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_0165
LOG Titel: §. 146. Composition zweier einigen Formen. Fundamentalsatz
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

$$(B-b)\,(B-b') = BB-(b+b')B+bb'$$

ist, so folgt zunächst, dass die Forderungen (2) vollständig übereinstimmen mit den folgenden

$$a'B \equiv a'b,\ aB \equiv ab',\ (b+b')B \equiv bb'+D \pmod{aa'}, \quad (5)$$

welche, mit h', h, h'' multiplicirt und addirt, die Congruenz (4) nach sich ziehen. Dass umgekehrt jede durch die Congruenz (4) bestimmte Zahl B den Bedingungen (2) oder (5) genügt, ergiebt sich leicht, wenn man aus (3) und (4) der Reihe nach h', h, h'' eliminirt und hierbei die Voraussetzungen (1) berücksichtigt.

Wir bemerken schliesslich, dass die Zahlen a, a', $2B$ keinen gemeinschaftlichen Theiler haben; denn ist δ ein solcher, so folgt aus (2) auch $b \equiv b' \equiv B \pmod{\delta}$, also $b+b' \equiv 2B \equiv 0 \pmod{\delta}$; mithin ist δ gemeinschaftlicher Theiler von a, a', $b+b'$, und folglich $\delta = 1$.

§. 146.

Zwei binäre quadratische Formen (a, b, c), (a', b', c') von gleicher Determinante D sollen *einig**) heissen, wenn die Zahlen $a, a', b+b'$ keinen gemeinschaftlichen Theiler haben. Da unter dieser Voraussetzung auch $bb \equiv D \pmod{a}$, $b'b' \equiv D \pmod{a'}$ ist, so folgt aus dem vorhergehenden Lemma unmittelbar die Existenz von unendlich vielen (nach §. 56 äquivalenten) Formen (aa', B, C) derselben Determinante D, deren mittlere Coefficienten B den Bedingungen $B \equiv b \pmod{a}$, $B \equiv b' \pmod{a'}$ genügen; jede solche Form (aa', B, C) heisse *zusammengesetzt***) (*composita*) *aus* (a, b, c) *und* (a', b', c').

Wir bemerken zunächst, dass (nach §. 56) die Formen (a, b, c), (a', b', c') resp. den Formen $(a, B, a'C)$, (a', B, aC) äquivalent sind; diese letzteren sind ebenfalls einig, weil die Zahlen a, a', $2B$, keinen gemeinschaftlichen Theiler haben (§. 145), und aus ihnen ist ebenfalls die Form (aa', B, C) zusammengesetzt. Bedeuten nun x, y, x', y' variabele Grössen, und setzt man

---

*) Diese Benennung soll an die *radices concordantes* von *Dirichlet* erinnern.

**) Vergl. *Gauss*: *D. A.* artt. 235, 242, 243, 244.

$$X = xx' - Cyy', \quad Y = (ax + By)\, y' + (a'x' + By')y, \qquad (1)$$

so wird

$$(ax + (B + \sqrt{D})y)(a'x' + (B + \sqrt{D})y') = aa' X + (B + \sqrt{D})\, Y; \qquad (2)$$

ersetzt man hierin $\sqrt{D}$ durch $-\sqrt{D}$ und multiplicirt die so entstehende Gleichung mit der vorstehenden, so ergiebt sich nach Wegwerfung des beiden Seiten gemeinschaftlichen Factors aa' die Gleichung

$$\begin{aligned}(ax^2 + 2Bxy + a'Cy^2)\,(a'x'^2 + 2Bx'y' + aCy'^2) \\ = aa' X^2 + 2BXY + CY^2,\end{aligned} \qquad (3)$$

d. h. *die Form* (aa', B, C) *geht durch die bilineare Substitution* (1) *in das Product aus den beiden Formen* $(a, B, a'C)$, (a', B, aC) *über.*

Auf dem vorstehenden Resultate beruht zugleich der Beweis des folgenden Fundamentalsatzes*):

Sind die beiden einigen Formen (a, b, c), (a', b', c') *resp. äquivalent den beiden einigen Formen* (m, n, l), (m', n', l'), *so ist auch die aus den beiden ersteren zusammengesetzte Form* (aa', B, C) *äquivalent der aus den beiden letzteren zusammengesetzten Form* (mm', N, L).

