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_0179
LOG Titel: §. 160. Ganze algebraische Zahlen
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

Wir fügen diesen Entwicklungen endlich noch folgende leicht zu beweisende Bemerkungen hinzu. Die ausgeführte Form der Gleichung (32) oder (6) ist folgende

$$0 = H - \delta H \frac{\omega}{1} + \delta^2 H \frac{\omega^2}{1.2} - \delta^3 H \frac{\omega^3}{1.2.3} + \cdots; \quad (37)$$

es ist ferner

$$H = \Pi \omega = N(\omega), \quad (7)$$

wo das Productzeichen Π sich auf alle n Wurzeln ω bezieht; ebenso findet man (wenn man in (3) d durch δ' ersetzt)

$$H = \omega \omega', \quad (8)$$

wo

$$\omega' = \delta' \omega = \Sigma h_i' \omega_i \quad (38)$$

zu ω adjungirt ist, und

$$S = \Sigma \omega, \quad 2T = \Sigma \omega^2, \quad (39)$$

wo die Summenzeichen sich ebenfalls auf alle n Wurzeln beziehen. Die quadratische Form T ist charakteristisch für die Anzahl der reellen Wurzeln; bildet man ferner die Hesse'sche Determinante des Productes $H = \Pi \omega$, so ergiebt sich durch Vergleichung mit (29) die Discriminante

$$\Delta(\omega_1, \omega_2 \ldots \omega_n) = \Sigma \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}, \quad (40)$$

was auch unmittelbar aus (39) folgt.

§. 160.

Der Inbegriff *aller* algebraischen Zahlen bildet offenbar ebenfalls einen Körper*). Wir wollen nun, indem wir unserem eigent-

*) Dass es ausser den algebraischen noch andere, sogenannte *transcendente* Zahlen giebt, ist meines Wissens zuerst von *Liouville* bewiesen (*Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques;* Journ. de Math. T. XVI. 1851). Man vermuthet, dass die Ludolph'sche Zahl π eine solche transcendente Zahl ist; allein selbst die als specieller Fall hierin enthaltene Behauptung, dass die Quadratur des Zirkels unmöglich sei, ist bis auf den heutigen Tag noch nicht erwiesen. (Vergl. *Euler: De relatione inter ternas pluresve quantitates instituenda.* §. 10. Opusc. anal. T. II. 1785.)

lichen Gegenstande näher treten, eine Zahl α eine *ganze algebraische Zahl* nennen, wenn sie die Wurzel einer Gleichung ist, deren Coefficienten rationale ganze Zahlen sind, wobei wir ein- für allemal bemerken, dass wir unter den *Coefficienten* einer Function $m$ten Grades

$$F(x) = cx^m + c_1 x^{m-1} + c_2 x^{m-2} + \cdots + c_m$$

oder der Gleichung $F(x) = 0$ stets die m Quotienten

$$-\frac{c_1}{c}, \quad +\frac{c_2}{c} \cdots (-1)^m \frac{c_m}{c}$$

verstehen. Aus dieser Erklärung folgt zunächst, dass eine rationale Zahl stets und nur dann eine ganze algebraische Zahl ist, wenn sie eine ganze Zahl im gewöhnlichen Sinne des Wortes ist (vergl. §. 5, 4.); diese Zahlen wollen wir von jetzt ab *rationale ganze Zahlen*, alle algebraischen ganzen Zahlen aber kurz *ganze Zahlen* nennen. Dieses vorausgeschickt, schreiten wir zum Beweise der folgenden Fundamentalsätze.

1. *Die Summe, die Differenz und das Product zweier ganzen Zahlen α, β sind wieder ganze Zahlen.*

Sind a, b resp. die Grade der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$, deren Coefficienten rationale ganze Zahlen sind, und bezeichnet man mit $\omega_1, \omega_2 \ldots \omega_n$ die sämmtlichen ab Producte von der Form $\alpha^{a'}\beta^{b'}$, wo a' irgend eine der Zahlen $0, 1, 2 \ldots (a-1)$, und b' irgend eine der Zahlen $0, 1, 2 \ldots (b-1)$ bedeutet, so wird, wenn $\omega = \alpha + \beta$, oder $= \alpha - \beta$, oder $= \alpha\beta$ ist, jedes der n Producte $\omega\omega_1, \omega\omega_2 \ldots \omega\omega_n$ mit Zuziehung der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ auf die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ gebracht werden können, wo $r_1, r_2 \ldots r_n$ rationale ganze Zahlen sind. Eliminirt man die n Grössen $\omega_1, \omega_2 \ldots \omega_n$ aus diesen n Gleichungen, so ergiebt sich für ω eine Gleichung vom $n$ten Grade (wie (6) in §. 159), deren Coefficienten rationale ganze Zahlen sind, was zu beweisen war (vergl. §. 139).

