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_0183
LOG Titel: §. 164. Idealclassen und Composition derselben
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

lative Primideale werden; die sämmtlichen Zahlen des Ideals $\mathfrak{a}$ sind dann von der Form $\eta\omega + \eta'\omega'$, wo ω, ω' alle Zahlen in $\mathfrak{o}$ durchlaufen.

§. 164.

Wir gehen nun zu einer Eintheilung der Ideale des Körpers Ω in *Classen* über, welche auf folgenden Grundlagen beruht.

1. Das System E aller Hauptideale besitzt folgende fundamentale Eigenschaften*).

I. *Jedes Product aus zwei Idealen in E ist wieder ein Ideal in E.* Denn es ist $\mathfrak{i}(\eta)\,\mathfrak{i}(\eta') = \mathfrak{i}(\eta\eta')$.

II. *Sind $\mathfrak{e}$ und $\mathfrak{e}\mathfrak{e}'$ Ideale in E, so ist auch $\mathfrak{e}'$ ein Ideal in E.* Ist nämlich $\mathfrak{e} = \mathfrak{i}(\eta)$, $\mathfrak{e}\mathfrak{e}' = \mathfrak{i}(\eta'')$, so ist η'' theilbar durch η, also $\eta'' = \eta\eta'$, woraus $\mathfrak{e}' = \mathfrak{i}(\eta')$ folgt.

III. *Ist $\mathfrak{a}$ ein beliebiges Ideal, so gibt es immer ein Ideal $\mathfrak{m}$ der Art, dass $\mathfrak{a}\mathfrak{m}$ ein Ideal in E wird.* Denn es sei η irgend eine von Null verschiedene Zahl in $\mathfrak{a}$, so ist das Ideal $\mathfrak{e} = \mathfrak{i}(\eta)$ theilbar durch $\mathfrak{a}$, und folglich existirt (nach §. 163, 6. oder 7.) ein Ideal $\mathfrak{m}$, welches der Bedingung $\mathfrak{a}\mathfrak{m} = \mathfrak{e}$ genügt.

Wir nennen nun zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ *äquivalent*, wenn ein Ideal $\mathfrak{m}$ der Art existirt, dass beide Producte $\mathfrak{a}\mathfrak{m}$, $\mathfrak{a}'\mathfrak{m}$ dem System E angehören**). Sind ferner $\mathfrak{a}'$, $\mathfrak{a}''$ äquivalent, giebt es also ein Ideal $\mathfrak{m}'$ der Art, dass $\mathfrak{a}'\mathfrak{m}'$, $\mathfrak{a}''\mathfrak{m}'$ Ideale in E sind, so gehören, wenn $\mathfrak{a}'\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$ gesetzt wird, auch die Producte $\mathfrak{a}\mathfrak{m}'' = (\mathfrak{a}\mathfrak{m})(\mathfrak{a}'\mathfrak{m}')$ und $\mathfrak{a}''\mathfrak{m}'' = (\mathfrak{a}'\mathfrak{m})(\mathfrak{a}''\mathfrak{m}')$ dem System E an (zufolge I.), d. h. die

*) Diese drei Eigenschaften sind aber nicht charakteristisch für das System E der Hauptideale, sondern sie kommen auch anderen Systemen zu, für welche dann nothwendig dieselben Gesetze der Classification gelten. Giebt es z. B. in Ω keine Einheit, deren Norm $= -1$ ist, und nimmt man ein Ideal $\mathfrak{i}(\eta)$ nur dann in das System E auf, wenn $N(\eta)$ *positiv* ist, so hat auch dieses System E dieselben drei Eigenschaften (vergl. *Kronecker: Ueber die Classenanzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen;* Monatsber. d. Berliner Ak. 23. Juli 1863). Ebenso könnte man in E alle Ideale einer ganzen *Gruppe* von Classen aufnehmen, z. B. alle diejenigen, welche dem Hauptgeschlecht angehören.

**) Diese Definition kann offenbar auch durch die folgende ersetzt werden: zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ heissen äquivalent, wenn es zwei Ideale $\mathfrak{e}$, $\mathfrak{e}'$ in E giebt, welche der Bedingung $\mathfrak{a}\mathfrak{e}' = \mathfrak{a}'\mathfrak{e}$ genügen.

dem Ideale $\mathfrak{a}'$ äquivalenten Ideale $\mathfrak{a}$, $\mathfrak{a}''$ sind auch einander äquivalent. Hieraus allein folgt schon die Möglichkeit, alle Ideale in Classen einzutheilen: eine *Classe* ist der Inbegriff aller Ideale, welche einem bestimmten Ideal äquivalent sind.

