XLVII.

Über die Komposition der binären quadratischen Formen.

[Supplement X von Dirichlets Vorlesungen über Zahlentheorie, 2. Auflage, S. 423—462 (1871).]

Inhalt.

	Seite
§ 159. Endliche Körper	223
§ 160. Ganze algebraische Zahlen	236
§ 161. Theorie der Moduln	242
§ 162. Ganze Zahlen eines endlichen Körpers	245
§ 163. Theorie der Ideale eines endlichen Körpers	251

§ 159.

Die Theorie der binären quadratischen Formen, ihrer Äquivalenz und Komposition bildet nur einen speziellen Fall von der Theorie derjenigen homogenen Formen $n$ten Grades mit n Veränderlichen, welche sich in lineare Faktoren mit algebraischen Koeffizienten zerlegen lassen. Diese Formen sind zuerst von Lagrange*) betrachtet; später hat Dirichlet**) sich vielfach mit diesem Gegenstande beschäftigt, aber er hat von seinen weitgehenden Untersuchungen nur diejenige veröffentlicht, welche die Transformationen solcher Formen in sich selbst (vgl. §§ 61, 62) oder, was dasselbe ist, die Theorie der Einheiten für die entsprechenden algebraischen Zahlen behandelt; endlich hat Kummer***) durch die Schöpfung der idealen Zahlen einen neuen Weg betreten, welcher nicht nur zu einer sehr bequemen Ausdrucksweise, sondern auch zu einer tieferen Einsicht in die wahre Natur der algebraischen Zahlen führt. Indem wir versuchen, den

*) Sur la solution des problèmes indéterminés du second degré. § VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. (Œuvres de L. T. II, 1868, p. 375.) — Additions aux Éléments d'Algèbre par L. Euler. § IX.

**) Vgl. Anm. zu § 141.

***) Vgl. Anm. zu § 16.

Leser in diese neuen Ideen einzuführen, stellen wir uns auf einen etwas höheren Standpunkt und beginnen damit, einen Begriff einzuführen, welcher wohl geeignet scheint, als Grundlage für die höhere Algebra und die mit ihr zusammenhängenden Teile der Zahlentheorie zu dienen.

I. Unter einem Körper wollen wir jedes System von unendlich vielen reellen oder komplexen Zahlen verstehen, welches in sich so abgeschlossen und vollständig ist, daß die Addition, Subtraktion, Multiplikation und Division von je zwei dieser Zahlen immer wieder eine Zahl desselben Systems hervorbringt. Der einfachste Körper wird durch alle rationalen, der größte Körper durch alle Zahlen gebildet. Wir nennen einen Körper A einen Divisor des Körpers M, diesen ein Multiplum von jenem, wenn alle in A enthaltenen Zahlen sich auch in M vorfinden; man findet leicht, daß der Körper der rationalen Zahlen ein Divisor von jedem andern Körper ist. Der Inbegriff aller Zahlen, welche gleichzeitig in zwei Körpern A, B enthalten sind, bildet wieder einen Körper D, welcher der größte gemeinschaftliche Divisor der beiden Körper A, B genannt werden kann, weil offenbar jeder gemeinschaftliche Divisor von A und B notwendig ein Divisor von D ist; ebenso existiert immer ein Körper M, welcher das kleinste gemeinschaftliche Multiplum von A und B heißen soll, weil er ein Divisor von jedem andern gemeinschaftlichen Multiplum der beiden Körper ist. Entspricht ferner einer jeden Zahl a des Körpers A eine Zahl $b = \varphi(a)$ in der Weise, daß $\varphi(a + a') = \varphi(a) + \varphi(a')$, und $\varphi(aa') = \varphi(a)\varphi(a')$ ist, so bilden die Zahlen b (falls sie nicht sämtlich verschwinden) ebenfalls einen Körper $B = \varphi(A)$, welcher mit A konjugiert ist und durch die Substitution φ aus A hervorgeht; dann ist rückwärts auch $A = \psi(B)$ mit B konjugiert. Zwei mit einem dritten konjugierte Körper sind auch miteinander konjugiert, und jeder Körper ist mit sich selbst konjugiert. Korrespondierende Zahlen in zwei konjugierten Körpern A und B, wie a und $b = \varphi(a)$, sollen konjugierte Zahlen heißen.

Die einfachsten Körper sind diejenigen, welche nur eine endliche Anzahl von Divisoren besitzen. Nennt man m bestimmte Zahlen α_1, α_2, ..., α_m voneinander abhängig oder unabhängig, je nachdem die Gleichung $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m = 0$ in rationalen Zahlen x_1, x_2, ..., x_m, die nicht sämtlich verschwinden, lösbar ist oder nicht, so

findet man durch sehr einfache Betrachtungen, auf die wir aber hier nicht eingehen wollen, daß aus einem Körper Ω von der angegebenen Art*) nur eine endliche Anzahl n von unabhängigen Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ sich auswählen läßt, daß also jede Zahl ω des Körpers stets und nur auf eine einzige Art durch die Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n = \Sigma h_\iota \omega_\iota \tag{1}$$

darstellbar ist, wo $h_1, h_2, \ldots, h_n$ rationale Zahlen bedeuten. Wir wollen die Zahl n den Grad, ferner den Komplex der n unabhängigen Zahlen ω_ι eine Basis des Körpers Ω, und die n Zahlen h_ι die dieser Basis entsprechenden Koordinaten der Zahl ω nennen; offenbar bilden je n Zahlen von der Form (1) wieder eine solche Basis, wenn die aus den entsprechenden n^2 Koordinaten gebildete Determinante von Null verschieden ist; einer solchen Transformation der Basis durch eine lineare Substitution entspricht eine Transformation der Koordinaten durch die sogenannte transponierte Substitution.

Die Forderung, daß die Zahlen ω des Körpers Ω durch Addition und Subtraktion sich reproduzieren sollen, wird durch ihre gemeinsame Form (1) schon erfüllt; für die Reproduktion durch Multiplikation ist ferner erforderlich und hinreichend, daß jedes Produkt $\omega_\iota\omega_{\iota'}$ wieder in der Form (1) enthalten ist; diese Bedingungen, deren Anzahl gleich $\frac{1}{2}n(n+1)$ ist, lassen sich am einfachsten zusammenfassen, indem man die Koordinaten h_ι als veränderlich ansieht und

$$\omega^2 = 2\Sigma H_\iota \omega_\iota \tag{2}$$

setzt, wo nun $H_1, H_2, \ldots, H_n$ bestimmte, mit rationalen Koeffizienten behaftete, ganze homogene quadratische Funktionen der Koordinaten bedeuten. Durch diese n Funktionen H_ι, auf deren analytische Eigenschaften wir unten zurückkommen werden, ist die Konstitution des Körpers Ω vollständig bestimmt, und es läßt sich zunächst zeigen, daß die Zahlen von der Form (1) auch durch Division sich wieder erzeugen. Durch totale Differentiation von (2) erhält man

$$\omega\, d\omega = \Sigma\, dH_\iota \omega_\iota; \tag{3}$$

legt man den Koordinaten h_ι und ihren Differentialen dh_ι beliebige rationale Werte bei, so ist durch die vorstehende Gleichung das

*) Ersetzt man die rationalen Zahlen überall durch Zahlen eines Körpers R, so gelten die nachfolgenden Betrachtungen auch für einen Körper Ω, welcher nur eine endliche Anzahl solcher Divisoren besitzt, die zugleich Multipla von R sind.

Produkt aus zwei beliebigen Zahlen ω und $d\omega$ des Körpers Ω auf die Form (1) zurückgeführt. Speziell ergibt sich aus (3)

$$\omega\,\omega_r = \sum \frac{\partial H_\iota}{\partial h_r}\,\omega_\iota; \tag{4}$$

legt man nun den Koordinaten h_ι beliebige rationale Werte bei, welche aber nicht sämtlich verschwinden, so kann auch der entsprechende Wert der Funktional-Determinante

$$H = \sum \pm \frac{\partial H_1}{\partial h_1}\frac{\partial H_2}{\partial h_2}\cdots\frac{\partial H_n}{\partial h_n} \tag{5}$$

nicht verschwinden; denn sonst ließen sich bekanntlich n rationale Zahlen dh_ι, die nicht sämtlich verschwinden, so bestimmen, daß für jeden Index r

$$dH_r = \sum \frac{\partial H_r}{\partial h_\iota}\,dh_\iota = 0,$$

und folglich auch $\omega\,d\omega = 0$ würde, während doch keine der beiden Zahlen ω und $d\omega$ verschwindet. Hieraus folgt weiter durch Umkehrung der n Gleichungen (4), daß die n Quotienten $\omega_\iota : \omega$ wieder Zahlen von der Form (1) sind; dasselbe gilt daher auch von jedem Quotienten $\alpha : \omega$, wo α irgendeine Zahl von der Form (1) bedeutet. Mithin bilden alle Zahlen von der Form (1) wirklich einen Körper.

Durch Elimination der n Zahlen ω_ι aus den n Gleichungen (4) ergibt sich die Gleichung

$$\begin{vmatrix} \frac{\partial H_1}{\partial h_1} - \omega, & \frac{\partial H_2}{\partial h_1} & \cdots \frac{\partial H_n}{\partial h_1} \\ \frac{\partial H_1}{\partial h_2}, & \frac{\partial H_2}{\partial h_2} - \omega & \cdots \frac{\partial H_n}{\partial h_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \frac{\partial H_1}{\partial h_n}, & \frac{\partial H_2}{\partial h_n} & \cdots \frac{\partial H_n}{\partial h_n} - \omega \end{vmatrix} = 0 \tag{6}$$

mithin ist jede Zahl ω des Körpers Ω die Wurzel einer (von der Wahl der Basis unabhängigen) Gleichung $n$ten Grades mit rationalen Koeffizienten, also eine algebraische Zahl, und es läßt sich leicht zeigen, daß in dem Körper Ω auch Zahlen existieren, welche keiner Gleichung mit rationalen Koeffizienten von niedrigerem als dem $n$ten Grade genügen, für welche also die vorstehende Gleichung irreduktibel

ist*). Bedeutet θ eine solche Zahl, so bilden offenbar die Potenzen $1, \theta, \theta^2, \ldots, \theta^{n-1}$ ebenfalls eine Basis des Körpers Ω, und Ω ist das System aller Zahlen, welche sich durch beliebige Wiederholung der vier arithmetischen Grundoperationen aus θ ableiten lassen. Substituiert man nun für θ der Reihe nach alle Wurzeln derselben irreduktiblen Gleichung, so entstehen ebensoviele entsprechende Körper, welche offenbar mit Ω und folglich auch miteinander konjugiert sind, und es ließe sich leicht zeigen, daß außer diesen Körpern kein anderer

---

*) Der Beweis dieser Behauptung kann z. B. auf das folgende Lemma gestützt werden:

Genügt eine homogene lineare Funktion $\omega = \Sigma h_\iota \omega_\iota$ der n Variablen h_ι einer Identität von der Form

$$A\omega^m + A_1\omega^{m-1} + \cdots + A_m = 0, \tag{1}$$

wo $A, A_1, \ldots, A_m$ ganze Funktionen der Variablen h_ι mit rationalen Koeffizienten bedeuten, die nicht sämtlich identisch verschwinden, und ist der Grad m kleiner als die Anzahl n der Variablen, so sind die n Größen ω_ι voneinander abhängig.

Durch totale Differentiation der Identität (1) ergibt sich zunächst

$$M\,d\omega + \omega^m\,dA + \omega^{m-1}\,dA_1 + \cdots + dA_m = 0, \tag{2}$$

wo zur Abkürzung

$$M = mA\omega^{m-1} + (m-1)A_1\omega^{m-2} + \cdots + A_{m-1}$$

gesetzt ist. Man kann nun offenbar annehmen, daß keine solche Identität (1) von noch niedrigerem Grade als m existiert, daß also das Produkt AM nicht identisch verschwindet; nun lege man, was stets möglich ist, den Variablen h_ι solche rationale Werte bei, für welche AM einen von Null verschiedenen Wert erhält; hierauf kann man, weil $m < n$ ist, den n Differentialen dh_ι solche rationale Werte beilegen, welche den m homogenen linearen Gleichungen

$$A\,dA_1 = A_1\,dA,\ A\,dA_2 = A_2\,dA \ \ldots\ A\,dA_m = A_m\,dA$$

genügen und nicht sämtlich verschwinden; multipliziert man nun (1) mit dA, (2) mit A, und subtrahiert, so folgt $AM\,d\omega = 0$, also auch $d\omega = \Sigma\,dh_\iota\omega_\iota = 0$, was zu beweisen war.

Hieraus folgt zunächst, daß, wenn die Größen ω_ι und ω wieder ihre alte Bedeutung erhalten, die aus den Koordinaten der n Größen $1, \omega, \omega^2, \ldots, \omega^{n-1}$ gebildete Determinante D, welche eine homogene Funktion der Variablen h_ι vom Grade $\frac{1}{2}n(n-1)$ ist, nicht identisch verschwinden kann, weil sonst ω einer Identität von der obigen Form (1) und von niedrigerem Grade als n genügte, und folglich die Größen ω_ι voneinander abhängig wären. Gibt man nun den Koordinaten h_ι solche rationale Werte, für welche D einen von Null verschiedenen Wert erhält, so folgt unmittelbar, daß die entsprechende Zahl ω des Körpers Ω die Wurzel einer irreduktiblen Gleichung $n$ten Grades ist.

