

LV.

Anzeige der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie.

[Göttingische gelehrte Anzeigen, Jahrgang 1871, S. 1481—1494.]

Die erste im Jahre 1863 erschienene Auflage dieses Werkes ist von mir in diesen Blättern (27. Januar 1864) angezeigt, und ich kann hinsichtlich der Entstehung und des Inhaltes im wesentlichen auf meine damaligen Mittheilungen verweisen. Die neue Auflage unterscheidet sich von der ersten durch eine große Anzahl von Vervollständigungen, welche theils in Anmerkungen, theils im Texte selbst hinzugefügt sind. Viele Paragraphen sind auch gänzlich umgearbeitet. Diese Veränderungen, welche indessen den wesentlichen Kern des Dirichletschen Vortrages nicht berühren, sind hauptsächlich durch den Entschluß hervorgerufen, in einem neuen Anhang, dem zehnten Supplement, die Lehre von der Komposition der binären quadratischen Formen darzustellen, welche aus damals erwähnten Gründen in der ersten Auflage nicht behandelt war. Die umfassende Allgemeinheit, mit welcher Gauß diese Lehre in der fünften Sektion der *Disquisitiones Arithmeticae* vorgetragen hat, enthält für den Anfänger bedeutende Schwierigkeiten des Verständnisses; dieser Umstand hat Dirichlet Veranlassung gegeben zur Veröffentlichung der Abhandlung: *De formarum binariarum secundi gradus compositione*. 1851. Er sagt in der Einleitung zu derselben: *De formarum compositione tunc non egi, quod argumentum ab illustrissimo Gauß in „Disquisitionum Arithmeticarum“ sectione quinta maxima quidem generalitate sed per calculos tam prolixos tractatum esse constat, ut perpauci compositionis naturam percipere valuerint eo magis quod summus geometra, ut ipse monuit, brevitati consulens theorematum difficiliorum demonstrationes synthetice adornavit, suppressa analysi per quam erant eruta. Quare confidere posse mihi videor, hujus argumenti expositionem novam et plane elementarem artis analyticae*

cultoribus non fore ingrati. Da in dieser Abhandlung nur der erste Hauptsatz der in Rede stehenden Theorie bewiesen, aber keine Andeutung über den weiteren Verlauf gegeben wird, so habe ich einen etwas abweichenden Weg eingeschlagen, welcher mit dem von Dirichlet darin übereinstimmt, daß nur ein spezieller Fall der Komposition betrachtet wird. Die §§ 145—149 enthalten die allgemeinen Sätze über die Komposition der Formen und Formenklassen. Dieselben werden in den §§ 150, 151 dazu benutzt, das Verhältnis der Klassenzahlen für zwei Determinanten zu finden, welche sich wie zwei Quadratzahlen verhalten; es ist dies dieselbe Aufgabe, welche nach Dirichletschen Prinzipien schon in den §§ 97, 99, 100 behandelt ist. In den §§ 152—154 folgt die Komposition der Geschlechter und der zweite Beweis von Gauß für den Reziprozitätssatz in der Theorie der quadratischen Reste. Die §§ 155—158 enthalten einen Beweis des Satzes von Gauß, daß jede Klasse des Hauptgeschlechtes durch Duplikation entsteht; derselbe stützt sich auf einen Satz von Lagrange und Legendre über die Auflösung der unbestimmten Gleichungen zweiten Grades mit zwei Unbekannten in rationalen Zahlen.

