

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_0086

LOG Titel: S. 78. Eintheilung der reducirten Formen von positiver Determinante in Perioden von gerader Gliederanzahl.

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

cirte Form eine und nur eine nach links benachbarte reducirte Form besitzt. Doch ist es bequemer, diesen Fall auf den eben behandelten durch die einleuchtende Bemerkung (§. 74 Anm.) zurückzuführen, dass die beiden Formen (a, b, a') und (a', b, a) gleichzeitig reducirte, oder gleichzeitig nicht reducirte Formen sind. Wenn nun die reducirte Form (a, b, a') eine nach links benachbarte und ebenfalls reducirte Form (a', b, a) besitzt, so hat die reducirte Form (a', b, a) die nach rechts benachbarte Form (a, b, a') , welche ebenfalls reducirt ist; und umgekehrt, sobald die Form (a, b, a') der reducirten Form (a', b, a) nach rechts benachbart und zugleich reducirt ist, so ist die Form (a', b, a) ebenfalls reducirt und der Form (a, b, a') nach links benachbart. Da wir nun gesehen haben, dass eine reducirte Form (a', b, a) immer eine und nur eine nach rechts benachbarte reducirte Form (a, b, a') hat, so folgt:

Jede reducirte Form (a, b, a') besitzt stets eine und nur eine nach links benachbarte reducirte Form (a', b, a) .

§. 78.

Aus den soeben bewiesenen Sätzen über die nach rechts und links benachbarten reducirten Formen ergibt sich, dass man sämtliche reducirte Formen einer positiven Determinante D in *Perioden**) einteilen kann, die auf folgende Weise zu bilden sind. Man wähle irgend eine reducirte Form φ_0 und bilde die nach rechts und links fortgesetzte Reihe

$$\dots \varphi_{-2}, \varphi_{-1}, \varphi_0, \varphi_1, \varphi_2 \dots$$

der successiven nach rechts und nach links benachbarten reducirten Formen, welche durch das eine Glied φ_0 vollständig bestimmt sind. Da es nur eine endliche Anzahl von reducirten Formen der Determinante D giebt, und die ersten Coefficienten zweier auf einander folgenden Formen stets entgegengesetzte Zeichen haben, so muss einmal auf eine Form φ_μ dieser Reihe nach einer geraden Anzahl $2n$ von Gliedern eine mit φ_μ identische Form $\varphi_{\mu+2n}$ folgen; und da eine Form φ_μ oder $\varphi_{\mu+2n}$ nur eine

*) Gauss: D. A. art. 186.

einzige nach rechts, und nur eine einzige nach links benachbarte reducirte Form besitzt, so müssen auch die beiden Formen $\varphi_{\mu+1}$ und $\varphi_{\mu+1+2n}$, ebenso die beiden Formen $\varphi_{\mu-1}$ und $\varphi_{\mu-1+2n}$, und also auch allgemein je zwei Formen dieser Reihe identisch sein, deren Indices dieselbe Differenz $2n$ haben. In der ganzen Reihe sind daher höchstens $2n$ verschiedene Formen

$$\varphi_0, \varphi_1, \varphi_2 \dots \varphi_{2n-2}, \varphi_{2n-1};$$

und diese werden in der That alle von einander verschieden sein, wenn keine der Formen $\varphi_2, \varphi_4 \dots \varphi_{2n-2}$ mit φ_0 identisch ist; denn wären φ_ν und $\varphi_{\nu+2n'}$ zwei identische Formen, so müsste auch $\varphi_{2n'}$ mit φ_0 identisch sein. Nehmen wir also an, dass $2n$ die Anzahl der wirklich verschiedenen Formen dieser Reihe ist, so besteht dieselbe aus einer nach beiden Seiten sich unendlich oft periodisch wiederholenden Folge dieser $2n$ Formen; je zwei Formen φ_μ und φ_ν , deren Indices eine durch $2n$ theilbare Differenz $\mu - \nu$ haben, sind identisch; und umgekehrt, sind die Formen φ_μ und φ_ν identisch, so ist $\mu \equiv \nu \pmod{2n}$.

