

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_0070

LOG Titel: S. 62. Reduction des Problems, alle Substitutionen zu finden, durch welche eine Form in sich selbst übergeht, auf die vollständige Auflösung der Pell'schen Gleichung.

LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

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

Der grösste gemeinschaftliche Theiler τ der drei Coefficienten a, b, c einer Form (a, b, c) ist im ersten Fall $= \sigma$, im zweiten $= \frac{1}{2}\sigma$; ist nun $\tau = 1$, so heisst die Form eine *ursprüngliche* *) (*forma primitiva*), und zwar, wenn $\sigma = 1$ ist, eine Form der *ersten Art* **) (*forma proprie primitiva* oder *forma propria* nach Gauss), dagegen, wenn $\sigma = 2$ und also $D \equiv 1 \pmod{4}$ ist, eine Form der *zweiten Art* (*forma improprie primitiva* oder *forma impropria*). Ist ferner $\tau > 1$, und $a = \tau a', b = \tau b', c = \tau c', b'b' - a'c' = D', D = \tau^2 D'$, so heisst die Form (a, b, c) *abgeleitet* (*derivata*) aus der ursprünglichen Form (a', b', c') der Determinante D' .

Aus den Formeln der Transformation [§. 54, (2)] geht nun hervor, dass, wenn eine Form (a', b', c') unter einer Form (a, b, c) enthalten ist, jeder gemeinschaftliche Theiler der Zahlen $a, 2b, c$ auch gemeinschaftlicher Theiler der Zahlen $a', 2b', c'$ sein muss, woraus unmittelbar folgt, dass je zwei äquivalente Formen denselben Theiler σ besitzen; mithin kommt dieser Theiler allen zu einer und derselben Classe gehörigen Formen gemeinschaftlich zu, und kann daher füglich *der Theiler der Formenclasse* genannt werden. Dasselbe gilt offenbar von dem grössten gemeinschaftlichen Theiler τ der Coefficienten a, b, c einer jeden zu einer bestimmten Classe gehörigen Form (a, b, c) . Hiernach leuchtet von selbst ein, was unter der *einfachsten Classe vom Theiler σ* , unter der *Hauptclasse*, unter einer *ursprünglichen Classe der ersten oder zweiten Art*, oder unter einer *abgeleiteten Classe* zu verstehen ist. Endlich bildet der Inbegriff aller Formen von gleicher Determinante D und von gleichem Theiler σ eine sogenannte *Ordnung* ***) (*ordo*), und aus dem Vorhergehenden folgt, dass dieselbe der Complex aller *Classen* der Determinante D ist, welche den Theiler σ haben.

§. 62.

Es sei nun $\left(\begin{smallmatrix} \lambda \\ \mu \\ \nu \end{smallmatrix} \rho\right)$ irgend eine Substitution, durch welche die Form (a, b, c) von der Determinante D und vom Theiler σ in sich selbst übergeht, so ist zunächst

$$\lambda \rho - \mu \nu = 1 \quad (1)$$

*) Gauss: *D. A.* art. 226.

**) Dirichlet: *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres.* 2^e partie. §. 7. Crelle's Journal XXI.

***) Gauss: *D. A.* art. 226.

und ferner (nach §. 54)

$$a\lambda^2 + 2b\lambda\nu + c\nu^2 = a; \quad (2)$$

$$a\lambda\mu + b(\lambda\rho + \mu\nu) + c\nu\rho = b; \quad (3)$$

da aus diesen drei Gleichungen schon folgt, dass (a, b, c) in eine äquivalente Form übergeht, deren erster und zweiter Coefficient a und b sind, so ist der letzte Coefficient c' der neuen Form wegen der Gleichheit der Determinanten nothwendig $= c$; und folglich drücken diese Gleichungen vollständig aus, dass $(\lambda, \mu, \nu, \rho)$ eine Substitution der verlangten Art ist (dies würde nicht ebenso vollständig geschehen, wenn man die Gleichung $\lambda\rho - \mu\nu = 1$ durch die andere Gleichung $a\mu^2 + 2b\mu\rho + c\rho^2 = c$ ersetzen wollte; denn dann würde man rückwärts nur schliessen können, dass $\lambda\rho - \mu\nu = \pm 1$ ist).

