Zahlen, wenn ferner γ ein vollständiges Restsystem (mod. p) durchläuft, so bilden die Zahlen $\gamma + \delta$ (zufolge 2.) ein vollständiges Restsystem (mod. p^e), und es ist $N(p^e) = rN(p)$, also $r = N(p^{e-1})$; nun ist aber eine solche Zahl $\gamma + \delta$ stets und nur dann relative Primzahl zu p^e , wenn γ nicht $\equiv 0$ (mod. p) ist, und folglich ist die Anzahl der Zahlen $\gamma + \delta$, welche relative Primzahlen zu p^e sind, gleich $r(N(p) - 1)$, was zu beweisen war.

Bedeutet p ein Primideal, so giebt es (zufolge 4.) immer eine Zahl λ , welche durch p , aber nicht durch p^2 theilbar ist, mithin auch eine Zahl λ^e , welche durch p^e , aber nicht durch p^{e+1} theilbar ist. Sind nun $p, p', p'' \dots$ von einander verschiedene Primideale, und haben $\lambda', \lambda'' \dots$ ähnliche Bedeutung für $p', p'' \dots$, wie λ für p , so existirt immer, wenn $e, e', e'' \dots$ gegebene Exponenten bedeuten, eine Zahl η , welche den gleichzeitigen Congruenzen

$$\begin{aligned} \eta &\equiv \lambda^e \pmod{p^{e+1}}, & \eta &\equiv \lambda'^{e'} \pmod{p'^{e'+1}}, \\ & & \eta &\equiv \lambda''^{e''} \pmod{p''^{e''+1}} \dots \end{aligned}$$

genügt, weil die Moduln relative Primideale sind. Dann ist offenbar $i(\eta) = m p^e p'^{e'} p''^{e''} \dots$, und das Ideal m ist durch keines der Primideale p, p', p'' theilbar. Hieraus folgt unmittelbar der Satz:

Sind a, b zwei beliebige Ideale, so giebt es immer ein solches relatives Primideal m zu b , dass am ein Hauptideal wird. Sind nämlich $p, p', p'' \dots$ alle von einander verschiedenen in ab aufgehenden Primideale, und ist $a = p^e p'^{e'} p''^{e''} \dots$ (wo die Exponenten $e, e', e'' \dots$ auch $= 0$ sein können), so giebt es, wie eben gezeigt ist, ein durch a theilbares Hauptideal $i(\eta) = am$ der Art, dass b und m relative Primideale sind.

Hieraus folgt auch, dass jedes Ideal a , welches kein Hauptideal ist, immer als der grösste gemeinschaftliche Theiler von *zwei* Hauptidealen angesehen werden kann; hat man nämlich nach Belieben ein durch a theilbares Hauptideal $i(\eta') = ab$ gewählt, so kann man immer ein zweites $i(\eta) = am$ so wählen, dass b und m re-

lative Primideale werden; die sämtlichen Zahlen des Ideals \mathfrak{a} sind dann von der Form $\eta\omega + \eta'\omega'$, wo ω, ω' alle Zahlen in \mathfrak{o} durchlaufen.

§. 164.

Wir gehen nun zu einer Eintheilung der Ideale des Körpers Ω in *Classen* über, welche auf folgenden Grundlagen beruht.

1. Das System E aller Hauptideale besitzt folgende fundamentale Eigenschaften *).

I. *Jedes Product aus zwei Idealen in E ist wieder ein Ideal in E .* Denn es ist $i(\eta)i(\eta') = i(\eta\eta')$.

II. *Sind e und e' Ideale in E , so ist auch e' ein Ideal in E .* Ist nämlich $e = i(\eta)$, $e' = i(\eta')$, so ist η' theilbar durch η , also $\eta'' = \eta\eta'$, woraus $e' = i(\eta'')$ folgt.

III. *Ist \mathfrak{a} ein beliebiges Ideal, so giebt es immer ein Ideal m der Art, dass $\mathfrak{a}m$ ein Ideal in E wird.* Denn es sei η irgend eine von Null verschiedene Zahl in \mathfrak{a} , so ist das Ideal $e = i(\eta)$ theilbar durch \mathfrak{a} , und folglich existirt (nach §. 163, 6. oder 7.) ein Ideal m , welches der Bedingung $\mathfrak{a}m = e$ genügt.

Wir nennen nun zwei Ideale $\mathfrak{a}, \mathfrak{a}'$ *äquivalent*, wenn ein Ideal m der Art existirt, dass beide Producte $\mathfrak{a}m, \mathfrak{a}'m$ dem System E angehören**). Sind ferner $\mathfrak{a}', \mathfrak{a}''$ äquivalent, giebt es also ein Ideal m' der Art, dass $\mathfrak{a}'m', \mathfrak{a}''m'$ Ideale in E sind, so gehören, wenn $\mathfrak{a}'m'm' = m''$ gesetzt wird, auch die Producte $\mathfrak{a}m'' = (\mathfrak{a}m)(\mathfrak{a}'m')$ und $\mathfrak{a}''m'' = (\mathfrak{a}'m)(\mathfrak{a}''m')$ dem System E an (zufolge I.), d. h. die

*) Diese drei Eigenschaften sind aber nicht charakteristisch für das System E der Hauptideale, sondern sie kommen auch anderen Systemen zu, für welche dann nothwendig dieselben Gesetze der Classification gelten. Giebt es z. B. in Ω keine Einheit, deren Norm $= -1$ ist, und nimmt man ein Ideal $i(\eta)$ nur dann in das System E auf, wenn $N(\eta)$ positiv ist, so hat auch dieses System E dieselben drei Eigenschaften (vergl. Kronecker: *Ueber die Classenanzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen*; Monatsber. d. Berliner Ak. 23. Juli 1863). Ebenso könnte man in E alle Ideale einer ganzen Gruppe von Classen aufnehmen, z. B. alle diejenigen, welche dem Hauptgeschlecht angehören.

***) Diese Definition kann offenbar auch durch die folgende ersetzt werden: zwei Ideale $\mathfrak{a}, \mathfrak{a}'$ heissen äquivalent, wenn es zwei Ideale e, e' in E giebt, welche der Bedingung $\mathfrak{a}e' = \mathfrak{a}'e$ genügen.

dem Ideale a' äquivalenten Ideale a, a'' sind auch einander äquivalent. Hieraus allein folgt schon die Möglichkeit, alle Ideale in Classen einzutheilen: eine *Classe* ist der Inbegriff aller Ideale, welche einem bestimmten Ideal äquivalent sind.

Das System E selbst bildet eine solche Classe. Gehören nämlich e, e', e'' diesem System an, so gilt (zufolge I.) dasselbe von den Producten $ee'', e'e''$, d. h. e, e' sind äquivalent und gehören folglich in eine und dieselbe Classe. Sind umgekehrt e, e' äquivalent, und gehört e dem System E an, so gilt dasselbe von e' ; denn, wenn $e, ee'', e'e''$ Ideale in E sind, so gehört (zufolge II.) auch e'' , mithin auch e' dem Systeme E an. Diese Classe E soll die *Hauptclasse* heissen.

Durchläuft nun a alle Ideale einer Classe A , b alle Ideale einer Classe B , so gehören alle Producte ab einer und derselben Classe an, welche *aus A und B zusammengesetzt* heissen und mit AB bezeichnet werden soll; gehören nämlich $am, a'm, bn, b'n$ der Hauptclasse E an, so gilt (zufolge I.) dasselbe von $(ab)(mn) = (am)(bn)$ und $(a'b')(mn) = (a'm)(b'n)$. Offenbar ist $AB = BA, (AB)C = A(BC)$ u. s. w. (vergl. §. 147).

Ist a ein beliebiges Ideal, e ein Ideal in E , so sind a und ae äquivalent; gehört nämlich am dem System E an, so gilt dasselbe von $(ae)m = (am)e$. Hieraus folgt $AE = A$ (vergl. §. 148, 1.).

Da ferner jedes gegebene Ideal a (zufolge III.) durch Multiplication mit einem Ideal m in ein Ideal der Hauptclasse E verwandelt werden kann, so gehört zu jeder gegebenen Classe A auch eine *entgegengesetzte* Classe M (oder A^{-1}) der Art, dass $AM = E$ wird, und zwar nur eine einzige, weil aus $AM' = E$ auch $AM'M = EM$, d. h. $M' = M$ folgt. Allgemein ergibt sich hieraus, dass aus $AB = AC$ stets $B = C$ folgt (vergl. §. 148, 2.).

2. Dass nun die Anzahl aller Idealclassen *endlich* ist, beruht auf einer tieferen Eigenschaft des Systems E aller Hauptideale, welche jetzt zu besprechen ist. Bilden die ganzen Zahlen $\omega_1, \omega_2 \dots \omega_n$ eine Grundreihe (oder irgend eine Basis) des Körpers Ω , und setzen wir (wie in §. 159) $\omega = \sum h_i \omega_i, H = N(\omega)$, so ist H eine homogene Function n ten Grades der Coordinaten h_i mit *ganzen* rationalen Coefficienten; bedeutet nun s die Summe der absoluten Werthe dieser Coefficienten, so besteht folgender Satz:

Ist a irgend ein Ideal, so giebt es immer ein durch a theilbares Hauptideal, dessen Norm $\leq sN(a)$ ist. Man gebe jeder der n Coordinaten h_i alle $(k+1)$ Werthe $0, 1, 2 \dots k$, wo $k \leq \sqrt[n]{N(a)} < k+1$;

da die Anzahl $(k + 1)^n$ der so entstehenden ganzen Zahlen ω grösser als $N(\alpha)$ ist, so müssen zwei ungleiche von ihnen einander congruent (mod. α) sein; ihre Differenz η wird dann eine von Null verschiedene, durch α theilbare Zahl, und da die absoluten Werthe ihrer Coordinaten den Werth k nicht übersteigen, so ist $N(\eta)$ absolut genommen $\leq sk^n \leq sN(\alpha)$; das Hauptideal $i(\eta)$ hat daher die geforderte Eigenschaft. Derselbe Satz kann offenbar auch so ausgesprochen werden: *Jedes Ideal α kann in ein Hauptideal verwandelt werden durch Multiplication mit einem Ideal m , dessen Norm $\leq s$ ist.*

Hierzu tritt folgende Ueberlegung. Durchläuft ϱ ein vollständiges Restsystem (mod. m), so nimmt auch $1 + \varrho$ lauter incongruente Werthe an, woraus durch Addition leicht folgt, dass die Zahl $m = N(m)$ durch m theilbar, dass also m ein Theiler des Hauptideals $i(m)$ ist. Da nun jedes Ideal nur eine endliche Anzahl von Theilern besitzt (§. 163, 2.), so giebt es auch nur eine endliche Anzahl von Idealen m , deren Normen einen gegebenen Werth m besitzen, mithin auch nur eine endliche Anzahl von Idealen m , deren Normen einen gegebenen Werth s nicht übertreffen. Zufolge des vorhergehenden Satzes giebt es daher eine *endliche* Anzahl von Idealen m der Art, dass jedes beliebige Ideal α durch Multiplication mit einem dieser Ideale m in ein Hauptideal verwandelt werden kann; dieser wichtige Zusatz zu der Eigenschaft III. des Systems E kann offenbar auch so gefasst werden: *Die Anzahl der Idealclassen, d. h. die Anzahl der nicht äquivalenten Ideale ist endlich.*

3. Es leuchtet nun ein, dass alle Sätze über Perioden oder über Gruppen von Classen quadratischer Formen (§. 149) ohne Weiteres auf unsere Idealclassen übertragen werden können. Wir heben hier nur die einzige Folgerung hervor:

Jedes Ideal kann durch Potenzirung in ein Hauptideal verwandelt werden. Ist also α ein Ideal, so giebt es immer einen positiven ganzen rationalen Exponenten m (Divisor der Classenzahl) der Art, dass α^m ein Hauptideal $i(\eta)$ wird; ist nun α irgend eine Zahl des Ideals α , so ist α^m theilbar durch η , mithin α theilbar durch die ganze Zahl $\sqrt[m]{\eta}$ (§. 160, 3.). Ist p^e die höchste in α aufgehende Potenz eines Primideals p , so ist $m e$ der Exponent der höchsten in η aufgehenden Potenz von p ; hieraus folgt leicht, dass umgekehrt jede durch $\sqrt[m]{\eta}$ theilbare Zahl α in α dem Ideale α angehört; denn da

α^m theilbar durch η ist, so ist, wenn p^a die höchste in α aufgehende Potenz von p bedeutet, $ma \geq me$, also $a \geq e$, mithin geht p^e auch in α auf (§. 163, 5.). Das Ideal α besteht daher aus allen durch $\sqrt[m]{\eta}$ theilbaren Zahlen in \mathfrak{o} .

