Ueber die Begründung der Idealtheorie.

Von

R. Dedekind.

Aus den Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen.
Mathematisch-physikalische Klasse. 1895. Heft 1.

Aus den Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen.
Mathematisch-physikalische Klasse. 1895. Heft 1.

Ueber die Begründung der Idealtheorie.

Von

R. Dedekind in Braunschweig, ausw. Mitglied.

(Vorgelegt in der Sitzung vom 26. Januar 1895.)

Von mehreren Seiten bin ich aufgefordert, meine Ansicht zu äußern über die kürzlich in diesen Nachrichten (1894. Nr. 4) von Herrn Hurwitz veröffentlichte Begründung der Idealtheorie und über deren Beziehungen zu der in der vierten Auflage von Dirichlet's Zahlentheorie (welche ich im Folgenden mit D. bezeichnen will) enthaltenen Darstellung desselben Gegenstandes. Wenn ich nun hierauf erkläre, daß ich der letzteren, also der meinigen den Vorzug gebe, so glaube ich diese Meinung ganz unbefangen aussprechen zu dürfen, weil ich schon im Februar 1887 denselben Weg wie Herr Hurwitz mit demselben Erfolge eingeschlagen habe, und weil ich erst von hieraus im November 1888 mit Hülfe neuer Beweismittel zu derjenigen Darstellung gelangt bin, welche ich später (1893) in das Werk von Dirichlet aufgenommen habe. Ich erlaube mir im Folgenden diesen Hergang etwas genauer zu beschreiben, weil die hierbei auftretende Einkleidung eines und desselben Grundgedankens in äußerlich verschiedene Formen wohl von allgemeinerem Interesse ist.

In §. 172 der dritten Auflage der Zahlentheorie und ebenso in §. 23 meiner Schrift Sur la théorie des nombres entiers algébriques habe ich hervorgehoben, daß die größte Schwierigkeit, welche bei der Begründung der Idealtheorie zu überwinden war, in dem Beweise des folgenden Satzes bestand:

1. Ist das Ideal $\mathfrak{c}$ theilbar [1]) durch das Ideal $\mathfrak{a}$, so giebt es

1) Dieses Wort gebrauche ich, wie bisher immer, in dem Sinne, daß jede Zahl des Ideals $\mathfrak{c}$ auch in $\mathfrak{a}$ enthalten ist; ich muß, um Verwirrung zu vermeiden, hierauf aufmerksam machen, weil Herr Hurwitz in seinem Aufsatze (II. 5) mit demselben Worte gerade die im Nachsatze ausgesprochene Beziehung zwischen $\mathfrak{c}$ und $\mathfrak{a}$ bezeichnet.

ein Ideal $\mathfrak{b}$, welches der Bedingung $\mathfrak{ab} = \mathfrak{c}$ genügt (vergl. D. S. 553. VII).

Daß dieser Satz, durch welchen der Zusammenhang zwischen der Theilbarkeit und der Multiplication der Ideale festgestellt wird, bei der damaligen Darstellung erst nahezu am Schlusse der Theorie beweisbar wurde, machte sich in der drückendsten Weise fühlbar, besonders dadurch, daß einige der wichtigsten Sätze nur allmälich durch schrittweise Befreiung von beschränkenden Voraussetzungen zu der ihnen zukommenden Allgemeinheit erhoben werden konnten. Ich bin daher im Laufe der Jahre öfter auf diesen Cardinalpunct mit der Absicht zurückgekommen, einen einfachen, unmittelbar an den Begriff der ganzen Zahl anknüpfenden Beweis des Satzes 1. oder eines der drei folgenden Sätze zu gewinnen, welche, wie man leicht erkennt, von gleicher Bedeutung für die Begründung der Theorie sind:

2. Jedes Ideal $\mathfrak{m}$ kann durch Multiplication mit einem Ideal $\mathfrak{n}$ in ein Hauptideal verwandelt werden (vergl. D. S. 554. IX).

3. Jeder endliche, von Null verschiedene Modul $\mathfrak{m}$ der aus ganzen oder gebrochenen algebraischen Zahlen besteht, kann durch Multiplication mit einem Modul $\mathfrak{n}$, dessen Zahlen aus denen von $\mathfrak{m}$ auf rationale Weise gebildet sind, in einen Modul $\mathfrak{mn}$ verwandelt werden, welcher die Zahl 1 enthält und aus lauter ganzen Zahlen besteht (vergl. D. S. 528. VI).

4. Aus je m algebraischen Zahlen μ_r, die nicht alle verschwinden, kann man auf rationale Weise m Zahlen ν_s ableiten, welche der Gleichung

$$\mu_1\nu_1 + \mu_2\nu_2 + \cdots + \mu_m\nu_m = 1$$

und außerdem der Bedingung genügen, daß alle m^2 Producte $\mu_r\nu_s$ ganze Zahlen sind (vergl. D. S. 530. VII).

Wenn nun auch diese vier Sätze insofern vollständig gleichwerthig sind, als jeder von ihnen ohne jede Schwierigkeit aus jedem der drei übrigen abgeleitet werden kann [1]), so geschieht es doch in solchen Fällen nicht selten, daß der eine Satz durch seine einfachere Fassung einem directen Beweise leichter zugänglich wird als die anderen. In dem vorliegenden Beispiele zeichnet sich offen-

1) Um dies einzusehen, braucht man nur die hinter den Sätzen bemerkten Citate zu verfolgen und zu bedenken, daß jeder endliche algebraische Modul $\mathfrak{m}$ durch Multiplication mit einer geeigneten, von Null verschiedenen Zahl in einen ganzen Modul, und jeder von Null verschiedene ganze Modul eines endlichen Körpers durch Multiplication mit jedem Ideal in ein Ideal verwandelt wird.

bar der Satz 4. oder auch der Satz 3., welcher sich von jenem nur äußerlich durch die Benutzung des Modul-Begriffs unterscheidet, an Einfachheit vor den Sätzen 1. und 2. aus, in welchen der complicirtere Begriff des Ideals auftritt. Es ist mir dann auch bald gelungen, den Satz 3. wenigstens für zweigliedrige Moduln $\mathfrak{m}$, also den Satz 4. für den Fall $m = 2$ zu beweisen, und zwar stimmt dieser Beweis, auf welchen ich unten zurückkommen werde, wesentlich mit demjenigen überein, welchen ich später in das Werk von Dirichlet (D. S. 529) aufgenommen habe. Aber es gelang mir damals nicht, diese Methode auf drei- und mehrgliedrige Moduln $\mathfrak{m}$ auszudehnen.

Eine neue Anregung zur Beschäftigung mit diesem Gegenstande empfing ich im Frühjahr 1882 durch die große Abhandlung „Grundzüge einer arithmetischen Theorie der algebraischen Größen“ von Leopold Kronecker. Das Studium derselben veranlaßte mich, eine Reihe von „bunten Bemerkungen“ aufzuschreiben, von denen Nr. 20 sich auf den für mich wichtigsten §. 14, also auf die Begründung der Idealtheorie bezieht. Obgleich ich mich mit dem hier auftretenden „methodischen Hülfsmittel der unbestimmten Coefficienten“ nicht befreunden konnte, so suchte ich doch in das Wesen der Methode einzudringen, um wo möglich daraus einen Nutzen für meine Auffassung der Theorie zu ziehen, weil in dem hier gewonnenen Resultate auch der obige Satz 3. oder 4. offenbar enthalten ist. Nun schien und scheint mir noch heute in der Beweisführung Kronecker's eine Lücke oder wenigstens eine zweifelhafte Stelle zu sein; setzt man unter sonstiger Beibehaltung der dortigen Bezeichnungen der Kürze wegen

$$(x + u'x' + u''x'' + \cdots)\, G = F \tag{1}$$

und

$$(x + v'x' + v''x'' + \cdots)\, G = Q, \tag{2}$$

so ist G eine ganze Function der unbestimmten Größen u, während Q außerdem von den unbestimmten Größen v abhängt, und wenn ich die etwas dunkele Stelle richtig verstehe, so soll bewiesen werden, daß alle Coefficienten dieser Function Q ganze Größen des hier betrachteten Bereichs $(\mathfrak{R})$ sind. Nun wird zwar gezeigt, daß Q einer Gleichung von der Form

$$Q^n + C_1 Q^{n-1} + \cdots + C_{n-1} Q + C_n = 0 \tag{3}$$

genügt, wo $C_1, C_2 \ldots C_n$ ebenfalls ganze und zwar solche ganze Functionen der Variabelen u, v bedeuten, deren Coefficienten ganze

Größen in $(\mathfrak{R})$ sind; aber es bedarf meiner Ansicht nach doch noch eines besonderen Beweises, daß sich hieraus die oben bezeichnete Eigenschaft der Coefficienten von Q als nothwendige Folge ergiebt; ich habe wenigstens in den vorausgehenden §§. 1—13 keine Stelle gefunden, aus welcher dies hervorgeht. Für den vorzugsweise mich interessirenden Fall, wo der Bereich $(\mathfrak{R})$ der Körper aller algebraischen Zahlen ist, also keine Variabelen enthält, gelang es mir auch einen solchen Beweis zu finden, den ich hier aber nur andeuten will, weil er in der Folge nicht weiter verwendet wird. Man sieht leicht ein, daß der fragliche Satz zufolge (3) auf den folgenden zurückkommt: „Wenn eine ganze rationale Function Q von Variabelen stets eine ganze (algebraische) Zahl wird, sobald diese Variabelen ganze Zahlen werden, so ist auch jeder Coefficient der Function Q eine ganze Zahl." Und diesen Satz bewies ich, freilich auf eine ziemlich künstliche Weise, indem ich für die Variabelen beliebige Wurzeln der Einheit einsetzte. Durch diese Vervollständigung der Beweisführung von Kronecker war nun, wie schon oben bemerkt, auch zugleich für den Satz 3. ein Beweis gewonnen, welcher von meiner bisherigen Idealtheorie unabhängig war und folglich zu einer neuen Begründung derselben dienen konnte. Aber dieser Weg entspricht durchaus nicht meinen Wünschen, theils weil die Benutzung der Functionen von Variabelen mir immer als ein der Sache fremdes Hülfsmittel erscheint, theils weil die Durchführung aller Beweise ohne Zweifel einen größeren Raum erfordert, als in meiner damaligen Theorie.

So ruhte diese Frage mehrere Jahre ohne jeden Fortschritt, und sie kam erst auf's Neue in Bewegung, als mein Freund H. Weber mir am 10. Februar 1887 von Marburg aus eine von ihm ausgearbeitete „Theorie der algebraischen Zahlen nach Kronecker" zuschickte, in welcher die Hauptsätze ausführlich und vollständig bewiesen wurden. Bei angestrengtem Nachdenken über diese Darstellung fand ich nun am 15. Februar den folgenden Satz, durch welchen nach meiner Ansicht die Theorie von Kronecker noch eine wesentliche Vereinfachung gewinnt:

5. Wenn das Product GH aus zwei ganzen rationalen Functionen G, H von beliebig vielen unabhängigen Variabelen u lauter ganze Coefficienten hat, so ist auch jedes Einzel-Product aus jedem Coefficienten von G und jedem Coefficienten von H eine ganze Größe.

Um nämlich zu beweisen, daß die oben mit Q bezeichnete Function lauter ganze Coefficienten hat, braucht man nicht mehr, wie es bei Kronecker geschieht, die Gleichung (3) zu bilden,

welcher Q genügt, sondern dies folgt jetzt unmittelbar daraus, daß das Product F in (1) lauter ganze Coefficienten hat, also auch jedes Product aus jeder Größe x, x', x''... und aus jedem Coefficienten der Function G ganz ist.

Diese Bemerkung und ein vollständiger Beweis des Satzes 5. bildeten den Hauptinhalt meiner am 20. Februar 1887 abgesendeten Antwort an H. Weber; dieser Beweis ist später in §. 3 meiner Abhandlung „Ueber einen arithmetischen Satz von Gauss“ veröffentlicht, welche sich in den Mittheilungen der Deutschen mathematischen Gesellschaft in Prag (1892) findet, und auf S. 7 daselbst, ebenso auch in der Vorrede zur vierten Auflage von Dirichlet's Zahlentheorie, habe ich auch die Wichtigkeit des Satzes 5. für die Theorie von Kronecker besonders betont. Herr Hurwitz, dem diese Abhandlung erst nach Abschluß seiner Arbeit bekannt geworden ist, knüpft an denselbeu Satz 5. an, für welchen er einen anderen Beweis giebt, und leitet daraus den Satz 2. ab. Ebenso weise ich in meinem Briefe vom 20. Februar 1887 wieder darauf hin, daß der zur Abkürzung meiner Idealtheorie brauchbare Satz 3. eine unmittelbare Folge des Satzes 5. ist, aber dies geschieht mit dem ausdrücklichen Zusatz, ich würde mir zehnmal überlegen, wie eine solche Abkürzung durchzuführen sei, ohne den einheitlichen Charakter der Theorie zu stören!

Hiermit komme ich zum letzten Theile meiner Erzählung. Ich erinnere zunächst an eine schöne Stelle der Disquisitiones Arithmeticae, die schon in meiner Jugend den tiefsten Eindruck auf mich gemacht hat. Im Art. 76 berichtet Gauss, daß der Wilson'sche Satz zuerst von Waring bekannt gemacht ist, und fährt fort: Sed neuter demonstrare potuit, et cel. Waring fatetur demonstrationem eo difficiliorem videri, quod nulla notatio fingi possit, quae numerum primum exprimat. — At nostro quidem judicio hujusmodi veritates ex notionibus potius quam ex notationibus hauriri debebant. — In diesen letzten Worten liegt, wenn sie im allgemeinsten Sinne genommen werden, der Ausspruch eines großen wissenschaftlichen Gedankens, die Entscheidung für das Innerliche im Gegensatz zu dem Aeußerlichen. Dieser Gegensatz wiederholt sich auch in der Mathematik auf fast allen Gebieten; man denke nur an die Functionen-Theorie, an Riemann's Definition der Functionen durch innerliche charakteristische Eigenschaften, aus welchen die äußerlichen Darstellungs-Formen mit Nothwendigkeit entspringen. Aber auch auf dem bei Weitem enger begrenzten und einfacheren Gebiete der Idealtheorie kommen beide Richtungen zur Geltung, und ich habe mich an verschiedenen

Stellen meiner oben erwähnten Schrift Sur la théorie des nombres entiers algébriques (am Schluß von §. 12 und namentlich in der Einleitung) so ausführlich über die Anforderungen ausgesprochen, die ich mir damals wie heute bei dem Aufbau der Theorie stellte, daß ich nicht mehr darauf zurückzukommen brauche. Hiernach wird man es auch erklärlich finden, daß ich meiner Definition des Ideals durch eine charakteristische innerliche Eigenschaft den Vorzug gebe vor derjenigen durch eine äußerliche Darstellungsform, von welcher Herr Hurwitz in seiner Abhandlung (II. 1.) ausgeht. Aus denselben Gründen konnte der oben erwähnte Beweis des Satzes 3., welcher sich auf den Satz 5. stützt, mich noch nicht völlig befriedigen, weil durch die Einmischung der Functionen von Variabelen die Reinheit der Theorie nach meiner Ansicht getrübt wird, und ich will jetzt berichten, auf welchem Wege es mir gelungen ist, das erstrebte Ziel zu erreichen.