Es kann nun sein, dass diese $2n$ Formen alle reducirten Formen der Determinante D erschöpfen; aber es ist auch möglich, dass ausser ihnen noch andere reducirte Formen derselben Determinante existiren. Im letztern Fall sei ψ_0 eine solche, in der obigen Periode nicht enthaltene reducirte Form, so entspricht ihr ebenso eine Periode von $2m$ unter einander verschiedenen Formen

$$\psi_0, \psi_1, \psi_2 \dots \psi_{2m-2}, \psi_{2m-1};$$

alle diese Formen der zweiten Periode werden auch von denen der ersten verschieden sein; denn besäßen beide Perioden eine gemeinschaftliche Form, so wären beide Reihen vollständig identisch, da von dieser gemeinschaftlichen Form aus die Reihe nur auf eine einzige Weise nach rechts und links fortgesetzt werden kann.

In derselben Weise kann man fortfahren, bis endlich alle reducirten Formen in verschiedene Perioden eingetheilt sind; die Anzahl der Perioden ist nothwendig eine endliche; die Anzahl der Glieder kann in verschiedenen Perioden verschieden sein, jedenfalls ist sie stets gerade*).

*) Von besonderem Interesse sind noch folgende Bemerkungen (*Gauss: D. A. artt. 187, 194*). Wenn (a, b, c) eine reducirte Form ist, so gilt Dasselbe von ihrem Gefährten (c, b, a) (§. 74); sind die Perioden dieser beiden Formen entwickelt, und die beiden Formen selbst nach den Plätzen, welche sie in diesen Perioden einnehmen, mit φ_μ und ψ_ν bezeichnet, so leuchtet

Beispiel 1: Wir haben (§. 75) das System der reducirten Formen für die Determinante $D = 13$ aufgestellt; nehmen wir z. B. für φ_0 die Form $(3, 1, -4)$, so erhalten wir folgende Periode von zehn Formen

$$\begin{aligned}\varphi_0 &= (3, 1, -4); \varphi_1 = (-4, 3, 1); \\ \varphi_2 &= (1, 3, -4); \varphi_3 = (-4, 1, 3); \\ \varphi_4 &= (3, 2, -3); \varphi_5 = (-3, 1, 4); \\ \varphi_6 &= (4, 3, -1); \varphi_7 = (-1, 3, 4); \\ \varphi_8 &= (4, 1, -3); \varphi_9 = (-3, 2, 3).\end{aligned}$$

ein, dass auch $\varphi_{\mu+1}$ und $\psi_{\nu-1}$, allgemeiner je zwei Formen $\varphi_{\mu+h}$ und $\psi_{\nu-h}$ Gefährten sind, wo h jede beliebige ganze Zahl bedeutet. Hieraus geht hervor, dass beide Perioden aus gleich vielen Gliedern bestehen werden.

Es ist nun möglich, dass beide Perioden identisch sind, dass also ψ_{ν} selbst ein Glied in der Periode der Form φ_{μ} ist; und dann wird offenbar der Gefährte einer jeden Form dieser Periode ein Glied derselben Periode sein. Ist nun φ_r der Gefährte von φ_0 , so ist; weil die äusseren Coefficienten einer reducirten Form entgegengesetzte Vorzeichen, und ausserdem die ersten Coefficienten der auf einander folgenden Formen abwechselnde Vorzeichen haben, nothwendig r ungerade $= 2m - 1$; da nun φ_0 und φ_{2m-1} Gefährten sind, so gilt Dasselbe von φ_h und φ_{2m-1-h} , also auch von φ_m und φ_{m-1} , und ebenso, wenn $2n$ die Anzahl der Glieder der Periode bedeutet, von φ_{m+n} und $\varphi_{m-1-n} = \varphi_{m+n-1}$; bezeichnet man daher irgend eine der beiden Formen φ_m oder φ_{m+n} mit (A, B, C) , so ist die ihr nach links benachbarte Form identisch mit (C, B, A) , und folglich ist $2B \equiv 0 \pmod{A}$, d. h. φ_m und φ_{m+n} sind *ambige* Formen; und sie sind verschieden, weil m nicht $\equiv m+n \pmod{2n}$ ist.