Eine unmittelbare Folgerung aus dem Vorhergehenden ist der wichtige Satz: *Je zwei ganze Zahlen μ, ν besitzen einen grössten gemeinschaftlichen Divisor δ der Art, dass die Quotienten $\mu : \delta, \nu : \delta$ relative Primzahlen werden.* Denn bildet man in irgend einem Körper Ω , welchem die beiden Zahlen μ, ν angehören, den grössten gemeinschaftlichen Theiler α der beiden Hauptideale $i(\mu), i(\nu)$, so wird, wenn $\alpha^m = i(\eta)$ ist, $\sqrt[m]{\eta} = \delta$ ein solcher grösster gemeinschaftlicher Divisor von μ, ν ; natürlich giebt es unendlich viele solche Zahlen δ , welche aber nicht wesentlich verschieden sind (§. 160, 6.).

Auf die weitere Entwicklung unserer Theorie der Ideale, wie z. B. auf die Untersuchung des Zusammenhangs zwischen den Idealen zweier verschiedenen Körper müssen wir hier verzichten.

§. 165.

Die Theorie der Ideale eines Körpers Ω hängt unmittelbar zusammen mit der Theorie der zerlegbaren Formen, welche demselben Körper entsprechen; wir beschränken uns hier darauf, diesen Zusammenhang in seinen Grundzügen anzudeuten.

1. Ist F ein Product aus n homogenen linearen Functionen $f_1, f_2 \dots f_n$ von n Variablen $h_1, h_2 \dots h_n$, so wollen wir das Determinantenquadrat

$$\left(\sum \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \dots \frac{\partial f_n}{\partial h_n} \right)^2 = \mathcal{A}(F)$$

setzen und die Determinante der homogenen zerlegbaren Function F nennen*). Aus

$$\frac{\partial^2 \log F}{\partial h_r \partial h_s} = - \sum \frac{\partial \log f_i}{\partial h_r} \frac{\partial \log f_i}{\partial h_s}$$

folgt die Gleichung

$$F^2 \sum \pm \frac{\partial^2 \log F}{\partial h_1^2} \dots \frac{\partial^2 \log F}{\partial h_n^2} = (-1)^n \mathcal{A}(F),$$

*) Für quadratische Formen ist diese Determinante das Vierfache von der in §. 53 definirten Determinante.

welcher man verschiedene andere Formen, z. B. auch die folgende

$$\begin{vmatrix} F & \frac{\partial F}{\partial h_1} & \cdots & \frac{\partial F}{\partial h_n} \\ \frac{\partial F}{\partial h_1} & \frac{\partial^2 F}{\partial h_1^2} & \cdots & \frac{\partial^2 F}{\partial h_1 \partial h_n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial F}{\partial h_n} & \frac{\partial^2 F}{\partial h_n \partial h_1} & \cdots & \frac{\partial^2 F}{\partial h_n^2} \end{vmatrix} = (-1)^n F^{n-1} \mathcal{A}(F)$$

geben kann. Besitzt F lauter ganze rationale Coefficienten, so wollen wir ihren grössten gemeinschaftlichen Theiler t auch den *Theiler der Form F* nennen (vergl. §. 61); da sich nun leicht allgemein zeigen lässt, dass der Theiler eines Productes aus beliebigen Formen mit ganzen rationalen Coefficienten gleich dem Producte aus den Theilern der einzelnen Formen ist*), so folgt aus der vorstehenden Gleichung, dass $\mathcal{A}(F)$ eine ganze rationale, durch t^2 theilbare Zahl ist.

2. Aus der Definition eines Ideals α (§. 163, 1.) ergibt sich (zufolge §. 161), dass die sämtlichen in ihm enthaltenen Zahlen α von der Form

$$\alpha = \sum x_i \alpha_i \quad (1)$$

sind, wo die Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$ particuläre Zahlen des Ideals α bedeuten, während $x_1, x_2 \dots x_n$ alle ganzen rationalen Zahlen durchlaufen dürfen. Bilden nun die Zahlen $\omega_1, \omega_2 \dots \omega_n$ eine bestimmte Grundreihe des Körpers Ω (§. 162, 1.), so wollen wir die n Zahlen

$$\alpha_r = \sum \alpha_i^{(r)} \omega_i, \quad (2)$$

welche eine Basis des Ideals α bilden, in ihrer Aufeinanderfolge immer so wählen, dass ihre Coordinaten $\alpha_i^{(r)}$ eine *positive* Determinante

$$a = \sum \pm \alpha_1' \alpha_2'' \dots \alpha_n^{(n)} = N(\alpha) \quad (3)$$

besitzen; ferner ist die von der Wahl der Basis unabhängige Discriminante

$$\mathcal{A}(\alpha_1, \alpha_2 \dots \alpha_n) = a^2 \mathcal{A}(\Omega). \quad (4)$$

Damit die Zahlen α wirklich ein Ideal bilden, ist erforderlich und hinreichend, dass die sämtlichen Producte $\alpha_i \omega_j$ wieder Zahlen in α sind; es wird daher

*) Vergl. Gauss: *D. A.* art. 42.

$$\alpha \omega_r = \sum X_r^{(i)} \alpha_i = \sum X_r^{(i)} a_i^{(i)} \omega_i, \quad (5)$$

wo die n^2 Grössen $X_r^{(i)}$ homogene lineare Functionen der Veränderlichen $x_1, x_2 \dots x_n$ mit ganzen rationalen Coefficienten bedeuten, und hieraus folgt

$$N(\alpha) = a X, \quad (6)$$

wo die Determinante

$$X = \sum \pm X_1' X_2'' \dots X_n^{(n)} \quad (7)$$

eine homogene Form n ten Grades von $x_1, x_2 \dots x_n$ bedeutet; ihre Coefficienten sind ganze rationale Zahlen, und man erkennt leicht, dass diese Form X irreductibel ist, weil sie durch die lineare Function α und folglich auch durch alle mit α conjugirten Functionen algebraisch theilbar ist (vergl. §. 159). Aus (4) und (6) folgt ihre Determinante

$$\Delta(X) = \Delta(\Omega). \quad (8)$$

Ist ferner k eine gegebene ganze rationale (von Null verschiedene) Zahl, so kann man den Variabeln x_i stets solche ganze rationale Werthe beilegen, dass X relative Primzahl zu k wird. Man kann nämlich a durch Multiplication mit einem Ideal m , welches ein relatives Primideal zu $i(k)$ ist, in ein Hauptideal $i(\alpha) = am$ verwandeln (§. 163, 7.); ist nun \wp irgend ein in m aufgehendes Primideal, und p die durch \wp theilbare rationale Primzahl (§. 163, 3.), so kann k nicht durch p theilbar sein, und da $N(m)$ ein Product aus Potenzen solcher Primzahlen p ist (§. 163, 5.), so ist $N(m)$ relative Primzahl zu k . Nun ist α in a enthalten, also von der Form (1), wo die Grössen x_i bestimmte ganze rationale Werthe haben, und $N(\alpha) = a X$; da andererseits $i(\alpha) = am$, also $N(\alpha) = \pm a N(m)$ ist (§. 163, 6.), so ergiebt sich, dass $X = \pm N(m)$ relative Primzahl zu k ist, was zu beweisen war (vergl. §. 93). Hieraus folgt von selbst, dass X eine *ursprüngliche* Form ist, d. h. dass ihre Coefficienten keinen gemeinschaftlichen Theiler haben.

Wenn in dem Körper Ω keine Einheit existirt, deren Norm $= -1$ ist, so wollen wir ein Hauptideal $i(\eta)$ nur dann in die Hauptklasse E aufnehmen, wenn $N(\eta)$ positiv ist; ebenso sollen zwei Ideale a, a' nur dann äquivalent heissen und in dieselbe Classe aufgenommen werden, wenn beide durch Multiplication mit demselben Ideale m in Ideale der Hauptklasse E verwandelt werden (vergl. §. 164. Anm.). Gehört nun das Ideal a der Classe A an, so leuchtet ein, dass jeder positive Werth der Form X , welcher

ganzenrationalen Werthen x_i entspricht, die Norm eines zur entgegengesetzten Classe A^{-1} gehörenden Ideals \mathfrak{m} ist, und dass umgekehrt die Norm eines jeden solchen Ideals \mathfrak{m} durch die Form X dargestellt werden kann.

Wählt man statt der Basiszahlen $\alpha_1, \alpha_2 \dots \alpha_n$ des Ideals andere $\beta_1, \beta_2 \dots \beta_n$, welche aber ebenfalls der Bedingung genügen, dass die aus ihren Coordinaten gebildete Determinante positiv ist, so ist

$$\beta_r = \sum c_{r,i} \alpha_i, \quad \sum \pm c_{1,1} c_{2,2} \dots c_{n,n} = +1, \quad (9)$$

und die der Basis $\alpha_1, \alpha_2 \dots \alpha_n$ entsprechende Form X geht durch die Substitution

$$x_r = \sum c_{i,r} y_i, \quad (10)$$

deren Coefficienten $c_{i,r}$ ganze rationale Zahlen sind, in eine äquivalente Form Y über, welche der neuen Basis entspricht. Umgekehrt: ist Y eine mit X äquivalente Form, d. h. geht X durch eine ganzzahlige Substitution (10), deren Determinante $= +1$ ist, in Y über, so giebt es offenbar eine Basis des Ideals \mathfrak{a} , welcher diese Form Y entspricht. Allen Basen desselben Ideals \mathfrak{a} entspricht daher eine bestimmte *Formenklasse*, d. h. ein System von Formen X, Y, \dots , der Art, dass je zwei von ihnen einander äquivalent sind, und wir wollen sagen, dass diese Formenklasse dem Ideale \mathfrak{a} entspricht. Ist ferner η eine ganze Zahl von positiver Norm, so bilden die n Producte $\eta \alpha_i$ eine Basis des Ideals $\mathfrak{a}(\eta)$, und hieraus folgt unmittelbar, dass allen mit \mathfrak{a} äquivalenten Idealen, also einer ganzen Idealclasse, auch dieselbe Formenklasse entspricht. Auf die Frage, wie vielen Idealclassen eine und dieselbe Formenklasse entspricht, gehen wir hier nicht ein.