Wir behandeln diese drei Gleichungen mit den vier Unbekannten λ, μ, ν, ρ auf folgende Weise.

Wird $\lambda\rho$ durch $\mu\nu \pm 1$ ersetzt, so nimmt die Gleichung (3) die Form

$$a\lambda\mu + 2b\mu\nu + c\nu\rho = 0$$

an; verbindet man hiermit die Gleichung (2) und eliminirt einmal $2b$, dann c , so erhält man unter Berücksichtigung der Gleichung (1) die beiden folgenden:

$$a\mu + c\nu = 0; \quad a(\lambda - \rho) + 2b\nu = 0.$$

Da a von Null verschieden ist (weil sonst D eine Quadratzahl wäre), so kann man folglich

$$\nu = \frac{a}{\sigma}u, \quad \mu = -\frac{c}{\sigma}u, \quad \lambda - \rho = -\frac{2b}{\sigma}u \quad (4)$$

setzen, worin u eine neue unbekannte, aber *ganze* Zahl bedeutet, weil $\nu, \mu, \lambda - \rho$ ganze Zahlen sind, und σ der grösste gemeinschaftliche Divisor von $a, c, 2b$ ist. Setzen wir diese Ausdrücke für μ und ν in die Gleichung (1), so erhalten wir

$$\lambda\rho = -\frac{ac}{\sigma^2}u^2 + 1,$$

und hieraus in Verbindung mit dem vorstehenden Ausdruck für $\lambda - \rho$ die Gleichung

$$(\lambda + \rho)^2 = (\lambda - \rho)^2 + 4\lambda\rho = \frac{4(Du^2 + \sigma^2)}{\sigma^2}$$

oder

$$\left(\frac{\sigma(\lambda + \rho)}{2}\right)^2 = Du^2 + \sigma^2.$$

Hieraus ergibt sich, dass $\frac{1}{2}\sigma(\lambda + \varrho)$ jedenfalls eine ganze Zahl sein muss, die wir mit t bezeichnen wollen, so dass

$$\lambda + \varrho = \frac{2t}{\sigma} \text{ und } t^2 = Du^2 + \sigma^2 \quad (5)$$

ist.

Wir können die vorstehende Untersuchung mit Rücksicht auf (4) und (5) in Folgendem zusammenfassen*):

Ist $\begin{pmatrix} \lambda & \mu \\ \nu & \varrho \end{pmatrix}$ eine Substitution, durch welche die Form (a, b, c) von der Determinante D und vom Theiler σ in sich selbst übergeht, so ist stets

$$\begin{aligned} \lambda &= \frac{t - bu}{\sigma}, & \mu &= -\frac{cu}{\sigma} \\ \nu &= \frac{au}{\sigma}, & \varrho &= \frac{t + bu}{\sigma} \end{aligned} \quad (I)$$

wo t, u zwei ganze Zahlen bedeuten, welche der unbestimmten Gleichung

$$t^2 - Du^2 = \sigma^2 \quad (II)$$

Genüge leisten.

Aber dieser Satz lässt sich auch umkehren:

Sind t, u zwei ganze der Gleichung (II) genügende Zahlen, so sind die durch die Gleichungen (I) bestimmten Zahlen $\lambda, \mu, \nu, \varrho$ die ganzzahligen Coefficienten einer Substitution $\begin{pmatrix} \lambda & \mu \\ \nu & \varrho \end{pmatrix}$, durch welche die Form (a, b, c) in sich selbst übergeht.