Der am 15. Februar 1887 von mir gefundene Beweis des Satzes 5. geht so zu Werke (vergl. §. 3 der Prager Abhandlung), daß zunächst der folgende sehr specielle Fall bewiesen wird, in welchem der eine Factor eine lineare Function ist:

6. Hat die ganze Function

$$f(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n$$

lauter ganze Coefficienten, so gilt dasselbe von der ganzen Function

$$\frac{f(x)}{x-\omega} = a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n,$$

wo ω eine Wurzel der Gleichung $f(\omega) = 0$ bedeutet.

Vergleicht man aber den Beweis dieses speciellen Satzes mit dem zu Anfang erwähnten, viel früher gefundenen Beweise (D. S. 529) des speciellen Falles des Satzes 3., in welchem $\mathfrak{m}$ ein zweigliedriger Modul $[\alpha, \beta]$ ist, so erkennt man leicht ihre vollständige Identität; denn wenn man $\alpha = \beta\omega$ setzt, so stimmt die Reihe der n Producte $\beta\nu_r$, welche in dem letzteren auftreten, mit den obigen Coefficienten a_r überein [1]). Da nun der vollständige Beweis des Satzes 5. (für Functionen von einer Variabelen, deren Betrachtung hier genügt) sich lediglich durch eine wiederholte Anwendung des speciellen Satzes 6. ergiebt, so lag die Vermuthung

1) Es ist dies dieselbe Zahlenreihe, welche mir schon früher bei verschiedenen Gelegenheiten gute Dienste geleistet hatte (vergl. z. B. den Schluß von §. 8 meiner Abhandlung Ueber die Discriminanten endlicher Körper oder D. §. 167).

nahe, daß auch der allgemeine Satz 3. oder 4. durch wiederholte Anwendung des speciellen Falles, wo $\mathfrak{m}$ ein zweigliedriger Modul, oder $m = 2$ ist, sich würde ableiten lassen. Bei erneuter Beschäftigung mit dieser Frage ergab sich dies in der That am 22. October 1888, und zwar auf folgende unerwartet einfache Weise durch die vollständige Induction.

Ist n eine natürliche Zahl, und nimmt man an, der Satz 4. sei schon für alle Fälle bewiesen, wo $m < n+2$, so kann man aus $n+2$ gegebenen algebraischen Zahlen

$$\alpha,\ \beta,\ \mu_1,\ \mu_2 \ldots \mu_n$$

auf rationale Weise $2n+4$ Zahlen

$$\begin{array}{l} \alpha',\ \beta' \\ \alpha'',\ \nu_1,\ \nu_2 \ldots \nu_n \\ \beta'',\ \varrho_1,\ \varrho_2 \ldots \varrho_n \end{array}$$

ableiten, welche den drei Gleichungen

$$\begin{array}{ll} & \alpha\alpha' + \beta\beta' = 1 \\ (4) & \alpha\alpha'' + \mu_1\nu_1 + \cdots + \mu_n\nu_n = 1 \\ & \beta\beta'' + \mu_1\varrho_1 + \cdots + \mu_n\varrho_n = 1 \end{array}$$

und zugleich den Bedingungen genügen, daß alle Producte

$$\begin{array}{ll} & \alpha\alpha',\ \alpha\beta',\ \beta\alpha',\ \beta\beta' \\ (5) & \alpha\alpha'',\ \alpha\nu_r,\ \mu_r\alpha'',\ \mu_r\nu_s \\ & \beta\beta'',\ \beta\varrho_r,\ \mu_r\beta'',\ \mu_r\varrho_s \end{array}$$

ganze Zahlen werden, wo r, s beliebige Zahlen aus der Reihe $1, 2 \ldots n$ bedeuten. Setzt man nun

$$\alpha''' = \alpha\alpha'\alpha'',\ \beta''' = \beta\beta'\beta'',\ \sigma_r = \alpha\alpha'\nu_r + \beta\beta'\varrho_r,$$

so sind auch diese $n+2$ Zahlen aus den gegebenen auf rationale Weise gebildet; zufolge (4) befriedigen sie die Gleichung

$$\alpha\alpha''' + \beta\beta''' + \mu_1\sigma_1 + \cdots + \mu_n\sigma_n = 1,$$