3. Bilden die Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$ die Basis eines Ideals \mathfrak{a} , ebenso die Zahlen $\beta_1, \beta_2 \dots \beta_n$ die Basis eines Ideals \mathfrak{b} , so hängen die Basiszahlen $\gamma_1, \gamma_2 \dots \gamma_n$ des Productes $\mathfrak{c} = \mathfrak{a} \mathfrak{b}$ mit denen der Ideale $\mathfrak{a}, \mathfrak{b}$ durch Gleichungen von der Form

$$\alpha_r \beta_s = \sum p_i^{r,s} \gamma_i, \quad \gamma_r = \sum q_i^{r,\nu} \alpha_i \beta_\nu, \quad (11)$$

zusammen, wo die sämmtlichen $2n^2$ Grössen p und q ganze rationale Zahlen bedeuten; durch Substitution erhält man

$$\sum p_i^{r,s} q_i^{t,\nu} = 1 \quad \text{oder} \quad = 0, \quad (12)$$

je nachdem $r = s$ ist oder nicht. Bezeichnet man mit P alle aus den Zahlen p gebildeten Determinanten n ten Grades, mit Q die ent-

sprechenden Determinanten aus den Zahlen q , so folgt hieraus nach einem bekannten Satze

$$\sum PQ = 1; \quad (13)$$

also haben die Determinanten P keinen gemeinschaftlichen Theiler. Führt man nun drei Systeme von je n Variabeln x, y, z ein, und setzt

$$\alpha = \sum x_i \alpha_i, \quad \beta = \sum y_i \beta_i, \quad \gamma = \sum z_i \gamma_i, \quad (14)$$

so wird

$$N(\alpha) = aX, \quad N(\beta) = bY, \quad N(\gamma) = cZ, \quad (15)$$

wo X, Y, Z die zu a, b, c gehörigen Formen bedeuten, und

$$a = N(a), \quad b = N(b), \quad c = N(c) = ab \quad (16)$$

ist. Zwischen diesen Formen findet nun folgender Zusammenhang Statt. Setzt man

$$\alpha\beta = \gamma, \quad (17)$$

so werden die Variabeln z bilineare Functionen von den Variabeln x und y , nämlich

$$z_r = \sum p_r^{i,j} x_i y_j, \quad (18)$$

und da gleichzeitig $N(\alpha)N(\beta) = N(\gamma)$, d. h.

$$XY = Z \quad (19)$$

wird, so geht die Form Z durch diese bilineare Substitution in das Product der beiden Formen X, Y über, und wir wollen sagen, die Form Z sei aus den beiden Formen X, Y *zusammengesetzt*. Zwischen diesen Formen und der bilinearen Substitution findet nun ein einfacher Zusammenhang Statt; da nämlich

$$\alpha\beta_r = \sum \frac{\partial z_i}{\partial y_r} \gamma_i, \quad \beta\alpha_r = \sum \frac{\partial z_i}{\partial x_r} \gamma_i \quad (20)$$

ist, so erhält man, wenn man r die Werthe $1, 2, \dots, n$ durchlaufen lässt, für Ω die n mit Ω conjugirten Körper setzt und die Determinanten nimmt,

$$X = \sum \pm \frac{\partial z_1}{\partial y_1} \dots \frac{\partial z_n}{\partial y_n}, \quad Y = \sum \pm \frac{\partial z_1}{\partial x_1} \dots \frac{\partial z_n}{\partial x_n}; \quad (21)$$

die Formen X, Y sind daher durch die Substitution (18) völlig bestimmt. Bezeichnet man ferner mit

$$\alpha' = \sum x'_i \alpha_i \quad (22)$$

die zu α adjungirte Function (§. 159, (8) und (38)), so ist

$$N(\alpha) = aX = \alpha\alpha', \quad (23)$$

und die n Grössen x' sind homogene Functionen $(n-1)$ ten Grades von den Variabeln x mit rationalen Coefficienten. Durch Multiplication mit β ergibt sich

$$a X \sum y_i \beta_i = \gamma \alpha'; \quad (24)$$

mithin sind die n Grössen

$$v_i = X y_i \quad (25)$$

bilineare Functionen von den Variablen x', z mit rationalen Coefficienten; da ferner

$$a \sum \frac{\partial v_i}{\partial x'_r} \beta_i = \gamma \alpha_r, \quad (26)$$

so ergibt sich, wie oben,

$$Z = a^{n-2} \sum \pm \frac{\partial v_1}{\partial x'_1} \dots \frac{\partial v_n}{\partial x'_n}. \quad (27)$$

Hieraus folgt, dass auch die Form Z durch die bilineare Substitution (18) vollständig bestimmt ist; denn bezeichnet man mit $u_i^{(r)}$ den Coefficienten des Elementes

$$\frac{\partial z_i}{\partial y_r} \text{ in } \sum \pm \frac{\partial z_1}{\partial y_1} \dots \frac{\partial z_n}{\partial y_n},$$

so ist auch

$$v_r = \sum u_i^{(r)} z_i, \quad (28)$$

und die n^2 Grössen $u_i^{(r)}$, welche homogene Functionen $(n-1)$ ten Grades der Variablen x mit ganzen rationalen Coefficienten sind, lassen sich folglich als homogene *lineare* Functionen der n Grössen x' darstellen. Statt der letzteren kann man auch n solche lineare Functionen von den n^2 Grössen $u_i^{(r)}$ mit ganzen rationalen Coefficienten einführen, durch welche sich umgekehrt auch die n^2 Grössen $u_i^{(r)}$ als lineare Functionen mit ganzen rationalen Coefficienten darstellen lassen. Auf die nähere Untersuchung dieser Eigenschaften der hier auftretenden bilinearen Substitutionen können wir aber nicht mehr eingehen.

4. Die ursprünglichen Formen X , welche den sämtlichen Idealen des Körpers Ω entsprechen und alle dieselbe Determinante $\mathcal{A}(\Omega)$ besitzen, bilden nur einen speciellen Fall der Formen H , welche jeder beliebigen Basis $\omega_1, \omega_2 \dots \omega_n$ des Körpers Ω entsprechen (§. 159). Für die Untersuchung dieser Formen ist es zweckmässig, den Begriff eines Ideals so zu erweitern, dass darunter ein System a von ganzen Zahlen α des Körpers Ω verstanden wird, welche sich durch Addition, Subtraction und Multiplication reproduciren, mit der ferneren Bedingung, dass dieses System n unabhängige Zahlen enthält, oder dass, was dasselbe sagt, jede Zahl des Körpers durch Multiplication mit einer rationalen, von Null ver-

schiedenen Zahl in eine Zahl α des Systems \mathfrak{a} verwandelt werden kann. Congruenzen in Bezug auf ein solches Ideal \mathfrak{a} als Modul können addirt, subtrahirt und mit beliebigen Zahlen des Ideals multiplicirt werden. Von besonderer Wichtigkeit ist aber das System *aller* Zahlen, mit welchen solche Congruenzen multiplicirt werden dürfen, d. h. aller Zahlen, welche durch Multiplication mit allen Zahlen des Ideals \mathfrak{a} in Zahlen desselben Ideals \mathfrak{a} verwandelt werden; man erkennt sofort, dass dies System selbst ein Ideal ist, welches die Zahl 1 enthält. Dieses Ideal kann die *Ordnung von* \mathfrak{a} oder auch ein *Einheitsideal* genannt werden, weil für die in ihm enthaltenen Zahlen die von *Dirichlet**) aufgestellte Theorie der Einheiten gilt, und wir wollen uns im Folgenden auf die Darstellung dieser Dirichlet'schen Principien beschränken, indem wir auf die weitere Entwicklung der allgemeinen Theorie der Ideale verzichten.

§. 166.

Wir nehmen im Folgenden an, dass die Basiszahlen $\omega_1, \omega_2 \dots \omega_n$ des Körpers \mathfrak{Q} zugleich die Basiszahlen einer *Ordnung* \mathfrak{o} sind, d. h. dass die Zahl 1 und alle Producte $\omega_i \omega_j$ ganze Coordinaten haben, woraus schon folgt, dass die Basiszahlen selbst ganze Zahlen sind. Die Zahlen in \mathfrak{o} , d. h. alle Zahlen $\omega = \sum h_i \omega_i$, deren Coordinaten h ganze rationale Zahlen sind, haben nun folgende Eigenschaften.

1. Ist ω eine Zahl in \mathfrak{o} , so ist auch die zu ihr adjungirte Zahl ω' in \mathfrak{o} enthalten.

Da nämlich ω einer Gleichung n ten Grades mit ganzen rationalen Coefficienten genügt, deren letzter $= N(\omega) = \omega \omega'$ ist, so erhält man durch Division mit ω eine Gleichung von der Form

$$\omega' = c + c_1 \omega + c_2 \omega^2 + \dots,$$

wo $c, c_1, c_2 \dots$ ganze rationale Zahlen bedeuten; mithin ist ω' in \mathfrak{o} enthalten.

2. Den mit \mathfrak{Q} conjugirten n Körpern entsprechen ebensoviele homogene lineare Functionen ω der Coordinaten h , und ihr Product $N(\omega)$ wird, wenn die Coordinaten ganze Zahlen sind, ebenfalls

*) Vergl. §. 141, Anm.

eine ganze rationale Zahl und folglich absolut ≥ 1 , ausgenommen, wenn alle Coordinaten verschwinden. Die n mit Ω conjugirten Körper enthalten entweder nur reelle Zahlen, oder es treten auch Paare von zwei solchen Körpern auf, dass wenn der eine die imaginäre Zahl $x + yi$ enthält, die conjugirte Zahl $x - yi$ sich in dem andern vorfindet. Wir wollen die Anzahl dieser imaginären Paare mit $n - \nu$, also die Anzahl der reellen Körper mit $2\nu - n$ bezeichnen; dann ist ν die Gesamtanzahl aller reellen Körper und imaginären Paare. Die einem imaginären Paare entsprechenden beiden Functionen ω sind von der Form $u + vi$ und $u - vi$, wo u und v zwei homogene lineare Functionen der Coordinaten bedeuten. Diese $2(n - \nu)$ Functionen u, v und die den reellen Körpern entsprechenden $(2\nu - n)$ Functionen ω bilden ein System von n reellen Functionen, die wir gemeinschaftlich mit w bezeichnen wollen, und deren Functionaldeterminante

$$= (2i)^{\nu-n} \sqrt{\Delta(\omega_1, \omega_2 \dots \omega_n)},$$

also von Null verschieden ist, weil die Zahlen $\omega_1, \omega_2 \dots \omega_n$ von einander unabhängig sind. Die Variablen h sind daher umgekehrt völlig bestimmte lineare Functionen von den Grössen w ; durchlaufen nun die letzteren stetig alle reellen Werthe, welche absolut kleiner als eine gegebene Constante sind, so bleiben auch die absoluten Werthe der Grössen h kleiner als eine entsprechende Constante und folglich wird auf diese Weise nur eine endliche Anzahl von Zahlen der Ordnung ν erzeugt, vielleicht gar keine.

Verstehen wir, wie üblich, unter dem Modulus $M(z)$ einer complexen Grösse $z = x + yi$ die positive Quadratwurzel aus $(x^2 + y^2)$, so können wir dies Resultat auch so aussprechen: *Es giebt in ν nur eine endliche Anzahl von Zahlen ω der Art, dass die Moduln aller mit ω conjugirten Zahlen, also auch die absoluten Werthe der Grössen w kleiner als eine vorgeschriebene Constante ausfallen.*

3. Wir theilen nun die n Körper, also auch die n Functionen ω nach Belieben in zwei Reihen, doch so, dass jede dieser Reihen wenigstens eine Function enthält, und dass je zwei Functionen $u \pm vi$ eines imaginären Paares in eine und dieselbe Reihe fallen (also ist der Fall $n = 1$ auszunehmen, ebenso der Fall $n = 2$ bei negativer Grundzahl). Bedeutet ferner c den grössten Werth, welchen die Modulsumme $\sum M(\omega_i)$ in irgend einer der n Functionen ω erreicht, so gilt folgender Satz:

Ist a ein beliebig kleiner, b ein beliebig grosser positiver gegebener Werth, so giebt es in ν eine solche Zahl ω , dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$, und dass $N(\omega)$ absolut $< (3c)^n$ wird.