Dies ergibt sich auf folgende Weise. Zunächst ist zu beweisen, dass $\lambda, \mu, \nu, \varrho$ ganze Zahlen werden; da σ in a und in c aufgeht, so sind ν und μ ganze Zahlen; da ferner σ^2 in $4D$ und zufolge (II) auch in $4t^2$ aufgeht, so ist $2t$ theilbar durch σ , und da σ auch in $2b$ aufgeht, so sind 2λ und 2ϱ ebenfalls ganze Zahlen, deren Summe $= 4t : \sigma$, also eine gerade Zahl ist; mithin sind 2λ und 2ϱ entweder beide gerade oder beide ungerade; da aber ihr Product

$$= 4 \frac{t^2 - b^2u^2}{\sigma^2} = 4 \frac{\sigma^2 - acu^2}{\sigma^2} = 4 \left(1 - \frac{a}{\sigma} \frac{c}{\sigma} u^2 \right)$$

gerade ist, so sind 2λ und 2ϱ gerade Zahlen, also λ und ϱ ganze Zahlen.

Nachdem dieser erste Punkt sichergestellt ist, findet man leicht durch wirkliche Substitution der Ausdrücke (I) unter Berücksichtigung der Gleichung (II), dass die drei Relationen (1),

*) Vergl. Gauss: D. A. art. 162.

(2) und (3) identisch erfüllt sind, dass also in der That die Form (a, b, c) durch die Substitution (λ, μ) in sich selbst übergeht.

Aus jeder bekannten Substitution (λ, μ) kann daher (z. B. durch die Gleichungen $u = \sigma v : a, t = \sigma \lambda + b u$) eine Auflösung t, u der Gleichung (II) gefunden werden, und umgekehrt. Es ist aber wichtig, zu bemerken, dass zwei verschiedenen Substitutionen auch zwei verschiedene Auflösungen der Gleichung (II) entsprechen, und umgekehrt zwei verschiedenen Auflösungen der Gleichung (II) auch zwei verschiedene Transformationen der Form (a, b, c) in sich selbst. Denn die Relationen (I) sind derartig, dass gegebenen Werthen t, u ein und nur ein System von Werthen $\lambda, \mu, \nu, \varrho$, und umgekehrt gegebenen Werthen von $\lambda, \mu, \nu, \varrho$ ein und nur ein System von Werthen t, u entspricht.

Hiermit ist also unser Problem nicht vollständig gelöst, sondern nur auf das andere reducirt:

Alle ganzzahligen Auflösungen der unbestimmten Gleichung (II) zu finden.

Dieses letztere bietet nun nicht die geringste Schwierigkeit dar, sobald die Determinante D negativ ist. Wenn nämlich Δ ihr absoluter Werth, also $D = -\Delta$ ist, so hat die Gleichung (II)

$$t^2 + \Delta u^2 = \sigma^2$$

nur eine *endliche* Anzahl von Auflösungen t, u ; und zwar ist, wenn

1. $D \equiv 0 \pmod{\sigma^2}$, die Anzahl der Auflösungen der Gleichung immer = 2, sobald $\Delta > \sigma^2$ ist; diese Auflösungen sind offenbar

$$t = +\sigma, u = 0 \quad \text{und} \quad t = -\sigma, u = 0;$$

im Fall $\Delta = \sigma^2$ ist aber die Anzahl der Auflösungen = 4; diese sind

$$\begin{aligned} t = \sigma, u = 0; & \quad t = -\sigma, u = 0; \\ t = 0, u = 1; & \quad t = 0, u = -1. \end{aligned}$$

2. Ist $4D \equiv \sigma^2 \pmod{4\sigma^2}$ und folglich $4\Delta \equiv 3\sigma^2 \pmod{4\sigma^2}$, so ist die Anzahl der Auflösungen der Gleichung stets = 2, so oft $4\Delta > 3\sigma^2$, also $4\Delta \geq 7\sigma^2$; diese sind

$$t = \sigma, u = 0; \quad \text{und} \quad -t = -\sigma, u = 0;$$

im Fall $4\Delta = 3\sigma^2$ ist aber die Anzahl der Auflösungen = 6; diese sind

$$\begin{aligned} t = +\sigma, u = 0; & \quad t = +\frac{1}{2}\sigma, u = +1; & \quad t = +\frac{1}{2}\sigma, u = -1; \\ t = -\sigma, u = 0; & \quad t = -\frac{1}{2}\sigma, u = -1; & \quad t = -\frac{1}{2}\sigma, u = +1. \end{aligned}$$