Jeder Lösung der Gleichung $D = 0$ in rationalen Zahlen h_ι entspricht eine Zahl ω, welche einem Divisor des Körpers Ω von niedrigerem als dem $n$ten Grade angehört; der Grad eines solchen Divisors ist immer ein Divisor von n.

mit Ω konjugiert ist. Dabei bemerken wir aber, um Mißverständnissen vorzubeugen, daß diese n Körper, was ihren gesamten Zahleninhalt anbetrifft, sehr wohl teilweise oder auch sämtlich identisch sein können, obgleich sie durch n verschiedene Substitutionen aus einem von ihnen hervorgehen*).

Da nun vermöge des Begriffes konjugierter Körper die Gleichungen (4) gültig bleiben, wenn die Zahlen des Körpers Ω durch die entsprechenden Zahlen eines konjugierten Körpers ersetzt werden, so folgt leicht, daß die sämtlichen Wurzeln der Gleichung (6) die mit ω konjugierten Zahlen sind. Bezeichnet man daher mit $N(\omega)$ die sogenannte Norm der Zahl ω, d. h. das Produkt aus allen n konjugierten Wurzeln, die auch gruppenweise einander gleich sein können, so ist zufolge (6)

$$N(\omega) = H, \tag{7}$$

d. h. die homogene Funktion H ist das Produkt aus n konjugierten Faktoren ersten Grades mit algebraischen Koeffizienten. Aus dieser Definition geht unmittelbar der Satz hervor: die Norm eines Produktes ist immer gleich dem Produkt aus den Normen der Faktoren. Setzt man ferner

$$N(\omega) = \omega\,\omega', \tag{8}$$

so ist ω', weil $N(\omega)$ als rationale Zahl in Ω enthalten ist, ebenfalls eine Zahl des Körpers Ω, was auch aus (6) hervorgeht, und zwar ist

$$N(\omega') = N(\omega)^{n-1}; \tag{9}$$

nennen wir ω' die zu ω adjungierte Zahl**), so ist die zu ω' adjungierte Zahl $= \omega\, N(\omega)^{n-2}$.

Sind $\alpha_1, \alpha_2, \ldots, \alpha_n$ beliebige Zahlen des Körpers Ω, und bedeuten $\beta_\iota, \gamma_\iota, \ldots, \lambda_\iota$ die übrigen $(n-1)$ mit α_ι konjugierten Zahlen, so setzen wir zur Abkürzung

$$(\Sigma \pm \alpha_1 \beta_2 \ldots \lambda_n)^2 = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \tag{10}$$

---

*) Durch die weitere Verfolgung dieses Gegenstandes gelangt man unmittelbar zu den von Galois in die Algebra eingeführten Prinzipien (Sur les conditions de résolubilité des équations par radicaux; Journ. de Math. p. p. Liouville. T. XI. 1846); hierbei ist es zweckmäßig, zunächst die einfachen Reziprozitätsgesetze aufzusuchen, welche zwischen irgend zwei solchen Körpern wie Ω, ihrem größten gemeinschaftlichen Divisor und ihrem kleinsten gemeinschaftlichen Multiplum herrschen.

**) Dieser Ausdruck wird hier in ganz anderer Bedeutung gebraucht wie von Galois.

und nennen dieses Determinantenquadrat die Diskriminante der n Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$; sie ist eine symmetrische Funktion der n mit θ konjugierten Zahlen und folglich eine rationale Zahl, und zwar ist

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = m^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n), \tag{11}$$

wo m die aus den Koordinaten der Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ gebildete Determinante bedeutet; da die Diskriminante $\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1})$ bekanntlich das Produkt aller Differenzen zwischen den mit θ konjugierten Zahlen und folglich von Null verschieden ist (weil eine irreduktible Gleichung nur ungleiche Wurzeln haben kann), so ist $\Delta(\alpha_1 \ldots \alpha_n)$ stets und nur dann $= 0$, wenn die Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ voneinander abhängig sind. Endlich ist allgemein

$$\Delta(\omega\alpha_1, \omega\alpha_2, \ldots, \omega\alpha_n) = N(\omega)^2 \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n). \tag{12}$$

II. Im vorhergehenden sind die Begriffe und Sätze entwickelt, deren wir in der Folge bedürfen; zur Erläuterung mögen aber hier noch die wichtigsten und nächstliegenden Resultate aus dem großen Reichtume analytischer Entwicklungen mitgeteilt werden, welche sich an die Betrachtung der Funktionen H_ι anknüpfen. Zwischen diesen n Funktionen bestehen fundamentale Relationen, welche man erhält, wenn man das Produkt aus drei beliebigen Zahlen des Körpers Ω auf alle möglichen Arten bildet (vgl. §§ 1, 2). Bedeutet d' wieder eine beliebige Variation, so ist zufolge (4)

$$d'\omega\,\omega_r = \sum d'\left(\frac{\partial H_\iota}{\partial h_r}\right)\omega_\iota;$$

multipliziert man nun (3) mit $d'\omega$, und ersetzt die Produkte $d'\omega\,\omega_\iota$ der vorstehenden Gleichung gemäß durch Summen, so folgt

$$\omega\, d\omega\, d'\omega = \sum d H_\iota\, d'\left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right)\omega_{\iota'};$$

da die linke Seite symmetrisch in bezug auf d und d' ist, und da die n Zahlen $\omega_{\iota'}$ unabhängig sind, so ergibt sich, daß die Funktionen H_ι den n Differentialgleichungen

$$\sum d H_\iota\, d'\left(\frac{\partial H_r}{\partial h_\iota}\right) = \sum d' H_\iota\, d\left(\frac{\partial H_r}{\partial h_\iota}\right) \tag{13}$$

genügen, wo r irgendeinen der Indizes $1, 2, \ldots, n$ bedeutet. Um die Bedeutung dieser Relationen mehr hervortreten zu lassen, wollen wir sie den folgenden Entwicklungen zugrunde legen, ohne den Zusammenhang der Funktionen H_ι mit dem Körper Ω zu benutzen.

Zunächst wollen wir zeigen, daß die Funktionaldeterminante H, welche zufolge ihrer Definition (5) eine ganze homogene Funktion $n$ten Grades mit rationalen Koeffizienten ist, sich durch Multiplikation reproduziert; gehen die Formen K und L dadurch aus H hervor, daß die Koordinaten h_ι bzw. durch dh_ι und durch dH_ι ersetzt werden, so ist

$$L = HK; \tag{14}$$

denn wenn man die Koordinaten h_ι durch dh_ι ersetzt, so geht jede homogene lineare Funktion

$$\frac{\partial H_r}{\partial H_s} \text{ in } d\left(\frac{\partial H_r}{\partial h_s}\right),$$

und folglich H in

$$K = \sum \pm d\left(\frac{\partial H_1}{\partial h_1}\right) d\left(\frac{\partial H_2}{\partial h_2}\right) \cdots d\left(\frac{\partial H_n}{\partial h_n}\right)$$

über; werden aber die Koordinaten h_ι durch die bilinearen Funktionen dH_ι ersetzt, so geht zufolge (13)

$$\frac{\partial H_r}{\partial h_s} \text{ in } \sum \frac{\partial}{\partial h_s}\left(\frac{\partial H_r}{\partial h_\iota}\right) dH_\iota = \sum \frac{\partial H_\iota}{\partial h_s} d\left(\frac{\partial H_r}{\partial h_\iota}\right),$$

und folglich H in $L = HK$ über, was zu beweisen war. Dies ist der schon oben angeführte Satz über die Norm eines Produktes.

Bedeutet φ eine willkürliche Funktion der Koordinaten h_ι, und definiert man die Variation δ dadurch, daß

$$\delta\varphi = \sum \frac{\partial \varphi}{\partial H_\iota} h_\iota, \text{ also } \delta H_\iota = h_\iota \tag{15}$$

wird, so ergibt sich aus (13), wenn man d' durch δ ersetzt,

$$\sum dH_\iota \delta\left(\frac{\partial H_r}{\partial h_\iota}\right) = \sum h_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right) = dH_r,$$

weil H_r eine homogene Funktion zweiten Grades ist, mithin

$$\delta\left(\frac{\partial H_r}{\partial h_s}\right) = 1 \text{ oder } = 0, \tag{16}$$

je nachdem r und s gleich oder ungleich sind; hieraus folgt, daß die n Variationen δh_ι konstante, rationale Zahlen sind. Wird ferner die Variation δ' durch

$$\delta'\varphi = H \sum \frac{\partial \varphi}{\partial H_\iota} \delta h_\iota, \text{ also } \delta' H_\iota = H \delta h_\iota \tag{17}$$

definiert, so ergibt sich, wenn man in (13) d' durch δ' ersetzt,

$$\sum d H_\iota \delta' \left(\frac{\partial H_r}{\partial h_\iota}\right) = H \sum \delta h_\iota d \left(\frac{\partial H_r}{\partial h_\iota}\right) = H d \sum \frac{\partial H_r}{\partial h_\iota} \delta h_\iota$$
$$= H d \delta H_r = H d h_r,$$

folglich

$$\delta' \left(\frac{\partial H_r}{\partial h_s}\right) = H \frac{\partial h_r}{\partial H_s}; \tag{18}$$

da nun der Ausdruck rechter Hand der Koeffizient des Elementes

$$\frac{\partial H_s}{\partial h_r}$$

in der Determinante H, also eine ganze homogene Funktion $(n-1)$ten Grades der Koordinaten h_ι mit rationalen Koeffizienten ist, so gilt dasselbe von den Größen

$$h'_r = \delta' h_r = H \sum \frac{\partial h_r}{\partial H_\iota} \delta h_\iota, \tag{19}$$

und umgekehrt geht aus (18) hervor, daß die Koeffizienten der einzelnen n^2 Elemente in der Determinante H sich als homogene lineare Funktionen der soeben definierten n Größen h'_ι darstellen lassen. Wir wollen, wenn φ eine beliebige Funktion der Koordinaten h_ι bedeutet, mit φ' dieselbe Funktion der Größen h'_ι bezeichnen; dann lautet die Gleichung (18)

$$\frac{\partial H'_r}{\partial h'_s} = H \frac{\partial h_r}{\partial H_s}, \tag{20}$$

und hieraus folgt zugleich

$$H' = H^{n-1}; \quad H \frac{\partial h'_s}{\partial H'_r} = \frac{\partial H_s}{\partial h_r}. \tag{21}$$

Da H eine Funktionaldeterminante ist, so ist bekanntlich*)

$$d \log H = \sum \frac{\partial d H_\iota}{\partial H_\iota} - \sum \frac{\partial d h_\iota}{\partial h_\iota},$$

*) Jacobi: De determinantibus functionalibus § 9 (Crelles Journal XXII); in der obigen Form ist auch der Fall berücksichtigt, daß die Differentiale $d h_\iota$ Funktionen von den Veränderlichen h_ι sind. Ersetzt man d durch δ', so folgt aus (17) und (19) unmittelbar

$$\sum \frac{\partial h'_\iota}{\partial h_\iota} = 0.$$

und folglich ergibt sich unter Berücksichtigung von (13)

$$\sum \frac{\partial \log H}{\partial h_\iota} dH_\iota = \sum \frac{\partial}{\partial H_{\iota'}} \left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right) dH_\iota$$
$$= \sum d\left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right) \frac{\partial H_\iota}{\partial H_{\iota'}} = d \sum \frac{\partial H_\iota}{\partial h_\iota};$$

führt man daher die homogene lineare Funktion

$$S = \sum \frac{\partial H_\iota}{\partial h_\iota} \tag{22}$$

ein, so ist

$$\sum \frac{\partial \log H}{\partial h_\iota} dH_\iota = dS; \quad \frac{\partial \log H}{\partial h_r} = \frac{\partial S}{\partial H_r}, \tag{23}$$

also mit Rücksicht auf (20)

$$\frac{\partial H}{\partial h_r} = H \sum \frac{\partial S}{\partial h_\iota} \frac{\partial h_\iota}{\partial H_r} = \sum \frac{\partial S}{\partial h_\iota} \frac{\partial H'_\iota}{\partial h'_r};$$

man führe daher die ganze homogene Funktion zweiten Grades

$$T = \sum \frac{\partial S}{\partial h_\iota} H_\iota \tag{24}$$

ein, so wird

$$\frac{\partial H}{\partial h_r} = \frac{\partial T'}{\partial h'_r}; \quad dH = \sum \frac{\partial T'}{\partial h'_\iota} dh_\iota, \tag{25}$$

mithin sind auch die Derivierten der Form H darstellbar als homogene lineare Funktionen der in (19) definierten Größen h'_ι, und rückwärts diese durch jene. Da ferner zufolge (20)

$$\sum \frac{\partial H'_\iota}{\partial h'_s} \frac{\partial H_r}{\partial h_\iota} = H \quad \text{oder} \quad = 0$$

ist, je nachdem r und s gleich oder ungleich sind, so folgt durch Multiplikation mit h'_s oder dh'_s und Summation in bezug auf s

$$2 \sum H'_\iota \frac{\partial H_r}{\partial h_\iota} = H h'_r; \quad \sum dH'_\iota \frac{\partial H_r}{\partial h_\iota} = H dh'_r$$

und hieraus durch Differentiation

$$h'_r dH - H dh'_r = 2 \sum H'_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right). \tag{26}$$

Mit Hilfe von (25) und (26) ist man imstande, auch die Differentiale höherer Ordnung von H zu bilden; auf diese Weise findet man

$$H dd'H - dH d'H = 2H \sum \frac{\partial H}{\partial h_\iota} dd'h_\iota - 2 \sum \frac{\partial^2 T}{\partial h_\iota \partial h_{\iota'}} H'_\iota dd'H_{\iota'}; \tag{27}$$

außerdem ergibt sich aus Gleichung (26), welcher man mit Hilfe von (13) auch die Form

$$h'_r\, dH - H\, dh'_r = \sum \frac{\partial H'_\iota}{\partial h'_{\iota'}} \frac{\partial H'_\tau}{\partial h'_\iota}\, dh_{\iota'}$$

geben kann, die Funktionaldeterminante

$$\sum \pm \frac{\partial h'_1}{\partial h_1} \frac{\partial h'_2}{\partial h_2} \cdots \frac{\partial h'_n}{\partial h_n} = (-1)^{n-1}(n-1)\, H^{n-2} \tag{28}$$

und folglich aus (25) die Hessesche Determinante der Form H, nämlich

$$\sum \pm \frac{\partial^2 H}{\partial h_1^2} \cdots \frac{\partial^2 H}{\partial h_n^2} = (-1)^{n-1}(n-1) H^{n-2} \sum \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}. \tag{29}$$

Aus den Gleichungen (16), (22), (24), (25), (26), (27) ergeben sich unmittelbar folgende auf die Variation δ bezüglichen Resultate:

$$\begin{aligned} &\delta S = n; \quad \delta T = S; \quad h'_r \delta H - H \delta h'_r = 2 H'_r; \\ &\delta H = S'; \; \delta' H = \delta H^2 - H \delta^2 H = 2 T'. \end{aligned} \tag{30}$$

III. Alle diese Sätze sind abgeleitet aus der Voraussetzung, daß das System der n ganzen homogenen Funktionen H_ι vom zweiten Grade den Bedingungen (13) genügt, und daß ihre Funktionaldeterminante H nicht identisch verschwindet; fügt man noch die Voraussetzung hinzu, daß die Koeffizienten dieser Funktionen rationale Zahlen sind, und daß die Form H irreduktibel, d. h. nicht zerlegbar ist in Faktoren niedrigeren Grades, deren Koeffizienten ebenfalls rationale Zahlen sind, so läßt sich umgekehrt beweisen, daß zu diesem Funktionensystem ein algebraischer Zahlkörper Ω von der oben betrachteten Art gehört. Der Kürze halber führen wir eine Charakteristik ε ein, welche folgenden Sinn hat: ist φ irgendeine Funktion der Koordinaten h_ι, und ersetzt man die letzteren durch $h_\iota - \omega \delta h_\iota$, wo ω vorläufig eine willkürliche Funktion bedeutet, so geht φ in eine neue Funktion über, welche mit $\varepsilon(\varphi)$ bezeichnet werden soll. Aus dieser Definition folgt sofort

$$d\,\varepsilon(\varphi) = \varepsilon(d\varphi) - \varepsilon(\delta\varphi)\, d\omega; \tag{31}$$

unter der Voraussetzung, daß die Differentiale dh_ι konstant sind. Hierauf definiere man die Funktion ω als Wurzel der Gleichung $n$ten Grades

$$\varepsilon(H) = 0, \tag{32}$$

welche zufolge (16) vollständig mit der Gleichung (6) übereinstimmt, so läßt sich beweisen, daß ω eine ganze (homogene) Funktion ersten

Grades, d. h. daß $d\,d'\,\omega = 0$ ist, wenn die Differentiale $d\,h_\iota$, $d'\,h_\iota$ als konstant vorausgesetzt werden. In der Tat ergibt sich durch sukzessive Differentiation der Identität (32) nach der in (31) ausgesprochenen Regel

$$\varepsilon(\delta H)\,d\,\omega = \varepsilon(d\,H) \tag{33}$$

und

$$\varepsilon(\delta H)^3\,d\,d'\,\omega = \varepsilon(R), \tag{34}$$

wo zur Abkürzung die homogene Funktion $(3n-4)$ten Grades

$$\left\{\begin{array}{c} \delta H^3\,d\,d'\,H + \delta^2 H\,d\,H\,d'\,H \\ -\delta H\,d\,H\,d'\,\delta H - \delta H\,d'\,H\,d\,\delta H \end{array}\right\} = R$$

gesetzt ist. Daß diese Funktion R durch H teilbar, in Zeichen, daß $R \equiv 0$ ist*), ergibt sich auf folgende Weise.

Aus (30) folgt

$$h'_r\,\delta H = 2\,H'_r + H\,\delta\,h'_r \equiv 2\,H'_r$$

ferner

$$h'_r\,\delta^2 H = 2\,\delta\,H'_r + H\,\delta^2\,h'_r \equiv 2\,\delta\,H'_r$$

und hieraus durch Elimination von h'_r

$$\delta^2 H\,H'_r - \delta H\,\delta\,H'_r \equiv 0;$$

da nun zufolge (27) $d\,H\,d'\,H - H\,d\,d'\,H$ eine homogene lineare Funktion der n Größen H'_ι ist, so folgt auch, daß

$$\delta^2 H(d\,H\,d'\,H - H\,d\,d'\,H) - \delta H\,\delta(d\,H\,d'\,H - H\,d\,d'\,H) \equiv 0$$

ist; die linke Seite unterscheidet sich aber von R nur um Bestandteile, welche durch H teilbar sind. Mithin ist $R = PH$, wo P eine ganze Funktion bedeutet, und folglich $\varepsilon(R) = \varepsilon(P)\,\varepsilon(H) = 0$. Da sich nun aus den Voraussetzungen über H beweisen läßt, daß $\varepsilon(\delta H)$ nicht identisch verschwindet, so folgt aus (34) $d\,d'\,\omega = 0$, d. h. die Wurzel ω der Gleichung (32) ist eine ganze Funktion ersten Grades; daß sie zugleich homogen ist, versteht sich von selbst, weil H, δH, …, $\delta^{n-1} H$ und folglich auch ω gleichzeitig mit den Koordinaten h_ι verschwinden. Setzt man nun

$$\frac{\partial\,\omega}{\partial\,h_\iota} = \omega_\iota, \quad \omega = \sum h_\iota\,\omega_\iota, \tag{1}$$

---

*) Dies gilt allgemein von dem Ausdruck

$$d'\,H\,d'''\,H\,d\,d''\,H + d\,H\,d''\,H\,d'\,d'''\,H - d'''\,H\,d\,H\,d'\,d''\,H - d'\,H\,d''\,H\,d\,d'''\,H.$$

so ergibt sich aus (33), daß

$$\Sigma \delta h_\iota \omega_\iota = \delta \omega = 1 \tag{35}$$

und

$$\varepsilon\left(\frac{\partial H}{\partial h_\iota}\right) = \varepsilon(\delta H)\,\omega_\iota \tag{36}$$

ist. Da ferner zufolge (23)

$$\sum \frac{\partial H}{\partial h_\iota} d H_\iota = H d S \equiv 0$$

und

$$\varepsilon(d H_\iota) = d H_\iota - \omega\, d \delta H_\iota = d H_\iota - \omega\, d h_\iota$$

ist, so folgt

$$0 = \varepsilon(H) d S = \sum \varepsilon\left(\frac{\partial H}{\partial h_\iota}\right) \varepsilon(d H_\iota)$$

$$= \varepsilon(\delta H) \Sigma \omega_\iota (d H_\iota - \omega\, d h_\iota),$$

mithin

$$\omega\, d \omega = \Sigma\, d H_\iota \omega_\iota, \tag{3}$$

also auch

$$\omega^2 = 2 \Sigma H_\iota \omega_\iota, \tag{2}$$

wodurch wir rückwärts zu unseren ursprünglichen Annahmen zurückgekehrt sind; und man kann auch beweisen — worauf wir hier nicht eingehen wollen —, daß aus den Voraussetzungen über H die Unabhängigkeit der n Zahlen ω_ι folgt.

Wir fügen diesen Entwicklungen endlich noch folgende leicht zu beweisende Bemerkungen hinzu. Die ausgeführte Form der Gleichung (32) oder (6) ist folgende

$$0 = H - \delta H \frac{\omega}{1} + \delta^2 H \frac{\omega^2}{1 \cdot 2} - \delta^3 H \frac{\omega^3}{1 \cdot 2 \cdot 3} + \cdots; \tag{37}$$

es ist ferner

$$H = \Pi \omega = N(\omega), \tag{7}$$

wo das Produktzeichen Π sich auf alle n Wurzeln ω bezieht; ebenso findet man [wenn man in (3) d durch δ' ersetzt]

$$H = \omega \omega', \tag{8}$$

wo

$$\omega' = \delta' \omega = \Sigma h'_\iota \omega_\iota \tag{38}$$

zu ω adjungiert ist, und

$$S = \Sigma \omega, \quad 2 T = \Sigma \omega^2, \tag{39}$$

wo die Summenzeichen sich ebenfalls auf alle n Wurzeln beziehen. Die quadratische Form T ist charakteristisch für die Anzahl der reellen Wurzeln; bildet man ferner die Hessesche Determinante des Produktes $H = \Pi\omega$, so ergibt sich durch Vergleichung mit (29) die Diskriminante

$$(40) \qquad \Delta(\omega_1, \omega_2, \ldots, \omega_n) = \sum \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2},$$

was auch unmittelbar aus (39) folgt.

§ 160.

Der Inbegriff aller algebraischen Zahlen bildet offenbar ebenfalls einen Körper*). Wir wollen nun, indem wir unserem eigentlichen Gegenstande näher treten, eine Zahl α eine ganze algebraische Zahl nennen, wenn sie die Wurzel einer Gleichung ist, deren Koeffizienten rationale ganze Zahlen sind, wobei wir ein für allemal bemerken, daß wir unter den Koeffizienten einer Funktion $m$ten Grades

$$F(x) = c\,x^m + c_1\,x^{m-1} + c_2\,x^{m-2} + \cdots + c_m$$

oder der Gleichung $F(x) = 0$ stets die m Quotienten

$$-\frac{c_1}{c}, \quad +\frac{c_2}{c} \cdots (-1)^m \frac{c_m}{c}$$

verstehen. Aus dieser Erklärung folgt zunächst, daß eine rationale Zahl stets und nur dann eine ganze algebraische Zahl ist, wenn sie eine ganze Zahl im gewöhnlichen Sinne des Wortes ist (vgl. § 5, 4.); diese Zahlen wollen wir von jetzt ab rationale ganze Zahlen, alle algebraischen ganzen Zahlen aber kurz ganze Zahlen nennen. Dieses vorausgeschickt, schreiten wir zum Beweise der folgenden Fundamentalsätze.

1. Die Summe, die Differenz und das Produkt zweier ganzen Zahlen α, β sind wieder ganze Zahlen.

---

*) Daß es außer den algebraischen noch andere, sogenannte transzendente Zahlen gibt, ist meines Wissens zuerst von Liouville bewiesen (Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques; Journ. de Math. T. XVI, 1851). Man vermutet, daß die Ludolphsche Zahl π eine solche transzendente Zahl ist; allein selbst die als spezieller Fall hierin enthaltene Behauptung, daß die Quadratur des Zirkels unmöglich sei, ist bis auf den heutigen Tag noch nicht erwiesen. (Vgl. Euler: De relatione inter ternas pluresve quantitates instituenda. § 10. Opusc. anal. T. II, 1785.)

Sind a, b bzw. die Grade der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$, deren Koeffizienten rationale ganze Zahlen sind, und bezeichnet man mit $\omega_1, \omega_2, \ldots, \omega_n$ die sämtlichen ab Produkte von der Form $\alpha^{a'} \beta^{b'}$, wo a' irgendeine der Zahlen 0, 1, 2, ..., $(a-1)$, und b' irgendeine der Zahlen 0, 1, 2, ..., $(b-1)$ bedeutet, so wird, wenn $\omega = \alpha + \beta$, oder $= \alpha - \beta$, oder $= \alpha\beta$ ist, jedes der n Produkte $\omega\omega_1, \omega\omega_2, \ldots, \omega\omega_n$ mit Zuziehung der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ auf die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ gebracht werden können, wo $r_1, r_2, \ldots, r_n$ rationale ganze Zahlen sind. Eliminiert man die n Größen $\omega_1, \omega_2, \ldots, \omega_n$ aus diesen n Gleichungen, so ergibt sich für ω eine Gleichung vom $n$ten Grade [wie (6) in § 159], deren Koeffizienten rationale ganze Zahlen sind, was zu beweisen war (vgl. § 139).

