Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Werk Id: PPN30976923X

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN30976923X|LOG_0166

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

§. 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, aC) 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', $2B$, aC; 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 Formenclassen* 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 Formenclasse $\mathfrak{K}$ von derselben Determinante D angehören, deren Theiler nach dem Obigen $= \sigma\sigma'$ ist. Wir werden daher sagen, dass diese *Classe* $\mathfrak{K}$ *aus den beiden einigen Classen* K, K' *zusammengesetzt* ist, und werden dies durch die symbolische Gleichung*)

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

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

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

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

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

und jede der Classen $(KK')K''$, $(KK'')K'$, $(K'K'')K$ enthält folglich dieselbe Form $(aa'a'', B, C)$; 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 ergiebt 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.