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_0069
LOG Titel: §. 61. Reduction des zweiten Problems, aus einer gegebenen Substitution, durch welche eine Form in eine ihr äquivalente Form übergeht, alle ähnlichen Substitutionen zu finden, auf den Fall, in welchem beide
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 m durch keine einzige Form der Determinante D eigentlich darstellbar; im erstern Fall bestimme man alle incongruenten Wurzeln der Congruenz (4), und verfahre mit jeder einzelnen, wie folgt. Es sei n ein bestimmter Repräsentant einer bestimmten Wurzel, und zwar $n^2 = D + ml$, so ist (m, n, l) eine bestimmte Form von der Determinante D. Giebt es nun eine Darstellung (x, y) der Zahl m durch (a, b, c), welche zu der durch n repräsentirten Wurzel der Congruenz (4) gehört, so ist die Form (a, b, c) äquivalent mit (m, n, l), und die Darstellung (x, y) liefert eine und nur eine Substitution $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$, durch welche die erstere in die letztere übergeht. Es muss daher zunächst entschieden werden, ob die beiden gegebenen Formen (a, b, c) und (m, n, l) von der Determinante D äquivalent sind, oder nicht — dies ist das *erste* der beiden genannten Probleme; gesetzt nun, die beiden Formen erweisen sich als nicht äquivalent, so existirt keine einzige zu dieser Wurzel n gehörige Darstellung der Zahl m durch die Form (a, b, c). Zeigt es sich aber, dass die beiden Formen äquivalent sind, so müssen alle Substitutionen $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$ aufgesucht werden, durch welche (a, b, c) in (m, n, l) übergeht — dies ist das *zweite* Problem. Der erste und dritte Coefficient (x und y) einer jeden solchen Substitution bilden dann auch wirklich eine eigentliche zu der Wurzel n gehörige Darstellung der Zahl m durch (a, b, c), und da, wie schon bemerkt, aus jeder solchen Darstellung (x, y) umgekehrt eine und nur eine solche Substitution $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$ entspringt, so erhält man durch die sämmtlichen Substitutionen der angegebenen Art auch *alle* zu n gehörigen Darstellungen, und jede nur *ein Mal*. Genau in derselben Weise verfährt man mit den übrigen Wurzeln der Congruenz (4), deren Anzahl, falls m und D relative Primzahlen sind, nach §. 37 zu bestimmen ist.

§. 61.

Nachdem wir uns in der vorhergehenden Digression davon überzeugt haben, dass in der That die Theorie der Darstellung vollständig auf die beiden (in §. 59) erwähnten Probleme der Lehre von der Aequivalenz zurückgeführt werden kann, so wenden wir uns nun zu der Lösung derselben. Das *erste*, zu erkennen, ob zwei Formen von gleicher Determinante äquivalent sind oder nicht, erfordert von vorn herein ganz verschiedene Methoden, je nachdem

die Determinante *positiv* oder *negativ* ist; in beiden Fällen ist aber die Lösung von der Art, dass, wenn die Aequivalenz der beiden Formen erkannt wird, zu gleicher Zeit auch eine Transformation der einen in die andere gefunden wird. Da also bei zwei wirklich äquivalenten Formen immer eine solche Transformation durch die Lösung der ersten Aufgabe gefunden ist, so besteht das *zweite* Problem nur noch darin, aus *einer* solchen Transformation *alle anderen* zu finden; und da die Lösung desselben zunächst nicht von dem Vorzeichen der Determinante abhängt, sondern für positive wie für negative Determinanten Anfangs eine gleichmässige Behandlung zulässt, so stellen wir es dem andern voran.