In den nun noch folgenden Paragraphen habe ich versucht, den Leser in ein höheres Gebiet einzuführen, in welchem Algebra und Zahlentheorie sich auf das Innigste miteinander verbinden. Im Laufe der Vorlesungen über Kreisteilung und höhere Algebra, welche ich zu Göttingen im Winter 1856—1857 vor den Herrn Sommer und Bachmann, im Winter 1857—1858 vor den Herrn Selling und Auwers gehalten habe, drängte sich mir die Überzeugung auf, daß das Studium der algebraischen Verwandtschaft der Zahlen am zweckmäßigsten auf einen Begriff gegründet wird, welcher unmittelbar an die einfachsten arithmetischen Prinzipien anknüpft. Den damals von mir benutzten Namen „rationales Gebiet“ habe ich später mit dem Worte „Körper“ vertauscht; ich verstehe darunter ein System von unendlich vielen Zahlen, welches die Eigenschaft besitzt, daß die Summen, Differenzen, Produkte und Quotienten von je zwei dieser Zahlen wieder demselben System angehören. Ich nenne einen Körper A einen Divisor eines Körpers M , diesen ein Multiplum von jenem, wenn alle in A enthaltenen Zahlen sich auch in M vorfinden. Je zwei Körper A, B besitzen immer ein kleinstes gemeinschaftliches Multiplum, welches mit AB bezeichnet werden kann, und ebenso

einen größten gemeinschaftlichen Divisor. Wenn jeder Zahl a eines Körpers A eine Zahl $b = \varphi(a)$ in der Weise entspricht, daß $\varphi(a + a') = \varphi(a) + \varphi(a')$, und $\varphi(aa') = \varphi(a)\varphi(a')$ ist, so bilden die Zahlen b einen mit A konjugierten Körper $B = \varphi(A)$, welcher durch die Substitution φ aus A hervorgeht. Diese Begriffe leiten nach der algebraischen Richtung hin zu den Prinzipien von Galois, nach der zahlentheoretischen Seite hin zu Kummers Schöpfung der idealen Zahlen.

In § 159 sind die allgemeinsten Eigenschaften eines Körpers Ω entwickelt, welcher nur eine endliche Anzahl von Divisoren besitzt; in einem solchen gibt es immer eine endliche Anzahl von Zahlen $\omega_1, \omega_2, \dots, \omega_n$ der Art, daß jede beliebige Zahl ω des Körpers stets und nur auf eine einzige Art in die Form

$$h_1 \omega_1 + h_2 \omega_2 + \dots + h_n \omega_n$$

gebracht werden kann, wo h_1, h_2, \dots, h_n rationale Zahlen bedeuten, die ich die Koordinaten der Zahl ω in bezug auf die Basis $\omega_1, \omega_2, \dots, \omega_n$ nenne; die Zahl n heißt der Grad des Körpers Ω . Dann ergibt sich leicht, daß jede Zahl des Körpers eine algebraische Zahl, nämlich die Wurzel einer Gleichung n ten Grades ist, deren Koeffizienten rationale Zahlen sind, und daß der Körper Ω durch n verschiedene Substitutionen in n konjugierte Körper übergeht. Das Produkt aus den n Werten, in welche eine bestimmte Zahl ω des Körpers durch diese n Substitutionen übergeht, heißt die Norm von ω und ist eine homogene Funktion der Koordinaten mit rationalen Koeffizienten, also eine rationale Zahl, welche mit $N(\omega)$ bezeichnet wird. Bildet man ferner, wenn ein System von n Zahlen $\alpha_1, \alpha_2, \dots, \alpha_n$ des Körpers Ω gegeben ist, die Determinante aus den n^2 korrespondierenden Zahlen der n konjugierten Körper, so ist das Quadrat derselben eine rationale Zahl, welche ich die Diskriminante der Zahlen $\alpha_1, \alpha_2, \dots, \alpha_n$ nenne und mit $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$ bezeichne. Auf die analytischen Entwicklungen einzugehen, welche sich an diese Begriffe anknüpfen, ist hier nicht möglich und auch nicht nötig; dieselben sind auch in diesem Paragraphen nur so weit mitgeteilt, wie es mir zum besseren Verständnis zweckmäßig erschien.

In dem folgenden § 160 werden alle algebraischen Zahlen (welche ebenfalls einen Körper bilden) in ganze und gebrochene Zahlen eingeteilt; unter einer ganzen Zahl wird jede Wurzel einer Gleichung

verstanden, deren höchster Koeffizient = 1, und deren übrige Koeffizienten rationale und zwar ganze Zahlen sind. Aus diesem Begriffe werden die einfachsten Sätze über die Teilbarkeit, über Einheiten und über relative Primzahlen abgeleitet, von denen später Gebrauch gemacht wird.

Der folgende § 161 enthält einen Hilfssatz aus einer Theorie, durch welche der zuerst von Gauß eingeführte Begriff der Kongruenz der Zahlen verallgemeinert wird. Unter einem Modul verstehe ich ein System m von Zahlen, deren Summen und Differenzen demselben System angehören, und die Kongruenz $\omega \equiv \omega' \pmod{m}$ soll bedeuten, daß die Differenz $\omega - \omega'$ eine Zahl des Systems m ist. Dieser Begriff besitzt eine größere Tragweite, als seine außerordentliche Einfachheit zu versprechen scheint; doch ist hier nur das mitgeteilt, was zur Erleichterung der nachfolgenden Darstellung dienen kann.

Nach diesen Vorbereitungen werden im § 162 die ganzen Zahlen eines Körpers Ω vom n ten Grade näher untersucht; sie bilden einen Modul \mathfrak{o} , und es wird zunächst gezeigt, daß man stets n solche ganze Zahlen $\omega_1, \omega_2, \dots, \omega_n$ als Basiszahlen des Körpers wählen kann, für welche jede ganze Zahl

$$\omega = h_1 \omega_1 + h_2 \omega_2 + \dots + h_n \omega_n$$

auch ganze Zahlen h_1, h_2, \dots, h_n zu Koordinaten hat. Die Diskriminante $\Delta(\omega_1, \omega_2, \dots, \omega_n)$ einer solchen Basis, welche ich eine Grundreihe nenne, hat absolut genommen den möglich kleinsten Wert, und da diese ganze rationale, von Null verschiedene Zahl von besonders wichtiger Bedeutung für den Körper Ω ist, so wird sie die Diskriminante oder die Grundzahl desselben genannt und mit $\Delta(\Omega)$ bezeichnet. Sie geht in der Diskriminante eines jeden Systems von n ganzen Zahlen auf, und der Quotient ist ein Quadrat. Ist ferner μ eine bestimmte, von Null verschiedene Zahl in \mathfrak{o} , so ist die Anzahl der in \mathfrak{o} enthaltenen, in bezug auf μ inkongruenten Zahlen gleich dem absoluten Wert der Norm $N(\mu)$. Sodann wird auf eine merkwürdige Erscheinung aufmerksam gemacht, welche zuerst bei den aus der Kreisteilung entspringenden Körpern beobachtet ist; sie besteht darin, daß eine ganze Zahl, welche nicht weiter in ein Produkt von ganzen Zahlen zerlegbar ist, durchaus nicht immer die Rolle einer wahren Primzahl spielt. Dies ist der Ausgangspunkt für Kummers Schöpfung der idealen Zahlen gewesen.

Ich versuche nun, in dem folgenden § 163 eine neue Theorie aufzustellen, welche alle Körper umfaßt; ihr Grundgedanke besteht in folgendem. Ist μ eine von Null verschiedene Zahl in \mathfrak{o} , so hat das System \mathfrak{m} aller durch μ teilbaren Zahlen in \mathfrak{o} die beiden folgenden Eigenschaften:

I. Die Summe und die Differenz je zweier Zahlen in \mathfrak{m} sind wieder Zahlen in \mathfrak{m} ; d. h. \mathfrak{m} ist ein Modul.

II. Jedes Produkt aus einer Zahl in \mathfrak{m} und einer Zahl in \mathfrak{o} ist wieder eine Zahl in \mathfrak{m} .

Man kann aber nicht umgekehrt behaupten, daß ein jedes System \mathfrak{m} von ganzen Zahlen des Körpers, welches die beiden vorstehenden Eigenschaften besitzt, und welches ich von nun an ein Ideal nenne, aus allen durch eine angebbare Zahl μ teilbaren Zahlen besteht; wenn dies aber der Fall ist, so nenne ich \mathfrak{m} ein Hauptideal und bezeichne es durch das Symbol $\mathfrak{i}(\mu)$. Es werden nun die Eigenschaften aller Ideale des Körpers Ω untersucht, und es ergibt sich folgendes Hauptresultat. Multipliziert man jede Zahl eines Ideals \mathfrak{a} mit jeder Zahl eines Ideals \mathfrak{b} , so bilden diese Produkte und deren Summen ein Ideal, welches das Produkt aus den Faktoren \mathfrak{a} und \mathfrak{b} genannt und mit $\mathfrak{a}\mathfrak{b}$ bezeichnet wird. Zufolge dieser Erklärung ist $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$, und aus $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ folgt $\mathfrak{b} = \mathfrak{c}$. Nennt man ein von \mathfrak{o} verschiedenes Ideal \mathfrak{p} ein Primideal, wenn es keinen von \mathfrak{o} und \mathfrak{p} verschiedenen Faktor besitzt, so läßt sich jedes andere, zusammengesetzte Ideal stets und nur auf eine einzige Art als ein Produkt von Primidealen darstellen. Versteht man ferner unter der Norm $N(\mathfrak{a})$ eines Ideals \mathfrak{a} die Anzahl der in \mathfrak{o} enthaltenen Zahlen, welche in bezug auf den Modul \mathfrak{a} inkongruent sind, so ist $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$. Auf diese Weise ist die vollständige Analogie mit den Gesetzen der Teilbarkeit in der rationalen Zahlentheorie hergestellt.

Diese ganze Theorie hängt auf das innigste mit der sogenannten Theorie der höheren Kongruenzen zusammen, welche man der Anregung von Gauß und den Arbeiten von Galois, Schönemann und anderen verdankt; ich bin zuerst durch die Abhandlungen Kummers über die idealen Zahlen der Kreisteilung und durch das Studium der algebraischen Untersuchungen von Galois veranlaßt, mich mit der Theorie der höheren Kongruenzen eingehend zu beschäftigen, und ich habe damals auch einen kurzen Abriß dieser Theorie ver-

öffentlich (Crelles Journal Bd. 54). Später versuchte ich, mit ihrer Hilfe eine allgemeine Theorie der idealen Zahlen aufzustellen, wurde dann durch andere Arbeiten von der Vollendung derselben abgezogen, bis die Vorarbeiten für die Herausgabe des vorliegenden Werkes mich demselben Gegenstande wieder zuwandten; die erneuten Anstrengungen führten mich auf meine jetzige Theorie der Ideale, welche mir deshalb den Vorzug vor meiner früheren Behandlungsweise zu verdienen scheint, weil sie sich auf viel einfachere Begriffe gründet. Auf den Zusammenhang mit der Theorie der höheren Kongruenzen bin ich in meiner Darstellung nicht näher eingegangen, weil ich befürchtete, den Umfang dieses Anhangs gar zu sehr zu vergrößern. Für diejenigen Leser, welche sich genauer mit diesem Zusammenhang beschäftigen wollen, füge ich hier folgende Bemerkungen hinzu, welche ihnen wohl nützlich sein können.

Bedeutet ω eine beliebige Zahl in \mathfrak{o} , und setzt man

$$\mathcal{A}(1, \omega, \omega^2, \dots, \omega^{n-1}) = D^2 \mathcal{A}(\Omega),$$

so ist D immer eine ganze rationale Zahl, nämlich eine homogene Funktion der Koordinaten vom Grade $\frac{1}{2}n(n-1)$ mit ganzen rationalen Koeffizienten. Ist nun p eine rationale Primzahl, und gibt es eine Zahl ω , für welche D nicht durch p teilbar wird, so läßt sich die Zerlegung des Hauptideals $\mathfrak{i}(p)$ in ein Produkt von Primidealen leicht auf die Theorie der höheren Kongruenzen zurückführen. Genügt nämlich ω der Gleichung n ten Grades $F(\omega) = 0$, und ist

$$F(x) \equiv P_1(x)^{e_1} P_2(x)^{e_2} \dots P_m(x)^{e_m} \pmod{p},$$

wo P_1, P_2, \dots, P_m voneinander verschiedene Primfunktionen der Variablen x bzw. vom Grade f_1, f_2, \dots, f_m bedeuten, so ist

$$\mathfrak{i}(p) \equiv \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_m^{e_m},$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ voneinander verschiedene Primideale bedeuten, deren Normen bzw. $p^{f_1}, p^{f_2}, \dots, p^{f_m}$ sind. Hieraus folgt mit Leichtigkeit der für algebraische und zahlentheoretische Untersuchungen überaus fruchtbare Satz:

Die Primzahl p geht stets und nur dann in der Grundzahl $\mathcal{A}(\Omega)$ des Körpers auf, wenn p durch das Quadrat eines Primideals teilbar ist.