Das System E selbst bildet eine solche Classe. Gehören nämlich $\mathfrak{e}$, $\mathfrak{e}'$, $\mathfrak{e}''$ diesem System an, so gilt (zufolge I.) dasselbe von den Producten $\mathfrak{e}\mathfrak{e}''$, $\mathfrak{e}'\mathfrak{e}''$, d. h. $\mathfrak{e}$, $\mathfrak{e}'$ sind äquivalent und gehören folglich in eine und dieselbe Classe. Sind umgekehrt $\mathfrak{e}$, $\mathfrak{e}'$ äquivalent, und gehört $\mathfrak{e}$ dem System E an, so gilt dasselbe von $\mathfrak{e}'$; denn, wenn $\mathfrak{e}$, $\mathfrak{e}\mathfrak{e}''$, $\mathfrak{e}'\mathfrak{e}''$ Ideale in E sind, so gehört (zufolge II.) auch $\mathfrak{e}''$, mithin auch $\mathfrak{e}'$ dem Systeme E an. Diese Classe E soll die *Hauptclasse* heissen.

Durchläuft nun $\mathfrak{a}$ alle Ideale einer Classe A, $\mathfrak{b}$ alle Ideale einer Classe B, so gehören alle Producte $\mathfrak{a}\mathfrak{b}$ einer und derselben Classe an, welche *aus A und B zusammengesetzt* heissen und mit AB bezeichnet werden soll; gehören nämlich $\mathfrak{a}\mathfrak{m}$, $\mathfrak{a}'\mathfrak{m}$, $\mathfrak{b}\mathfrak{n}$, $\mathfrak{b}'\mathfrak{n}$ der Hauptclasse E an, so gilt (zufolge I.) dasselbe von $(\mathfrak{a}\mathfrak{b})(\mathfrak{m}\mathfrak{n}) = (\mathfrak{a}\mathfrak{m})(\mathfrak{b}\mathfrak{n})$ und $(\mathfrak{a}'\mathfrak{b}')(\mathfrak{m}\mathfrak{n}) = (\mathfrak{a}'\mathfrak{m})(\mathfrak{b}'\mathfrak{n})$. Offenbar ist $AB = BA$, $(AB)C = A(BC)$ u. s. w. (vergl. §. 147).

Ist $\mathfrak{a}$ ein beliebiges Ideal, $\mathfrak{e}$ ein Ideal in E, so sind $\mathfrak{a}$ und $\mathfrak{a}\mathfrak{e}$ äquivalent; gehört nämlich $\mathfrak{a}\mathfrak{m}$ dem System E an, so gilt dasselbe von $(\mathfrak{a}\mathfrak{e})\mathfrak{m} = (\mathfrak{a}\mathfrak{m})\mathfrak{e}$. Hieraus folgt $AE = A$ (vergl. §. 148, 1.).

Da ferner jedes gegebene Ideal $\mathfrak{a}$ (zufolge III.) durch Multiplication mit einem Ideal $\mathfrak{m}$ in ein Ideal der Hauptclasse E verwandelt werden kann, so gehört zu jeder gegebenen Classe A auch eine *entgegengesetzte* Classe M (oder A^{-1}) der Art, dass $AM = E$ wird, und zwar nur eine einzige, weil aus $AM' = E$ auch $AM'M = EM$, d. h. $M' = M$ folgt. Allgemein ergiebt sich hieraus, dass aus $AB = AC$ stets $B = C$ folgt (vergl. §. 148, 2.).