2. Die ganze Zahl α heisst *theilbar* durch die ganze Zahl β, oder ein *Multiplum* von β, wenn der Quotient $\alpha : \beta$ ebenfalls eine ganze Zahl ist; umgekehrt heisst β ein *Divisor* oder *Theiler* von α (vergl. §. 3). Ebenso setzen wir $\alpha \equiv \beta \pmod{\gamma}$, wenn $\alpha - \beta$ durch γ theilbar ist, und nennen α, β *congruent nach dem Modul γ* (vergl. §. 17). Man erkennt sofort (zufolge 1.), dass die Sätze des §. 3 und auch die des §. 17 (mit *vorläufiger* Ausnahme von 6. und 8.; vergl. §. 164, 3.) ihre Gültigkeit behalten.

3. *Jede Wurzel ω einer Gleichung, deren Coefficienten ganze Zahlen sind, ist ebenfalls eine ganze Zahl.*

Ist ω die Wurzel einer Gleichung $m$ten Grades $F(\omega) = 0$, deren Coefficienten $\alpha, \beta \ldots$ ganze Zahlen sind, sind ferner $a, b \ldots$ resp. die Grade der mit rationalen ganzen Coefficienten behafteten Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0 \ldots$, so führe man die sämmtlichen $m\,a\,b \ldots$ Producte $\omega_1, \omega_2 \ldots \omega_n$ von der Form $\omega^{m'} \alpha^{a'} \beta^{b'} \ldots$ ein, wo die ganzen rationalen Exponenten den Bedingungen $0 \leqq m' < m$, $0 \leqq a' < a$, $0 \leqq b' < b \ldots$ genügen; dann lässt sich vermöge der Gleichungen $F(\omega) = 0$, $\varphi(\alpha) = 0$, $\psi(\beta) = 0 \ldots$ jedes der n Producte $\omega\omega_1$, $\omega\omega_2 \ldots \omega\omega_n$ wieder in die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ bringen, wo $r_1, r_2 \ldots r_n$ rationale ganze Zahlen bedeuten, und hieraus folgt unmittelbar die Richtigkeit des Satzes.

Ist daher z. B. α eine ganze Zahl, und r eine beliebige (ganze oder gebrochene) *positive* rationale Zahl, so ist auch α^r eine ganze Zahl (vergl. §. 5, 4.).

4. Bekanntlich lassen sich die Begriffe der Theilbarkeit und des Vielfachen von den ganzen rationalen Zahlen unmittelbar auf die ganzen rationalen Functionen übertragen, und es giebt einen Algorithmus zur Auffindung des grössten gemeinschaftlichen Divisors $\varphi(x)$ zweier gegebenen Functionen $F(x), f(x)$, welcher demjenigen der Zahlentheorie (§. 4) vollständig analog ist. Sind die Coefficienten von $F(x)$ und $f(x)$ sämmtlich in einem Körper K enthalten, so werden auch die Coefficienten von $\varphi(x)$ Zahlen des Körpers K sein, weil sie durch Addition, Multiplication, Subtraction und Division aus den Coefficienten von $F(x)$ und $f(x)$ entstehen. Hieraus folgt leicht, dass, wenn α die Wurzel einer solchen Gleichung $F(\alpha) = 0$ ist, deren Coefficienten Zahlen des Körpers K sind, nothwendig auch eine solche Gleichung $\varphi(\alpha) = 0$ von *niedrigstem Grade* existiren muss, welche *irreductibel in K* heissen soll und welche offenbar keine anderen Wurzeln besitzen, kann als die Gleichung $F(\alpha) = 0$. Hieraus folgt der Satz:

Ist α eine ganze Zahl, und K ein bestimmter Körper, so sind alle Coefficienten der in K irreductibelen Gleichung $\varphi(\alpha) = 0$ ganze Zahlen.

Denn weil α eine ganze Zahl, also die Wurzel einer Gleichung $F(\alpha) = 0$ ist, deren Coefficienten rationale ganze Zahlen und folg-

lich auch Zahlen des Körpers K sind (§. 159), so kann die in K irreductibele Gleichung $\varphi(\alpha) = 0$, welcher α genügt, nur ganze Zahlen zu Wurzeln haben; da aber die Coefficienten einer Gleichung durch Addition und Multiplication aus ihren Wurzeln entstehen, so sind (zufolge 1.) auch die Coefficienten der Gleichung $\varphi(\alpha) = 0$ ganze Zahlen, was zu beweisen war.

