Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Werk Id: PPN30976923X

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN30976923X|LOG_0181

OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

Contact

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

wo zufolge (5)

$$h'_r = h_r + a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \cdots + a_r^{(n)} x_n$$

ist, und hieraus folgt, dass man successive die willkürlichen rationalen ganzen Zahlen $x_n, x_{n-1} \ldots x_2, x_1$ stets und nur auf eine einzige Art so bestimmen kann, dass die n Zahlen h'_r den Bedingungen

$$0 \leqq h'_r < a_r^{(r)} \tag{7}$$

genügen. In jeder Classe existirt daher ein und nur ein *Repräsentant* ω' von der Form (6), welcher diesen Bedingungen (7) genügt; mithin ist die *Anzahl* der verschiedenen Classen (mod. $\mathfrak{a}$), aus welchen der Modul $\mathfrak{o}$ besteht, gleich dem Producte $a'_1 a''_2 \ldots a_n^{(n)}$, d. h. gleich der *Determinante* des Coefficientensystems in den n particulären Zahlen α_r von der Form (3), welche eine Basis von $\mathfrak{a}$ bilden *).

§. 162.

Wir beschränken uns von jetzt an auf die Untersuchung der ganzen Zahlen, welche in einem endlichen Körper Ω (§. 159) enthalten sind.

1. Da jede algebraische Zahl (zufolge §. 160, 5.) durch Multiplication mit einer rationalen ganzen von Null verschiedenen Zahl in eine ganze Zahl verwandelt werden kann, so dürfen wir annehmen, dass die Zahlen $\omega_1, \omega_2 \ldots \omega_n$, welche eine Basis des Körpers Ω bilden, sämmtlich *ganze* Zahlen sind, und es wird dann (zufolge §. 160, 1.) jede Zahl

$$\omega = \sum h_\iota \omega_\iota \tag{1}$$

gewiss eine ganze Zahl sein, wenn ihre Coordinaten h_ι rationale ganze Zahlen sind; aber dies lässt sich im Allgemeinen nicht umkehren, d. h. es kann ω sehr wohl eine ganze Zahl sein, auch wenn ihre Coordinaten theilweise oder sämmtlich gebrochene Zahlen

*) Die weitere Entwicklung der allgemeinen Theorie der Moduln würde uns hier zu weit führen (vergl. §. 163); wir erwähnen nur noch folgenden Satz: Sind die Basiszahlen eines endlichen Moduls von einander abhängig, so giebt es immer eine aus unabhängigen Zahlen bestehende Basis desselben Moduls. Die eleganteste Methode, die neue Basis aufzufinden, besteht in einer Verallgemeinerung der von *Gauss* angewandten Behandlung der partialen Determinanten (*D. A.* artt. 234, 236, 279).

sind. Dies ist einer der wichtigsten Puncte der Theorie und muss deshalb vor Allem aufgeklärt werden.

Wir schicken zunächst die einleuchtende Bemerkung voraus, dass die Discriminante (§. 159, (10)) eines jeden Systems von n unabhängigen ganzen Zahlen gewiss eine von Null verschiedene rationale und zwar *ganze* Zahl ist, weil sie durch Addition, Subtraction und Multiplication aus lauter ganzen Zahlen gebildet ist. Giebt es nun wirklich in Ω eine *ganze* Zahl

$$\beta = \frac{\sum k_\iota \omega_\iota}{s} \tag{2}$$

wo $s, k_1, k_2 \ldots k_n$ ganze rationale Zahlen ohne gemeinschaftlichen Theiler bedeuten, deren erste $s \geqq 1$ ist, so behaupten wir, dass s^2 in der Discriminante $\Delta(\omega_1, \omega_2 \ldots \omega_n)$ aufgeht, und dass man eine neue Basis von ganzen Zahlen $\beta_1, \beta_2 \ldots \beta_n$ aufstellen kann, deren Discriminante absolut genommen $< \Delta(\omega_1, \omega_2 \ldots \omega_n)$ ist.

Um dies zu beweisen, bezeichnen wir mit $\mathfrak{m}$ den aus allen durch s theilbaren ganzen Zahlen bestehenden Modul, ebenso mit $\mathfrak{o}$ das System aller Zahlen ω von der Form (1), deren Coordinaten h_ι *ganze* Zahlen sind; da jedes Product $s\omega$ eine Zahl des Moduls $\mathfrak{m}$ ist, so können wir die allgemeine Untersuchung des vorigen Paragraphen auf unsern Fall anwenden. Alle durch s theilbaren Zahlen α des Systems $\mathfrak{o}$ sind daher von der Form

$$\alpha = \sum x_\iota \alpha_\iota = s \sum x_\iota \beta_\iota,$$

wo die n Zahlen $\alpha_\iota = s\beta_\iota$ particuläre Zahlen α, also die β_ι *ganze* Zahlen des Körpers Ω, und die x_ι willkürliche rationale ganze Zahlen bedeuten.

Da nun alle Zahlen $s\omega$ auch solche Zahlen α sind, so kann man

$$\omega_r = \sum b_\iota^{(r)} \beta_\iota, \quad \Delta(\omega_1, \omega_2 \ldots \omega_n) = b^2 \Delta(\beta_1, \beta_2 \ldots \beta_n)$$

setzen, wo die Coefficienten $b_\iota^{(r)}$ rationale ganze Zahlen sind, und b die aus ihnen gebildete Determinante bedeutet; durch Umkehrung ergiebt sich, dass die n Producte $b\beta_\iota$, mithin auch alle Quotienten $b\alpha : s$ *Zahlen des Systems* $\mathfrak{o}$ sind.

Wenden wir dies Resultat auf die obige Voraussetzung (2) an, dass die Zahl β eine ganze Zahl, ihr Zähler $\sum k_\iota \omega_\iota$ also eine Zahl α ist, obgleich die Zahlen $s, k_1, k_2 \ldots k_n$ keinen gemeinschaftlichen Theiler haben, so folgt unmittelbar, dass b *durch* s *theilbar* ist, wodurch zugleich die obigen Behauptungen erwiesen sind.

Da nun die Discriminante eines jeden Systems von n unabhängigen ganzen Zahlen des Körpers Ω eine von Null verschiedene ganze rationale Zahl ist, so giebt es unter allen diesen Discriminanten eine solche, deren Werth — abgesehen vom Vorzeichen — ein *Minimum* ist, und aus der vorstehenden Untersuchung folgt unmittelbar, dass, wenn eine Basis aus solchen ganzen Zahlen $\omega_1, \omega_2 \ldots \omega_n$ besteht, deren Discriminante diesen Minimumwerth besitzt, die entsprechenden Coordinaten h_ι einer jeden *ganzen* Zahl ω des Körpers nothwendig *ganze* rationale Zahlen sein müssen. Eine solche Basis $\omega_1, \omega_2 \ldots \omega_n$ wollen wir eine *Grundreihe* des Körpers Ω nennen; aus ihr ergeben sich alle anderen Grundreihen desselben Körpers, wenn man n ganze Zahlen ω von der Form (1) so wählt, dass die aus den n^2 zugehörigen Coordinaten gebildete Determinante $= \pm 1$ wird.

Die wichtigste Rolle spielt aber die Minimaldiscriminante selbst, sowohl hinsichtlich der inneren*) Constitution des Körpers Ω, als auch hinsichtlich seiner Verwandtschaft mit anderen Körpern**); wir wollen daher diese positive oder negative ganze rationale Zahl die *Grundzahl* oder die *Discriminante des Körpers* Ω nennen und mit $\Delta(\Omega)$ bezeichnen; sie ist offenbar zugleich die Grundzahl eines jeden mit Ω conjugirten Körpers.

Die Zahlen eines quadratischen Körpers sind z. B. von der Form $t + u\sqrt{D}$, wo t, u alle rationalen Zahlen durchlaufen, und D eine ganze rationale Zahl bedeutet, welche kein Quadrat und auch durch kein Quadrat ausser 1 theilbar ist. Ist $D \equiv 1 \pmod 4$, so bilden die Zahlen 1 und $\frac{1}{2}(1 + \sqrt{D})$ eine Grundreihe des Körpers, und seine Grundzahl ist $= D$; ist dagegen $D \equiv 2$ oder $\equiv 3 \pmod 4$, so bilden die Zahlen 1 und $\sqrt{D}$ eine Grundreihe des Körpers, und seine Grundzahl ist $= 4D$.

---

*) Vergl. *Kronecker: Ueber die algebraisch auflösbaren Gleichungen* (Monatsbericht der Berliner Ak. 14. April 1856).

**) Die erste Spur dieser Beziehungen hat sich bei einer schönen Untersuchung von *Kronecker* gezeigt (*Mémoire sur les facteurs irréductibles de l'expression* $x^n - 1$; Journ. de Math., p. p. Liouville; T. XIX. 1854). Um den Charakter dieser Gesetze, deren Entwicklung ich mir auf eine andere Gelegenheit verspare, näher anzudeuten, führe ich nur das einfachste Beispiel an: das kleinste gemeinschaftliche Multiplum zweier von einander verschiedenen quadratischen Körper A, B ist ein biquadratischer Körper K, der noch einen dritten quadratischen Körper C zum Divisor hat; die Grundzahl von K ist gleich dem Product aus den Grundzahlen von A, B, C, und zwar eine Quadratzahl.

Ist ferner θ eine primitive Wurzel der Gleichung $\theta^m = 1$ (§. 139), wo $m > 2$, so bilden die Zahlen $1, \theta, \theta^2 \ldots \theta^{n-1}$ die Grundreihe eines Körpers vom Grade $n = \varphi(m)$, dessen Grundzahl

$$\left(\frac{m\sqrt{-1}}{\sqrt[a-1]{a}\,\sqrt[b-1]{b}\,\sqrt[c-1]{c}\ldots}\right)^n$$

ist, wo $a, b, c \ldots$ alle verschiedenen in m aufgehenden Primzahlen bedeuten. Ist $m = 3$ (oder $= 6$), so ist dieser Körper ein quadratischer, seine Grundzahl $= -3$; ist $m = 4$, so ist die Grundzahl des quadratischen Körpers $= -4$.

2. Aus den vorstehenden Principien ergiebt sich leicht der folgende Fundamentalsatz:

Ist μ eine von Null verschiedene ganze Zahl des Körpers Ω, so ist die Anzahl der nach dem Modul μ incongruenten ganzen Zahlen des Körpers gleich dem absoluten Werth der Norm des Moduls μ.

Es sei $\mathfrak{m}$ das System aller durch μ theilbaren ganzen Zahlen (welche sich durch Addition und Subtraction reproduciren), und $\mathfrak{o}$ das System *aller* ganzen Zahlen des Körpers Ω, d. h. aller Zahlen ω von der Form (1), wo die Zahlen ω_ι eine *Grundreihe* des Körpers bilden, und die Coordinaten h_ι beliebige ganze rationale Zahlen bedeuten; da jeder Quotient $\omega : \mu$ (zufolge §. 160, 5.) durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl in eine ganze Zahl verwandelt werden kann, so ist die Untersuchung des vorigen Paragraphen auf unsern Fall anwendbar. Mithin sind alle durch μ theilbaren Zahlen α des Systems $\mathfrak{o}$ von der Form

$$\alpha = \Sigma x_\iota \alpha_\iota = \mu \Sigma x_\iota \beta_\iota,$$

wo die n Zahlen $\alpha_\iota = \mu\beta_\iota$ particuläre Zahlen α bedeuten, also die Zahlen β_ι in $\mathfrak{o}$ enthalten sind, und die Grössen x_ι alle rationalen ganzen Zahlwerthe annehmen dürfen; die Anzahl der *Classen*, in welche das System $\mathfrak{o}$ in Bezug auf den Modul μ zerfällt, ist ferner gleich der aus den Coordinaten der n Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ gebildeten Determinante a. Zugleich ist (nach §. 159, (11), (12))

$$\Delta(\alpha_1 \ldots \alpha_n) = a^2 \Delta(\Omega) = N(\mu)^2 \Delta(\beta_1 \ldots \beta_n);$$

da nun jede durch μ theilbare Zahl $\alpha = \mu\omega$ des Systems $\mathfrak{o}$ die Form $\mu \Sigma x_\iota \beta_\iota$ besitzt, so ist jede Zahl ω des Systems $\mathfrak{o}$ auch von der Form $\Sigma x_\iota \beta_\iota$; mithin bilden die Zahlen β_ι ebenfalls eine *Grund-*

reihe des Körpers, und folglich ist $\Delta(\beta_1 \ldots \beta_n) = \Delta(\Omega)$, also $a = \pm N(\mu)$, was zu beweisen war.

Zugleich leuchtet ein, dass nach der Methode des vorigen Paragraphen ein System von a incongruenten Repräsentanten der verschiedenen Classen, also ein *vollständiges Restsystem für den Modul* μ aufgestellt werden kann*).

3. Will man jetzt zwei gegebene ganze Zahlen θ, μ darauf prüfen, ob sie relative Primzahlen sind, so braucht man offenbar ω nur ein vollständiges Restsystem (mod. μ) durchlaufen zu lassen und nachzusehen, wie oft $\theta\omega \equiv 0 \pmod{\mu}$ wird; zeigt sich, dass dies nur dann eintritt, wenn $\omega \equiv 0 \pmod{\mu}$ ist, so ist also jede durch θ und μ theilbare ganze Zahl $\theta\omega$ auch theilbar durch $\theta\mu$, mithin sind θ, μ relative Primzahlen; besitzt aber die Congruenz $\theta\omega \equiv 0 \pmod{\mu}$ auch eine Wurzel ω, welche nicht $\equiv 0 \pmod{\mu}$ ist, so ist die entsprechende Zahl $\theta\omega$ durch θ und μ, aber nicht durch $\theta\mu$ theilbar, mithin sind θ, μ keine relative Primzahlen.