und zufolge (5) sind alle Producte

$$\begin{array}{l} \alpha\alpha''',\ \alpha\beta''',\ \alpha\sigma_r \\ \beta\alpha''',\ \beta\beta''',\ \beta\sigma_r \\ \mu_r\alpha''',\ \mu_r\beta''',\ \mu_r\sigma_s \end{array}$$

ganze Zahlen, weil sie in der Form

$$\begin{array}{llll} \alpha\alpha'\cdot\alpha\alpha'', & \alpha\beta'\cdot\beta\beta'', & \alpha\alpha'\cdot\alpha\nu_r+\alpha\beta'\cdot\beta\varrho_r \\ \alpha\alpha''\cdot\beta\alpha', & \beta\beta'\cdot\beta\beta'', & \alpha\nu_r\cdot\beta\alpha'+\beta\beta'\cdot\beta\varrho_r \\ \alpha\alpha'\cdot\mu_r\alpha'', & \beta\beta'\cdot\mu_r\beta'', & \alpha\alpha'\cdot\mu_r\nu_s+\beta\beta'\cdot\mu_r\varrho_s \end{array}$$

darstellbar sind, w. z. b. w.

Hiermit war endlich das, was ich so lange gesucht hatte, ein wirklich sachgemäßer Beweis der Sätze 3. und 4., also auch die Grundlage für die Neugestaltung meiner Idealtheorie gefunden. Indessen war ich auch mit diesem Inductionsbeweise noch nicht ganz zufrieden, weil in ihm die mechanische Rechnung vorherrscht, und bei längerem Nachdenken über den eigentlichen Grund seines Erfolges entdeckte ich am 9. November 1888 den allgemeinen Modulsatz

$$(\mathfrak{a}+\mathfrak{b}+\mathfrak{c})(\mathfrak{b}\mathfrak{c}+\mathfrak{c}\mathfrak{a}+\mathfrak{a}\mathfrak{b}) = (\mathfrak{b}+\mathfrak{c})(\mathfrak{c}+\mathfrak{a})(\mathfrak{a}+\mathfrak{b}),$$

woraus die schließliche Form des Beweises entsprang (D. S. 530). Ich bemerke beiläufig, daß statt des dortigen Moduls

$$\mathfrak{n} = (\mathfrak{b}\mathfrak{c}+\mathfrak{c}\mathfrak{a}+\mathfrak{a}\mathfrak{b})\,\mathfrak{a}'\mathfrak{b}'\mathfrak{c}'$$

auch der Modul

$$\mathfrak{n} = \mathfrak{a}\mathfrak{b}'\mathfrak{c}'+\mathfrak{b}\mathfrak{c}'\mathfrak{a}'+\mathfrak{c}\mathfrak{a}'\mathfrak{b}'$$

hätte gewählt werden können, dessen Bau wohl etwas einfacher ist und sich genauer an den vorstehenden Inductionsbeweis anschließt; doch ziehe ich die erstere Wahl vor, weil bei der letzteren der Beweis, daß der Modul $\mathfrak{z} = [1]$ durch $\mathfrak{m}\mathfrak{n}$ theilbar ist, sich weniger einfach gestaltet.

Bedenkt man nun, mit wie wenigen Schritten man jetzt (D. §. 173) von dem Begriffe der ganzen Zahl zu dem Satze 3. und hiermit zur vollen Beherrschung der Idealtheorie gelangt, so kann, wie ich meine, gar kein Zweifel darüber bestehen, daß dieser Weg vor allen Dingen sachgemäßer, aber zugleich auch einfacher und bei Weitem kürzer ist, als der im Februar 1887 gefundene, welcher zunächst zu dem Functionen-Satze 5. und erst von diesem zu dem Zahlen-Satze 3. oder (wie in der Abhandlung des Herrn Hurwitz) zu dem gleichwerthigen Satze 2. führt. Hierin bestehen die Gründe, auf denen mein im Eingange dieser Mittheilung ausgesprochenes Urtheil beruht.

Braunschweig, am 14. Januar 1895.