Unsere Aufgabe ist also die, aus *einer* Substitution L, durch welche eine Form φ in eine äquivalente Form ψ übergeht, *alle* Substitutionen S zu finden, welche denselben Erfolg haben. Wir können dieselbe sogleich durch einige Bemerkungen bedeutend vereinfachen, indem wir sie auf den einfachsten Fall reduciren, in welchem beide Formen identisch sind. Denn gesetzt, wir kennen *alle* Substitutionen T, durch welche die Form φ in sich selbst übergeht, so geht φ offenbar durch alle Substitutionen TL in die andere Form ψ über. Alle diese Substitutionen TL gehören also zu den gesuchten Substitutionen S. Jetzt behaupten wir auch umgekehrt, dass auf diese Weise alle Substitutionen S erzeugt werden, und jede nur ein einziges Mal; denn bezeichnen wir mit L' die inverse Substitution von L (durch welche also die Form ψ in die Form φ zurückkehrt), so ist jede in der Form SL' enthaltene Substitution eine solche, durch welche die Form φ in sich selbst übergeht, und gehört mithin zu den mit T bezeichneten Substitutionen, so dass wir $SL' = T$ setzen können. Da nun die aus L' und L zusammengesetzte Substitution $L'L = \left(\begin{smallmatrix} 1, & 0 \\ 0, & 1 \end{smallmatrix}\right)$ ist, so folgt hieraus $SL'L = S = TL$, also wird wirklich jede Substitution S auf die angegebene Art erzeugt. Dass endlich jede Substitution S nur ein einziges Mal erzeugt wird, leuchtet hieraus ebenfalls ein; ist nämlich $TL = S$, so ist $T = SL'$, also ist die Substitution T, durch welche eine bestimmte Substitution S erzeugt wird, immer eine vollkommen bestimmte, so dass zwei verschiedene Substitutionen T auch zwei verschiedene Substitutionen S erzeugen.

Da also der Complex der Substitutionen S vollständig mit dem Complex der Substitutionen TL übereinstimmt, wo L die gegebene Substitution bedeutet, durch welche die Form φ in die äquivalente Form ψ übergeht, so kommt es nur noch darauf an,

alle Substitutionen T zu finden; unser Problem ist daher auf das folgende zurückgeführt:

Alle Substitutionen zu finden, durch welche eine Form in sich selbst übergeht.

Bevor wir zur Lösung desselben schreiten, stellen wir eine Betrachtung an, welche für die Folge von grosser Wichtigkeit ist. Bedeutet σ den grössten (positiven) gemeinschaftlichen Theiler der drei Zahlen a, $2b$, c, so leuchtet ein, dass alle durch die Form (a, b, c) darstellbaren Zahlen durch σ theilbar sind, und wir wollen, wo kein Missverständniss zu besorgen ist, diese Zahl σ kurz *den Theiler der Form* (a, b, c) nennen. Dann sind zwei Fälle möglich:

1. Ist $2b : \sigma$ eine gerade Zahl, so geht σ in b, und folglich σ^2 in der Determinante $D = b^2 - ac$ auf; und umgekehrt, wenn σ^2 in D aufgeht, so ist b durch σ theilbar, also $2b : \sigma$ eine gerade Zahl; zugleich ist dann σ der grösste gemeinschaftliche Theiler der drei Coefficienten a, b, c.

2. Ist $2b : \sigma$ eine ungerade Zahl, so ist σ jedenfalls gerade, und σ^2 geht nicht in D, wohl aber in $4D$ auf, und zwar ist

$$\frac{4D}{\sigma^2} = \left(\frac{2b}{\sigma}\right)^2 - 4\frac{a}{\sigma}\frac{c}{\sigma} \equiv 1 \pmod 4,$$

also $4D \equiv \sigma^2 \pmod{4\sigma^2}$; und umgekehrt, wenn $4D \equiv \sigma^2 \pmod{4\sigma^2}$, so ist auch $(2b)^2 \equiv \sigma^2 \pmod{4\sigma^2}$, folglich $2b : \sigma$ eine ungerade Zahl; zugleich ist $\frac{1}{2}\sigma$ der grösste gemeinschaftliche Theiler der drei Coefficienten a, b, c.

Der Theiler σ einer jeden Form von der Determinante D genügt daher entweder der Bedingung $D \equiv 0 \pmod{\sigma^2}$, oder dieser $4D \equiv \sigma^2 \pmod{4\sigma^2}$; umgekehrt, ist σ eine positive Zahl, welche der einen oder andern dieser Bedingungen genügt, so existiren auch Formen (a, b, c) von der Determinante D, deren Theiler σ ist; je nachdem nämlich σ der ersten oder der zweiten Bedingung genügt, ist

$$\left(\sigma, 0, \frac{-D}{\sigma}\right) \quad \text{oder} \quad \left(\sigma, \tfrac{1}{2}\sigma, \frac{\sigma^2 - 4D}{4\sigma}\right)$$

eine Form von der Determinante D und vom Theiler σ, und zwar die sogenannte *einfachste* solche Form (*forma simplicissima*); die einfachste Form $(1, 0, -D)$ vom Theiler 1 heisst die *Hauptform* (*forma principalis*) der Determinante D*).

*) *Gauss: D. A.* artt. 231, 25.