Der einfachste Fall, in welchem K der Körper der rationalen Zahlen ist, findet sich bei *Gauss**).

5. *Ist ϱ irgend eine algebraische Zahl, so giebt es immer unendlich viele (von Null verschiedene) rationale ganze Zahlen h von der Beschaffenheit, dass $h\varrho$ eine ganze Zahl wird, und zwar stimmen diese sämmtlichen Zahlen h mit den sämmtlichen rationalen Vielfachen der kleinsten unter ihnen überein.*

Da ϱ eine algebraische Zahl, also die Wurzel einer Gleichung von der Form

$$c\varrho^m + c_1\varrho^{m-1} + c_2\varrho^{m-2} + \cdots + c_m = 0$$

ist, wo $c, c_1, c_2 \ldots c_m$ rationale ganze Zahlen bedeuten, so ergiebt sich durch Multiplication mit c^{m-1}, dass $c\varrho$ eine ganze Zahl ist. Sind ferner $a\varrho$, $b\varrho$ ganze Zahlen, wo a, b rationale ganze Zahlen bedeuten, deren grösster gemeinschaftlicher Theiler $= h$ ist, so folgt leicht (aus 1. und §. 4), dass auch $h\varrho$ eine ganze Zahl ist. Hieraus ergiebt sich unmittelbar der zu beweisende Satz.

6. Versteht man unter einer *Einheit* eine ganze Zahl ε, welche in *allen* ganzen Zahlen aufgeht, so ist zunächst erforderlich, dass sie auch in 1 aufgeht, dass also $1 = \varepsilon\varepsilon'$, und ε' eine ganze Zahl ist; wenn nun

$$\varepsilon^m + c_1\varepsilon^{m-1} + \cdots + c_m = 0$$

die im Körper der rationalen Zahlen irreductibele Gleichung ist, welcher ε genügt, so muss (zufolge 4.) $c_m = \pm 1$ sein, weil ε' der ebenfalls irreductibelen Gleichung

$$c_m\varepsilon'^m + c_{m-1}\varepsilon'^{m-1} + \cdots + c_1\varepsilon' + 1 = 0$$

genügt; umgekehrt, ist dies der Fall, so geht ε in 1 und folglich in allen ganzen Zahlen auf, ist also eine Einheit. Die Anzahl der Einheiten ist offenbar unbegrenzt.

Ist α theilbar durch α', und sind ε, ε' irgend welche Einheiten, so ist offenbar auch $\varepsilon\alpha$ durch $\varepsilon'\alpha'$ theilbar; hinsichtlich der Theilbarkeit verhalten sich daher alle Zahlen $\varepsilon\alpha$, welche den sämmt-

*) *D. A.* art. 42.

lichen Einheiten ε entsprechen, genau wie α. Zwei ganze Zahlen, deren Quotient keine Einheit ist, wollen wir *wesentlich verschieden* nennen.

7. Will man nun den Begriff der *Primzahl* so fassen, dass sie ausser sich selbst und den Einheiten keine wesentlich verschiedene Theiler besitzt und auch selbst keine Einheit ist, so erkennt man sofort, dass gar keine solche Zahl existirt; ist nämlich α eine ganze Zahl, aber keine Einheit, so besitzt sie immer unendlich viele wesentlich verschiedene Divisoren, z. B. die Zahlen $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$, $\sqrt[4]{\alpha}$ u. s. f., welche (zufolge 3.) ganze Zahlen sind.

Dagegen lässt sich der Begriff von *relativen Primzahlen* vollständig definiren, und diese Frage wird uns überhaupt auf den richtigen Weg leiten, welcher bei den ferneren Untersuchungen einzuschlagen ist. Da von einem grössten gemeinschaftlichen Theiler zweier ganzen Zahlen *vorläufig* (vergl. §. 164, 3.) nicht gesprochen werden kann, so ist es auch unmöglich, die Definition von relativen Primzahlen so zu fassen, wie sie in der Theorie der rationalen Zahlen aufgestellt wird (§. 5); aber aus dieser Definition ergaben sich mehrere Sätze, deren jeder umgekehrt das Verhalten zweier relativen Primzahlen vollständig charakterisirt, ohne die Kenntniss ihrer sämmtlichen Divisoren vorauszusetzen. Ein solcher Satz ist z. B. der folgende (§. 7): Sind a, b relative Primzahlen, so ist jede durch a und b theilbare Zahl auch durch ab theilbar. Dieser Satz lässt sich in der That umkehren: Ist jede durch a und b theilbare Zahl auch durch ab theilbar, so sind a, b relative Primzahlen. Hätten nämlich die beiden Zahlen $a = ha'$, $b = hb'$ einen gemeinschaftlichen Theiler $h > 1$, so wäre $ha'b'$ eine durch a und b, aber nicht durch ab theilbare Zahl.