2. Die ganze Zahl α heißt teilbar durch die ganze Zahl β, oder ein Multiplum von β, wenn der Quotient $\alpha : \beta$ ebenfalls eine ganze Zahl ist; umgekehrt heißt β ein Divisor oder Teiler von α (vgl. § 3). Ebenso setzen wir $\alpha \equiv \beta \pmod{\gamma}$, wenn $\alpha - \beta$ durch γ teilbar ist, und nennen α, β kongruent nach dem Modul γ (vgl. § 17). Man erkennt sofort (zufolge 1.), daß die Sätze des § 3 und auch die des § 17 (mit vorläufiger Ausnahme von 6. und 8.; vgl. § 164, 3.) ihre Gültigkeit behalten.

3. Jede Wurzel ω einer Gleichung, deren Koeffizienten ganze Zahlen sind, ist ebenfalls eine ganze Zahl.

Ist ω die Wurzel einer Gleichung $m$ten Grades $F(\omega) = 0$, deren Koeffizienten α, β ... ganze Zahlen sind, sind ferner a, b ... bzw. die Grade der mit rationalen ganzen Koeffizienten behafteten Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ ..., so führe man die sämtlichen mab ... Produkte $\omega_1, \omega_2, \ldots, \omega_n$ von der Form $\omega^{m'} \alpha^{a'} \beta^{b'}$ ... ein, wo die ganzen rationalen Exponenten den Bedingungen $0 \leqq m' < m$, $0 \leqq a' < a$, $0 \leqq b' < b$ ... genügen; dann läßt sich vermöge der Gleichungen $F(\omega) = 0$, $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ ... jedes der n Produkte $\omega\omega_1, \omega\omega_2, \ldots, \omega\omega_n$ wieder in die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ bringen, wo $r_1, r_2, \ldots, r_n$ rationale ganze Zahlen bedeuten, und hieraus folgt unmittelbar die Richtigkeit des Satzes.

Ist daher z. B. α eine ganze Zahl, und r eine beliebige (ganze oder gebrochene) positive rationale Zahl, so ist auch α^r eine ganze Zahl (vgl. § 5, 4.).

4. Bekanntlich lassen sich die Begriffe der Teilbarkeit und des Vielfachen von den ganzen rationalen Zahlen unmittelbar auf die ganzen rationalen Funktionen übertragen, und es gibt einen Algorithmus zur Auffindung des größten gemeinschaftlichen Divisors $\varphi(x)$ zweier gegebenen Funktionen $F(x)$, $f(x)$, welcher demjenigen der Zahlentheorie (§ 4) vollständig analog ist. Sind die Koeffizienten von $F(x)$ und $f(x)$ sämtlich in einem Körper K enthalten, so werden auch die Koeffizienten von $\varphi(x)$ Zahlen des Körpers K sein, weil sie durch Addition, Multiplikation, Subtraktion und Division aus den Koeffizienten von $F(x)$ und $f(x)$ entstehen. Hieraus folgt leicht, daß, wenn α die Wurzel einer solchen Gleichung $F(\alpha) = 0$ ist, deren Koeffizienten Zahlen des Körpers K sind, notwendig auch eine solche Gleichung $\varphi(\alpha) = 0$ von niedrigstem Grade existieren muß, welche irreduktibel in K heißen soll und welche offenbar keine anderen Wurzeln besitzen kann als die Gleichung $F(\alpha) = 0$. Hieraus folgt der Satz:

Ist α eine ganze Zahl, und K ein bestimmter Körper, so sind alle Koeffizienten der in K irreduktiblen Gleichung $\varphi(\alpha) = 0$ ganze Zahlen.

Denn weil α eine ganze Zahl, also die Wurzel einer Gleichung $F(\alpha) = 0$ ist, deren Koeffizienten rationale ganze Zahlen und folglich auch Zahlen des Körpers K sind (§ 159), so kann die in K irreduktible Gleichung $\varphi(\alpha) = 0$, welcher α genügt, nur ganze Zahlen zu Wurzeln haben; da aber die Koeffizienten einer Gleichung durch Addition und Multiplikation aus ihren Wurzeln entstehen, so sind (zufolge 1.) auch die Koeffizienten der Gleichung $\varphi(\alpha) = 0$ ganze Zahlen, was zu beweisen war.

Der einfachste Fall, in welchem K der Körper der rationalen Zahlen ist, findet sich bei Gauß*).

5. Ist ϱ irgendeine algebraische Zahl, so gibt es immer unendlich viele (von Null verschiedene) rationale ganze Zahlen h von der Beschaffenheit, daß $h\varrho$ eine ganze Zahl wird, und zwar stimmen diese sämtlichen Zahlen h mit den sämtlichen rationalen Vielfachen der kleinsten unter ihnen überein.

*) D. A. art. 42.

Da ϱ eine algebraische Zahl, also die Wurzel einer Gleichung von der Form

$$c\varrho^m + c_1\varrho^{m-1} + c_2\varrho^{m-2} + \cdots + c_m = 0$$

ist, wo c, c_1, c_2, …, c_m rationale ganze Zahlen bedeuten, so ergibt sich durch Multiplikation mit c^{m-1}, daß $c\varrho$ eine ganze Zahl ist. Sind ferner $a\varrho$, $b\varrho$ ganze Zahlen, wo a, b rationale ganze Zahlen bedeuten, deren größter gemeinschaftlicher Teiler $= h$ ist, so folgt leicht (aus 1. und § 4), daß auch $h\varrho$ eine ganze Zahl ist. Hieraus ergibt sich unmittelbar der zu beweisende Satz.

6. Versteht man unter einer Einheit eine ganze Zahl ε, welche in allen ganzen Zahlen aufgeht, so ist zunächst erforderlich, daß sie auch in 1 aufgeht, daß also $1 = \varepsilon\varepsilon'$, und ε' eine ganze Zahl ist; wenn nun

$$\varepsilon^m + c_1\varepsilon^{m-1} + \cdots + c_m = 0$$

die im Körper der rationalen Zahlen irreduktible Gleichung ist, welcher ε genügt, so muß (zufolge 4.) $c_m = \pm 1$ sein, weil ε' der ebenfalls irreduktiblen Gleichung

$$c_m\varepsilon'^m + c_{m-1}\varepsilon'^{m-1} + \cdots + c_1\varepsilon' + 1 = 0$$

genügt; umgekehrt, ist dies der Fall, so geht ε in 1 und folglich in allen ganzen Zahlen auf, ist also eine Einheit. Die Anzahl der Einheiten ist offenbar unbegrenzt.

Ist α teilbar durch α', und sind ε, ε' irgendwelche Einheiten, so ist offenbar auch $\varepsilon\alpha$ durch $\varepsilon'\alpha'$ teilbar; hinsichtlich der Teilbarkeit verhalten sich daher alle Zahlen $\varepsilon\alpha$, welche den sämtlichen Einheiten ε entsprechen, genau wie α. Zwei ganze Zahlen, deren Quotient keine Einheit ist, wollen wir wesentlich verschieden nennen.

7. Will man nun den Begriff der Primzahl so fassen, daß sie außer sich selbst und den Einheiten keine wesentlich verschiedene Teiler besitzt und auch selbst keine Einheit ist, so erkennt man sofort, daß gar keine solche Zahl existiert; ist nämlich α eine ganze Zahl, aber keine Einheit, so besitzt sie immer unendlich viele wesentlich verschiedene Divisoren, z. B. die Zahlen $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$, $\sqrt[4]{\alpha}$ usf., welche (zufolge 3.) ganze Zahlen sind.

Dagegen läßt sich der Begriff von relativen Primzahlen vollständig definieren, und diese Frage wird uns überhaupt auf den richtigen Weg leiten, welcher bei den ferneren Untersuchungen einzuschlagen ist. Da von einem größten gemeinschaftlichen Teiler

zweier ganzen Zahlen vorläufig (vgl. § 164, 3.) nicht gesprochen werden kann, so ist es auch unmöglich, die Definition von relativen Primzahlen so zu fassen, wie sie in der Theorie der rationalen Zahlen aufgestellt wird (§ 5); aber aus dieser Definition ergaben sich mehrere Sätze, deren jeder umgekehrt das Verhalten zweier relativen Primzahlen vollständig charakterisiert, ohne die Kenntnis ihrer sämtlichen Divisoren vorauszusetzen. Ein solcher Satz ist z. B. der folgende (§ 7): Sind a, b relative Primzahlen, so ist jede durch a und b teilbare Zahl auch durch ab teilbar. Dieser Satz läßt sich in der Tat umkehren: Ist jede durch a und b teilbare Zahl auch durch ab teilbar, so sind a, b relative Primzahlen. Hätten nämlich die beiden Zahlen $a = ha'$, $b = hb'$ einen gemeinschaftlichen Teiler $h > 1$, so wäre $ha'b'$ eine durch a und b, aber nicht durch ab teilbare Zahl.

Diese Betrachtung veranlaßt uns, folgende für das Gebiet aller ganzen algebraischen Zahlen gültige Erklärung aufzustellen:

Zwei von Null verschiedene ganze Zahlen α, β heißen relative Primzahlen, wenn jede durch α und β teilbare Zahl auch durch $\alpha\beta$ teilbar ist.

Vor allem bemerken wir, daß zwei relative Primzahlen im alten Sinne des Wortes, d. h. zwei rationale ganze Zahlen a, b, deren größter gemeinschaftlicher Divisor $= 1$ ist, auch im neuen Sinne relative Primzahlen bleiben; ist nämlich eine ganze algebraische Zahl γ teilbar durch a und b, so ist der Quotient $\varrho = \gamma : ab$ eine algebraische Zahl der Art, daß $a\varrho$ und $b\varrho$ ganze Zahlen sind; mithin muß (zufolge 5.) auch ϱ eine ganze Zahl, also γ teilbar durch ab sein, was zu beweisen war. Daß ferner umgekehrt zwei relative Primzahlen im neuen Sinne des Wortes, welche zugleich rational sind, auch relative Primzahlen im alten Sinne sind, versteht sich zufolge der der neuen Erklärung vorausgeschickten Erörterung von selbst.

Wir nennen ferner die ganzen Zahlen α, β, γ, δ ... kurz relative Primzahlen, wenn jede von ihnen relative Primzahl zu jeder der anderen ist (vgl. § 6); ist dann eine ganze Zahl ω durch jede von ihnen teilbar, so ist sie auch durch ihr Produkt teilbar (vgl. § 7), weil, wie man leicht findet, auch der folgende Satz (§ 5, 3.) seine Gültigkeit behält: Ist jede der Zahlen α', β', γ' ... relative Primzahl zu jeder der Zahlen α'', β'', γ'', δ'' ..., so sind auch die Produkte $\alpha'\beta'\gamma'$ ... und $\alpha''\beta''\gamma''\delta''$ ... relative Primzahlen und umgekehrt.

Aber wie soll man definitiv entscheiden, ob zwei gegebene ganze Zahlen α, β relative Primzahlen sind? Man könnte versuchen, folgenden Weg einzuschlagen. Da α^{-1} und β^{-1} algebraische Zahlen sind, so gibt es (zufolge 5.) immer zwei kleinste positive ganze rationale Zahlen a, b von der Art, daß $a\alpha^{-1}$ und $b\beta^{-1}$ ganze Zahlen, d. h. daß a, b bzw. durch α, β teilbar werden; zeigt sich nun, daß a, b relative Primzahlen sind, so sind auch α, β gewiß relative Primzahlen. Aber man muß sich hüten zu glauben, daß auch das Umgekehrte stattfindet, daß also die kleinsten rationalen Multipla a, b von zwei relativen Primzahlen α, β notwendig selbst relative Primzahlen sein müssen. So z. B. sind in der Tat die beiden konjugierten Zahlen $\alpha = 2 + i$ und $\beta = 2 - i$ relative Primzahlen, und doch ist $a = b = 5$. Eine wesentliche Reduktion unserer Aufgabe wird aber durch den folgenden Satz bewirkt:

Wenn zwei ganze Zahlen α, β sich in einem Körper K, dem sie selbst angehören, als relative Primzahlen bewähren, d. h. wenn jede durch α und β teilbare Zahl des Körpers K auch durch $\alpha\beta$ teilbar ist, so sind α, β wirklich relative Primzahlen.

