IV. Ueber die Geschlechter, in welche die Classen der quadratischen Formen von bestimmter Determinante zerfallen *).

§. 121.

Ist (a, b, c) eine quadratische Form von der Determinante $b^2 - ac = D$, und sind z, z' irgend zwei durch diese Form darstellbare Zahlen (wobei es gleichgültig ist, ob die darstellenden Zahlen relative Primzahlen sind oder nicht), so lässt sich das Product zz' stets in die Form $x^2 - Dy^2$ bringen, wo x und y ganze Zahlen bedeuten; denn aus der Annahme

$$z = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \quad z' = a\beta^2 + 2b\beta\delta + c\delta^2$$

folgt (nach §. 54), dass die Form (a, b, c) durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in eine Form (z, x, z') übergeht, deren Determinante $x^2 - zz'$ von der Form Dy^2 ist. Aus dieser Bemerkung lassen sich folgende Schlüsse ziehen **).

1. Ist l eine ungerade in D aufgehende Primzahl, so hat für alle durch l nicht theilbaren Zahlen n, welche durch die Form (a, b, c) darstellbar sind, das Symbol

$$\left(\frac{n}{l}\right)$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche durch l nicht theilbare und durch (a, b, c) darstellbare

*) *Dirichlet: Recherches sur diverses applications* etc. §§. 3, 6 (Crelle's Journal XIX).

**) Vergl. *Gauss: D. A.* artt. 229—231.

Zahlen, so folgt aus $nn' = x^2 - Dy^2$, dass $nn' \equiv x^2 \pmod{l}$, und folglich

$$\left(\frac{nn'}{l}\right) = +1, \quad \text{also} \quad \left(\frac{n}{l}\right) = \left(\frac{n'}{l}\right)$$

ist.

2. Ist $D \equiv 3 \pmod{4}$, so hat für alle ungeraden durch die Form darstellbaren Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche ungerade Zahlen, so ist

$$nn' = x^2 - Dy^2 \equiv x^2 + y^2 \pmod{4};$$

da ferner nn' eine ungerade Zahl ist, so muss eine der beiden Zahlen x, y gerade, die andere ungerade sein; hieraus folgt $nn' \equiv 1 \pmod{4}$, also auch $n \equiv n' \pmod{4}$, und hieraus

$$(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}.$$

3. Ist $D \equiv 2 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 - 2y^2 \pmod{8}$$

folgt, da x ungerade ist, $nn' \equiv \pm 1 \pmod{8}$, also auch $n \equiv \pm n'$ (mod. 8), woraus die obige Behauptung sich unmittelbar ergiebt.

4. Ist $D \equiv 6 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1) + \frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 + 2y^2 \pmod{8}$$

folgt, da x ungerade ist, $nn' \equiv 1$ oder $\equiv 3 \pmod{8}$, je nachdem y gerade oder ungerade ist; dann ist entsprechend $n \equiv n'$ oder $\equiv 3n' \pmod{8}$, und man findet leicht, dass in beiden Fällen

$$\frac{n-1}{2} + \frac{n^2-1}{8} \equiv \frac{n'-1}{2} + \frac{n'^2-1}{8} \pmod{2}$$

ist, was zu beweisen war.

5. Ist $D \equiv 4 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck