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_0180
LOG Titel: §. 161. Theorie der Moduln
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

die ganzen Zahlen $\alpha' = \omega : \alpha$ und $\beta' = \omega : \beta$ resp. den in K irreductibelen Gleichungen

$$(\alpha\alpha')^m + \gamma_1(\alpha\alpha')^{m-1} + \cdots + \gamma_m = 0$$
$$(\beta\beta')^m + \gamma_1(\beta\beta')^{m-1} + \cdots + \gamma_m = 0$$

genügen, so sind (zufolge 4.) auch die Quotienten $\gamma_n : \alpha^n$ und $\gamma_n : \beta^n$ ganze Zahlen des Körpers K; da ferner nach Voraussetzung jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist, so ergiebt sich leicht, dass auch jede durch α^n und β^n theilbare Zahl γ_n des Körpers K durch $\alpha^n\beta^n$ theilbar, also von der Form $\alpha^n\beta^n\gamma'_n$ ist, wo γ'_n eine ganze Zahl bedeutet; setzt man nun $\omega = \alpha\beta\omega'$, so genügt ω' der Gleichung

$$\omega'^m + \gamma'_1\omega'^{m-1} + \cdots + \gamma'_m = 0,$$

deren Coefficienten ganze Zahlen sind; mithin ist ω' (zufolge 3.) eine ganze Zahl, d. h. ω ist auch theilbar durch $\alpha\beta$, was zu beweisen war.

Hieraus geht hervor, dass man, um das gegenseitige Verhalten zweier ganzen Zahlen α, β zu untersuchen, nur den kleinsten Körper K zu bilden braucht, welchem sie beide angehören; und dieser Körper ist, wie man leicht erkennt, immer von der im vorigen Paragraphen betrachteten Beschaffenheit.

§. 161.

Um den späteren Verlauf der Darstellung nicht zu unterbrechen, schalten wir hier eine sehr allgemeine Betrachtung ein, welche für die nachfolgenden, sowie für viele andere, unserem Gegenstande fremde Untersuchungen von grossem Nutzen ist.

1. Ein System $\mathfrak{a}$ von reellen oder complexen Zahlen α, deren *Summen* und *Differenzen* demselben System $\mathfrak{a}$ angehören, soll ein *Modul* heissen; wenn die Differenz zweier Zahlen ω, ω' in $\mathfrak{a}$ enthalten ist, so wollen wir sie *congruent nach* $\mathfrak{a}$ nennen und dies durch die Congruenz

$$\omega \equiv \omega' \pmod{\mathfrak{a}}$$

andeuten. Solche Congruenzen können addirt, subtrahirt und folglich auch mit beliebigen ganzen rationalen Zahlen multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen

auch einander congruent sind, so kann man alle existirenden Zahlen in *Classen* (mod. $\mathfrak{a}$) eintheilen, indem man je zwei congruente Zahlen in dieselbe Classe, je zwei incongruente in zwei verschiedene Classen aufnimmt.

2. Wenn alle Zahlen eines Moduls $\mathfrak{a}$ auch Zahlen eines Moduls $\mathfrak{b}$ sind, so heisse $\mathfrak{a}$ ein *Vielfaches* von $\mathfrak{b}$, und $\mathfrak{b}$ ein *Theiler* von $\mathfrak{a}$; oder wir sagen auch, $\mathfrak{b}$ gehe in $\mathfrak{a}$ auf, $\mathfrak{a}$ sei theilbar durch $\mathfrak{b}$. Aus jeder Congruenz $\omega \equiv \omega'$ (mod. $\mathfrak{a}$) folgt auch $\omega \equiv \omega'$ (mod. $\mathfrak{b}$). Offenbar *besteht* $\mathfrak{b}$ aus einer endlichen oder unendlichen Anzahl von Classen (mod. $\mathfrak{a}$).

Sind $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Moduln, so bilden alle die Zahlen, welche gleichzeitig in $\mathfrak{a}$ und in $\mathfrak{b}$ enthalten sind, das *kleinste* gemeinschaftliche Vielfache $\mathfrak{m}$ von $\mathfrak{a}$ und $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ auch durch den Modul $\mathfrak{m}$ theilbar ist. Durchläuft α alle Zahlen des Moduls $\mathfrak{a}$, β alle Zahlen des Moduls $\mathfrak{b}$, so bilden die Zahlen $\alpha + \beta$ den *grössten* gemeinschaftlichen Theiler von $\mathfrak{a}$ und $\mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}$ und $\mathfrak{b}$ auch in dem Modul $\mathfrak{b}$ aufgeht.

3. Sind $\omega_1, \omega_2 \ldots \omega_n$ gegebene Zahlen, so bilden alle Zahlen von der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n, \qquad (1)$$

wo $h_1, h_2 \ldots h_n$ alle ganzen rationalen Zahlen durchlaufen, einen *endlichen* Modul $\mathfrak{o}$, und wir wollen den Complex der n Zahlen $\omega_1, \omega_2 \ldots \omega_n$, mögen sie abhängig oder unabhängig von einander sein, eine *Basis* des Moduls $\mathfrak{o}$ nennen. Dann besteht folgender Satz:

Wenn alle Zahlen ω eines endlichen Moduls $\mathfrak{o}$ durch Multiplication mit rationalen, von Null verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{m}$ verwandelt werden können, so enthält $\mathfrak{o}$ nur eine endliche Anzahl incongruenter Zahlen (mod. $\mathfrak{m}$).

Da es nämlich n rationale, von Null verschiedene Zahlen r_1, $r_2 \ldots r_n$ der Art giebt, dass die Producte $r_1\omega_1$, $r_2\omega_2 \ldots r_n\omega_n$ in $\mathfrak{m}$ enthalten sind, so giebt es auch eine ganze rationale, von Null verschiedene Zahl s der Art, dass alle Producte $s\omega \equiv 0$ (mod. $\mathfrak{m}$) sind. Lässt man daher jede der n ganzen rationalen Zahlen $h_1, h_2 \ldots h_n$ ein vollständiges Restsystem (mod. s) durchlaufen, so entstehen s^n Zahlen ω von der Form (1), und jede Zahl des Moduls $\mathfrak{o}$ ist wenigstens einer derselben congruent (mod. $\mathfrak{m}$); mithin ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ incongruenten Zahlen *höchstens* $= s^n$, was zu beweisen war.

Allein es ist wichtig, die Anzahl dieser incongruenten Zahlen *genau* zu bestimmen. Zu diesem Zweck betrachten wir das kleinste gemeinschaftliche Vielfache $\mathfrak{a}$ der beiden Moduln $\mathfrak{o}$ und $\mathfrak{m}$; da je zwei nach $\mathfrak{m}$ congruente Zahlen ω, ω' des Modul $\mathfrak{o}$ auch nach $\mathfrak{a}$ congruent sind, und umgekehrt, so ist unsere Aufgabe die, die Anzahl der Classen (mod. $\mathfrak{a}$) zu bestimmen, aus welchen $\mathfrak{o}$ besteht. Wir suchen daher zunächst die allgemeine Form aller in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha = k_1\omega_1 + k_2\omega_2 + \cdots + k_n\omega_n \tag{2}$$

aufzustellen, wo $k_1, k_2 \ldots k_n$ jedenfalls ganze rationale Zahlen bedeuten. Ist nun r ein bestimmter Index aus der Reihe $1, 2 \ldots n$, so giebt es unter allen den Zahlen $\alpha = \theta_r$, in welchen $k_{r+1} = 0$, $k_{r+2} = 0 \ldots k_n = 0$ ist, auch solche, in denen k_r von Null verschieden ist (z. B. $s\,\omega_r$), und unter diesen sei

$$\alpha_r = a_1^{(r)}\omega_1 + a_2^{(r)}\omega_2 + \cdots + a_r^{(r)}\omega_r \tag{3}$$

eine solche, in welcher k_r den *kleinsten* positiven Werth $a_r^{(r)}$ besitzt. Dann leuchtet ein, dass der Werth von k_r in jeder Zahl θ_r durch $a_r^{(r)}$ theilbar, also von der Form $a_r^{(r)}x_r$ ist, wo x_r eine ganze rationale Zahl bedeutet, und dass folglich $\theta_r - x_r\alpha_r = \theta_{r-1}$ eine Zahl α ist, in welcher $k_r, k_{r+1} \ldots k_n$ verschwinden. Hieraus folgt sofort, dass, nachdem man für jeden Index r eine solche particuläre Zahl α_r des Moduls $\mathfrak{a}$ aufgestellt hat*), jede Zahl α gewiss in die Form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \tag{4}$$

gebracht werden kann, wo $x_1, x_2 \ldots x_n$ ganze rationale Zahlen bedeuten, aus welchen die in der Form (2) vorkommenden Zahlen $k_1, k_2 \ldots k_n$ durch die Gleichungen

$$k_r = a_r^{(r)}x_r + a_r^{(r+1)}x_{r+1} + \cdots + a_r^{(n)}x_n \tag{5}$$

abgeleitet werden; und umgekehrt sind alle Zahlen α von der Form (4) in $\mathfrak{a}$ enthalten.

Ist nun eine Zahl ω von der Form (1) gegeben, sind also $h_1, h_2 \ldots h_n$ gegebene rationale ganze Zahlen, so sind *alle* Zahlen ω' des Moduls $\mathfrak{o}$, welche ihr nach $\mathfrak{m}$ congruent sind, welche also eine Classe (mod. $\mathfrak{a}$) bilden, von der Form

$$\omega' = \omega + \alpha = h_1'\omega_1 + h_2'\omega_2 + \cdots + h_n'\omega_n, \tag{6}$$

---

*) Das System dieser n particulären Zahlen wird ein vollständig bestimmtes, wenn man die Bedingung hinzufügt, dass $0 \leq a_r^{(r')} < a_r^{(r)}$ sein soll, wenn $r' > r$ ist.