Ist nämlich ω irgendeine durch α und durch β teilbare ganze Zahl, und ist

$$\omega^m + \gamma_1 \omega^{m-1} + \gamma_2 \omega^{m-2} + \cdots + \gamma_m = 0$$

die in K irreduktible Gleichung, welcher ω genügt, so sind (zufolge 4.) die Zahlen $\gamma_1, \gamma_2, \ldots, \gamma_m$ ganze Zahlen des Körpers K; da ferner die ganzen Zahlen $\alpha' = \omega : \alpha$ und $\beta' = \omega : \beta$ bzw. den in K irreduktiblen 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 teilbare Zahl des Körpers K auch durch $\alpha\beta$ teilbar ist, so ergibt sich leicht, daß auch jede durch α^n und β^n teilbare Zahl γ_n des Körpers K durch $\alpha^n\beta^n$ teilbar, 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 Koeffizienten ganze Zahlen sind; mithin ist ω' (zufolge 3.) eine ganze Zahl, d. h. ω ist auch teilbar 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 komplexen 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 kongruent nach $\mathfrak{a}$ nennen und dies durch die Kongruenz

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

andeuten. Solche Kongruenzen können addiert, subtrahiert und folglich auch mit beliebigen ganzen rationalen Zahlen multipliziert werden, wie Gleichungen. Da je zwei einer dritten kongruente Zahlen auch einander kongruent sind, so kann man alle existierenden Zahlen in Klassen (mod $\mathfrak{a}$) einteilen, indem man je zwei kongruente Zahlen in dieselbe Klasse, je zwei inkongruente in zwei verschiedene Klassen 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 Teiler von $\mathfrak{a}$; oder wir sagen auch, $\mathfrak{b}$ gehe in $\mathfrak{a}$ auf, $\mathfrak{a}$ sei teilbar durch $\mathfrak{b}$. Aus jeder Kongruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$ folgt auch $\omega \equiv \omega' \pmod{\mathfrak{b}}$. Offenbar besteht $\mathfrak{b}$ aus einer endlichen oder unendlichen Anzahl von Klassen (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 $\mathfrak{m}$ teilbar 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 Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, weil jeder gemeinschaftliche Teiler 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

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n, \tag{1}$$

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

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

Da es nämlich n rationale, von Null verschiedene Zahlen $r_1, r_2, \ldots, r_n$ der Art gibt, daß die Produkte $r_1\omega_1, r_2\omega_2, \ldots, r_n\omega_n$ in $\mathfrak{m}$ enthalten sind, so gibt es auch eine ganze rationale, von Null verschiedene Zahl s der Art, daß alle Produkte $s\omega \equiv 0 \pmod{\mathfrak{m}}$ 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 kongruent (mod $\mathfrak{m}$); mithin ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ inkongruenten Zahlen höchstens $= s^n$, was zu beweisen war.

Allein es ist wichtig, die Anzahl dieser inkongruenten Zahlen genau zu bestimmen. Zu diesem Zwecke betrachten wir das kleinste gemeinschaftliche Vielfache $\mathfrak{a}$ der beiden Moduln $\mathfrak{o}$ und $\mathfrak{m}$; da je zwei nach $\mathfrak{m}$ kongruente Zahlen ω, ω' des Moduls $\mathfrak{o}$ auch nach $\mathfrak{a}$ kongruent sind, und umgekehrt, so ist unsere Aufgabe die, die Anzahl der Klassen (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 gibt 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 Wert $a_r^{(r)}$ besitzt. Dann leuchtet ein, daß der Wert von k_r in jeder Zahl θ_r durch $a_r^{(r)}$

teilbar, 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 partikuläre 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 $\mathfrak{m}$ kongruent sind, welche also eine Klasse (mod $\mathfrak{a}$) bilden, von der Form

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

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 sukzessive 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 Klasse existiert daher ein und nur ein Repräsentant ω' von der Form (6), welcher diesen Bedingungen (7) genügt; mithin ist die Anzahl der verschiedenen Klassen (mod $\mathfrak{a}$), aus welchen der Modul $\mathfrak{o}$ besteht, gleich dem Produkte $a_1' a_2'' \ldots a_n^{(n)}$, d. h. gleich der Determinante des Koeffizientensystems in den n partikulären Zahlen α_r von der Form (3), welche eine Basis von $\mathfrak{a}$ bilden**).

---

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

**) Die weitere Entwicklung der allgemeinen Theorie der Moduln würde uns hier zu weit führen (vgl. § 163); wir erwähnen nur noch folgenden Satz: Sind die Basiszahlen eines endlichen Moduls voneinander abhängig, so gibt 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).

§ 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 Multiplikation 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, sämtlich ganze Zahlen sind, und es wird dann (zufolge § 160, 1.) jede Zahl

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

gewiß eine ganze Zahl sein, wenn ihre Koordinaten 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 Koordinaten teilweise oder sämtlich gebrochene Zahlen sind. Dies ist einer der wichtigsten Punkte der Theorie und muß deshalb vor allem aufgeklärt werden.

Wir schicken zunächst die einleuchtende Bemerkung voraus, daß die Diskriminante [§ 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, Subtraktion und Multiplikation aus lauter ganzen Zahlen gebildet ist. Gibt es nun wirklich in Ω eine ganze Zahl

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

wo $s, k_1, k_2, \ldots, k_n$ ganze rationale Zahlen ohne gemeinschaftlichen Teiler bedeuten, deren erste $s > 1$ ist, so behaupten wir, daß s^2 in der Diskriminante $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ aufgeht, und daß man eine neue Basis von ganzen Zahlen $\beta_1, \beta_2, \ldots, \beta_n$ aufstellen kann, deren Diskriminante 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 teilbaren ganzen Zahlen bestehenden Modul, ebenso mit $\mathfrak{o}$ das System aller Zahlen ω von der Form (1), deren Koordinaten h_ι ganze Zahlen sind; da jedes Produkt $s\omega$ eine Zahl des Moduls $\mathfrak{m}$ ist, so können wir die allgemeine Untersuchung des vorigen Paragraphen auf unsern

Fall anwenden. Alle durch s teilbaren Zahlen α des Systems $\mathfrak{o}$ sind daher von der Form

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

wo die n Zahlen $\alpha_\iota = s\beta_\iota$ partikuläre 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

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

setzen, wo die Koeffizienten $b_\iota^{(r)}$ rationale ganze Zahlen sind und b die aus ihnen gebildete Determinante bedeutet; durch Umkehrung ergibt sich, daß die n Produkte $b\beta_\iota$, 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 $\Sigma k_\iota \omega_\iota$ also eine Zahl α ist, obgleich die Zahlen $s, k_1, k_2, \ldots, k_n$ keinen gemeinschaftlichen Teiler haben, so folgt unmittelbar, daß b durch s teilbar ist, wodurch zugleich die obigen Behauptungen erwiesen sind.

Da nun die Diskriminante eines jeden Systems von n unabhängigen ganzen Zahlen des Körpers Ω eine von Null verschiedene ganze rationale Zahl ist, so gibt es unter allen diesen Diskriminanten eine solche, deren Wert — 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 Diskriminante diesen Minimumwert besitzt, die entsprechenden Koordinaten h_ι einer jeden ganzen Zahl ω des Körpers notwendig 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 Koordinaten gebildete Determinante $= \pm 1$ wird.

Die wichtigste Rolle spielt aber die Minimaldiskriminante selbst, sowohl hinsichtlich der inneren*) Konstitution des Körpers Ω, als

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

auch hinsichtlich seiner Verwandtschaft mit anderen Körpern*); wir wollen daher diese positive oder negative ganze rationale Zahl die Grundzahl oder die Diskriminante des Körpers Ω nennen und mit $\Delta(\Omega)$ bezeichnen; sie ist offenbar zugleich die Grundzahl eines jeden mit Ω konjugierten 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 teilbar 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 $= 4D$.

Ist ferner θ eine primitive Wurzel der Gleichung $\theta^m = 1$ (§ 139), wo $m > 2$, so bilden die Zahlen 1, θ, θ^2, ..., θ^{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 Prinzipien ergibt 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 inkongruenten ganzen Zahlen des Körpers gleich dem absoluten Wert der Norm des Moduls μ.

Es sei $\mathfrak{m}$ das System aller durch μ teilbaren ganzen Zahlen (welche sich durch Addition und Subtraktion reproduzieren) und $\mathfrak{o}$

*) 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 erspare, näher anzudeuten, führe ich nur das einfachste Beispiel an: das kleinste gemeinschaftliche Multiplum zweier voneinander 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 Produkt aus den Grundzahlen von A, B, C, und zwar eine Quadratzahl.

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 Koordinaten h_ι beliebige ganze rationale Zahlen bedeuten; da jeder Quotient $\omega : \mu$ (zufolge § 160, 5.) durch Multiplikation mit einer von Null verschiedenen ganzen rationalen Zahl in eine ganze Zahl verwandelt werden kann, so ist die Untersuchung des vorigen Paragraphen auf unseren Fall anwendbar. Mithin sind alle durch μ teilbaren 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 $\alpha_\iota = \mu \beta_\iota$ partikuläre Zahlen α bedeuten, also die Zahlen β_ι in $\mathfrak{o}$ enthalten sind, und die Größen x_ι alle rationalen ganzen Zahlwerte annehmen dürfen; die Anzahl der Klassen, in welche das System $\mathfrak{o}$ in bezug auf den Modul μ zerfällt, ist ferner gleich der aus den Koordinaten 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 teilbare 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 Grundreihe 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 inkongruenten Repräsentanten der verschiedenen Klassen, 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

*) Bilden die n Zahlen ω_ι irgendeine Basis des Körpers Ω, und ist $\mathfrak{o}$ das System aller der Zahlen ω von der Form (1), deren Koordinaten ganze Zahlen sind, so reproduzieren sich die Zahlen des Systems $\mathfrak{o}$ durch Addition und Subtraktion; nimmt man ferner an, daß sie sich auch durch Multiplikation reproduzieren, woraus zugleich folgt, daß sie ganze Zahlen sind, und nennt man zwei solche Zahlen ω, ω' stets und nur dann kongruent 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 inkongruenten Zahlen ebenfalls $= \pm N(\mu)$. Vgl. § 165, 4.

μ teilbare ganze Zahl $\theta\omega$ auch teilbar durch $\theta\mu$, mithin sind θ, μ relative Primzahlen; besitzt aber die Kongruenz $\theta\omega \equiv 0 \pmod{\mu}$ 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 $\theta\mu$ teilbar, 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 Kongruenz $\theta\omega \equiv \theta' \pmod{\mu}$ immer eine und nur eine Wurzel ω (vgl. § 22); ist ferner $\psi(\mu)$ die Anzahl aller Klassen, deren Zahlen relative Primzahlen zum Modul μ sind, so durchläuft $\theta\omega$ gleichzeitig mit ω die Repräsentanten aller dieser Klassen, und da das Produkt dieser Zahlen ω auch relative Primzahl zu μ ist, so ergibt sich der Satz

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

welcher dem Fermatschen 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 Faktoren auf, welche demselben System $\mathfrak{o}$ angehören, 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 eigentümliches Phänomen auf, das schon früher (§ 16) gelegentlich erwähnt ist*). Nennt man eine Zahl in $\mathfrak{o}$ zerlegbar, wenn sie das Produkt 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 Produkt aus einer endlichen Anzahl von unzerlegbaren Zahlen (vgl. § 8), weil die Norm von μ gleich dem Produkte aus den Normen der einzelnen Faktoren ist (§ 159); aber es zeigt sich häufig, daß diese Zerlegung nicht

*) 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 Tat 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 $\varkappa^2 = -5$ entsprechenden quadratischen Körper an dem Beispiel $3 \cdot 7 = (1+2\varkappa)(1-2\varkappa)$ wirklich auf (vgl. § 71; die beiden Zahlen 3, 7 sind durch die Hauptform der Determinante -5 nicht darstellbar).

eine vollkommen bestimmte ist, sondern daß mehrere wesentlich verschiedene Zerlegungen derselben Zahl in unzerlegbare Faktoren existieren (§ 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 teilbare Produkt $\eta\varrho$ wenigstens einen durch μ teilbaren Faktor η oder ϱ besitzt.

Es ergibt sich dann sofort, daß die höchste in einem Produkte aufgehende Potenz einer Primzahl μ das Produkt aus den höchsten in den einzelnen Faktoren aufgehenden Potenzen von μ, und daß jede durch μ nicht teilbare Zahl relative Primzahl zu μ ist. Man erkennt ferner leicht, daß die kleinste durch μ teilbare rationale ganze Zahl p notwendig 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), existieren also zwei durch μ nicht teilbare Zahlen η, ϱ, deren Produkt $\eta\varrho$ durch μ teilbar ist, so schreiten wir zu einer Zerlegung von μ in wirkliche oder ideale, d. h. fingierte Faktoren. Gibt es nämlich in $\mathfrak{o}$ einen größten gemeinschaftlichen Teiler 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 Faktoren ν und μ' zerlegt, von denen keiner eine Einheit ist, weil weder ϱ noch η durch μ teilbar ist. Der Faktor μ' ist wesentlich dadurch bestimmt, daß alle Wurzeln α' der Kongruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ durch μ' teilbar sind (z. B. auch $\alpha' = \varrho$), und daß ebenso jede durch μ' teilbare Zahl α' auch der vorstehenden Kongruenz genügt. Umgekehrt, gibt es in $\mathfrak{o}$ eine Zahl μ', welche in allen Wurzeln α' der Kongruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ und nur in diesen aufgeht, so ist auch μ teilbar durch μ', und der Quotient $\nu = \mu : \mu'$ ist der größte gemeinschaftliche Teiler 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 fingieren und dieselbe als ideale Zahl einzuführen; die Teilbarkeit einer Zahl α' durch diese ideale Zahl μ' besteht lediglich darin, daß α' eine Wurzel der Kongruenz $\eta\,\alpha' \equiv 0 \pmod{\mu}$ ist, und da diese idealen Zahlen in der Folge immer nur als Teiler oder Moduln auftreten, so hat diese Art ihrer Einführung durchaus keine Bedenken. Allein die Befürchtung, daß die unmittelbare Übertragung 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.

§ 163.

Wir gründen die Theorie der in $\mathfrak{o}$ enthaltenen Zahlen, d. h. aller ganzen Zahlen des Körpers Ω, auf den folgenden neuen Begriff.