Diese Betrachtung veranlasst uns, folgende für das Gebiet aller ganzen algebraischen Zahlen gültige Erklärung aufzustellen:

Zwei von Null verschiedene ganze Zahlen α, β heissen relative Primzahlen, wenn jede durch α und β theilbare Zahl auch durch $\alpha\beta$ theilbar ist.

Vor Allem bemerken wir, dass zwei relative Primzahlen im alten Sinne des Wortes, d. h. zwei rationale ganze Zahlen a, b, deren grösster gemeinschaftlicher Divisor $= 1$ ist, auch im neuen Sinne relative Primzahlen bleiben; ist nämlich eine ganze algebraische Zahl γ theilbar durch a und b, so ist der Quotient $\varrho = \gamma : ab$ eine algebraische Zahl der Art, dass $a\varrho$ und $b\varrho$ ganze Zahlen sind; mithin muss (zufolge 5.) auch ϱ eine ganze Zahl, also γ theilbar durch

ab sein, was zu beweisen war. Dass ferner umgekehrt zwei relative Primzahlen im neuen Sinne des Wortes, welche zugleich rational sind, auch relative Primzahlen im alten Sinne sind, versteht sich zufolge der der neuen Erklärung vorausgeschickten Erörterung von selbst.

Wir nennen ferner die ganzen Zahlen $\alpha, \beta, \gamma, \delta \ldots$ kurz relative Primzahlen, wenn jede von ihnen relative Primzahl zu jeder der andern ist (vergl. §. 6); ist dann eine ganze Zahl ω durch jede von ihnen theilbar, so ist sie auch durch ihr Product theilbar (vergl. §. 7), weil, wie man leicht findet, auch der folgende Satz (§. 5, 3.) seine Gültigkeit behält: Ist jede der Zahlen $\alpha', \beta', \gamma' \ldots$ relative Primzahl zu jeder der Zahlen $\alpha'', \beta'', \gamma'', \delta'' \ldots$, so sind auch die Producte $\alpha'\beta'\gamma' \ldots$ und $\alpha''\beta''\gamma''\delta'' \ldots$ relative Primzahlen und umgekehrt.

Aber wie soll man definitiv entscheiden, ob zwei gegebene ganze Zahlen α, β relative Primzahlen sind? Man könnte versuchen, folgenden Weg einzuschlagen. Da α^{-1} und β^{-1} algebraische Zahlen sind, so giebt es (zufolge 5.) immer zwei kleinste positive ganze rationale Zahlen a, b von der Art, dass $a\alpha^{-1}$ und $b\beta^{-1}$ ganze Zahlen, d. h. dass a, b resp. durch α, β theilbar werden; zeigt sich nun, dass a, b relative Primzahlen sind, so sind auch α, β gewiss relative Primzahlen. Aber man muss sich hüten zu glauben, dass auch das Umgekehrte Statt findet, dass also die *kleinsten rationalen Multipla* a, b von zwei relativen Primzahlen α, β nothwendig selbst relative Primzahlen sein müssen. So z. B. sind in der That die beiden conjugirten Zahlen $\alpha = 2 + i$ und $\beta = 2 - i$ relative Primzahlen, und doch ist $a = b = 5$. Eine wesentliche Reduction unserer Aufgabe wird aber durch den folgenden Satz bewirkt:

Wenn zwei ganze Zahlen α, β sich in einem Körper K, dem sie selbst angehören, als relative Primzahlen bewähren, d. h. wenn jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist; so sind α, β wirklich relative Primzahlen.

Ist nämlich ω irgend eine durch α und durch β theilbare ganze Zahl, und ist

$$\omega^m + \gamma_1 \omega^{m-1} + \gamma_2 \omega^{m-2} + \cdots + \gamma_m = 0$$

die in K irreductibele Gleichung, welcher ω genügt, so sind (zufolge 4.) die Zahlen $\gamma_1, \gamma_2 \ldots \gamma_m$ ganze Zahlen des Körpers K; da ferner