α^m theilbar durch η ist, so ist, wenn $\mathfrak{p}^a$ die höchste in α aufgehende Potenz von $\mathfrak{p}$ bedeutet, $ma \geqq me$, also $a \geqq e$, mithin geht $\mathfrak{p}^e$ auch in α auf (§. 163, 5.). *Das Ideal* $\mathfrak{a}$ *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 $\mathfrak{a}$ der beiden Hauptideale $\mathfrak{i}(\mu)$, $\mathfrak{i}(\nu)$, so wird, wenn $\mathfrak{a}^m = \mathfrak{i}(\eta)$ 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 $f_1, f_2 \ldots f_n$ von n Variabeln $h_1, h_2 \ldots h_n$, so wollen wir das Determinantenquadrat

$$\left(\Sigma \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \cdots \frac{\partial f_n}{\partial h_n}\right)^2 = \varDelta(F)$$

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

$$\frac{\partial^2 \log F}{\partial h_r \partial h_s} = -\Sigma \frac{\partial \log f_\iota}{\partial h_r} \frac{\partial \log f_\iota}{\partial h_s}$$

folgt die Gleichung

$$F^2 \Sigma \pm \frac{\partial^2 \log F}{\partial h_1^2} \cdots \frac{\partial^2 \log F}{\partial h_n^2} = (-1)^n \varDelta(F),$$

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

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

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

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 $\Delta(F)$ eine ganze rationale, durch t^2 theilbare Zahl ist.

2. Aus der Definition eines Ideals $\mathfrak{a}$ (§. 163, 1.) ergiebt sich (zufolge §. 161), dass die sämmtlichen in ihm enthaltenen Zahlen α von der Form

$$\alpha = \sum x_\iota \alpha_\iota \tag{1}$$

sind, wo die Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$ particuläre Zahlen des Ideals $\mathfrak{a}$ 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

$$\alpha_r = \sum a_\iota^{(r)} \omega_\iota, \tag{2}$$

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

$$a = \sum \pm a_1' a_2'' \dots a_n^{(n)} = N(\mathfrak{a}) \tag{3}$$

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

$$\Delta(\alpha_1, \alpha_2 \dots \alpha_n) = a^2 \Delta(\Omega). \tag{4}$$

Damit die Zahlen α wirklich ein Ideal bilden, ist erforderlich und hinreichend, dass die sämmtlichen Producte $\alpha_\iota \omega_{\iota'}$ wieder Zahlen in $\mathfrak{a}$ sind; es wird daher

---

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

$$\alpha\,\omega_r = \sum X_r^{(\iota)}\,\alpha_\iota = \sum X_r^{(\iota)}\,a_{\iota'}^{(\iota)}\,\omega_{\iota'}, \tag{5}$$