1. Ein System $\mathfrak{a}$ von unendlich vielen in $\mathfrak{o}$ enthaltenen Zahlen soll ein Ideal heißen, wenn es den beiden Bedingungen genügt:

I. Die Summe und die Differenz je zweier Zahlen in $\mathfrak{a}$ sind wieder Zahlen in $\mathfrak{a}$.

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

Ist α in $\mathfrak{a}$ enthalten, so sagen wir, α sei teilbar durch $\mathfrak{a}$, $\mathfrak{a}$ gehe in α auf, weil die Ausdrucksweise hierdurch an Leichtigkeit gewinnt. Wir nennen ferner zwei in $\mathfrak{o}$ enthaltene Zahlen ω, ω', deren Differenz durch $\mathfrak{a}$ teilbar ist, kongruent nach $\mathfrak{a}$ (vgl. § 161), und bezeichnen dies durch die Kongruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$; solche Kongruenzen dürfen (zufolge I.) addiert, subtrahiert und (zufolge II.) multipliziert werden, wie Gleichungen. Da je zwei einer dritten kongruente Zahlen auch einander kongruent sind, so kann man alle Zahlen in Klassen (mod $\mathfrak{a}$) einteilen, indem man je zwei kongruente Zahlen in dieselbe, je zwei inkongruente Zahlen in zwei verschiedene Klassen wirft; da nun, wenn μ eine von Null verschiedene Zahl in $\mathfrak{a}$ bedeutet, je zwei nach μ kongruente Zahlen (zufolge II.) auch nach $\mathfrak{a}$ kongruent sind — woraus zugleich folgt, daß $\mathfrak{a}$ aus einer oder

mehreren Klassen (mod μ) besteht —, so ist (zufolge § 162, 2.) die Anzahl der Klassen (mod $\mathfrak{a}$), in welche $\mathfrak{o}$ zerfällt, endlich*). Wählt man aus jeder Klasse ein Individuum als Repräsentanten, so bilden dieselben ein vollständiges Restsystem (mod $\mathfrak{a}$); die Anzahl dieser Klassen oder inkongruenten Zahlen soll die Norm von $\mathfrak{a}$ heißen und mit $N(\mathfrak{a})$ bezeichnet werden.

Ist η eine von Null verschiedene Zahl in $\mathfrak{o}$, so bilden alle durch η teilbaren Zahlen in $\mathfrak{o}$ ein Ideal, welches mit $\mathfrak{i}(\eta)$ bezeichnet werden soll; solche Ideale sind besonders ausgezeichnet und sollen Hauptideale heißen; die Norm von $\mathfrak{i}(\eta)$ ist $= \pm N(\eta)$; ist η eine Einheit, so ist $\mathfrak{i}(\eta) = \mathfrak{o}$, und umgekehrt.

2. Wenn alle Zahlen eines Ideals $\mathfrak{a}$ auch in einem Ideal $\mathfrak{b}$ enthalten sind, so besteht offenbar $\mathfrak{b}$ aus einer oder mehreren Klassen (mod $\mathfrak{a}$), und wir wollen sagen, $\mathfrak{a}$ sei ein Multiplum von $\mathfrak{b}$ oder teilbar durch $\mathfrak{b}$, $\mathfrak{b}$ sei ein Teiler von $\mathfrak{a}$ oder gehe in $\mathfrak{a}$ auf.

Besteht $\mathfrak{b}$ aus r Klassen (mod $\mathfrak{a}$), so ist $N(\mathfrak{a}) = rN(\mathfrak{b})$. Durchläuft nämlich δ die Repräsentanten dieser r Klassen und γ ein vollständiges Restsystem (mod $\mathfrak{b}$), so bilden die $rN(\mathfrak{b})$ Zahlen $\gamma + \delta$ ein vollständiges Restsystem (mod $\mathfrak{a}$); denn erstens ist jede Zahl in $\mathfrak{o}$ kongruent einer Zahl γ (mod $\mathfrak{b}$), also $\equiv \gamma + \delta$ (mod $\mathfrak{a}$), und zweitens folgt aus $\gamma + \delta \equiv \gamma' + \delta'$ (mod $\mathfrak{a}$), wo γ', δ' ähnliche Bedeutung haben wie γ, δ, sukzessive $\gamma + \delta \equiv \gamma' + \delta'$ (mod $\mathfrak{b}$), $\gamma \equiv \gamma'$ (mod $\mathfrak{b}$), $\gamma = \gamma'$, also $\delta \equiv \delta'$ (mod $\mathfrak{a}$), $\delta = \delta'$, d. h. die sämtlichen Zahlen $\gamma + \delta$ sind inkongruent (mod $\mathfrak{a}$).

Ein Ideal besitzt folglich nur eine endliche Anzahl von Teilern. Ist $\mathfrak{m}$ teilbar durch $\mathfrak{a}$, $\mathfrak{a}$ durch $\mathfrak{b}$, so ist auch $\mathfrak{m}$ durch $\mathfrak{b}$ teilbar. Das Hauptideal $\mathfrak{o}$ selbst geht in jedem Ideal auf und ist zugleich das einzige Ideal, welches die Zahl 1 oder überhaupt Einheiten enthält, und dessen Norm $= 1$ ist.

Das System aller derjenigen Zahlen, welche gleichzeitig in zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind, ist das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ von $\mathfrak{a}$, $\mathfrak{b}$, insofern jedes gemeinschaftliche Multiplum von $\mathfrak{a}$, $\mathfrak{b}$ durch das Ideal $\mathfrak{m}$ teilbar ist. Durchläuft α alle Zahlen in $\mathfrak{a}$, β alle Zahlen in $\mathfrak{b}$, so ist das System aller Zahlen $\alpha + \beta$ der

*) Dasselbe ergibt sich unmittelbar aus § 161; ist nämlich ω irgendeine Zahl in $\mathfrak{o}$, so kann durch Multiplikation mit einer von Null verschiedenen ganzen rationalen Zahl der Quotient $\omega : \mu$ in eine ganze Zahl, also ω (zufolge II.) in eine Zahl des Ideals $\mathfrak{a}$ verwandelt werden.

größte gemeinschaftliche Teiler $\mathfrak{d}$ der Ideale $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideale $\mathfrak{d}$ aufgeht*).

Ist r die Anzahl der in $\mathfrak{b}$ enthaltenen Zahlen, welche (mod $\mathfrak{a}$) inkongruent sind, so besteht $\mathfrak{b}$ aus r Klassen (mod $\mathfrak{m}$), und $\mathfrak{d}$ aus r Klassen (mod $\mathfrak{a}$); also ist $N(\mathfrak{m}) = rN(\mathfrak{b})$, $N(\mathfrak{a}) = rN(\mathfrak{d})$ und $N(\mathfrak{m})N(\mathfrak{d}) = N(\mathfrak{a})N(\mathfrak{b})$.

Ist $\mathfrak{b}$ ein Hauptideal $= \mathfrak{i}(\eta)$, so ist die Anzahl r der in $\mathfrak{b}$ enthaltenen Zahlen $\beta = \eta\omega$, welche (mod $\mathfrak{a}$) inkongruent sind, zugleich die Norm des aus allen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0$ (mod $\mathfrak{a}$) bestehenden Ideals $\mathfrak{r}$, weil zwei Zahlen ω, ω' stets und nur dann kongruent (mod $\mathfrak{r}$) sind, wenn $\eta\omega \equiv \eta\omega'$ (mod $\mathfrak{a}$) ist. Mithin ist in diesem Falle $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$.

3. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$, welches keinen von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenen Teiler besitzt, soll ein Primideal heißen. Dann gilt folgender Satz:

Ist $\eta\varrho \equiv 0$ (mod $\mathfrak{p}$), so ist wenigstens eine der beiden Zahlen η, ϱ durch $\mathfrak{p}$ teilbar. Ist nämlich η nicht $\equiv 0$ (mod $\mathfrak{p}$), so bilden die sämtlichen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0$ (mod $\mathfrak{p}$) offenbar ein in $\mathfrak{p}$ aufgehendes Ideal, welches, da es die Zahl 1 nicht enthält, von $\mathfrak{o}$ verschieden und folglich mit $\mathfrak{p}$ identisch ist, was zu beweisen war.

Dieser Satz ist charakteristisch für ein Primideal, da er sich folgendermaßen umkehren läßt: Enthält jedes durch ein (von $\mathfrak{o}$ verschiedenes) Ideal $\mathfrak{p}$ teilbare Produkt mindestens einen durch $\mathfrak{p}$ teilbaren Faktor, so ist $\mathfrak{p}$ ein Primideal. Ist nämlich $\mathfrak{q}$ ein Teiler des Ideals $\mathfrak{p}$, aber verschieden von $\mathfrak{p}$, so gibt es in $\mathfrak{q}$ eine nicht in $\mathfrak{p}$ enthaltene Zahl ω; dann ist (zufolge der Annahme) auch keine der Potenzen ω^2, ω^3 ... durch $\mathfrak{p}$ teilbar; da aber nur eine endliche Anzahl von inkongruenten Zahlen (mod $\mathfrak{p}$) existiert, so muß einmal für zwei verschiedene Exponenten m und $m + s > m$ notwendig $\omega^{m+s} \equiv \omega^m$ (mod $\mathfrak{p}$), also das Produkt $\omega^m(\omega^s - 1)$ durch $\mathfrak{p}$ teilbar sein; da nun ω^m nicht durch $\mathfrak{p}$ teilbar ist, so muß (zufolge der Annahme) der andere Faktor $\omega^s - 1$ durch $\mathfrak{p}$, und folglich auch durch $\mathfrak{q}$ teilbar sein; nun ist ω und, weil $s > 0$ ist, auch $\omega^s \equiv 0$ (mod $\mathfrak{q}$), mithin ist auch die Zahl 1 in $\mathfrak{q}$ enthalten, also $\mathfrak{q} = \mathfrak{o}$, was zu beweisen war.

*) Die Erweiterung dieser Definitionen von $\mathfrak{m}$ und $\mathfrak{d}$ für mehr als zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ ... liegt auf der Hand.

Nennt man ein von $\mathfrak{o}$ verschiedenes Ideal zusammengesetzt, wenn es kein Primideal ist, so läßt sich dieser Satz auch so aussprechen: Ist $\mathfrak{a}$ ein zusammengesetztes Ideal, so gibt es zwei durch $\mathfrak{a}$ nicht teilbare Zahlen η, ϱ, deren Produkt $\eta\varrho$ durch $\mathfrak{a}$ teilbar ist. Wir beweisen ihn zum zweiten Male auf folgende Art. Es sei $\mathfrak{e}$ ein von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedener Teiler von $\mathfrak{a}$, so gibt es in $\mathfrak{e}$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η, und der größte gemeinschaftliche Teiler $\mathfrak{d}$ von $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ ist teilbar durch $\mathfrak{e}$, also von $\mathfrak{o}$ verschieden, mithin ist $N(\mathfrak{d}) > 1$. Das aus allen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0 \pmod{\mathfrak{a}}$ bestehende Ideal $\mathfrak{r}$ ist ein Teiler von $\mathfrak{a}$, und da (zufolge 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d}) > N(\mathfrak{r})$ ist, so ist $\mathfrak{r}$ verschieden von $\mathfrak{a}$ und enthält folglich eine durch $\mathfrak{a}$ nicht teilbare Zahl ϱ, was zu beweisen war.

Es leuchtet nun ein, daß die kleinste (von Null verschiedene) rationale Zahl p, welche in einem Primideale $\mathfrak{p}$ enthalten ist, notwendig eine Primzahl (im rationalen Zahlkörper) sein muß; da ferner $\mathfrak{p}$ in $\mathfrak{i}(p)$ aufgeht, so ist $N(\mathfrak{p})$ ein Teiler von $N(p) = p^n$, also ebenfalls eine Potenz p^f der rationalen Primzahl p, und man findet leicht (vgl. § 162, 3.), daß jede in $\mathfrak{o}$ enthaltene Zahl ω der Kongruenz

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}}$$

genügt*). Auch hat es keine Schwierigkeit, die allgemeinen Sätze der §§ 26, 27, 29, 30, 31 auf Kongruenzen in bezug auf den Modul $\mathfrak{p}$ zu übertragen.

---

*) Hierauf beruht das Eingreifen der Theorie der höheren Kongruenzen (vgl. § 26), welche zur Bestimmung der Primideale dient. Für die Körper vom Grade $n = \varphi(m)$, welche aus den primitiven Wurzeln θ der Gleichung $\theta^m = 1$ entspringen, ist dieselbe zuerst ausgeführt, und zwar von Kummer, dem Schöpfer der Theorie der idealen Zahlen; den hierauf bezüglichen Teil seiner Untersuchungen findet man am vollständigsten zusammengestellt in den Abhandlungen: Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers (Journ. de Math. p. p. Liouville, T. XVI, 1851). — Theorie der idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist (Abh. der Berliner Ak. 1856). Das Hauptresultat ergibt sich mit größter Leichtigkeit aus unserer Theorie und lautet in unserer Ausdrucksweise folgendermaßen: Ist p eine rationale Primzahl und m' der größte durch p nicht teilbare Divisor von $m = p'm'$, gehört ferner p zum Exponenten $f \pmod{m'}$, wo $\varphi(m') = ef$ (§ 28), so ist $\mathfrak{i}(p) = (\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_e)^{\varphi(p')}$, wo $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_e$ voneinander verschiedene Primideale bedeuten, deren Normen $= p^f$ sind; wenn $p' > 1$, so ist $\mathfrak{i}(1-\theta^{m'}) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_e$. — Für komplexe Zahlen einer höheren Stufe vgl. Kummer: Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine

Ist das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ durch das Primideal $\mathfrak{p}$ teilbar, so geht $\mathfrak{p}$ wenigstens in einem der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ auf. Ist nämlich keins dieser Ideale durch $\mathfrak{p}$ teilbar, gibt es also in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ bzw. Zahlen $\alpha, \beta, \gamma, \ldots$, die nicht durch $\mathfrak{p}$ teilbar sind, so ist das in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$, also auch in $\mathfrak{m}$ enthaltene Produkt $\alpha\beta\gamma \ldots$ nicht teilbar durch das Primideal $\mathfrak{p}$, und folglich geht $\mathfrak{p}$ nicht in $\mathfrak{m}$ auf, was zu beweisen war.