Ist θ relative Primzahl zu μ (z. B. $\theta = 1$), so durchläuft $\theta\omega$ gleichzeitig mit ω ein vollständiges Restsystem (mod. μ); folglich hat jede Congruenz $\theta\omega \equiv \theta' \pmod{\mu}$ immer eine und nur eine Wurzel ω (vergl. §. 22); ist ferner $\psi(\mu)$ die Anzahl aller Classen, deren Zahlen relative Primzahlen zum Modul μ sind, so durchläuft $\theta\omega$ gleichzeitig mit ω die Repräsentanten aller dieser Classen, und da das Product dieser Zahlen ω auch relative Primzahl zu μ ist, so ergiebt sich der Satz

$$\theta^{\psi(\mu)} \equiv 1 \pmod{\mu},$$

welcher dem Fermat'schen Satze (§. 19) entspricht.

4. Verfolgt man diese Analogie mit der rationalen Zahlentheorie weiter, so drängt sich immer wieder die Frage nach der Zusammensetzung der Zahlen des Systems $\mathfrak{o}$ (d. h. der ganzen Zahlen des Körpers Ω) aus Factoren auf, welche demselben System $\mathfrak{o}$ an-

*) Bilden die n Zahlen ω_ι *irgend* eine Basis des Körpers Ω, und ist $\mathfrak{o}$ das System aller der Zahlen ω von der Form (1), deren Coordinaten *ganze* Zahlen sind, so reproduciren sich die Zahlen des Systems $\mathfrak{o}$ durch Addition und Subtraction; nimmt man ferner an, dass sie sich auch durch Multiplication reproduciren, woraus zugleich folgt, dass sie *ganze* Zahlen sind, und nennt man zwei solche Zahlen ω, ω' stets und nur dann congruent in Bezug auf eine dritte solche Zahl μ, wenn der Quotient $(\omega - \omega') : \mu$ wieder eine Zahl des Systems $\mathfrak{o}$ ist, so ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach μ incongruenten Zahlen ebenfalls $= \pm N(\mu)$. Vergl. §. 165, 4.

gehören, und es zeigt sich zunächst, dass die unbegrenzte Zerlegbarkeit der ganzen Zahlen, wie sie in dem unendlichen Körper *aller* algebraischen Zahlen auftrat (§. 160, 7.), in einem endlichen Körper Ω wieder verschwindet. Dafür tritt aber bei unendlich vielen solchen Körpern Ω ein höchst eigenthümliches Phänomen auf, das schon früher (§. 16) gelegentlich erwähnt ist*). Nennt man eine Zahl in $\mathfrak{o}$ *zerlegbar*, wenn sie das Product aus zwei Zahlen in $\mathfrak{o}$ ist, welche beide keine Einheiten sind, dagegen *unzerlegbar*, wenn dies nicht der Fall ist, so ist offenbar jede zerlegbare Zahl μ darstellbar als Product aus einer *endlichen* Anzahl von unzerlegbaren Zahlen (vergl. §. 8), weil die Norm von μ gleich dem Producte aus den Normen der einzelnen Factoren ist (§. 159); aber es zeigt sich häufig, dass diese Zerlegung nicht eine vollkommen bestimmte ist, sondern dass mehrere *wesentlich verschiedene* Zerlegungen derselben Zahl in unzerlegbare Factoren existiren (§. 160, 6.). Dies widerspricht so sehr dem in der rationalen Zahlentheorie herrschenden Begriffe des Primzahlcharakters (§. 8), dass wir deshalb eine unzerlegbare Zahl als solche noch nicht als Primzahl anerkennen wollen; wir suchen daher für den wahren Primzahlcharakter ein kräftigeres Kriterium als diese unzulängliche Unzerlegbarkeit aufzustellen, ähnlich wie früher bei dem Begriffe der relativen Primzahl (§. 160, 7.), indem wir die zu untersuchende Zahl μ nicht zerlegen, sondern ihr Verhalten als *Modul*-betrachten:

Eine ganze Zahl μ, welche keine Einheit ist, soll eine Primzahl heissen, wenn jedes durch μ theilbare Product $\eta\varrho$ wenigstens einen durch μ theilbaren Factor η oder ϱ besitzt.