Anfangs hielt ich es für sehr wahrscheinlich, daß für jede bestimmte Primzahl p auch eine ganze Zahl ω existierte, welcher eine

durch p nicht teilbare Zahl D entspräche; erst als alle meine Versuche, die Existenz einer solchen Zahl ω nachzuweisen, fruchtlos blieben, stellte ich mir die Aufgabe, die Unrichtigkeit dieser Vermutung darzutun. Wäre sie richtig, so müßten jedesmal, wenn p durch r verschiedene Primideale \mathfrak{p} teilbar ist, deren Normen denselben Wert p' haben, auch mindestens r verschiedene Primfunktionen P vom Grade f existieren, und umgekehrt, wenn diese letztere Voraussetzung immer erfüllt wäre, so könnte man auch die Existenz einer Zahl ω von der angegebenen Beschaffenheit beweisen. Im einfachsten Fall, wenn $f = 1$, gibt es genau p verschiedene Primfunktionen ersten Grades; es fragt sich also, ob nicht ein Körper Ω existiert, in welchem p durch mindestens $(p + 1)$ verschiedene Primideale teilbar ist, welche alle dieselbe Norm p besitzen; der Grad des Körpers muß dann mindestens $= p + 1$ sein. Der einfachste Fall wird entstehen, wenn man $p = 2$ nimmt, und man kann fragen: gibt es kubische Körper, in welchen die Zahl 2 durch drei verschiedene Primideale teilbar ist? In einem solchen würde D stets eine gerade Zahl sein. Als Grundreihe eines kubischen Körpers kann man immer die Zahl 1 und zwei andere ganze Zahlen α, β wählen, deren Produkt rational ist. Es wird dann

$$\begin{aligned} \alpha \alpha &= a' \alpha + b \beta - b b' \\ \beta \beta &= a \alpha + b' \beta - a a' \\ \alpha \beta &= a b, \end{aligned}$$

wo a, b, a', b' ganze rationale Zahlen bedeuten, die jedenfalls keinen gemeinschaftlichen Teiler haben, und man findet

$$\Delta(\Omega) = \Delta(1, \alpha, \beta) = a'^2 b'^2 + 18 a b a' b' - 4 a a'^3 - 4 b b'^3 - 27 a^2 b^2.$$

Setzt man ferner

$$\omega = z + x \alpha + y \beta,$$

wo z, x, y willkürliche ganze rationale Zahlen bedeuten, so wird

$$\begin{aligned} \omega^3 &= z^3 - b b' x^2 - a a' y^2 + 2 a b x y + (a' x^2 + a y^2 + 2 x z) \alpha \\ &\quad + (b x^2 + b' y^2 + 2 y z) \beta, \end{aligned}$$

und folglich

$$D = b x^3 - a' x^2 y + b' x y^2 - a y^3$$

unabhängig von z , was wegen der Bedeutung von D notwendig erfolgen mußte. Obgleich nun a, b, a', b' keinen gemeinschaftlichen Teiler haben, so wird dennoch D stets eine gerade Zahl werden, wenn a und b gerade, a' und b' ungerade sind. Dann muß also auch die

Zahl 2 durch drei verschiedene Primideale teilbar sein. Dies bestätigt sich vollständig an dem Beispiel

$$a = b = 2, \quad a' = -b' = 1, \quad \mathcal{A}(\Omega) = -503;$$

es ist

$$i(2) = abc, \quad i(\alpha) = a^2c, \quad i(\beta) = b^2c,$$

wo a, b, c drei verschiedene Primideale bedeuten.