Umgekehrt, ist in einer Periode eine ambige Form (A, B, C) enthalten, so ist ihr linker Nachbar ihr Gefährte (C, B, A) , und folglich findet sich in derselben Periode noch eine zweite ambige Form. Ausser diesen beiden ambigen Formen φ_m und φ_{m+n} giebt es aber keine andere ambige Form in derselben Periode; denn, wenn φ_s eine ambige Form ist, so sind φ_{s-1} und φ_s , und folglich auch φ_{2s-1} und φ_0 Gefährten; mithin ist φ_{2s-1} identisch mit φ_{2m-1} , folglich $2s \equiv 2m \pmod{2n}$, also $s \equiv m$, oder $s \equiv m+n \pmod{2n}$.

Dieser Fall kann offenbar nur bei der Periode einer solchen Form eintreten (§§. 56, 58), welche ihrem Gefährten eigentlich und folglich sich selbst uneigentlich äquivalent ist, d. h. wenn die Form einer sogenannten *ambigen Classe* angehört. Dass umgekehrt jedes Mal, wenn diese Bedingung erfüllt ist, die Periode der Form auch ihren Gefährten und folglich zwei ambige Formen enthalten muss, ist eine unmittelbare Folge des weiter unten (§. 82) bewiesenen Hauptsatzes dieser ganzen Theorie. — Man vergleiche die Beispiele im Text.

Diese Rechnung geschieht am einfachsten auf folgende Art; um aus der reducirten Form (a, b, a') die ihr nach rechts benachbarte reducirte Form (a', b', a'') zu finden, braucht man nur ihren mittlern Coefficienten b' zu suchen, welcher durch die Bedingung $b' \equiv -b - a'\delta \equiv -b \pmod{a'}$ und die Nebenbedingungen

$$\lambda + 1 - (a') \leq b' \leq \lambda$$

stets vollständig bestimmt ist und durch den blossen Anblick der Form sogleich erkannt wird. In unserm Fall ist $\lambda = 3$; man findet daher den mittlern Coefficienten b' der Form φ_1 durch die Bedingungen

$$b' \equiv -1 \pmod{4}, \quad 0 \leq b' \leq 3,$$

nämlich $b' = 3$. Und nachdem so b' und $\delta = 1$ gefunden sind, ergibt sich

$$a'' = \frac{b'^2 - D}{a'} = a + (b - b')\delta,$$

also in unserm Fall $a'' = 1$. In derselben Weise ist fortzufahren, bis die erste Form φ_0 sich reproducirt; in unserm Beispiel wird der mittlere Coefficient von φ_{10} dadurch bestimmt, dass er $\equiv -2 \pmod{3}$ sein, und ausserdem nicht ausserhalb der Grenzen 1 und 3 liegen muss, woraus folgt, dass er $= 1$ ist; also wird φ_{10} identisch mit φ_0 .

Die so gefundenen zehn ursprünglichen Formen der ersten Art erschöpfen aber noch nicht alle reducirten Formen der Determinante 13; es bleiben noch zwei ursprüngliche Formen der zweiten Art übrig

$$\psi_0 = (2, 3, -2), \quad \psi_1 = (-2, 3, 2),$$

welche offenbar noch eine zweite Periode bilden.

Beispiel 2: Für $D = 19$ erhalten wir folgende zwei Perioden, jede von sechs Gliedern:

$$\varphi_0 = (3, 2, -5); \quad \varphi_1 = (-5, 3, 2)$$

$$\varphi_2 = (2, 3, -5); \quad \varphi_3 = (-5, 2, 3)$$

$$\varphi_4 = (3, 4, -1); \quad \varphi_5 = (-1, 4, 3)$$

und

$$\psi_0 = (-3, 2, 5); \quad \psi_1 = (5, 3, -2)$$

$$\psi_2 = (-2, 3, 5); \quad \psi_3 = (5, 2, -3)$$

$$\psi_4 = (-3, 4, 1); \quad \psi_5 = (1, 4, -3).$$