Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0168
LOG Titel: §. 149. Perioden und Gruppen von ursprünglichen Classen der ersten Art
LOG Typ: chapter

3. Ist K eine Classe vom Theiler σ, so kann man (nach §. 93) ihren Repräsentanten $(a\sigma, b, c)$ so wählen, dass a relative Primzahl zu σ ist; dann ist diese Form offenbar zusammengesetzt aus den beiden einigen Formen $(a, b, c\sigma)$ und (σ, b, ac), deren letztere den Theiler σ hat und der einfachsten Classe dieses Theilers angehört (§. 61), woraus von selbst folgt, dass die erstere Form eine ursprüngliche Form der ersten Art sein muss, was sich auch leicht direct nachweisen liesse. Wir haben daher das Resultat: *Ist S die einfachste, und K irgend eine Classe vom Theiler σ, so giebt es immer mindestens eine ursprüngliche Classe erster Art H von der Beschaffenheit, dass $SH = K$ ist.*

Man überzeugt sich leicht mit Hülfe von 2., dass der Satz 3. auch dann noch gilt, wenn S und K irgend welche Classen desselben Theilers bedeuten; ebenso leuchtet ein, dass aus den einfachsten Classen der Theiler σ, σ' stets die einfachste Classe des Theilers $\sigma\sigma'$ zusammengesetzt ist, natürlich unter der Voraussetzung, dass σ und σ' relative Primzahlen sind. Wir verweilen aber nicht länger bei diesen und anderen ebenso leicht zu beweisenden Sätzen, weil sie für die nachfolgenden Untersuchungen völlig entbehrlich sind.

§. 149.

Durch Composition einer *ursprünglichen Classe der ersten Art A* mit sich selbst, oder kürzer, durch *Duplication**) der Classe A entsteht eine Classe AA, welche man auch durch A^2 bezeichnen kann; ähnlich ist die allgemeine Bezeichnung A^m zu verstehen, wo m irgend eine positive ganze Zahl bedeutet. Durch Anwendung derselben Schlüsse, wie in §. 28, findet man nun leicht, dass immer ein kleinster positiver Exponent δ existirt, welcher der Bedingung $A^\delta = 1$ genügt; dann sind die Classen

$$1, A, A^2 \ldots A^{\delta-1},$$

welche die sogenannte *Periode***) der Classe A bilden, von einander verschieden; aus $A^r = A^s$ folgt $r \equiv s \pmod{\delta}$, und umgekehrt; verallgemeinert man hiernach die Bezeichnung A^m, in-

*) *Gauss: D. A.* art. 249.

**) *Gauss: D. A.* art. 306. II.

dem man sie auch auf negative Exponenten m (und auf $m = 0$) ausdehnt, so ist z. B. $A^{-1} = A^{\delta-1}$ das Symbol für die Classe, welche der Classe A entgegengesetzt ist (§. 148, 2.).

Eine solche Classenperiode bildet nur einen speciellen Fall des folgenden neuen Begriffs, welcher von der höchsten Wichtigkeit für die Gesetze der Composition ist: Ein System $\mathfrak{A}$ von ursprünglichen Classen der ersten Art soll eine *Gruppe**) heissen, wenn die Composition von je zwei Classen des Systems $\mathfrak{A}$ immer wieder eine Classe desselben Systems liefert; die Anzahl a der in $\mathfrak{A}$ enthaltenen verschiedenen Classen heisse der *Grad* dieser Gruppe $\mathfrak{A}$.

Aus dieser Erklärung folgt sofort, dass, wenn die Classe A in einer Gruppe $\mathfrak{A}$ enthalten ist, auch die ganze Periode der Classe A, also auch die entgegengesetzte Classe A^{-1} und die Hauptclasse sich in $\mathfrak{A}$ vorfindet. Setzt man ferner jede in der Gruppe $\mathfrak{A}$ enthaltene Classe A_1, $A_2 \ldots A_a$ mit einer ursprünglichen Classe erster Art B zusammen, so sind die entstehenden Classen $A_1 B$, $A_2 B \ldots A_a B$ von einander verschieden (§. 148, 2.) und bilden einen Complex, den wir kurz durch $\mathfrak{A}B$ bezeichnen können; zwei so gebildete Complexe $\mathfrak{A}B$ und $\mathfrak{A}B'$ sind nun entweder vollständig identisch (was wieder durch das Zeichen $=$ angedeutet werden soll), oder sie haben keine einzige gemeinschaftliche Classe; denn wenn sie eine gemeinschaftliche Classe $AB = A'B'$ haben, wo A und A' in $\mathfrak{A}$ enthalten sind, so folgt $B = A^{-1}A'B' = A''B'$, wo $A'' = A^{-1}A'$ eine ebenfalls in $\mathfrak{A}$ enthaltene Classe bedeutet, und hieraus $\mathfrak{A}B = \mathfrak{A}A''B' = \mathfrak{A}B'$, weil offenbar der Complex $\mathfrak{A}A''$ mit $\mathfrak{A}$ selbst identisch ist.

Stützt man sich auf diese fundamentale Eigenschaft einer Gruppe und wendet dieselbe Schlussfolgerung an, wie in §. 127, so ergiebt sich unmittelbar folgender Satz:

Sind alle a Classen einer Gruppe $\mathfrak{A}$ zugleich in einer Gruppe $\mathfrak{B}$ vom Grade b enthalten, so ist a ein Divisor von $b = \mu a$, und die Gruppe $\mathfrak{B}$ besteht aus μ Complexen von der Form $\mathfrak{A}B$; die Gruppe $\mathfrak{A}$ soll daher auch ein *Divisor* der Gruppe $\mathfrak{B}$, letztere ein *Multiplum* der ersteren heissen.

---

*) Ich wähle absichtlich diese von *Galois* in die Algebra eingeführte Benennung, weil seine Theorie und die obige, welche den sogenannten Abel'schen Gleichungen entspricht, gemeinschaftlich enthalten sind in der allgemeineren Theorie der Composition, in welcher $(KK')K'' = K(K'K'')$ ist, und ausserdem sowohl aus $KK' = KK''$, als auch aus $K'K = K''K$ stets $K' = K''$ folgt (vergl. §. 55).