Ein anderes Beispiel gewinnt man auf folgende Art. In bezug auf den Modul $p = 2$ gibt es nur eine einzige Primfunktion zweiten Grades, nämlich $x^2 + x + 1$; wenn daher in einem Körper Ω die Zahl 2 durch mindestens zwei verschiedene Primideale teilbar ist, deren Normen $= p^2 = 4$, so muß D stets gerade sein. Offenbar muß der Grad des Körpers mindestens $= 4$ sein, und die erwähnte Erscheinung tritt in der Tat bei dem biquadratischen Körper ein, welcher aus der Gleichung

$$\alpha^4 - \alpha^3 + \alpha^2 - 2\alpha + 4 = 0$$

entspringt; die Zahlen $1, \alpha, \beta = 2:\alpha$ und $\gamma = \alpha^2 - \alpha$ bilden eine Grundreihe desselben, seine Grundzahl ist $= 13^2 \cdot 17$.

Es gibt also Körper Ω , in welchen die sämtlichen Zahlen D durch gewisse singuläre Primzahlen p , deren Anzahl natürlich endlich ist, teilbar sind. Ich bemerke aber, daß hierdurch die allgemeine Gültigkeit des oben angeführten Satzes, durch welchen der Charakter der in der Grundzahl $\mathcal{A}(\Omega)$ eines Körpers aufgehenden rationalen Primzahlen definiert wird, keineswegs verlorengeht; doch würde es hier viel zu weit führen, wenn ich auf den Beweis dieses wichtigen Satzes oder auf seine tiefere Bedeutung für die Verwandtschaft der Körper eingehen wollte. —

Nach dieser Abschweifung fahre ich fort, den Inhalt der folgenden Paragraphen kurz anzugeben. Im § 164 werden sämtliche Ideale des Körpers Ω in eine endliche Anzahl von Klassen eingeteilt. Zwei Ideale heißen äquivalent, wenn sie beide durch Multiplikation mit einem und demselben Ideal in Hauptideale verwandelt werden; eine Idealklasse besteht aus allen Idealen, welche einem bestimmten Ideal äquivalent sind; die Hauptklasse besteht aus den Hauptidealen. Diese Idealklassen gestatten dann eine Komposition, in welcher dieselben Gesetze herrschen wie bei der Komposition der Klassen der quadratischen Formen.

Im § 165 wird der Zusammenhang zwischen der Komposition der Idealklassen und der der zerlegbaren homogenen Formen nach-

gewiesen, welche aus der Betrachtung desselben Körpers Ω entspringen.

Der § 166 gibt die Dirichletsche Theorie der Einheiten in einer etwas verallgemeinerten Form, die sich hier ganz von selbst darbietet, und in § 167 wird dieselbe benutzt, um einen Ausdruck für die Anzahl der Idealklassen in der Gestalt einer unendlichen Reihe zu gewinnen, genau wie bei der Bestimmung der Klassenanzahl der quadratischen Formen. An dieser Stelle aber breche ich die Durchführung des allgemeinen Problems ab, da meine weiteren Untersuchungen in dieser Richtung noch nicht von hinreichendem Erfolge gekrönt sind, um veröffentlicht werden zu können. Die nun noch folgenden §§ 168—170 sollen nur dazu dienen, die vorhergehenden allgemeinen Untersuchungen durch die Anwendung auf das Beispiel der quadratischen Körper zu erläutern.

Bis jetzt scheint die Theorie der idealen Zahlen nur für vier oder fünf Mathematiker Gegenstand ernstlicher Forschung gewesen zu sein; es ist mein inniger Wunsch, durch die neue Auflage von Dirichlets Vorlesungen über Zahlentheorie den Zugang zu diesem großen Gebiete zu erleichtern und womöglich eine größere Anzahl von Mathematikern zu veranlassen, ihre Kräfte demselben zuzuwenden, damit neben dem gewaltigen Aufschwunge, welchen die Geometrie und die Theorie der Funktionen in neuerer Zeit genommen haben, die Zahlentheorie nicht zurückbleiben möge.

22. Juli 1871.