Aus den Voraussetzungen folgt zunächst, dass die Formen $(a, B, a'C)$, (a', B, aC) resp. den Formen $(m, N, m'L)$, (m', N, mL) äquivalent sind, und hieraus (nach §. 60. Anmerkung) die Existenz von vier ganzen Zahlen x, y, x', y', welche den folgenden Bedingungen genügen

$$ax^2 + 2Bxy + a'Cy^2 = m, \quad a'x'^2 + 2Bx'y' + aCy'^2 = m' \qquad (4)$$

$$ax + (B + N)y \equiv 0, \quad (B - N)x + a'Cy \equiv 0 \pmod{m} \qquad (5)$$

$$a'x' + (B + N)y' \equiv 0, \quad (B - N)x' + aCy' \equiv 0 \pmod{m'}, \qquad (6)$$

und ebenso braucht man, um die Aequivalenz der beiden Formen (aa', B, C), (mm', N, L) darzuthun, nur die Existenz von zwei ganzen Zahlen X, Y nachzuweisen, welche die Forderungen

$$aa' X^2 + 2BXY + CY^2 = mm' \qquad (7)$$

$$aa' X + (B + N)\, Y \equiv 0 \pmod{mm'} \qquad (8)$$

$$(B - N)\, X + CY \equiv 0 \pmod{mm'} \qquad (9)$$

befriedigen. Es lässt sich nun leicht zeigen, dass die beiden (offenbar ganzen) Zahlen X, Y, welche nach (1) aus den vier ganzen

*) *Gauss: D. A.* art. 239. — *Dirichlet* a. a. O.

Zahlen x, y, x', y' gebildet sind, in der That den vorstehenden Bedingungen genügen. Zunächst folgt (7) unmittelbar aus (3) und (4). Da ferner aus jeder Gleichung von der Form

$$(t+uV\!D)\,(t'+u'V\!D) = (t''+u''V\!D)\,(t'''+u'''V\!D),$$

wo t, u, t' u. s. w. ganze Zahlen bedeuten, die in Bezug auf die Variabele z identische Gleichung

$$(t+uz)(t'+u'z) = (t''+u''z)(t'''+u'''z) + (uu'-u''u''')(zz-D),$$

und hieraus, da $NN \equiv D \pmod{mm'}$ ist, auch die Congruenz

$$(t+uN)\,(t'+u'N) \equiv (t''+u''N)\,(t'''+u'''N) \pmod{mm'}$$

hervorgeht, so folgt (8) unmittelbar aus (2) unter Berücksichtigung von (5) und (6). Dieselbe Gleichung (2) lässt sich endlich durch Multiplication mit $B-V\!D$, oder mit C, und durch Division mit a oder mit a' auf die folgenden vier Formen bringen

$$((B-V\!D)x+a'Cy)\,(a'x'+(B+V\!D)y') = a'U$$

$$(ax+(B+V\!D)y)\,((B-V\!D)x'+aCy') = aU$$

$$((B-V\!D)x+a'Cy)\,((B-V\!D)x'+aCy') = (B-V\!D)U$$

$$C(ax+(B+V\!D)y)\,(a'x'+(B+V\!D)y') = (B+V\!D)U,$$

wo zur Abkürzung

$$(B-V\!D)X+CY = U$$

gesetzt ist; ersetzt man überall $V\!D$ durch N, so gehen nach dem oben angeführten Princip diese Gleichungen wieder in Congruenzen nach dem Modulus mm' über; bezeichnet man den aus U hervorgehenden Ausdruck, d. h. die linke Seite der zu beweisenden Congruenz (9), mit V, so ergiebt sich unter Berücksichtigung von (5) und (6), dass die Producte $a'V$, aV, $(B-N)V$, $(B+N)V$, mithin auch $2BV$ durch mm' theilbar sind; da aber die Factoren a, a', $2B$ keinen gemeinschaftlichen Theiler haben, so muss der andere Factor V für sich allein durch mm' theilbar sein, also die Congruenz (9) wirklich Statt finden.

Mithin genügen die beiden ganzen Zahlen X, Y den Bedingungen (7), (8), (9), und hieraus folgt (nach §. 60. Anmerkung) die Aequivalenz der Formen (aa', B, C), (mm', N, L); was zu beweisen war.