2. Dass nun die Anzahl aller Idealclassen *endlich* ist, beruht auf einer tieferen Eigenschaft des Systems E aller Hauptideale, welche jetzt zu besprechen ist. Bilden die ganzen Zahlen ω_1, $\omega_2 \ldots \omega_n$ eine Grundreihe (oder irgend eine Basis) des Körpers Ω, und setzen wir (wie in §. 159) $\omega = \sum h_\iota \omega_\iota$, $H = N(\omega)$, so ist H eine homogene Function $n$ten Grades der Coordinaten h_ι mit *ganzen* rationalen Coefficienten; bedeutet nun s die Summe der absoluten Werthe dieser Coefficienten, so besteht folgender Satz:

Ist $\mathfrak{a}$ irgend ein Ideal, so giebt es immer ein durch $\mathfrak{a}$ theilbares Hauptideal, dessen Norm $\leqq sN(\mathfrak{a})$ ist. Man gebe jeder der n Coordinaten h_ι alle $(k+1)$ Werthe $0, 1, 2 \ldots k$, wo $k \leqq \sqrt[n]{N(\mathfrak{a})} < k+1$;

da die Anzahl $(k+1)^n$ der so entstehenden ganzen Zahlen ω grösser als $N(\mathfrak{a})$ ist, so müssen zwei ungleiche von ihnen einander congruent (mod. $\mathfrak{a}$) sein; ihre Differenz η wird dann eine von Null verschiedene, durch $\mathfrak{a}$ theilbare Zahl, und da die absoluten Werthe ihrer Coordinaten den Werth k nicht übersteigen, so ist $N(\eta)$ absolut genommen $\leqq s k^n \leqq s N(\mathfrak{a})$; das Hauptideal $\mathfrak{i}(\eta)$ hat daher die geforderte Eigenschaft. Derselbe Satz kann offenbar auch so ausgesprochen werden: *Jedes Ideal* $\mathfrak{a}$ *kann in ein Hauptideal verwandelt werden durch Multiplication mit einem Ideal* $\mathfrak{m}$, *dessen Norm* $\leqq s$ *ist.*

Hierzu tritt folgende Ueberlegung. Durchläuft ϱ ein vollständiges Restsystem (mod. $\mathfrak{m}$), so nimmt auch $1+\varrho$ lauter incongruente Werthe an, woraus durch Addition leicht folgt, dass die Zahl $m = N(\mathfrak{m})$ durch $\mathfrak{m}$ theilbar, dass also $\mathfrak{m}$ ein Theiler des Hauptideals $\mathfrak{i}(m)$ ist. Da nun jedes Ideal nur eine endliche Anzahl von Theilern besitzt (§. 163, 2.), so giebt es auch nur eine endliche Anzahl von Idealen $\mathfrak{m}$, deren Normen einen gegebenen Werth m besitzen, mithin auch nur eine endliche Anzahl von Idealen $\mathfrak{m}$, deren Normen einen gegebenen Werth s nicht übertreffen. Zufolge des vorhergehenden Satzes giebt es daher eine *endliche* Anzahl von Idealen $\mathfrak{m}$ der Art, dass jedes beliebige Ideal $\mathfrak{a}$ durch Multiplication mit einem dieser Ideale $\mathfrak{m}$ in ein Hauptideal verwandelt werden kann; dieser wichtige Zusatz zu der Eigenschaft III. des Systems E kann offenbar auch so gefasst werden: *Die Anzahl der Idealclassen, d. h. die Anzahl der nicht äquivalenten Ideale ist endlich.*

3. Es leuchtet nun ein, dass alle Sätze über Perioden oder über Gruppen von Classen quadratischer Formen (§. 149) ohne Weiteres auf unsere Idealclassen übertragen werden können. Wir heben hier nur die einzige Folgerung hervor:

Jedes Ideal kann durch Potenzirung in ein Hauptideal verwandelt werden. Ist also $\mathfrak{a}$ ein Ideal, so giebt es immer einen positiven ganzen rationalen Exponenten m (Divisor der Classenanzahl) der Art, dass $\mathfrak{a}^m$ ein Hauptideal $\mathfrak{i}(\eta)$ wird; ist nun α irgend eine Zahl des Ideals $\mathfrak{a}$, so ist α^m theilbar durch η, mithin α theilbar durch die ganze Zahl $\sqrt[m]{\eta}$ (§. 160, 3.). Ist $\mathfrak{p}^e$ die höchste in $\mathfrak{a}$ aufgehende Potenz eines Primideals $\mathfrak{p}$, so ist me der Exponent der höchsten in η aufgehenden Potenz von $\mathfrak{p}$; hieraus folgt leicht, dass umgekehrt jede durch $\sqrt[m]{\eta}$ theilbare Zahl α in $\mathfrak{o}$ dem Ideale $\mathfrak{a}$ angehört; denn da