Ist k eine bestimmte positive ganze rationale Zahl, und legt man jeder Coordinate h einen der $(k+1)$ Werthe $0, 1, 2 \dots k$ bei, so wird durchweg $M(\omega) \leq ck$, und die n Werthe w liegen zwischen den Grenzen $\pm ck$. Wir betrachten nun zunächst die der ersten Reihe angehörigen r Functionen ω oder w ; da $n > r > 0$, und $k > 0$ ist, so ist auch

$$(k+1)^{\frac{n}{r}} > k^{\frac{n}{r}} + 1,$$

und folglich kann man eine positive ganze rationale Zahl m so wählen, dass

$$(k+1)^n > m^r > k^n$$

wird; setzt man nun zur Abkürzung

$$d = \frac{2ck}{m} < 2ck^{1-\frac{n}{r}},$$

so wird das Gebiet aller zwischen den Grenzen $\pm ck$ liegenden reellen Werthe durch Einschaltung der $(m-1)$ Zahlen

$$-ck + d, \quad -ck + 2d \dots -ck + (m-1)d$$

in m Intervalle von gleicher Grösse d getheilt, wobei man diese $(m-1)$ Zahlen selbst nach Belieben dem einen oder anderen der beiden benachbarten Intervalle zurechnen kann. Da nun jeder der r Werthe w aus der ersten Reihe einem und nur einem dieser m Intervalle angehört, so ist m^r die Anzahl der verschiedenen denkbaren Fälle, welche die Vertheilung der r Werthe w auf diese m Intervalle darbieten kann. Da ferner, wenn jede der n Coordinaten h alle $(k+1)$ Werthe $0, 1, 2 \dots k$ durchläuft, $(k+1)^n$ solche Systeme von r zusammengehörigen Werthen w entstehen, so müssen, weil $(k+1)^n > m^r$ ist, mindestens zwei *verschiedene* solche Werthesysteme hinsichtlich ihrer Vertheilung auf die m Intervalle vollständig übereinstimmen, in der Art, dass je zwei Werthe w', w'' , welche eine und dieselbe Function w in diesen beiden Systemen annimmt, auch einem und demselben Intervall angehören. Wird nun das System der r Werthe w' durch die Coordinaten h'_i , ferner das System der r Werthe w'' durch die Coordinaten h''_i hervorgebracht, so entspricht den Coordinaten $h_i = h'_i - h''_i$ ein System von

r Werthen $w = w' - w''$, welche absolut den Werth d nicht übersteigen. Für diese ganzen Coordinaten h_v , welche absolut $\leq k$ sind und nicht sämmtlich verschwinden, wird daher in der *ersten* Reihe

$$M(\omega) \leq d\sqrt{2} < 3ck^{1-\frac{n}{r}}.$$

Ist ferner P das Product aus den r Werthen ω der ersten Reihe, und $N(\omega) = PQ$, so ergibt sich $M(P) < (3c)^r k^{r-n}$, $M(Q) \leq (ck)^{n-r}$, mithin absolut

$$N(\omega) < (3c)^n.$$

Da endlich $N(\omega)$ eine von Null verschiedene ganze rationale Zahl ist, so wird $M(PQ) = M(P)M(Q) \geq 1$, also $M(Q) > (3c)^{-r} k^{n-r}$; ist nun ω eine der $(n-r)$ Functionen der zweiten Reihe, und $Q = \omega\theta$, so ist $M(\theta) \leq (ck)^{n-r-1}$, und folglich wird in der *zweiten* Reihe

$$M(\omega) > (3c)^{1-n} k.$$

Offenbar kann nun, wie klein auch a , und wie gross auch b sein mag, k stets so gross gewählt werden, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$ ausfällt, während $N(\omega)$ absolut $< (3c)^n$ wird; was zu beweisen war.

4. Aus dem soeben bewiesenen Satze ergibt sich, indem man dieselbe Eintheilung in zwei Reihen beibehält, dass man eine nie abreissende Kette von aufeinander folgenden, von Null verschiedenen Zahlen ω in \mathfrak{o} aufstellen kann, deren Normen $< (3c)^n$ sind, und welche ausserdem noch die zweite Eigenschaft besitzen, dass $M(\omega)$ in der ersten Reihe kleiner, in der zweiten grösser ausfällt, als die Moduln aller *vorhergehenden* Zahlen ω und der mit ihnen conjugirten Zahlen; denn bezeichnet man mit a den kleinsten, mit b den grössten unter allen Moduln der schon gebildeten Zahlen ω und der mit ihnen conjugirten Zahlen, so giebt es zufolge des bewiesenen Satzes immer noch eine Zahl ω der Art, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$ ausfällt, während $N(\omega)$ absolut genommen ebenfalls $< (3c)^n$ wird; diese neue Zahl ω ist daher auch von Null und von allen vorhergehenden Zahlen ω verschieden. Wir theilen nun die Zahlen ω dieser Kette in Gruppen ein, indem wir zwei von ihnen stets und nur dann in dieselbe Gruppe aufnehmen, wenn sie dieselbe Norm m besitzen, und wenn ausserdem die Coordinaten ihrer Differenz sämmtlich durch m theilbar sind; da nun die hier auftretenden Normen m ganze rationale Zahlen

und absolut $< (3c)^n$ sind, und da die Coordinaten einer Zahl ω hinsichtlich ihrer Reste (mod. m) höchstens $(\pm m)^n$ verschiedene Fälle darbieten können, so kann in dieser Kette von Zahlen ω auch nur eine *endliche* Anzahl verschiedener Gruppen auftreten, und folglich muss bei hinreichender Fortsetzung der nie abbrechenden Kette eine Zahl β in ihr erscheinen, welche mit einer früheren Zahl α in dieselbe Gruppe fällt. Dann ist also $N(\alpha) = N(\beta) = \beta\beta' = m$, und $\alpha = \beta + m\gamma = \beta(1 + \gamma\beta') = \beta\varepsilon$, wo β' (zufolge 1.) und γ , folglich auch $\varepsilon = 1 + \gamma\beta'$ Zahlen in \mathfrak{o} bedeuten; zugleich ergibt sich, da $N(\alpha) = N(\beta) = N(\beta\varepsilon)$ von Null verschieden ist, $N(\varepsilon) = 1$, und aus $M(\alpha) = M(\beta)M(\varepsilon)$ folgt, dass $M(\varepsilon)$ in der ersten Reihe > 1 , in der zweiten < 1 ist. Versteht man unter einer *Einheit* im Folgenden stets eine Zahl in \mathfrak{o} , deren Norm $= +1$ ist, so haben wir daher folgendes Resultat gewonnen:

Es giebt eine Einheit von der Art, dass die Moduln der mit ihr conjugirten Zahlen in der ersten Reihe > 1 , in der zweiten < 1 sind.

5. Multiplicirt man je zwei zusammengehörige imaginäre Functionen $\omega = u \pm vi$ mit einander, so bilden diese $(n - \nu)$ Producte $(u^2 + v^2)$ und die $(2\nu - n)$ reellen Functionen ω ein System von ν reellen, theils quadratischen, theils linearen Functionen $f', f'' \dots f^{(\nu)}$ der Coordinaten; nennt man die *reellen* Bestandtheile ihrer Logarithmen kurz die (conjugirten) *Logarithmen von ω* , so kann man das eben erhaltene Resultat auch so aussprechen:

Theilt man die ν Functionen f nach Belieben in zwei Reihen, doch so, dass jede dieser Reihen wenigstens eine Function enthält, so existirt stets eine Einheit ε , deren Logarithmen $e', e'' \dots e^{(\nu)}$ positiv oder negativ sind, je nachdem sie der ersten oder der zweiten Reihe entsprechen.

Da die Summe der Logarithmen einer Zahl ω gleich dem reellen Bestandtheile des Logarithmen von $N(\omega)$ ist, so ist die Summe der Logarithmen $e', e'' \dots e^{(\nu)}$ einer Einheit ε stets $= 0$; hat man daher ν beliebige Einheiten $\varepsilon_1, \varepsilon_2 \dots \varepsilon_\nu$, so ist die aus den zugehörigen ν^2 Logarithmen gebildete Determinante

$$\Sigma \pm e'_1 e''_2 \dots e^{(\nu)}_\nu = 0;$$

lässt man aber einen dieser Logarithmen, z. B. den letzten $e^{(\nu)}$, welcher der Function $f^{(\nu)}$ entspricht, stets weg, so gilt folgender Fundamentalsatz:

Es gibt immer ein System S von $(\nu - 1)$ unabhängigen, d. h. solchen Einheiten $\varepsilon_1, \varepsilon_2 \dots \varepsilon_{\nu-1}$, dass die aus ihren Logarithmen gebildete Determinante

$$L = \Sigma \pm e'_1 e''_2 \dots e_{\nu-1}^{(\nu-1)}$$

einen positiven, also von Null verschiedenen Werth besitzt.

Ist nämlich $\nu = 2$, so folgt aus dem obigen Satze, wenn man f' in die erste, f'' in die zweite Reihe aufnimmt, die Existenz einer Einheit ε , für welche der Logarithme e' positiv ausfällt (hiermit ist für den nicht ausgeschlossenen Fall $n = 2$ die Theorie der Einheiten im Wesentlichen absolvirt; vergl. §. 142). Ist aber $\nu > 2$ und $m < \nu$, und hat man schon $m - 1$ Einheiten $\varepsilon_1, \varepsilon_2 \dots \varepsilon_{m-1}$ aufgestellt, für welche die Determinante

$$\Sigma \pm e'_1 e''_2 \dots e_{m-1}^{(m-1)}$$

einen positiven Werth $E^{(m)}$ hat, so kann man mit Hülfe desselben Satzes die Existenz einer Einheit ε_m beweisen, für welche auch die Determinante

$$\Sigma \pm e'_1 e''_2 \dots e_{m-1}^{(m-1)} e_m^{(m)}$$

positiv ausfällt; ordnet man dieselbe nach den Logarithmen $e'_m, e''_m \dots e_m^{(m)}$ der neuen Einheit ε_m , so nimmt sie die Form

$$E' e'_m + E'' e''_m + \dots + E^{(m-1)} e_m^{(m-1)} + E^{(m)} e_m^{(m)}$$

an, wo $E^{(m)}$ der Annahme zufolge positiv ist, während die übrigen aus den Logarithmen von $\varepsilon_1, \varepsilon_2 \dots \varepsilon_{m-1}$ gebildeten Determinanten $E', E'' \dots E^{(m-1)}$ positiv, negativ oder auch $= 0$ sein können. Nimmt man nun von den Functionen $f', f'' \dots f^{(m)}$ alle diejenigen in die erste Reihe auf, denen positive Werthe $E', E'' \dots E^{(m)}$ entsprechen, also jedenfalls die Function $f^{(m)}$, während die übrigen und die Functionen $f^{(m+1)} \dots f^{(\nu)}$, also jedenfalls $f^{(\nu)}$ in die zweite Reihe fallen, so existirt zufolge des obigen Satzes eine Einheit ε_m , deren Logarithmen $e'_m, e''_m \dots e_m^{(\nu)}$ positiv oder negativ ausfallen, je nachdem sie der ersten oder zweiten Reihe entsprechen; mithin enthält das obige Aggregat mindestens ein positives Glied $E^{(m)} e_m^{(m)}$, und die übrigen Glieder sind nicht negativ, so dass das Aggregat selbst einen positiven Werth erhält, was zu beweisen war. Auf diese Weise kann man offenbar von $m = 2$ bis $m = \nu - 1$ fortschliessen, und erhält zuletzt das in dem Satze ausgesprochene Resultat.

$m_2 \dots m_{\nu-1}$ der der Gruppe (S) angehörigen Einheit η solche ganze rationale Zahlen sein, dass die Exponenten von ϱ , also die Zahlen $x_1 - m_1, x_2 - m_2 \dots x_{\nu-1} - m_{\nu-1}$ sämmtlich < 1 und nicht negativ werden; dies kann immer und nur dadurch erreicht werden, dass man für $m_1, m_2 \dots m_{\nu-1}$ resp. die grössten in den reellen Werthen $x_1, x_2 \dots x_{\nu-1}$ enthaltenen ganzen rationalen Zahlen wählt (vergl. §§. 43, 44); also ist η und folglich auch ϱ vollständig bestimmt.

Ist r die Anzahl aller von einander verschiedenen reducirten Einheiten ϱ (unter denen sich auch die Zahl 1 befindet), und ε irgend eine Einheit, so ist ε^r eine der Gruppe (S) angehörige Einheit; durchläuft nämlich ϱ alle reducirten Einheiten, so ist jedes der r Producte $\varepsilon\varrho$ von der Form $\sigma\eta$, wo σ eine reducirte Einheit, η eine Einheit aus der Gruppe (S) bedeutet, und σ muss ebenfalls alle r reducirten Einheiten durchlaufen, weil aus $\varepsilon\varrho = \sigma\eta$ und $\varepsilon\varrho' = \sigma\eta'$ auch die Gleichung $\varrho'\eta = \varrho\eta'$ folgen würde, welche, wie oben gezeigt ist, nur dann bestehen kann, wenn $\varrho = \varrho'$ ist; multiplicirt man nun die r Gleichungen von der Form $\varepsilon\varrho = \sigma\eta$, und dividirt durch das Product der r reducirten Einheiten ϱ oder σ , so folgt, dass ε^r ein Product aus r Einheiten der Gruppe (S), mithin selbst eine Einheit dieser Gruppe ist.