Es ergiebt sich dann sofort, dass die höchste in einem Producte aufgehende Potenz einer Primzahl μ das Product aus den höchsten in den einzelnen Factoren aufgehenden Potenzen von μ,

*) Das dortige Beispiel passt freilich nicht ganz hierher, insofern die ganzen Zahlen des der Gleichung $\varrho^2 = -11$ entsprechenden quadratischen Körpers nicht durch die Form $t + u\varrho$, wohl aber durch die Form $t + u\theta$ erschöpft werden, wo $2\theta = 1 + \varrho$ ist; die Zahlen 3, 5, $2 + \varrho$, $2 - \varrho$ sind in der That zerlegbar: $3 = \theta(1-\theta)$, $5 = (1+\theta)(2-\theta)$, $2 - \varrho = -\theta(1+\theta)$, $2 + \varrho = -(1-\theta)(2-\theta)$; die vier Zahlen θ, $1-\theta$, $1+\theta$, $2-\theta$ sind Primzahlen in diesem Körper. Die in Rede stehende Erscheinung tritt aber in dem der Gleichung $x^2 = -5$ entsprechenden quadratischen Körper an dem Beispiel $3 \cdot 7 = (1+2x)(1-2x)$ wirklich auf (vergl. §. 71; die beiden Zahlen 3, 7 sind durch die Hauptform der Determinante -5 nicht darstellbar).

und dass jede durch μ nicht theilbare Zahl relative Primzahl zu μ ist. Man erkennt ferner leicht, dass die kleinste durch μ theilbare rationale ganze Zahl p nothwendig eine Primzahl (im Körper der rationalen Zahlen), und folglich die Norm von μ eine Potenz von p, nämlich ein rationaler Divisor von $N(p) = p^n$ sein muss. Es werden daher gewiss alle Primzahlen μ des Körpers Ω entdeckt, wenn die Divisoren aller rationalen Primzahlen p aufgesucht werden.

5. Ist aber μ keine Primzahl (und auch keine Einheit), existiren also zwei durch μ nicht theilbare Zahlen η, ϱ, deren Product $\eta\varrho$ durch μ theilbar ist, so schreiten wir zu einer Zerlegung von μ in wirkliche oder *ideale*, d. h. fingirte Factoren. Giebt es nämlich in $\mathfrak{o}$ einen grössten gemeinschaftlichen Theiler ν der beiden Zahlen η und $\mu = \nu\mu'$, der Art, dass die Quotienten $\eta : \nu$ und $\mu : \nu$ relative Primzahlen sind, so ist μ in die beiden Factoren ν und μ' zerlegt, von denen keiner eine Einheit ist, weil weder ϱ noch η durch μ theilbar ist. Der Factor μ' ist wesentlich dadurch bestimmt, dass alle Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ durch μ' theilbar sind (z. B. auch $\alpha' = \varrho$), und dass ebenso jede durch μ' theilbare Zahl α' auch der vorstehenden Congruenz genügt. Umgekehrt, giebt es in $\mathfrak{o}$ eine Zahl μ', welche in allen Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ und nur in diesen aufgeht, so ist auch μ theilbar durch μ', und der Quotient $\nu = \mu : \mu'$ ist der grösste gemeinschaftliche Theiler der beiden Zahlen η und μ.

Aber es kann sehr wohl der Fall eintreten, dass in $\mathfrak{o}$ keine solche Zahl μ' zu finden ist; als nun diese Erscheinung (bei den aus Einheitswurzeln gebildeten Zahlen) *Kummer* entgegentrat, so kam er auf den glücklichen Gedanken, trotzdem eine solche Zahl μ' zu fingiren und dieselbe als *ideale Zahl* einzuführen; die *Theilbarkeit* einer Zahl α' durch diese ideale Zahl μ' besteht lediglich darin, dass α' eine Wurzel der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ ist, und da diese idealen Zahlen in der Folge immer nur als Theiler oder Moduln auftreten, so hat diese Art ihrer Einführung durchaus keine Bedenken. Allein die Befürchtung, dass die unmittelbare Uebertragung der bei den *wirklichen* Zahlen üblichen Benennungen auf die idealen Zahlen im Anfang leicht Misstrauen gegen die Sicherheit der Beweisführung einflössen könnte, veranlasst uns, die Untersuchung dadurch in ein anderes Gewand einzukleiden, dass wir immer ganze *Systeme* von wirklichen Zahlen betrachten.