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_0174
LOG Titel: §. 155. Ueber die Anzahl der wirklich existirenden Geschlechter
LOG Typ: chapter

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Ist nämlich q Rest von p, so gilt Dasselbe von $-q$ (zufolge 1. und §. 33, I.), mithin kann man, nachdem man das Vorzeichen $\pm$ so gewählt hat, dass $\pm q \equiv 1 \pmod{4}$ wird, immer $\pm q = b^2 - cp$ setzen, und folglich ist (p, b, c) eine ursprüngliche Form erster Art von der Determinante $D = \pm q \equiv 1 \pmod{4}$, und zwar eine positive, wenn D negativ ist; sie gehört also dem Hauptgeschlechte an, und folglich ist p Rest von q. Ist aber q Nichtrest von p, so muss auch p Nichtrest von q sein, weil im entgegengesetzten Falle $p = b^2 - cq$ wäre, also eine ursprüngliche Form erster Art (q, b, c) der Determinante $D = p \equiv 1 \pmod{4}$ existirte, für welche $C = -1$ wäre, was unmöglich ist.

Sind aber beide Primzahlen p, $q \equiv 3 \pmod{4}$, so ist

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Dies ergiebt sich am einfachsten durch die Betrachtung der Determinante $D = pq \equiv 1 \pmod{4}$, für welche zwei Charaktere C, also höchstens zwei verschiedene Geschlechter existiren. Da nun die beiden ursprünglichen Formen $(1, 0, -pq)$, $(-1, 0, pq)$ erster Art (zufolge 1.) wirklich zwei verschiedenen Geschlechtern angehören, so muss jede andere ursprüngliche Form erster Art von derselben Determinante, z. B. die Form $(p, 0, -q)$ einem der durch diese beiden Formen repräsentirten Geschlechter angehören. Gehört sie in das Hauptgeschlecht, so ist gleichzeitig p Rest von q, und $-q$ Rest von p, folglich (nach 1.) q Nichtrest von p; gehört sie aber in dasselbe Geschlecht wie die Form $(-1, 0, pq)$, so ist gleichzeitig p Nichtrest von q, und $-q$ Nichtrest von p, folglich q Rest von p. Was zu beweisen war.

§. 155.

Mit Hülfe des so von Neuem bewiesenen Reciprocitätssatzes lässt sich nun wieder, wie in §. 123 geschehen ist, darthun, dass höchstens diejenigen τ Geschlechter existiren können, deren Totalcharaktere der dortigen Bedingung $\Pi C' = +1$ genügen; dass aber alle diese τ Geschlechter wirklich existiren (§. 125), hat *Gauss* mit Hülfe der von ihm gegründeten Theorie der ternären quadratischen Formen

$$Ax^2 + By^2 + Cz^2 + 2A'yz + 2B'zx + 2C'xy$$

bewiesen*). Da oben (§. 152) gezeigt ist, dass $ng = \alpha q$ ist, wo g die Anzahl der wirklich existirenden Geschlechter, n die Anzahl der in jedem derselben enthaltenen Classen, $\alpha = \tau$ die Anzahl der ambigen Classen oder also die Anzahl der Totalcharaktere, welche der Bedingung $\Pi C' = +1$ genügen, und q die Anzahl der durch Duplication entstehenden Classen bedeutet, so leuchtet ein, dass der zu beweisende Satz $g = \alpha$ wesentlich identisch ist mit dem Satze $n = q$; da ferner n die Anzahl aller Classen des Hauptgeschlechtes ist, und jede der durch Duplication entstehenden q Classen gewiss dem Hauptgeschlechte angehört (§. 152), so ist der zu beweisende Satz wesentlich identisch mit dem folgenden**):

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Wir können hier unmöglich darauf eingehen, den Beweis mitzutheilen, welchen *Gauss* auf die Theorie der ternären Formen gestützt hat; da dieses tiefe Theorem aber den schönsten Abschluss der Lehre von der Composition bildet, so können wir es uns nicht versagen, dasselbe auch ohne Hülfe der Dirichlet'schen Principien auf einem Wege abzuleiten, der zugleich die Grundlage für andere wichtige Untersuchungen bildet.

Um einen bestimmten Boden für diese Untersuchung zu gewinnen, heben wir zunächst eine charakteristische Eigenschaft aller der Classen Q hervor, welche durch Duplication entstehen: *alle Formen dieser Classen und nur diese Formen sind fähig, Quadratzahlen darzustellen, welche relative Primzahlen zu $2D$ sind.* Entsteht nämlich Q durch Duplication einer Classe K, so kann man aus K immer eine solche Form auswählen, deren erster Coefficient x relative Primzahl zu $2D$ ist; da alsdann diese Form mit sich selbst einig ist, so entsteht durch Duplication eine der Classe Q angehörige Form, deren erster Coefficient $= x^2$ ist, und folglich ist diese Quadratzahl durch die Formen der Classe Q eigentlich darstellbar. Umgekehrt, ist Q eine Classe, durch deren Formen eine Quadratzahl dargestellt werden kann, welche relative Primzahl zu $2D$ ist, so giebt es auch eine solche Quadratzahl x^2, welche durch diese Formen *eigentlich* darstellbar ist, und folglich findet sich in dieser Classe Q eine Form (x^2, x', x''), welche offenbar

*) *D. A.* art. 287.

**) *Gauss: D. A.* art. 286.