Ist die Zahl η nicht teilbar durch das Ideal $\mathfrak{a}$, so gibt es immer eine durch η teilbare Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ ein Primideal bilden. Alle Wurzeln β der Kongruenz $\eta\beta \equiv 0 \pmod{\mathfrak{a}}$ bilden ein in $\mathfrak{a}$ aufgehendes Ideal $\mathfrak{b}$, welches von $\mathfrak{o}$ verschieden ist, weil es die Zahl 1 nicht enthält; ist $\mathfrak{b}$ ein Primideal, so ist der Satz bewiesen. Ist $\mathfrak{b}$ kein Primideal, gibt es also zwei durch $\mathfrak{b}$ nicht teilbare Zahlen η', ϱ', deren Produkt $\eta'\varrho' \equiv 0 \pmod{\mathfrak{b}}$ ist, so bilden alle Wurzeln γ der Kongruenz $\eta'\gamma \equiv 0 \pmod{\mathfrak{b}}$, d. h. der Kongruenz $\eta\eta'\gamma \equiv 0 \pmod{\mathfrak{a}}$, ein in $\mathfrak{b}$ aufgehendes Ideal $\mathfrak{c}$, und zwar ist (zufolge 2.) $N(\mathfrak{c}) < N(\mathfrak{b})$, weil ϱ' in $\mathfrak{c}$, aber nicht in $\mathfrak{b}$ enthalten ist; außerdem ist $\mathfrak{c}$ von $\mathfrak{o}$ verschieden, weil η' nicht in $\mathfrak{b}$ und folglich die Zahl 1 nicht in $\mathfrak{c}$ enthalten ist; ist $\mathfrak{c}$ ein Primideal, so ist der Satz bewiesen. Ist aber $\mathfrak{c}$ kein Primideal, so kann man in derselben Weise fortfahren; endlich muß in der Reihe der Ideale $\mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$, deren Normen immer kleiner werden, aber stets > 1 bleiben, ein Primideal $\mathfrak{p}$ auftreten, welches aus allen Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ besteht, wo $\nu = \eta\eta'\eta'' \ldots$ durch η teilbar ist.

4. Ist μ eine von Null verschiedene Zahl in $\mathfrak{o}$ und keine Einheit, so existiert zufolge des zuletzt bewiesenen Satzes (in welchem man

---

Primzahl ist (Abh. der Berliner Ak. 1859). — Für diejenigen Körper Ω, deren konjugierte Körper mit Ω identisch sind, und welche ich Galoissche Körper nennen möchte, vgl. Selling: Über die idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzeln einer beliebigen irreduktibelen Gleichung rational gebildet sind (Schlömilchs Zeitschr. für Math. u. Phys. Bd. 10. 1865). — Ein spezieller Fall biquadratischer Körper ist vollständig durchgeführt von Bachmann: Die Theorie der komplexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind. 1867. — Für eine gewisse Klasse kubischer Körper vgl. Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken (Crelles Journ. XXVIII).

$\eta = 1$ nehmen kann) jedenfalls eine Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein Primideal $\mathfrak{p}$ bilden; Primideale, welche aus den sämtlichen Wurzeln einer solchen Kongruenz bestehen, wollen wir vorläufig einfache Ideale nennen. Ist nun r irgendein ganzer rationaler, nicht negativer Exponent, so bilden alle Wurzeln ϱ der Kongruenz $\varrho\nu^r \equiv 0 \pmod{\mu^r}$ ein Ideal, welches die $r$te Potenz von $\mathfrak{p}$ heißen und mit $\mathfrak{p}^r$ bezeichnet werden soll. Diese Definition ist unabhängig von dem zur Definition von $\mathfrak{p}$ benutzten Zahlenpaar μ, ν; ist nämlich μ' irgendeine von Null verschiedene, durch $\mathfrak{p}$ teilbare Zahl, also $\nu\mu' = \mu\nu'$, so folgt aus $\varrho\nu^r \equiv 0 \pmod{\mu^r}$ durch Multiplikation mit μ'^r und Division durch μ^r auch $\varrho\nu'^r \equiv 0 \pmod{\mu'^r}$, und umgekehrt. Von der größten Wichtigkeit sind aber die folgenden Sätze über einfache Ideale $\mathfrak{p}$:

Ist $s \geqq r$, so ist $\mathfrak{p}^s$ teilbar durch $\mathfrak{p}^r$. Ist nämlich σ in $\mathfrak{p}^s$ enthalten, also $\sigma\nu^s = \tau\mu^s$, so folgt, daß

$$\left(\frac{\sigma\nu^r}{\mu^r}\right)^s = \tau^r\sigma^{s-r}$$

eine ganze Zahl ist; mithin ist (nach § 160, 3.) der jedenfalls dem Körper Ω angehörige Quotient $\sigma\nu^r : \mu^r$ ebenfalls eine ganze Zahl, also in $\mathfrak{o}$ enthalten, weil $\mathfrak{o}$ alle ganzen Zahlen des Körpers Ω umfaßt*); also ist jede Zahl σ des Ideals $\mathfrak{p}^s$ auch in $\mathfrak{p}^r$ enthalten.

Ist ϱ eine von Null verschiedene Zahl in $\mathfrak{o}$, so gibt es immer eine höchste in ϱ aufgehende Potenz von $\mathfrak{p}$. Wäre nämlich für unendlich viele Exponenten r das Produkt $\varrho\nu^r$ teilbar durch μ^r, so müßte, da nur eine endliche Anzahl inkongruenter Zahlen (mod ϱ) existiert, für zwei verschiedene solche Exponenten r s notwendig einmal

$$\frac{\varrho\nu^r}{\mu^r} \equiv \frac{\varrho\nu^s}{\mu^s} \pmod{\varrho}, \quad \left(\frac{\nu}{\mu}\right)^r = \left(\frac{\nu}{\mu}\right)^s + \omega$$

werden, wo ω eine ganze Zahl; hieraus würde aber (nach § 160, 3.) folgen, daß ν durch μ teilbar wäre, was nicht der Fall ist, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre.

Sind $\mathfrak{p}^r$, $\mathfrak{p}^s$ bzw. die höchsten in ϱ, σ aufgehenden Potenzen, so ist $\mathfrak{p}^{r+s}$ die höchste in $\varrho\sigma$ aufgehende Potenz von $\mathfrak{p}$.

*) Sobald diese Bedingung nicht erfüllt ist, verlieren auch die obigen Sätze ihre allgemeine Gültigkeit; dies ist von Wichtigkeit für die Erweiterung der Definition der Ideale (vgl. § 165, 4.).

Denn da $\varrho\nu^r = \varrho'\mu^r$, $\sigma\nu^s = \sigma'\mu^s$ und keins der Produkte $\nu\varrho'$, $\nu\sigma'$ durch μ teilbar ist, so folgt $\varrho\sigma\nu^{r+s} = \varrho'\sigma'\mu^{r+s}$, und $\nu\varrho'\sigma'$ kann nicht durch μ teilbar sein, weil $\mathfrak{p}$ ein Primideal ist.

Ist $e \geqq 1$ der Exponent der höchsten in μ selbst aufgehenden Potenz von $\mathfrak{p}$, also $\mu\nu^e = \varkappa\mu^e$, wo $\nu\varkappa$ nicht teilbar durch μ, so folgt $\nu^e = \varkappa\mu^{e-1}$, d. h. der Exponent der höchsten in ν aufgehenden Potenz von $\mathfrak{p}$ ist $= e - 1$. Das Ideal $\mathfrak{p}^e$ besteht aus den sämtlichen Wurzeln θ der Kongruenz $\varkappa\theta \equiv 0 \pmod{\mu}$. Die ganze Zahl $\lambda = \varkappa\mu : \nu = \sqrt[e]{\mu\varkappa^{e-1}}$ ist durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar; mithin ist λ^r durch $\mathfrak{p}^r$, aber nicht durch $\mathfrak{p}^{r+1}$ teilbar, woraus beiläufig folgt, daß die Ideale $\mathfrak{p}^r$ und $\mathfrak{p}^{r+1}$ wirklich verschieden sind. Endlich leuchtet folgender Satz ein:

Jede Potenz $\mathfrak{p}^r$ eines einfachen Ideals $\mathfrak{p}$ ist durch kein von $\mathfrak{p}$ verschiedenes Primideal teilbar. Ist nämlich π irgendeine Zahl in $\mathfrak{p}$, so muß ein in $\mathfrak{p}^r$ aufgehendes Primideal in π^r, also (zufolge 3.) in π selbst, d. h. in $\mathfrak{p}$ aufgehen und folglich mit $\mathfrak{p}$ identisch sein.

5. Die Wichtigkeit der einfachen Ideale und ihre Analogie mit den rationalen Primzahlen tritt unmittelbar hervor in dem folgenden Hauptsatz:

Wenn alle in einer von Null verschiedenen Zahl μ aufgehenden Potenzen einfacher Ideale auch in einer Zahl η aufgehen, so ist η durch μ teilbar. Ist η nicht teilbar durch μ, so gibt es (zufolge 3.) eine durch η teilbare Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein in μ aufgehendes einfaches Ideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in μ aufgehende Potenz, so ist (nach 4.) $\mathfrak{p}^{e-1}$ die höchste in ν aufgehende Potenz, und da ν durch η teilbar ist, so kann η nicht durch $\mathfrak{p}^e$ teilbar sein, was zu beweisen war. Derselbe Satz läßt sich offenbar auch so aussprechen: Jedes Hauptideal $\mathfrak{i}(\mu)$ ist das kleinste gemeinschaftliche Multiplum aller in μ aufgehenden Potenzen von einfachen Idealen. Es folgt zunächst:

Jedes Primideal $\mathfrak{p}$ ist ein einfaches Ideal. Es sei μ irgendeine von Null verschiedene Zahl in $\mathfrak{p}$, so muß $\mathfrak{p}$ (zufolge 3.) in einer der Potenzen einfacher Ideale aufgehen, deren kleinstes gemeinschaftliches Multiplum $\mathfrak{i}(\mu)$ ist; mithin ist $\mathfrak{p}$ selbst (zufolge 4.) ein ein-

faches Ideal. — Wir sprechen daher künftig nur noch von Primidealen, nicht mehr von einfachen Idealen.

Wenn alle in einem Ideal $\mathfrak{m}$ aufgehenden Potenzen von Primidealen auch in einer Zahl η aufgehen, so ist η teilbar durch $\mathfrak{m}$. Ist η nicht teilbar durch $\mathfrak{m}$, so gibt es (nach 3.) eine durch η teilbare Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mathfrak{m}}$ ein Primideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in $\mathfrak{m}$ aufgehende Potenz von $\mathfrak{p}$, so gibt es in $\mathfrak{m}$ eine nicht durch $\mathfrak{p}^{e+1}$ teilbare Zahl μ, und das aus allen Wurzeln ϱ der Kongruenz $\nu\varrho \equiv 0 \pmod{\mu}$ bestehende Ideal $\mathfrak{r}$ ist teilbar durch $\mathfrak{p}$, weil $\nu\varrho \equiv 0 \pmod{\mathfrak{m}}$ ist. Sind nun $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... die sämtlichen höchsten in μ aufgehenden Potenzen verschiedener Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ..., so besteht $\mathfrak{r}$ zufolge des obigen Hauptsatzes aus allen gemeinschaftlichen Wurzeln ϱ der Kongruenzen $\nu\varrho \equiv 0 \pmod{\mathfrak{p}^e}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}'^{e'}}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}''^{e''}}$ usw., d. h. $\mathfrak{r}$ ist das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}''$, ..., welche bzw. aus den Wurzeln jeder einzelnen dieser Kongruenzen bestehen; da nun die Ideale $\mathfrak{q}'$, $\mathfrak{q}''$, ... als Teiler von $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... nicht durch $\mathfrak{p}$ teilbar sind, so muß, weil $\mathfrak{r}$ durch $\mathfrak{p}$ teilbar ist, auch $\mathfrak{q}$ (zufolge 3.) durch $\mathfrak{p}$ teilbar sein; es kann folglich $\mathfrak{p}^e$ nicht in ν aufgehen (weil sonst $\mathfrak{q} = \mathfrak{o}$, also nicht durch $\mathfrak{p}$ teilbar wäre), und da ν durch η teilbar ist, so kann $\mathfrak{p}^e$ auch nicht in η aufgehen, was zu beweisen war.