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

$$N(\alpha) = a\,X, \tag{6}$$

wo die Determinante

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

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

$$\Delta(X) = \Delta(\Omega). \tag{8}$$

Ist ferner k eine gegebene ganze rationale (von Null verschiedene) Zahl, so kann man den Variabeln x_ι stets solche ganze rationale Werthe beilegen, dass X relative Primzahl zu k wird. Man kann nämlich $\mathfrak{a}$ durch Multiplication mit einem Ideal $\mathfrak{m}$, welches ein relatives Primideal zu $\mathfrak{i}(k)$ ist, in ein Hauptideal $\mathfrak{i}(\alpha) = \mathfrak{a}\mathfrak{m}$ verwandeln (§. 163, 7.); ist nun $\mathfrak{p}$ irgend ein in $\mathfrak{m}$ aufgehendes Primideal, und p die durch $\mathfrak{p}$ theilbare rationale Primzahl (§. 163, 3.), so kann k nicht durch p theilbar sein, und da $N(\mathfrak{m})$ ein Product aus Potenzen solcher Primzahlen p ist (§. 163, 5.), so ist $N(\mathfrak{m})$ relative Primzahl zu k. Nun ist α in $\mathfrak{a}$ enthalten, also von der Form (1), wo die Grössen x_ι bestimmte ganze rationale Werthe haben, und $N(\alpha) = a\,X$; da andererseits $\mathfrak{i}(\alpha) = \mathfrak{a}\mathfrak{m}$, also $N(\alpha) = \pm\, a\,N(\mathfrak{m})$ ist (§. 163, 6.), so ergiebt sich, dass $X = \pm\, N(\mathfrak{m})$ 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 $\mathfrak{i}(\eta)$ nur dann in die Hauptclasse E aufnehmen, wenn $N(\eta)$ positiv ist; ebenso sollen zwei Ideale $\mathfrak{a}, \mathfrak{a}'$ nur dann äquivalent heissen und in dieselbe Classe aufgenommen werden, wenn beide durch Multiplication mit demselben Ideale $\mathfrak{m}$ in Ideale der Hauptclasse E verwandelt werden (vergl. §. 164. Anm.). Gehört nun das Ideal $\mathfrak{a}$ der Classe A an, so leuchtet ein, dass jeder positive Werth der Form X, welcher ganzen rationalen Werthen x_ι 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 $\alpha_1, \alpha_2 \ldots \alpha_n$ des Ideals andere $\beta_1, \beta_2 \ldots \beta_n$, welche aber ebenfalls der Bedingung genügen, dass die aus ihren Coordinaten gebildete Determinante *positiv* ist, so ist

$$\beta_r = \sum c_{r,\iota}\,\alpha_\iota\,, \quad \sum \pm c_{1,1}\,c_{2,2} \ldots c_{n,n} = +1, \tag{9}$$

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

$$x_r = \sum c_{\iota,r}\,y_\iota, \tag{10}$$

deren Coefficienten $c_{\iota,r}$ 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 *Formenclasse*, d. h. ein System von Formen $X, Y \ldots$, der Art, dass je zwei von ihnen einander äquivalent sind, und wir wollen sagen, dass diese Formenclasse dem Ideale $\mathfrak{a}$ entspricht. Ist ferner η eine ganze Zahl von positiver Norm, so bilden die n Producte $\eta\alpha_\iota$ eine Basis des Ideals $\mathfrak{a}\,\mathfrak{i}(\eta)$, und hieraus folgt unmittelbar, dass allen mit $\mathfrak{a}$ äquivalenten Idealen, also einer ganzen Idealclasse, auch dieselbe Formenclasse entspricht. Auf die Frage, wie vielen Idealclassen eine und dieselbe Formenclasse entspricht, gehen wir hier nicht ein.

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

$$\alpha_r\,\beta_s = \sum p_\iota^{r,s}\,\gamma_\iota, \quad \gamma_r = \sum q_r^{\iota,\iota'}\,\alpha_\iota\,\beta_{\iota'} \tag{11}$$

zusammen, wo die sämmtlichen $2n^3$ Grössen p und q ganze rationale Zahlen bedeuten; durch Substitution erhält man

$$\sum p_r^{\iota,\iota'}\,q_s^{\iota,\iota'} = 1 \quad \text{oder} \quad = 0, \tag{12}$$

je nachdem $r = s$ ist oder nicht. Bezeichnet man mit P alle aus den Zahlen p gebildeten Determinanten $n$ten Grades, mit Q die entsprechenden Determinanten aus den Zahlen q, so folgt hieraus nach einem bekannten Satze

$$\Sigma\, PQ = 1; \tag{13}$$

also haben die Determinanten P keinen gemeinschaftlichen Theiler. Führt man nun drei Systeme von je n Variabeln x, y, z ein, und setzt

$$\alpha = \Sigma\, x_\iota \alpha_\iota,\quad \beta = \Sigma\, y_\iota \beta_\iota,\quad \gamma = \Sigma\, z_\iota \gamma_\iota, \tag{14}$$

so wird

$$N(\alpha) = a X,\quad N(\beta) = b Y,\quad N(\gamma) = c Z, \tag{15}$$

wo X, Y, Z die zu $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ gehörigen Formen bedeuten, und