Die Exponenten von ε^r sind daher immer ganze rationale Zahlen $m_1, m_2 \dots m_{\nu-1}$, und folglich sind die Exponenten einer jeden Einheit ε stets *rationale* Zahlen mit dem gemeinschaftlichen Nenner r . Sind nun $\delta_1, \delta_2 \dots \delta_{\nu-1}$ beliebige Einheiten, deren Logarithmen mit d bezeichnet werden, so folgt, dass die ihnen entsprechende Determinante

$$= \Sigma \pm d'_1 d'_2 \dots d_{\nu-1}^{(\nu-1)} = \frac{mL}{r^{\nu-1}}$$

ist, wo m die aus den $(\nu - 1)^2$ Exponenten der Einheiten $\delta_1^r, \delta_2^r \dots \delta_{\nu-1}^r$ gebildete Determinante, also eine *ganze rationale Zahl* bedeutet, welche von Null verschieden ist, wenn $\delta_1, \delta_2 \dots \delta_{\nu-1}$ ebenfalls ein System von unabhängigen Einheiten bilden. Hieraus ergibt sich die wichtige Folgerung, dass es unter allen Systemen von $(\nu - 1)$ unabhängigen Einheiten ein solches geben muss, für welches die entsprechende Determinante absolut genommen einen *Minimalwerth* annimmt; denn unter allen hier auftretenden ganzen rationalen, von Null verschiedenen Zahlen m muss es eine absolut kleinste geben. Ein solches System von $(\nu - 1)$ unabhängigen Einheiten soll ein *Fundamentalsystem* heissen.

7. Wir wollen nun annehmen, das obige System S der $(\nu-1)$ unabhängigen Einheiten sei ein solches Fundamentalsystem, also L der eben erwähnte Minimalwerth, so folgt zunächst, dass die Exponenten $x_1, x_2 \dots x_{\nu-1}$ einer jeden in Bezug auf S reducirten Einheit ε sämmtlich $= 0$ sind; wäre nämlich z. B. x_1 von Null verschieden, also positiv und < 1 , so wäre die den $(\nu-1)$ Einheiten $\varepsilon, \varepsilon_2 \dots \varepsilon_{\nu-1}$ entsprechende Determinante

$$\Sigma \pm e' e'' \dots e_{\nu-1}^{(\nu-1)} = L x_1$$

von Null verschieden und absolut kleiner als L , was mit unserer Annahme streitet. Da ferner die Exponenten eines Productes zweier Einheiten durch Addition der entsprechenden Exponenten der beiden Factoren entstehen, so sind die Exponenten eines jeden Productes $\varrho \varrho' = \varrho''$ aus zwei reducirten Einheiten ϱ, ϱ' sämmtlich $= 0$, d. h. ein solches Product ist wieder eine reducirte Einheit. Hieraus folgt unmittelbar, dass die sämmtlichen r reducirten Einheiten ϱ die Wurzeln der Gleichung $\varrho^r = 1$ sind; durchläuft nämlich ϱ' alle reducirten Einheiten, so gilt dasselbe von $\varrho'' = \varrho \varrho'$; multiplicirt man diese r Gleichungen, und dividirt durch das Product aller reducirten Einheiten ϱ' oder ϱ'' , so folgt $\varrho^r = 1$. Da endlich schon (in 6.) gezeigt ist, dass jede Einheit ε von der Form $\varrho \eta$ ist, wo ϱ eine reducirte, und η eine Einheit aus der Gruppe (S) bedeutet, so haben wir hiermit den folgenden grossen Satz von *Dirichlet* bewiesen:

Bezeichnet ν die Gesamtanzahl der reellen und imaginären Paare unter den mit Ω conjugirten Körpern, so giebt es in jeder Ordnung ν immer $(\nu-1)$ Fundamenteinheiten von solcher Beschaffenheit, dass, wenn man dieselben beliebig oft in einander multiplicirt und dividirt und dem so gebildeten allgemeinen Product gewisse besondere Einheiten ϱ in endlicher Anzahl einzeln als Factor zugesellt, alle Einheiten dieser Ordnung und zwar jede nur einmal dargestellt werden; ist r die Anzahl dieser besonderen Einheiten ϱ , so sind sie die Wurzeln der Gleichung $\varrho^r = 1$.

§. 167.

Der eben bewiesene Satz bildet neben der Theorie der Ideale (§. 163) die wichtigste Grundlage für das tiefere Studium der ganzen Zahlen des Körpers Ω , und er ist unentbehrlich für die wirkliche Bestimmung der Anzahl der Idealclassen nach Dirichlet'schen Principien. Diese geschieht dadurch, dass der Grenzwert der über alle Ideale α ausgedehnten Summe

$$\sum \frac{s-1}{N(\alpha)^s}$$

für unendlich kleine positive Werthe von $(s-1)$ auf doppelte Weise ermittelt wird. Einmal muss das System aller Idealnomen $N(\alpha)$ genau defnirt werden, d. h. es muss von jeder positiven ganzen rationalen Zahl m festgestellt werden, wie gross die Anzahl $\tau(m)$ der verschiedenen Ideale α ist, deren Norm $= m$; die Beantwortung dieser Frage fällt der Theorie der Ideale zu. Die Summe nimmt dann die Form

$$(s-1) \sum \frac{\tau(m)}{m^s}$$

an, wo m alle positiven ganzen rationalen Zahlen durchlaufen muss*).

Das andere Mal theilt man die obige Summe in Partialsummen ein, deren jede alle die Glieder enthält, welche den sämtlichen Idealen α einer und derselben Classe entsprechen, und es sind bei

*) Hierbei zeigt sich, dass $\tau(mm') = \tau(m)\tau(m')$ ist, wenn m, m' relative Primzahlen sind; mithin ist $\tau(m)$ vollständig bekannt, wenn für jede rationale Primzahl p die Zerlegung von $i(p)$ in Primideale bekannt ist; die Primzahlen p zerfallen hiernach in eine endliche Anzahl verschiedener Arten, in der Weise, dass für alle Primzahlen p gleicher Art die Bestimmung von $\tau(p^e)$ nach derselben Regel geschieht. Die obige Summe lässt sich daher gewissen Umformungen unterwerfen, welche für *alle* Körper gültig sind; am einfachsten gestalten sich dieselben für Galois'sche Körper.

wo ω alle reducirten ganzen Zahlen durchlaufen muss, d. h. alle ganzen Zahlen $\omega = \sum h_i \omega_i$ von positiver Norm H , deren Exponenten den Bedingungen

$$0 \leq x_1 < 1, \quad 0 \leq x_2 < 1 \dots 0 \leq x_{\nu-1} < 1$$

genügen.

Zur Bestimmung des Grenzwertes g dieser Partialsumme für unendlich kleine positive Werthe von $(s-1)$ dienen nun die von *Dirichlet* aufgestellten Principien. Bedeutet t eine über alle Grenzen wachsende positive Grösse, T die Anzahl der hier auftretenden Normen H , welche nicht grösser als t sind, und nähert sich der Quotient $T:t$ einem endlichen Grenzwert k , so ist (§. 118)

$$g = \frac{k}{r}.$$

Um ferner den Grenzwert k des Quotienten $T:t$ zu ermitteln, muss der von *Dirichlet* benutzte geometrische Satz (§. 120) zu dem folgenden Princip erhoben werden, welches seinen unmittelbaren Grund in dem Begriff eines vielfachen bestimmten Integrals findet: Durchlaufen die n stetigen, reellen Variablen h_i ein endliches Gebiet G von n Dimensionen, und bedeutet T' , wenn δ eine beliebig kleine positive Grösse ist, die Anzahl derjenigen dem Gebiete G angehörigen Werthsysteme der Variablen h_i , für welche die n Quotienten $h_i : \delta$ ganze rationale Zahlen werden, so wird für unendlich kleine Werthe von δ

$$\lim (T' \delta^n) = \int dh_1 dh_2 \dots dh_n,$$

wo das n -fache Integral über das Gebiet G auszudehnen ist. Definiert man nun das Gebiet G durch die obigen Bedingungen für die Exponenten $x_1, x_2 \dots x_{\nu-1}$ von $\omega = \sum h_i \omega_i$ und durch die Bedingung

$$0 < H \leq 1,$$

und bedenkt, dass die Exponenten von ω nur von den *Verhältnissen* der Variablen h_i abhängen, während H eine homogene Function n ten Grades ist, so leuchtet unmittelbar ein, dass T' durchaus identisch mit T ist, sobald

$$\delta = \frac{1}{\sqrt[n]{t}}$$

genommen wird; denn wenn die ganzen rationalen Zahlen h_i durch $h_i \sqrt[n]{t} = h_i : \delta$ ersetzt werden, so geht die durch T reducirte ganze

Zahlen ω erfüllte Bedingung $0 < H \leq t$ in $0 < H \leq 1$ über, während die Bedingungen für die Exponenten ungeändert bleiben. Da zugleich $T' \delta^n = T : t$ ist, so ergibt sich also, dass der Grenzwert der auf die Hauptklasse E bezüglichen Partialsumme

$$g = \frac{1}{r} \int dh_1 dh_2 \dots dh_n$$

ist.

Um den Werth dieses Integrals zu erhalten, führe man als neue unabhängige Variable $H, x_1, x_2 \dots x_{\nu-1}$ und die zwischen den Grenzen 0 und 2π liegenden Winkel $\varphi_1, \varphi_2 \dots \varphi_{n-\nu}$ ein, welche den $(n - \nu)$ mit ω conjugirten imaginären Paaren $u \pm vi$ in der Weise entsprechen, dass

$$u + vi = \sqrt{f} \cdot e^{\varphi i}, \quad f = u^2 + v^2$$

wird. Jedem System der ursprünglichen Variablen h_i entspricht ein und nur ein System der neuen Variablen; umgekehrt aber entsprechen jedem System der neuen Variablen, wenn H positiv genommen wird, $2^{2\nu-n-1}$ verschiedene Systeme der alten Variablen h_i ; denn durch die Werthe von $H, x_1, x_2 \dots x_{\nu-1}$ werden nur die absoluten Werthe der $(2\nu - n)$ reellen mit ω conjugirten Functionen bestimmt, und da ihr Product positiv sein muss, so kann man ihnen, mit Ausnahme einer, sowohl das positive wie das negative Vorzeichen geben; nur in dem Falle $n = 2\nu$, wenn gar kein reeller Körper mit Ω conjugirt ist, muss diese Anzahl $2^{2\nu-n-1}$ wieder durch 1 ersetzt werden. Geht man ferner von den ursprünglichen Variablen h_i successive zu den mit ω conjugirten oder den n Functionen w , von diesen zu $f', f'' \dots f^{(\nu)}$, $\varphi_1, \varphi_2 \dots \varphi_{n-\nu}$, von diesen zu den neuen Variablen über, so findet man leicht, dass die entsprechende Functional-Determinante gleich

$$\frac{L}{i^{\nu-n} \sqrt{\Delta(\Omega)}} = \frac{\sum \pm e_1' e_2'' \dots e_{\nu-1}^{(\nu-1)}}{i^{\nu-n} \sqrt{\Delta(\Omega)}}$$

ist; mithin ist der auf die Hauptklasse E bezügliche Grenzwert g gleich

$$\frac{2^{\nu-1} \pi^{n-\nu} L}{r i^{\nu-n} \sqrt{\Delta(\Omega)'}}$$

oder doppelt so gross, falls $n = 2\nu$ ist (wenn zugleich $n = 2$ ist, so ist $L = 1$ zu setzen, und r bedeutet die Anzahl aller Einheiten).

An dieses Resultat knüpfen wir zunächst folgende Bemerkung. Nimmt man in die erste Partialsumme nicht alle Ideale der Haupt-

klasse E , sondern nur diejenigen Ideale e auf, welche zugleich durch ein bestimmtes Ideal m theilbar sind, so treten an die Stelle der Basiszahlen $\omega_1, \omega_2 \dots \omega_n$ von \mathfrak{o} die Basiszahlen $\mu_1, \mu_2 \dots \mu_n$ dieses Ideals m , während alles Uebrige unverändert bleibt; mithin ist $\Delta(\Omega)$ durch

$$\Delta(\mu_1, \mu_2 \dots \mu_n) = N(m)^2 \Delta(\Omega)$$

zu ersetzen, und der Grenzwert dieser auf alle Ideale e bezüglichen Summe ist $= g : N(m)$.