Dieser Fundamentalsatz läßt sich offenbar auch so aussprechen: Jedes Ideal ist das kleinste gemeinschaftliche Multiplum aller in ihm aufgehenden Potenzen von Primidealen. Er entspricht durchaus dem Fundamentalsatze der rationalen Zahlentheorie über die Zusammensetzung der Zahlen aus Primzahlen (§ 8); denn ihm zufolge ist jedes Ideal $\mathfrak{m}$ vollständig bestimmt, sobald die höchsten in $\mathfrak{m}$ aufgehenden Potenzen $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... von Primidealen gegeben sind; aus ihm ergibt sich auch ohne weiteres der folgende Satz: Ein Ideal $\mathfrak{m}$ ist stets und nur dann durch ein Ideal $\mathfrak{d}$ teilbar, wenn alle in $\mathfrak{d}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{m}$ aufgehen. Dies folgt unmittelbar aus dem Begriffe des kleinsten gemeinschaftlichen Multiplums.

Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Multiplum von $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ..., wo $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... voneinander verschiedene Primideale bedeuten, so ist $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{p}')^{e'} N(\mathfrak{p}'')^{e''} \ldots$ Es

gibt immer (zufolge 4.) eine durch $\mathfrak{p}^{e-1}$, aber nicht durch $\mathfrak{a} = \mathfrak{p}^e$ teilbare Zahl η; das aus allen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0 \pmod{\mathfrak{a}}$ bestehende Ideal $\mathfrak{r}$ ist verschieden von $\mathfrak{o}$ (weil es die Zahl 1 nicht enthält) und ein Teiler von $\mathfrak{p}$ (zufolge 4.), folglich identisch mit $\mathfrak{p}$; da ferner der größte gemeinschaftliche Teiler $\mathfrak{d}$ der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{i}(\eta)$ zufolge des eben bewiesenen Fundamentalsatzes $= \mathfrak{p}^{e-1}$ ist, so folgt (aus 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$, d. h. $N(\mathfrak{p}^e) = N(\mathfrak{p})N(\mathfrak{p}^{e-1})$, und hieraus allgemein $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. — Nun ist (zufolge der Definition 2.) das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ der Ideale $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... zugleich auch das der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{b}$, wo $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... bedeutet; da ferner (zufolge des Fundamentalsatzes) $\mathfrak{o}$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$ ist, so folgt (aus 2.) $N(\mathfrak{m}) = N(\mathfrak{a})N(\mathfrak{b})$, d. h. $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{b})$, und hieraus ergibt sich offenbar der zu beweisende Satz.

6. Multipliziert man alle Zahlen eines Ideals $\mathfrak{a}$ mit allen Zahlen eines Ideals $\mathfrak{b}$, so bilden diese Produkte und deren Summen ein durch $\mathfrak{a}$ und $\mathfrak{b}$ teilbares Ideal, welches das Produkt aus den Faktoren $\mathfrak{a}$ und $\mathfrak{b}$ heißen und mit $\mathfrak{a}\mathfrak{b}$ bezeichnet werden soll. Aus dieser Erklärung leuchtet sofort ein, daß $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, ferner $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ ist (vgl. §§ 1, 2, 147). Zugleich gilt folgender Satz:

Sind $\mathfrak{p}^a$, $\mathfrak{p}^b$ bzw. die höchsten in $\mathfrak{a}$, $\mathfrak{b}$ aufgehenden Potenzen des Primideals $\mathfrak{p}$, so ist $\mathfrak{p}^{a+b}$ die höchste in $\mathfrak{a}\mathfrak{b}$ aufgehende Potenz von $\mathfrak{p}$; und es ist $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Aus der Erklärung folgt nämlich unmittelbar (mit Rücksicht auf 4.), daß $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{p}^{a+b}$ teilbar ist; da ferner in $\mathfrak{a}$ eine durch $\mathfrak{p}^{a+1}$ nicht teilbare Zahl α, in $\mathfrak{b}$ eine durch $\mathfrak{p}^{b+1}$ nicht teilbare Zahl β existiert, so gibt es in $\mathfrak{a}\mathfrak{b}$ eine durch $\mathfrak{p}^{a+b+1}$ nicht teilbare Zahl $\alpha\beta$, womit der erste Teil des Satzes bewiesen ist. Ist also $\mathfrak{a}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$, ... der voneinander verschiedenen Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ..., und $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^b$, $\mathfrak{p}'^{b'}$, $\mathfrak{p}''^{b''}$, ..., so ist $\mathfrak{a}\mathfrak{b}$ dasjenige der Potenzen $\mathfrak{p}^{a+b}$, $\mathfrak{p}'^{a'+b'}$, $\mathfrak{p}''^{a''+b''}$, ..., woraus (mit Rücksicht auf 5.) auch der zweite Teil des Satzes folgt.

Da aus diesem Satze auch $\mathfrak{p}^a\mathfrak{p}^b = \mathfrak{p}^{a+b}$ folgt, so ist die oben (in 4.) gewählte Ausdrucks- und Bezeichnungsweise gerechtfertigt. Sind ferner $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... voneinander verschiedene Primideale, so ist $\mathfrak{p}^a\mathfrak{p}'^{a'}\mathfrak{p}''^{a''}$ ... das kleinste gemeinschaftliche Multiplum der Potenzen

$\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$, ... Auch leuchtet ein, daß der Begriff der Potenz durch die Definition $\mathfrak{a}^{r+1} = \mathfrak{a}\,\mathfrak{a}^r$ auf jedes Ideal $\mathfrak{a}$ ausgedehnt werden kann. Ist endlich $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, so gibt es immer ein und nur ein Ideal $\mathfrak{r}$ der Art, daß $\mathfrak{a} = \mathfrak{r}\,\mathfrak{b}$ wird; sind nämlich $\mathfrak{p}^a$, $\mathfrak{p}^d$ die höchsten bzw. in $\mathfrak{a}$, $\mathfrak{b}$ aufgehenden Potenzen eines Primideals $\mathfrak{p}$, so ist $d \leqq a$, und $\mathfrak{r}$ ist das Produkt aus allen Potenzen $\mathfrak{p}^{a-d}$. Mit Rücksicht hierauf erkennt man leicht, daß die früheren Sätze (in 2.) sich jetzt einfacher aussprechen lassen.

7. Wir nennen nun $\mathfrak{a}$ und $\mathfrak{b}$ relative Primideale, wenn ihr größter gemeinschaftlicher Teiler $= \mathfrak{o}$ ist; ebenso soll η relative Primzahl zum Ideal $\mathfrak{a}$ heißen, wenn $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ relative Primideale sind. Es leuchtet dann ein, daß die Sätze der rationalen Zahlentheorie über relative Primzahlen sich leicht auf die Theorie der Ideale übertragen lassen; wir begnügen uns aber hier, folgenden wichtigen Satz zu beweisen (vgl. § 25):

Sind $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale, und μ, ν zwei gegebene Zahlen, so gibt es immer eine und nur eine Klasse von Zahlen η (mod $\mathfrak{a}\,\mathfrak{b}$), welche den Bedingungen $\eta \equiv \mu$ (mod $\mathfrak{a}$), $\eta \equiv \nu$ (mod $\mathfrak{b}$) genügen. Durchlaufen nämlich μ, ν, η vollständige Restsysteme bzw. für die drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}\,\mathfrak{b}$, so entspricht jeder Zahl η eine und nur eine Kombination μ, ν der Art, daß $\mu \equiv \eta$ (mod $\mathfrak{a}$), $\nu \equiv \eta$ (mod $\mathfrak{b}$) ist; entspräche ferner zwei verschiedenen Zahlen η, η' des Restsystems für den Modul $\mathfrak{a}\,\mathfrak{b}$ eine und dieselbe Kombination μ, ν, so wäre $\eta - \eta'$ teilbar sowohl durch $\mathfrak{a}$ als durch $\mathfrak{b}$, also auch durch $\mathfrak{a}\,\mathfrak{b}$ (weil $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind), mithin wäre $\eta \equiv \eta'$ (mod $\mathfrak{a}\,\mathfrak{b}$), was gegen die Voraussetzung streitet. Durchläuft daher η alle seine Werte, deren Anzahl $= N(\mathfrak{a}\,\mathfrak{b}) = N(\mathfrak{a})\,N(\mathfrak{b})$ ist, so entstehen ebensoviele verschiedene Kombinationen μ, ν; und da genau ebensoviele verschiedene Kombinationen μ, ν wirklich existieren, so muß auch umgekehrt jede Kombination μ, ν einer Zahl η entsprechen, was zu beweisen war.

Bedeutet $\psi(\mathfrak{a})$ die Anzahl der (mod $\mathfrak{a}$) inkongruenten relativen Primzahlen zu $\mathfrak{a}$, so ist $\psi(\mathfrak{a}\,\mathfrak{b}) = \psi(\mathfrak{a})\,\psi(\mathfrak{b})$, wenn $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten. Ist ferner $\mathfrak{p}$ ein Primideal, und $e \geqq 1$, so ist $\psi(\mathfrak{p}^e) = N(\mathfrak{p}^e) - N(\mathfrak{p}^{e-1}) = N(\mathfrak{p})^{e-1}(N(\mathfrak{p}) - 1)$; denn, wenn δ alle r durch $\mathfrak{p}$ teilbaren und nach dem Modul $\mathfrak{p}^e$ inkongruenten Zahlen, wenn ferner γ ein vollständiges Restsystem (mod $\mathfrak{p}$) durchläuft, so bilden die Zahlen $\gamma + \delta$ (zufolge 2.) ein vollständiges Restsystem

(mod $\mathfrak{p}^e$), und es ist $N(\mathfrak{p}^e) = r\,N(\mathfrak{p})$, also $r = N(\mathfrak{p}^{e-1})$; nun ist aber eine solche Zahl $\gamma + \delta$ stets und nur dann relative Primzahl zu $\mathfrak{p}^e$, wenn γ nicht $\equiv 0 \pmod{\mathfrak{p}}$ ist, und folglich ist die Anzahl der Zahlen $\gamma + \delta$, welche relative Primzahlen zu $\mathfrak{p}^e$ sind, gleich $r(N(\mathfrak{p}) - 1)$, was zu beweisen war.

Bedeutet $\mathfrak{p}$ ein Primideal, so gibt es (zufolge 4.) immer eine Zahl λ, welche durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist, mithin auch eine Zahl λ^e, welche durch $\mathfrak{p}^e$, aber nicht durch $\mathfrak{p}^{e+1}$ teilbar ist. Sind nun $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ voneinander verschiedene Primideale, und haben $\lambda', \lambda'', \ldots$ ähnliche Bedeutung für $\mathfrak{p}', \mathfrak{p}'', \ldots$, wie λ für $\mathfrak{p}$, so existiert immer, wenn $e, e', e'', \ldots$ gegebene Exponenten bedeuten, eine Zahl η, welche den gleichzeitigen Kongruenzen

$$\eta \equiv \lambda^e \pmod{\mathfrak{p}^{e+1}}, \quad \eta \equiv \lambda'^{e'} \pmod{\mathfrak{p}'^{e'+1}},$$
$$\eta \equiv \lambda''^{e''} \pmod{\mathfrak{p}''^{e''+1}} \ldots$$

genügt, weil die Moduln relative Primideale sind. Dann ist offenbar $\mathfrak{i}(\eta) = \mathfrak{m}\,\mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''}\ldots$, und das Ideal $\mathfrak{m}$ ist durch keines der Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ teilbar. Hieraus folgt unmittelbar der Satz:

Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Ideale, so gibt es immer ein solches relatives Primideal $\mathfrak{m}$ zu $\mathfrak{b}$, daß $\mathfrak{a}\mathfrak{m}$ ein Hauptideal wird. Sind nämlich $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ alle voneinander verschiedenen in $\mathfrak{a}\mathfrak{b}$ aufgehenden Primideale, und ist $\mathfrak{a} = \mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''}\ldots$ (wo die Exponenten $e, e', e'', \ldots$ auch $= 0$ sein können), so gibt es, wie eben gezeigt ist, ein durch $\mathfrak{a}$ teilbares Hauptideal $\mathfrak{i}(\eta) = \mathfrak{a}\mathfrak{m}$ der Art, daß $\mathfrak{b}$ und $\mathfrak{m}$ relative Primideale sind.

Hieraus folgt auch, daß jedes Ideal $\mathfrak{a}$, welches kein Hauptideal ist, immer als der größte gemeinschaftliche Teiler von zwei Hauptidealen angesehen werden kann; hat man nämlich nach Belieben ein durch $\mathfrak{a}$ teilbares Hauptideal $\mathfrak{i}(\eta') = \mathfrak{a}\mathfrak{b}$ gewählt, so kann man immer ein zweites $\mathfrak{i}(\eta) = \mathfrak{a}\mathfrak{m}$ so wählen, daß $\mathfrak{b}$ und $\mathfrak{m}$ relative Primideale werden; die sämtlichen Zahlen des Ideals $\mathfrak{a}$ sind dann von der Form $\eta\omega + \eta'\omega'$, wo ω, ω' alle Zahlen in $\mathfrak{o}$ durchlaufen.

[Erläuterungen gemeinsam mit denen zu XLVI, XLVIII, XLIX am Schluß von XLIX.]