VII. Ueber einige Sätze aus der Theorie der Kreistheilung.

§. 138.

Sind $p, p', p'' \ldots$ positive und von einander verschiedene Primzahlen, so stimmen (nach §. 9) die Glieder des entwickelten Productes

$$(p+1)(p'+1)(p''+1)\ldots$$

mit den sämmtlichen Divisoren des Productes

$$P = pp'p'' \ldots$$

überein; dieselben Divisoren entstehen offenbar auch durch die Entwicklung des Productes

$$(p-1)(p'-1)(p''-1)\ldots,$$

aber die eine Hälfte derselben wird mit positivem, die andere mit negativem Zeichen behaftet sein; wir wollen die erstern mit δ_1, die letztern mit δ_2 bezeichnen, so dass

$$(p-1)(p'-1)(p''-1)\ldots = \Sigma\,\delta_1 - \Sigma\,\delta_2$$

wird, und wir bemerken, dass die Zahl P selbst zu der Classe der erstern gehört. Ist nun δ irgend ein Divisor von P, aber $< P$, so lässt sich leicht zeigen, dass die Anzahl der durch δ theilbaren Zahlen δ_1 genau gleich der Anzahl der durch δ theilbaren Zahlen δ_2 ist. Denn wenn man mit $q, q', q'' \ldots$ alle diejenigen Primfactoren von P bezeichnet, welche nicht in δ aufgehen, so stimmen die durch δ theilbaren Zahlen δ_1 und $-\delta_2$ resp. mit den positiven und negativen Gliedern des entwickelten Productes

$$\delta(q-1)(q'-1)(q''-1)\dots$$

überein, und da $\delta < P$ ist, also mindestens eine solche Primzahl q vorhanden ist, so ist die Anzahl der positiven Glieder dieses Productes genau gleich der Anzahl der negativen.

Dieser Satz lässt sich leicht verallgemeinern. Bedeutet m irgend eine positive ganze Zahl > 1, und sind $p, p', p'' \dots$ die sämmtlichen von einander verschiedenen in m aufgehenden positiven Primzahlen, so kann man

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\dots = \Sigma\,\mu_1 - \Sigma\,\mu_2$$

setzen, wo mit μ_1 und $-\mu_2$ resp. alle positiven und negativen Glieder des entwickelten Productes linker Hand bezeichnet sind. Behält man die vorhergehenden Bezeichnungen bei, so stimmen offenbar die Zahlen μ_1 und μ_2 resp. mit den Zahlen $m'\delta_1$ und $m'\delta_2$ überein, wenn zur Abkürzung $m = m'P$ gesetzt wird. Bedeutet nun μ irgend einen Divisor von m, mit Ausnahme von m selbst, so folgt hieraus wieder, dass unter den Zahlen μ_1 ebenso viele durch μ theilbar sein werden, wie unter den Zahlen μ_2. Denn, wenn μ' der grösste gemeinschaftliche Divisor von μ und m' ist, so kann man $\mu = \mu'\delta$ setzen, wo δ nothwendig ein Divisor von P, und zwar $< P$ sein muss; und da eine Zahl $\mu_1 = m'\delta_1$ oder $\mu_2 = m'\delta_2$ stets und nur dann durch $\mu = \mu'\delta$ theilbar ist, sobald resp. δ_1 oder δ_2 durch δ theilbar ist, so ergiebt sich in der That, dass die Anzahl der durch μ theilbaren Zahlen μ_1 genau gleich der Anzahl der durch μ theilbaren Zahlen μ_2 ist.

Von dieser Eigenschaft der Zahlen μ_1 und μ_2 kann man vielfache Anwendungen machen. Hängen z. B. zwei Functionen $f(m)$ und $F(m)$ einer beliebigen ganzen Zahl m durch eine der beiden Relationen

$$\Sigma\, f(\mu) = F(m)$$

oder

$$\Pi\, f(\mu) = F(m)$$

zusammen, wo das Summen- oder Productzeichen sich jedesmal auf alle Divisoren μ (incl. m) der Zahl m bezieht, so folgt daraus resp. die Umkehrung

$$f(m) = \Sigma\, F(\mu_1) - \Sigma\, F(\mu_2)$$

oder

$$f(m) = \frac{\Pi\, F(\mu_1)}{\Pi\, F(\mu_2)},$$

wo die Summen- oder Productzeichen sich auf alle Werthe von μ_1 oder auf alle Werthe von μ_2 beziehen; denn ersetzt man rechts jeden Werth $F(\mu_1)$ und $F(\mu_2)$ durch die Summe oder das Product der Werthe $f(\mu)$, die den sämmtlichen Divisoren μ von μ_1 oder μ_2 entsprechen, so werden zufolge der obigen Eigenschaft der Zahlen μ_1, μ_2 alle Werthe $f(\mu)$ sich aufheben, in welchen $\mu < m$ ist, und es wird allein der Werth $f(m)$ zurückbleiben.

Als Beispiel wählen wir die Aufgabe, die Anzahl $\varphi(m)$ der ganzen Zahlen zu bestimmen, welche relative Primzahlen zu m und nicht grösser als m sind; aus dieser Definition der Function $\varphi(m)$ ist in §. 13 ohne alle Rechnung der Satz abgeleitet, dass

$$\Sigma\, \varphi(\mu) = m$$

ist, wo das Summenzeichen sich auf alle Divisoren μ von m bezieht; setzen wir daher $F(m) = m$, so ergiebt sich umgekehrt

$$\varphi(m) = \Sigma\, \mu_1 - \Sigma\, \mu_2,$$

also

$$\varphi(m) = m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p'}\right)\left(1 - \frac{1}{p''}\right)\cdots;$$

diese Function ist daher durch den Satz des §. 13 schon vollständig charakterisirt.

Ein anderes Beispiel ist folgendes. Ist der Werth der Function $f(m) = p$, sobald die Zahl m eine Potenz einer Primzahl p ist, dagegen $= 1$, so oft $m = 1$ oder durch mehrere verschiedene Primzahlen theilbar ist, so leuchtet ein, dass

$$\Pi\, f(\mu) = m$$

ist, wo das Productzeichen sich auf alle Divisoren μ von m bezieht; hieraus folgt nach dem obigen Satze, dass umgekehrt der Quotient

$$\frac{\Pi\, \mu_1}{\Pi\, \mu_2} = f(m),$$

also nur dann von 1 verschieden ist, wenn m eine Potenz einer Primzahl ist; und zwar ist dieser Quotient dann gleich dieser Primzahl.

Aus der Definition der Divisoren μ_1 und μ_2 folgt endlich auch, dass stets

$$\psi(m')\,(\psi(p) - 1)\,(\psi(p') - 1)\,(\psi(p'') - 1)\ldots = \Sigma\,\psi(\mu_1) - \Sigma\,\psi(\mu_2)$$

ist, wenn die Function ψ die Eigenschaft $\psi(z)\,\psi(z') = \psi(zz')$ besitzt.