Durchläuft nun \mathfrak{a} alle Ideale einer beliebigen Classe A , so giebt es ein Ideal m der Art, dass alle Producte $\mathfrak{a}m$ Ideale der Hauptklasse E werden, und da umgekehrt, wenn e ein durch m theilbares Ideal $\mathfrak{a}m$ der Hauptklasse E ist, \mathfrak{a} gewiss der Classe A angehört, so ist

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

und folglich

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

d. h. jede auf eine bestimmte Idealclasse bezügliche Partialsumme nähert sich demselben Grenzwert g . Bezeichnet man daher mit $h(\Omega)$ die Anzahl aller dieser Idealclassen, so ist der Grenzwert der Totalsumme gleich $gh(\Omega)$, und folglich ist

$$h(\Omega) = \frac{r^{\nu-n} \sqrt{\Delta(\Omega)}}{2^{\nu-1} \pi^{n-\nu} L} \lim \sum \frac{(s-1)\tau(m)}{m^s}$$

oder halb so gross, wenn $n = 2\nu$ ist. Die Bestimmung der Classenzahl ist hiermit auf die von der Theorie der Ideale zu leistende Bestimmung der Function $\tau(m)$ zurückgeführt*).

*) Für die aus der Kreistheilung entspringenden Körper führt dieselbe, wie *Kummer* gezeigt hat, zu den Reihen, welche in dem Dirichlet'schen Beweise des Satzes über die arithmetische Progression (Supplement VI) auftreten; vergl. die Anm. zu §. 163, 3.

§. 168.

Wir wollen nun zum Schlusse die vorhergehenden allgemeinen Untersuchungen auf die quadratischen Körper anwenden, um von dem gewonnenen Standpunct aus den Hauptgegenstand dieses Werkes noch einmal zu überblicken.

Ist die ganze rationale Zahl D keine Quadratzahl und auch durch kein Quadrat (ausser 1) theilbar, so bilden die Zahlen $t + u\sqrt{D}$, wenn t, u alle rationalen Zahlen durchlaufen, einen quadratischen Körper, welcher durch die beiden Substitutionen $\varphi(t + u\sqrt{D}) = t \pm u\sqrt{D}$ in sich selbst übergeht. Setzt man $\theta = \frac{1}{2}(1 + \sqrt{D})$ oder $= \sqrt{D}$, je nachdem $D \equiv 1 \pmod{4}$ ist oder nicht, so bilden die Zahlen $1, \theta$ eine Grundreihe des Körpers, und seine Grundzahl Δ ist entsprechend $= D$ oder $= 4D$. Die quadratische Gleichung, welcher θ genügt, sei

$$f(\theta) = \theta^2 - b\theta + c = 0,$$

so ist $x + y\theta$ mit $x + y(b - \theta)$ conjugirt, und

$$\Delta = (2\theta - b)^2 = b^2 - 4c.$$

Ist nun \mathfrak{p} irgend ein Primideal des Körpers, und p die durch \mathfrak{p} theilbare positive rationale Primzahl, so ist $N(\mathfrak{p}) = p^2$ oder $= p$, je nachdem $i(\mathfrak{p}) = \mathfrak{p}$ oder ein Product aus zwei Primidealen $\mathfrak{p}, \mathfrak{p}'$ ist. Im letzteren Falle bilden die Zahlen $0, 1, 2 \dots (p - 1)$, weil sie incongruent sind, ein vollständiges Restsystem $(\text{mod. } \mathfrak{p})$, d. h. jede ganze Zahl des Körpers ist einer rationalen ganzen Zahl congruent; mithin giebt es auch eine rationale ganze Zahl t , welcher θ congruent ist, und folglich ist $f(t) = t^2 - bt + c$ eine ganze rationale durch \mathfrak{p} , also auch durch p theilbare Zahl, d. h.

$$t^2 - bt + c \equiv 0 \pmod{p},$$

oder in der Sprache der Theorie der höheren Congruenzen: die quadratische Function $f(x) = x^2 - bx + c$ ist nach dem Modul p congruent einem Producte aus zwei Functionen ersten Grades $(x - t)$ und $(x - b + t)$ mit rationalen Coefficienten. Umgekehrt: hat die Congruenz $f(x) \equiv 0 \pmod{p}$ eine rationale Wurzel $x \equiv t$, so ist

$$f(t) = (t - \theta)(t - b + \theta) \equiv 0 \pmod{p};$$

wäre nun $i(p)$ ein Primideal, so müsste wenigstens einer der Factoren $(t - \theta)$, $(t - b + \theta)$ durch p theilbar sein, was aber nicht der Fall ist, weil die Zahlen 1, θ eine *Grundreihe* des Körpers bilden; mithin ist $i(p) = pp'$ ein Product aus zwei Primidealen p und p' , deren Normen $= p$ sind; ist nun $t - \theta$ durch p theilbar, also $i(t - \theta) = pq$, so ist q nicht theilbar durch p' , weil sonst $(t - \theta)$ durch p theilbar wäre, und da $i(t - \theta)i(t - b + \theta) = pqi(t - b + \theta)$ durch $i(p) = pp'$ theilbar ist, so muss $(t - b + \theta)$ durch p' theilbar sein; man kann daher

$$\theta \equiv t \pmod{p}, \quad \theta \equiv b - t \pmod{p'}$$

setzen, und p, p' *conjugirte* Primideale nennen, weil aus $x + y\theta \equiv 0 \pmod{p}$ stets $x + y(b - \theta) \equiv 0 \pmod{p'}$ folgt.

Es fragt sich nun, ob diese beiden Primideale p, p' identisch sein können. Dann muss $\theta \equiv t \equiv b - t \pmod{p}$, also $2t - b$ durch p und folglich auch durch p theilbar sein, und da $4f(t) = (2t - b)^2 - \mathcal{A} \equiv 0 \pmod{p}$ ist, so muss

$$\mathcal{A} \equiv 0 \pmod{p}$$

sein. Umgekehrt: ist p eine in der Grundzahl $\mathcal{A} = b^2 - 4c$ aufgehende rationale Primzahl, so giebt es immer eine ganze rationale t , welche den beiden Congruenzen

$$f(t) \equiv 0, \quad 2t \equiv b \pmod{p}$$

genügt; ist nämlich p ungerade, so ist t durch die zweite Congruenz bestimmt, und aus $4f(t) = (2t - b)^2 - \mathcal{A}$ folgt $f(t) \equiv 0$; ist aber $p = 2$, also b gerade, so ist t durch die erste Congruenz $f(t) \equiv t^2 + c \equiv 0 \pmod{2}$ bestimmt, nämlich $t \equiv c \pmod{2}$, und die zweite Congruenz ist ebenfalls erfüllt. Aus der Existenz einer rationalen Wurzel t der Congruenz $f(t) \equiv 0$ folgt aber, wie oben gezeigt ist, $i(p) = pp'$, wo p und p' zwei Primideale bedeuten, für welche $\theta \equiv t \pmod{p}$, $\theta \equiv b - t \pmod{p'}$ ist; da nun ausserdem $t \equiv b - t \pmod{p}$ ist, so folgt, dass $(\theta - t)$ sowohl durch p als auch durch p' theilbar ist; wären nun p und p' verschieden, also relative Primideale, so müsste $(\theta - t)$ auch durch pp' , d. h. durch p theilbar sein; da dies nicht der Fall ist, so sind p und p' identisch, also ist $i(p) = p^2$. Wir sind mithin zu folgendem Resultat gelangt:

Geht die rationale Primzahl p in der Grundzahl \mathcal{A} auf, so ist $i(p) = p^2$ das Quadrat eines Primideals p ; ist p eine in \mathcal{A} nicht aufgehende Primzahl, so ist $i(p) = pp'$ ein Product aus zwei

verschiedenen Primidealen p, p' , oder $i(p)$ ein Primideal, je nachdem die Congruenz $f(t) \equiv 0 \pmod{p}$ eine rationale Wurzel t besitzt oder nicht.

Die Zahl $p = 2$ bietet den ersten Fall dar, wenn $\Delta \equiv 0 \pmod{4}$, also $D \equiv 2, 3 \pmod{4}$ ist; ist dagegen $\Delta = D \equiv 1 \pmod{4}$, so tritt der zweite oder dritte Fall ein, je nachdem c gerade oder ungerade, d. h. je nachdem $D \equiv 1$ oder $\equiv 5 \pmod{8}$ ist. Hieraus erklärt sich das eigenthümliche Verhalten der Zahl 2 in der Theorie der quadratischen Reste (§. 36).

Ist p eine ungerade, in Δ nicht aufgehende rationale Primzahl, so folgt aus $4f(t) = (2t - b)^2 - \Delta$, dass der zweite oder dritte Fall eintritt, je nachdem

$$\left(\frac{\Delta}{p}\right) = \left(\frac{D}{p}\right) = +1 \quad \text{oder} \quad -1$$

ist. Um alle Fälle am bequemsten zusammenzufassen, führen wir für jede positive ganze rationale Zahl m eine Charakteristik (Δ, m) der Art ein, dass

$$(\Delta, mm') = (\Delta, m) (\Delta, m')$$

und, wenn p eine rationale Primzahl bedeutet,

$$(\Delta, p) = 0, \quad = +1, \quad = -1$$

ist, je nachdem $i(p)$ Quadrat eines Primideals, oder ein Product aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist. Bedeutet nun $\tau(m)$ die Anzahl aller verschiedenen Ideale \mathfrak{a} , deren Normen $= m$ sind, so ist

$$\tau(p^r) = (\Delta, 1) + (\Delta, p) + (\Delta, p^2) + \dots + (\Delta, p^r),$$

und allgemein

$$\tau(m) = \sum (\Delta, n),$$

wo n alle Divisoren von m durchläuft. Hieraus folgt (vergl. §§. 89, 91, 124)

$$\sum \frac{\tau(m)}{m^s} = \sum \frac{1}{m^s} \sum \frac{(\Delta, m)}{m^s},$$

also, wenn $(s - 1)$ positiv unendlich klein wird,

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

wo m nur alle diejenigen positiven ganzen rationalen Zahlen zu durchlaufen braucht, welche relative Primzahlen zu Δ sind, oder auch

$$\lim \sum \frac{s-1}{N(\alpha)^s} = \frac{1}{1 - \frac{(D, 2)}{2}} \cdot \lim \sum \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo n alle relativen Primzahlen zu $2D$ durchläuft. Substituirt man dies in den allgemeinen Ausdruck des vorigen Paragraphen für die Anzahl der Idealclassen, so findet man, dass dieselbe vollständig übereinstimmt mit der Classenzahl der (positiven) ursprünglichen Formen der Determinante D , und zwar der zweiten Art, wenn $D \equiv 1 \pmod{4}$ ist; der Grund für diese Uebereinstimmung liegt, wie man leicht erkennt, darin, dass jede Formenklasse nur einer einzigen Idealclass entspricht (vergl. §. 165, 2.).

§. 169.