$$a = N(\mathfrak{a}),\quad b = N(\mathfrak{b}),\quad c = N(\mathfrak{c}) = ab \tag{16}$$

ist. Zwischen diesen Formen findet nun folgender Zusammenhang Statt. Setzt man

$$\alpha\beta = \gamma, \tag{17}$$

so werden die Variabeln z bilineare Functionen von den Variabeln x und y, nämlich

$$z_r = \Sigma\, p_r^{\iota,\iota'} x_\iota y_{\iota'}, \tag{18}$$

und da gleichzeitig $N(\alpha) N(\beta) = N(\gamma)$, d. h.

$$XY = Z \tag{19}$$

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

$$\alpha \beta_r = \Sigma\, \frac{\partial z_\iota}{\partial y_r} \gamma_\iota,\quad \beta \alpha_r = \Sigma\, \frac{\partial z_\iota}{\partial x_r} \gamma_\iota \tag{20}$$

ist, so erhält man, wenn man r die Werthe $1, 2 \ldots n$ durchlaufen lässt, für Ω die n mit Ω conjugirten Körper setzt und die Determinanten nimmt,

$$X = \Sigma \pm \frac{\partial z_1}{\partial y_1} \cdots \frac{\partial z_n}{\partial y_n},\quad Y = \Sigma \pm \frac{\partial z_1}{\partial x_1} \cdots \frac{\partial z_n}{\partial x_n}; \tag{21}$$

die Formen X, Y sind daher durch die Substitution (18) völlig bestimmt. Bezeichnet man ferner mit

$$\alpha' = \Sigma\, x'_\iota \alpha_\iota \tag{22}$$

die zu α adjungirte Function (§. 159, (8) und (38)), so ist

$$N(\alpha) = aX = \alpha\alpha', \tag{23}$$

und die n Grössen x' sind homogene Functionen $(n-1)$ten Grades von den Variabeln x mit rationalen Coefficienten. Durch Multiplication mit β ergiebt sich

$$a X \sum y_\iota \beta_\iota = \gamma \alpha'; \tag{24}$$

mithin sind die n Grössen

$$v_\iota = X y_\iota \tag{25}$$

bilineare Functionen von den Variabeln x', z mit rationalen Coefficienten; da ferner

$$a \sum \frac{\partial v_\iota}{\partial x'_r} \beta_\iota = \gamma \alpha_r, \tag{26}$$

so ergiebt sich, wie oben,

$$Z = a^{n-2} \sum \pm \frac{\partial v_1}{\partial x'_1} \cdots \frac{\partial v_n}{\partial x'_n}. \tag{27}$$

Hieraus folgt, dass auch die Form Z durch die bilineare Substitution (18) vollständig bestimmt ist; denn bezeichnet man mit $u_\iota^{(r)}$ den Coefficienten des Elementes

$$\frac{\partial z_\iota}{\partial y_r} \text{ in } \sum \pm \frac{\partial z_1}{\partial y_1} \cdots \frac{\partial z_n}{\partial y_n},$$

so ist auch

$$v_r = \sum u_\iota^{(r)} z_\iota, \tag{28}$$

und die n^2 Grössen $u_\iota^{(r)}$, welche homogene Functionen $(n-1)$ten Grades der Variabeln 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 $u_\iota^{(r)}$ mit ganzen rationalen Coefficienten einführen, durch welche sich umgekehrt auch die n^2 Grössen $u_\iota^{(r)}$ 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 sämmtlichen Idealen des Körpers Ω entsprechen und alle dieselbe Determinante $\Delta(\Omega)$ besitzen, bilden nur einen speciellen Fall der Formen H, welche jeder beliebigen Basis $\omega_1, \omega_2 \ldots \omega_n$ des Körpers Ω entsprechen (§. 159). Für die Untersuchung dieser Formen ist es zweckmässig, den Begriff eines Ideals so zu erweitern, dass darunter ein System $\mathfrak{a}$ 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-