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 $\mathfrak{D} B_1$, $\mathfrak{D} B_2 \ldots \mathfrak{D} B_\beta$, so bilden, wie man leicht erkennt, auch die β Complexe $\mathfrak{A} B_1$, $\mathfrak{A} B_2 \ldots \mathfrak{A} B_\beta$ 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 zusammenzusetzenden Elemente einen Einfluss auf das Compositum hat.

**) *D. A.* artt. 305—307; ferner *Démonstration de quelques théorèmes concernants 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 $\mathfrak{H}$ bildet, welche ein Multiplum der Gruppe $\mathfrak{R}$ ist (§. 149), so ist $h = rk$, und die Gruppe $\mathfrak{H}$ 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 σx, 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 ergiebt 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 ergiebt 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, ergiebt 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 $= \sigma$ 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-