Sind α, β zwei von einander unabhängige ganze Zahlen eines quadratischen Körpers Ω , und durchlaufen die Variablen x, y alle ganzen rationalen Zahlen, so bilden die Zahlen

$$\mu = x\alpha + y\beta \quad (1)$$

einen aus lauter ganzen Zahlen bestehenden Modul m (§. 161); umgekehrt, wenn ein Modul m aus ganzen Zahlen μ des Körpers Ω besteht und zwei von einander unabhängige Zahlen enthält, so sind alle Zahlen μ von der Form (1), wo α, β zwei particuläre Zahlen des Moduls bedeuten; bilden die Zahlen ω_1, ω_2 eine bestimmte Grundreihe des Körpers Ω , so kann man die Basiszahlen

$$\alpha = p_1\omega_1 + p_2\omega_2, \quad \beta = q_1\omega_1 + q_2\omega_2$$

immer so wählen, dass $(p_1q_2 - q_1p_2)$ positiv ausfällt, und dann mag α die erste, β die zweite Basiszahl des Moduls m heissen. Nun wird

$$N(\mu) = m(ax^2 + bxy + cy^2), \quad (2)$$

wo m den Theiler der quadratischen Form $N(\mu)$, also eine positive ganze rationale Zahl bedeutet, während a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Theiler sind. Setzt man

$$b^2 - 4ac = d, \quad (3)$$

und bezeichnet mit α_1, β_1 die resp. mit α, β conjugirten Zahlen, so ist

$$\alpha\alpha_1 = ma, \quad \alpha\beta_1 + \beta\alpha_1 = mb, \quad \beta\beta_1 = mc,$$

folglich die Discriminante

$$\Delta(\alpha, \beta) = dm^2. \quad (4)$$

Wählt man statt α, β irgend eine andere Basis desselben Moduls m , so leuchtet ein, dass die Zahlen m und d unverändert bleiben, und dass die entsprechenden ursprünglichen Formen $ax^2 + bxy + cy^2$ eine Formenklasse bilden; die Zahlen m und d können füglich die *Norm* und *Determinante des Moduls* m genannt werden. Ersetzt man die Variabeln x und y resp. durch β und $-\alpha$, so ergibt sich

$$a\beta^2 - b\alpha\beta + c\alpha^2 = 0, \quad b\beta - 2c\alpha = \beta Vd. \quad (5)$$

Ist ausserdem

$$g = h\alpha + k\beta$$

die kleinste positive ganze rationale Zahl des Moduls m , so sind h, k relative Primzahlen, und wenn man

$$ah^2 + bhk + ck^2 = e$$

setzt, so ergibt sich $N(g) = g^2 = me$; mithin ist e positiv und geht in g^2 auf. Da α, β ganze Zahlen sind, so findet man ferner leicht, dass dg^2 durch e^2 theilbar sein muss; bedeutet daher f^2 das grösste in d und e aufgehende Quadrat, so muss fg durch e theilbar sein. Soll ferner m ein Ideal im weiteren Sinne des Wortes sein (§. 165, 4.), sollen also $\alpha^2, \alpha\beta, \beta^2$ ebenfalls in m enthalten sein, so muss g durch e theilbar sein; doch werden wir im Folgenden von dieser Voraussetzung absehen.

Suchen wir nun die *Ordnung* n des Moduls m , d. h. das System aller Zahlen ν von der Art, dass jedes Product $\mu\nu$ in m enthalten ist (§. 165, 4.), so ist erforderlich und hinreichend, dass

$$\alpha\nu = x\alpha + y\beta, \quad \beta\nu = x'\alpha + y'\beta$$

wird, wo x, y, x', y' ganze rationale Zahlen bedeuten; hieraus folgt durch Elimination von ν

$$y\beta^2 - (y' - x)\alpha\beta - x'\alpha^2 = 0,$$

und hieraus durch Vergleichung mit (5)

$$y = az, \quad y' - x = bz, \quad -x' = cz,$$

wo z eine ganze rationale Zahl sein muss, weil a, b, c keinen gemeinschaftlichen Theiler haben. Mithin wird

$$\nu = x + \frac{\alpha\beta}{\alpha} z,$$

wo x und z willkürliche ganze rationale Zahlen bedeuten. Da aus (5)

$$N(v) = x^2 + bxz + acz^2$$

folgt, so sind die Norm und Determinante von n resp. $= 1$ und d .

Bezeichnet man ganz allgemein die Anzahl der in einem Modul b enthaltenen Zahlen, welche in Bezug auf einen Modul a incongruent sind, mit (b, a) , so ergibt sich aus

$$g = h\alpha + k\beta$$

$$g \frac{\alpha\beta}{\alpha} = -ck\alpha + (ah + bk)\beta$$

nach leicht zu beweisenden allgemeinen Sätzen*)

$$(n, m) = \frac{g^2}{u}, \quad (m, n) = \frac{e}{u}, \quad (n, m) = m(m, n),$$

wo u den grössten gemeinschaftlichen Divisor von g und e bedeutet. Ist m ein Ideal, also ein Vielfaches von n , so ist $(m, n) = 1$, $(n, m) = m$.

§. 170.

Sind m, m' zwei Moduln von der eben betrachteten Beschaffenheit, deren Zahlen μ, μ' demselben quadratischen Körper Ω angehören, so bilden alle Producte $\mu\mu'$ und deren Summen wieder einen solchen Modul $m'' = mm'$. Uebertragen wir die vorhergehenden Bezeichnungen durch Accentuation von m auf m' und m'' , so müssen *erstens*, weil alle Producte $\mu\mu'$ in m'' enthalten sind, acht ganze rationale Zahlen $p, q \dots p''', q'''$ existiren, welche den Gleichungen

$$\begin{aligned} \alpha\alpha' &= p\alpha'' + q\beta'' \\ \alpha\beta' &= p'\alpha'' + q'\beta'' \\ \beta\alpha' &= p''\alpha'' + q''\beta'' \\ \beta\beta' &= p'''\alpha'' + q'''\beta'' \end{aligned} \tag{1}$$

*) Vergl. §. 161. Anm. — Ich erwähne hier nur noch Folgendes. Nennt man zwei Moduln a, b verwandt, wenn (a, b) und (b, a) endlich sind, so sind zwei mit a verwandte Moduln b, c auch mit einander verwandt, und es ist

$$(a, b) (b, c) (c, a) = (b, a) (c, b) (a, c),$$

wovon man sich leicht durch die Betrachtung der kleinsten gemeinschaftlichen Vielfachen und grössten gemeinschaftlichen Theiler überzeugt.

genügen. Setzen wir zur Abkürzung*) die aus ihnen gebildeten partialen Determinanten

$$\begin{aligned} pq' - qp' &= P, & pq'' - qp'' &= Q, & pq''' - qp''' &= R, \\ p''q''' - q''p''' &= U, & p'q''' - q'p''' &= T, & p'q'' - q'p'' &= S, \end{aligned} \quad (2)$$

so ist

$$RS = QT - PU, \quad (3)$$

und durch Elimination von α'' , β'' aus je drei der Gleichungen (1) erhält man

$$\begin{aligned} * \quad U\alpha\beta' - T\beta\alpha' + S\beta\beta' &= 0 \\ -U\alpha\alpha' \quad * + R\beta\alpha' - Q\beta\beta' &= 0 \\ T\alpha\alpha' - R\alpha\beta' \quad * + P\beta\beta' &= 0 \\ -S\alpha\alpha' + Q\alpha\beta' - P\beta\alpha' \quad * &= 0. \end{aligned} \quad (4)$$

Eliminirt man T aus der ersten und dritten, ferner U aus der ersten und zweiten dieser Gleichungen, so erhält man

$$\begin{aligned} P\beta^2 - (R - S)\alpha\beta + U\alpha^2 &= 0, \\ Q\beta'^2 - (R + S)\alpha'\beta' + T\alpha'^2 &= 0, \end{aligned}$$

und folglich muss (zufolge (5) in §. 169)

$$\begin{aligned} P &= an', & R - S &= bn', & U &= cn', \\ Q &= a'n, & R + S &= b'n, & T &= c'n \end{aligned} \quad (5)$$

sein, wo n , n' ganze rationale, von Null verschiedene Zahlen bedeuten (denn n' muss eine ganze Zahl sein, weil a , b , c keinen gemeinschaftlichen Theiler haben, und wäre $n' = 0$, also auch $P = 0$, so wären α' , β' zufolge (1) nicht unabhängig von einander); hierdurch nimmt die erste der Gleichungen (4) die Form

$$(b\beta - 2c\alpha)\beta'n' = (b'\beta' - 2c'\alpha')\beta n$$

an, mithin ist (zufolge (5) in §. 169)

$$n'\sqrt{d} = n\sqrt{d'}, \quad (6)$$

und hiermit sind die vier Gleichungen (4) vollständig befriedigt. Das Product dd' ist, wie zu erwarten war, eine Quadratzahl.

Da zweitens alle Zahlen μ'' des Moduls m'' durch Addition von Producten $\mu\mu'$ entstehen, so existiren acht ganze rationale Zahlen u , v . . . u''' , v''' , welche den Bedingungen

*) Die Bezeichnungen schliessen sich an die an, welche Gauss in den artt. 235, 236 der *Disquisitiones Arithmeticae* gewählt hat; die nothwendigen Modificationen sind leicht zu erkennen.

$$\begin{aligned}\alpha'' &= u\alpha\alpha' + u'\alpha\beta' + u''\beta\alpha' + u'''\beta\beta' \\ \beta'' &= v\alpha\alpha' + v'\alpha\beta' + v''\beta\alpha' + v'''\beta\beta'\end{aligned}\quad (7)$$

genügen. Substituirt man hierin die Gleichungen (1), und berücksichtigt, dass die Zahlen α'' , β'' von einander unabhängig sind, so folgt

$$\begin{aligned}pu + p'u' + p''u'' + p'''u''' &= 1 \\ qu + q'u' + q''u'' + q'''u''' &= 0\end{aligned}\quad (8)$$

und

$$\begin{aligned}pv + p'v' + p''v'' + p'''v''' &= 0 \\ qv + q'v' + q''v'' + q'''v''' &= 1.\end{aligned}\quad (9)$$

Bildet man die Determinante aus diesen vier Summen, so erhält man eine Gleichung von der Form

$$PP_1 + QQ_1 + RR_1 + SS_1 + TT_1 + UU_1 = 1, \quad (10)$$

wo die Determinanten $P_1 \dots U_1$ auf dieselbe Weise aus den Zahlen $u, v \dots u''', v'''$ gebildet sind, wie $P \dots U$ aus $p, q \dots p''', q'''$, und hieraus folgt, dass die sechs Zahlen (2) keinen gemeinschaftlichen Theiler haben. Dasselbe Resultat erhält man auch auf folgendem Wege; eliminirt man jede der vier Zahlen u, u', u'', u''' aus den beiden Gleichungen (8), so folgt

$$\begin{aligned}q &= * - Pu' - Qu'' - Ru''' \\ q' &= Pu \quad * - Su'' - Tu''' \\ q'' &= Qu + Su' \quad * - Uu''' \\ q''' &= Ru + Tu' + Uu'' \quad *\end{aligned}\quad (11)$$

ebenso erhält man aus (9) die Gleichungen

$$\begin{aligned}p &= * \quad Pv' + Qv'' + Rv''' \\ p' &= -Pv \quad * + Sv'' + Tv''' \\ p'' &= -Qv - Sv' \quad * + Uv''' \\ p''' &= -Rv - Tv' - Uv'' \quad *\end{aligned}\quad (12)$$

Aus (11) folgt, dass jeder gemeinschaftliche Theiler der sechs Determinanten (2) in den vier Zahlen q, q', q'', q''' , mithin zufolge (9) auch in der Zahl 1 aufgeht, was zu beweisen war. Hieraus ergiebt sich leicht mit Rücksicht auf (3), dass auch die sechs Zahlen (5) keinen gemeinschaftlichen Theiler haben; geht nämlich e in $P, Q, R - S, R + S, T, U$ auf, so sind die Zahlen $2R, 2S$ ebenfalls theilbar durch e , und die Quotienten $2R:e$ und $2S:e$ sind ent-

weder beide gerade oder beide ungerade, weil ihre Summe gerade ist; wären sie nun beide ungerade, so wäre auch ihr Product $4RS:e^2$ ungerade, was gegen die Gleichung (3) streitet, der zufolge RS durch e^2 theilbar ist; mithin sind R und S durch e theilbar, und folglich ist $e = \pm 1$. Es ergibt sich daher, dass n und n' *relative Primzahlen* sind.

Durch Elimination der vier Zahlen $\alpha, \beta, \alpha', \beta'$ aus den Gleichungen (1) erhält man

$$(p'\alpha'' + q'\beta'')(p''\alpha'' + q''\beta'') = (p\alpha'' + q\beta'')(p'''\alpha'' + q'''\beta'')$$

oder

$$L\beta''^2 - M\alpha''\beta'' + N\alpha''^2 = 0, \quad (13)$$

wenn man zur Abkürzung

$$\begin{aligned} q'q'' - qq''' &= L, & p'p'' - pp''' &= N, \\ pq''' + qp''' - p'q'' - q'p'' &= M \end{aligned} \quad (14)$$

setzt. Wir zeigen zunächst, dass diese drei Zahlen durch nn' theilbar sind; da nämlich zufolge (5)

$$Q \equiv 0, \quad S \equiv -R, \quad T \equiv 0 \pmod{n}$$

ist, so ergibt sich aus (11) und (12) in Bezug auf denselben Modul

$$\begin{aligned} q &\equiv -Pu' - Ru'', & p &\equiv Pv' + Rv''' \\ q' &\equiv Pu + Ru'', & p' &\equiv -Pv - Rv'' \\ q'' &\equiv -Ru' - Uu''', & p'' &\equiv Rv' + Uv'' \\ q''' &\equiv Ru + Uu'', & p''' &\equiv -Rv - Uv'' \end{aligned}$$

und hieraus

$$\begin{aligned} L &\equiv (PU - R^2)(u'u'' - uu'''), & N &\equiv (PU - R^2)(v'v'' - vv'''), \\ M &\equiv (PU - R^2)(u'v'' + v'u'' - uv''' - vu'''); \end{aligned}$$

nun ist aber zufolge (3) $PU \equiv R^2 \pmod{n}$, folglich sind L, M, N theilbar durch n ; da ferner auf dieselbe Weise sich zeigen lässt, dass sie auch durch n' theilbar sind, so müssen sie, weil n, n' relative Primzahlen sind, auch durch nn' theilbar sein; was zu beweisen war.

Führt man endlich die unabhängigen Variablen x, y, x', y' und die bilinearen Functionen

$$\begin{aligned} x'' &= pxx' + p'xy' + p''yx' + p'''yy' \\ y'' &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned} \quad (15)$$

ein, so ergibt sich durch Elimination von xx', xy', yx', yy'

$$\begin{aligned}
 py'' - qx'' &= * Pxy' + Qyx' + Ryy' \\
 p'y'' - q'x'' &= -Pxx' * + Syx' + Tyy' \\
 p''y'' - q''x'' &= -Qxx' - Sxy' * + Uyy' \\
 p'''y'' - q'''x'' &= -Rxx' - Txy' - Uyx' *
 \end{aligned}$$

und hieraus folgt

$$\begin{aligned}
 (p'y'' - q'x'')(p''y'' - q''x'') - (py'' - qx'')(p'''y'' - q'''x'') & \quad (16) \\
 = (Px^2 + (R - S)xy + Uy^2)(Qx'^2 + (R + S)x'y' + Ty'^2),
 \end{aligned}$$

d. h.

$$\begin{aligned}
 Lx''^2 + Mx''y'' + Ny''^2 & \quad (17) \\
 = nn'(ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2).
 \end{aligned}$$

Da diese Gleichung eine Identität in Bezug auf die Variablen x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, so muss, wenn enn' den grössten gemeinschaftlichen Divisor von L, M, N bedeutet, e in allen neun Producten $aa', ab' \dots cc'$ aufgehen; diese letzteren haben aber keinen gemeinschaftlichen Theiler, weil dasselbe sowohl von den Zahlen a, b, c , wie von den Zahlen a', b', c' gilt; mithin ist $e = 1$, also nn' der grösste gemeinschaftliche Theiler von L, M, N . Nun ist ferner in Folge der bilinearen Substitution (15)

$$x''\alpha'' + y''\beta'' = (x\alpha + y\beta)(x'\alpha' + y'\beta'),$$

folglich auch

$$N(x''\alpha'' + y''\beta'') = N(x\alpha + y\beta)N(x'\alpha' + y'\beta'),$$

also

$$\begin{aligned}
 m''(a''x''^2 + b''x''y'' + c''y''^2) &= \\
 mm'(ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2);
 \end{aligned}$$

mithin ergibt sich durch Vergleichung mit (17)

$$nn'm''(a''x''^2 + b''x''y'' + c''y''^2) = mm'(Lx''^2 + Mx''y'' + Ny''^2);$$

diese Gleichung, welche eine Identität in Bezug auf die Variablen x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, muss deshalb auch eine Identität in Bezug auf x'', y'' sein; da ferner m, m', m'' positiv sind, und die Zahlen a'', b'', c'' keinen gemeinschaftlichen Theiler haben, so ergibt sich

$$m'' = mm' \quad (18)$$

und

$$L = a''nn', \quad M = b''nn', \quad N = c''nn', \quad (19)$$

also

$$\begin{aligned} & a''x'^2 + b''x'y'' + c''y''^2 \\ &= (ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2). \end{aligned} \quad (20)$$

Da endlich aus der Definition der Grössen (2) und (14), oder auch aus (16) sich leicht ergibt, dass

$$\begin{aligned} & M^2 - 4LN \\ &= (R - S)^2 - 4PU = (R + S)^2 - 4QT \end{aligned}$$

ist, so folgt hieraus schliesslich

$$d''n^2n'^2 = dn'^2 = d'n^2,$$

d. h. die Determinante d'' ist der grösste gemeinschaftliche Theiler der beiden Determinanten

$$d = d''n^2, \quad d' = d'n'^2, \quad (21)$$

woraus sich leicht ergibt, dass die Ordnung n'' des Productmoduls $m'' = mm'$ auch das Product nn' aus den Ordnungen n, n' von m, m' ist. Ist ferner m' das System \mathfrak{o} aller ganzen Zahlen des Körpers Ω , so wird m'' ein Ideal im engeren Sinne des Wortes, nämlich der grösste gemeinschaftliche Theiler der beiden Ideale $i(\alpha), i(\beta)$ oder aller Ideale $i(\mu)$; zugleich ist $m' = 1, m'' = m = N(m'')$, und $d' = d'' = \Delta(\Omega)$.

Wir stellen uns jetzt noch die Aufgabe, die Zahlen α'', β'' zu finden, wenn die Zahlen $\alpha, \beta, \alpha', \beta'$, also auch $a, b, c, \sqrt{d}, a', b', c', \sqrt{d'}$ gegeben sind; die nachfolgende Lösung ist, abgesehen von geringfügigen Aenderungen, der eleganten Methode entlehnt, welche von Gauss zu ähnlichem Zweck angewandt ist und sich in hohem Grade verallgemeinern lässt (vergl. §. 161, Anm.). Die beiden relativen Primzahlen n, n' sind durch (6), und folglich die sechs ganzen Zahlen $P \dots U$ durch (5) (bis auf einen gemeinschaftlichen Factor ± 1) aus den Daten vollständig bestimmt, und zwar so, dass sie die Gleichungen (3), (4) befriedigen und keinen gemeinschaftlichen Theiler haben*). Nun wähle man, durch die Gleichungen (11) geleitet, vier ganze rationale Zahlen $\Omega, \Omega', \Omega'', \Omega'''$ willkürlich, nur mit der einzigen Beschränkung, dass die folgenden vier Zahlen

*) Dass R und S (zufolge (5)) ganze Zahlen werden und keinen gemeinschaftlichen Theiler mit P, Q, T, U haben, geht unmittelbar aus der Gewissheit hervor, dass der Modul m'' und die Basiszahlen α'', β'' existiren; es lässt sich aber auch sehr leicht aus (5) und (6) beweisen, natürlich unter der Voraussetzung, dass dd' eine Quadratzahl ist.

$$\begin{aligned}
 & * P\Omega' + Q\Omega'' + R\Omega''' = r q \\
 - P\Omega & * + S\Omega'' + T\Omega''' = r q' \\
 - Q\Omega - S\Omega' & * + U\Omega''' = r q'' \\
 - R\Omega - T\Omega' - U\Omega'' & * = r q'''
 \end{aligned} \tag{22}$$

nicht sämmtlich verschwinden und folglich einen grössten gemeinschaftlichen Divisor r besitzen; nachdem hierdurch vier ganze Zahlen q, q', q'', q''' ohne gemeinschaftlichen Theiler gewonnen sind, wähle man (nach §. 24) vier ganze rationale Zahlen v, v', v'', v''' so, dass

$$q v + q' v' + q'' v'' + q''' v''' = 1 \tag{23}$$

wird, und bestimme die Zahlen p, p', p'', p''' durch die Gleichungen (12); endlich wähle man sechs ganze rationale Zahlen P', Q', R', S', T', U' (nach §. 24) so, dass

$$P P' + Q Q' + R R' + S S' + T T' + U U' = 1 \tag{24}$$

wird, setze hierauf

$$\begin{aligned}
 u & = * P' q' + Q' q'' + R' q''' \\
 u' & = - P' q * + S' q'' + T' q''' \\
 u'' & = - Q' q - S' q' * + U' q''' \\
 u''' & = - R' q - T' q' - U' q'' *
 \end{aligned} \tag{25}$$

und bestimme die Zahlen α'', β'' durch die Gleichungen (7), so bilden dieselben eine Basis des Moduls m'' , d. h. sie genügen den Gleichungen (1).

Um sich hiervon zu überzeugen, bemerke man zunächst, dass aus (22) mit Rücksicht auf (3) die Relationen

$$\begin{aligned}
 & * U q' - T q'' + S q''' = 0 \\
 - U q & * + R q'' - Q q''' = 0 \\
 T q - R q' & * + P q''' = 0 \\
 - S q + Q q' - P q'' & * = 0
 \end{aligned}$$

folgen; mit Hülfe derselben ergibt sich aus (12) und (23)

$$\begin{aligned}
 p q' - q p' & = (P v' + Q v'' + R v''') q' - (-P v + S v'' + T v''') q \\
 & = P (q v + q' v') + (Q q' - S q) v'' + (R q' - T q) v''' \\
 & = P (q v + q' v' + q'' v'' + q''' v''') = P,
 \end{aligned}$$

und auf ähnliche Weise erhält man die fünf anderen Gleichungen (2). Mithin folgt die erste der beiden Gleichungen (8), wenn man die Gleichungen (25) mit p, p', p'', p''' multiplicirt und mit Rück-

sicht auf (24) addirt; die zweite Gleichung (8) ergibt sich unmittelbar aus (25), wenn man mit q, q', q'', q''' multiplicirt und addirt. Es gelten daher auch die aus (8) und (2) abgeleiteten Gleichungen (11). Von den Gleichungen (9) findet die zweite zufolge (23) Statt, während die erste sich aus (12) ergibt, wenn man mit v, v', v'', v''' multiplicirt und addirt. Setzt man ferner zur Abkürzung

$$uv' - vu' = P_1, \quad uv'' - vu'' = Q_1, \quad uv''' - vu''' = R_1, \\ u'v''' - v'u''' = U_1, \quad u'v'' - v'u'' = T_1, \quad u'v' - v'u' = S_1,$$

so ergibt sich die Gleichung (10) entweder auf die dort angegebene Weise aus (8) und (9), oder auch aus (12), wenn man mit u, u', u'', u''' multiplicirt und unter Rücksicht auf (8) addirt. Substituirt man ferner für p, q ihre Ausdrücke aus (12) und (11), so erhält man

$$pu + qv = PP_1 + QQ_1 + RR_1 \\ pu' + qv' = QS_1 + RT_1 \\ pu'' + qv'' = -PS_1 + RU_1 \\ pu''' + qv''' = -PT_1 - QU_1.$$

Multiplicirt man diese Gleichungen mit $\alpha\alpha', \alpha\beta', \beta\alpha', \beta\beta'$ und addirt, so folgt aus den Definitionen (7) mit Rücksicht auf (4) und (10) die erste der Gleichungen (1); da die anderen sich auf ganz ähnliche Art ergeben, so bilden die durch die Gleichungen (7) definirten Zahlen α'', β'' in der That eine Basis des Productes $m'' = mm'$, was zu beweisen war.

Wir bemerken zum Schluss, dass man für die ersten Basiszahlen $\alpha, \alpha', \alpha''$ stets die kleinsten positiven ganzen rationalen Zahlen g, g', g'' wählen kann, welche in den Moduln m, m', m'' enthalten sind; dann wird $q = 0$, und die Bestimmung von m'' aus m und m' lässt sich auf ein System von Congruenzen reduciren, ähnlich wie in dem speciellen Falle, welcher in den §§. 145, 146 behandelt ist*).

*) Vergl. Arndt: *Auflösung einer Aufgabe in der Composition der quadratischen Formen*. Crelle's Journal LVI.