XXII.

Über einen arithmetischen Satz von Gauß.

[Mitteilungen der Deutschen mathematischen Gesellschaft in Prag, Jahrgang 1892, S. 1—11.]

§ 1.

Die folgenden Betrachtungen beziehen sich auf den im Art. 42 der Disquisitiones Arithmeticae enthaltenen Satz:

I. Wenn die Koeffizienten der beiden ganzen Funktionen

$$P = x^m + p_1 x^{m-1} + p_2 x^{m-2} + \cdots + p_m,$$
$$Q = x^n + q_1 x^{n-1} + q_2 x^{n-2} + \cdots + q_n$$

der Variablen x rationale, aber nicht sämtlich ganze Zahlen sind, so können auch die Koeffizienten ihres Produkts

$$PQ = x^{m+n} + r_1 x^{m+n-1} + \cdots + r_{m+n}$$

nicht sämtlich ganze Zahlen sein.

Derselbe kommt meines Wissens nur ein einziges Mal, nämlich im Art. 341 zur Anwendung, und für diese Anwendung reicht die obige Fassung auch vollständig aus. Aber bei näherer Prüfung erkennt man leicht, daß der im Art. 42 enthaltene Beweis eine viel größere Tragweite besitzt, als diese Fassung des Satzes erkennen läßt. Um dies ganz deutlich zu machen, wollen wir mit p', q', r' bzw. die Nenner der in den Funktionen P, Q, PQ auftretenden, in den kleinsten Zahlen ausgedrückten Koeffizienten p, q, r und mit h irgendeine Primzahl bezeichnen; ist nun unter den Nennern p' mindestens einer durch die Potenz h^μ, aber keiner durch $h^{\mu+1}$ teilbar, und ist ebenso mindestens einer der Nenner q' durch h^ν, aber keiner durch $h^{\nu+1}$ teilbar, so zeigt Gauß, daß mindestens einer der Nenner r' durch die Potenz $h^{\mu+\nu}$ teilbar ist, und hiermit ist der obige Satz bewiesen, weil es (nach Annahme) mindestens eine Primzahl h gibt, für welche $\mu + \nu > 0$ ist. Um aber von dem, was Gauß bewiesen hat, nichts zu opfern, wollen wir mit a_0 das kleinste gemeinsame

Vielfache der Nenner p', mit b_0 dasjenige der Nenner q', mit c_0 dasjenige der Nenner r' bezeichnen; nach der bekannten Regel für die Bildung des kleinsten gemeinsamen Vielfachen von gegebenen Zahlen sind dann h^μ, h^ν und (weil offenbar keiner der Nenner r' durch $h^{\mu+\nu+1}$ teilbar sein kann) $h^{\mu+\nu}$ die höchsten Potenzen von h, welche bzw. in a_0, b_0 und c_0 aufgehen; und weil Ähnliches für jede Primzahl gilt, so folgt hieraus offenbar

$$a_0 b_0 = c_0,$$

während im obigen Satze nur behauptet wird, daß c_0 gewiß nicht $= 1$ sein kann, wenn mindestens eine der beiden Zahlen a_0, $b_0 > 1$ ist.

Multipliziert man nun eine Funktion P, deren höchster Koeffizient $= 1$ ist, mit dem Generalnenner a_0 der übrigen (oder auch aller) Koeffizienten, so entsteht immer eine sogenannte ursprüngliche (primitive) Funktion, d. h. eine Funktion

$$A = a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_m,$$

deren Koeffizienten ganze Zahlen ohne gemeinsamen Teiler sind; und umgekehrt, dividiert man eine ursprüngliche Funktion A durch ihren höchsten Koeffizienten a_0, so entsteht eine Funktion P, deren höchster Koeffizient $= 1$ und deren übrige Koeffizienten den Generalnenner a_0 haben. Aus dieser Bemerkung ergibt sich sofort, daß der von Gauß bewiesene Satz $a_0 b_0 = c_0$ auch in folgender Form ausgesprochen werden kann:

II. Das Produkt von zwei ursprünglichen Funktionen ist wieder eine ursprüngliche Funktion.

Versteht man ferner unter dem Teiler einer mit beliebigen ganzen rationalen Koeffizienten behafteten Funktion den größten gemeinsamen Teiler dieser Koeffizienten, so ist jede solche Funktion offenbar das Produkt aus ihrem Teiler und aus einer ursprünglichen Funktion, und der vorstehende Satz nimmt folgende Form an, in welcher ich ihn gelegentlich*) in Dirichlets Vorlesungen über Zahlentheorie (S. 466 der zweiten, S. 545 der dritten Auflage) erwähnt habe:

III. Der Teiler eines Produktes von zwei Funktionen ist das Produkt aus den Teilern der beiden Faktoren.

*) Daß dieser naheliegende und so leicht zu beweisende Satz schon vor mir von anderen ausgesprochen sein mag, ist zwar sehr wahrscheinlich, aber ich habe keine solche Stelle finden können.

Offenbar gilt derselbe Satz auch für Funktionen mit gebrochenen rationalen Koeffizienten, wenn man unter dem Teiler einer solchen Funktion F diejenige vollständig bestimmte (positive) Zahl t versteht, für welche der Quotient $F:t$ eine ursprüngliche Funktion wird; dann sind z. B. die Teiler der oben mit P, Q, PQ bezeichneten Funktionen die umgekehrten Werte von a_0, b_0, c_0, und der Satz besteht wieder in der Gleichung $c_0 = a_0 b_0$. Man findet ferner leicht, daß der Satz für Produkte von beliebig vielen Faktoren und für Funktionen von beliebig vielen unabhängigen Variablen gilt. Statt aber auf solche Verallgemeinerungen einzugehen, ziehe ich es vor, dem Satze noch eine andere gleichwertige Form zu geben, welche insofern einfacher und deshalb leichter auf höhere Zahlengebiete zu übertragen ist, als in ihr der Begriff des Teilers gar nicht mehr auftritt:

IV. Sind alle Koeffizienten a der Funktion A und alle Koeffizienten b der Funktion B rationale Zahlen, und sind alle Koeffizienten c des Produktes AB ganze Zahlen, so sind auch alle Produkte ab ganze Zahlen.

Um dies zu beweisen, bezeichne ich mit α, β die Teiler der Funktionen $A = \alpha A'$, $B = \beta B'$ und mit a', b' alle Koeffizienten der ursprünglichen Funktionen A', B'; jedes Produkt ab ist dann von der Form $(\alpha a')(\beta b')$, und weil $\alpha\beta$ (nach II oder III) der Teiler der Funktion AB ist, diese aber (nach Annahme) lauter ganze Koeffizienten c hat, so ist $\alpha\beta$ und folglich auch jedes Produkt ab eine ganze Zahl, w. z. b. w.

Ebenso leicht ist es, aus diesem Satze IV umgekehrt den Satz II oder III abzuleiten, ohne nochmals auf den Nerv des Beweises von Gauß, also auf die Bildung der Koeffizienten eines Produktes aus denen der Faktoren zurückzugehen. Wäre nämlich ein Produkt aus zwei ursprünglichen Funktionen A, B, deren Koeffizienten mit a, b bezeichnet werden mögen, keine ursprüngliche Funktion, wären also alle (offenbar ganzen) Koeffizienten von AB durch eine Primzahl h teilbar, so müßten, weil dann das Produkt $\frac{A}{h} \cdot B$ lauter ganze Koeffizienten hätte, alle Produkte $\frac{a}{h} \cdot b$ (nach IV) ganze Zahlen sein, was offenbar nicht der Fall ist, weil sowohl in A als auch in B sich mindestens ein durch h nicht teilbarer Koeffizient a, b findet.

Der Satz IV ist daher vollkommen gleichwertig mit dem Satze II oder III; aber jeder dieser Sätze ist schärfer als der Satz I.

§ 2.

Ich gehe nun dazu über, den Satz in der Weise zu verallgemeinern, daß die Koeffizienten, welche bisher als rational angenommen waren, beliebige algebraische Zahlen sein dürfen. Unter einer algebraischen Zahl verstehe ich jede Wurzel einer Gleichung mit rationalen Koeffizienten, und ich nenne sie eine ganze algebraische Zahl oder kürzer eine ganze Zahl, wenn unter den unendlich vielen Gleichungen, deren Wurzel sie ist, es auch eine solche gibt, deren höchster Koeffizient $= 1$ und deren übrige Koeffizienten ganze rationale Zahlen sind (Dirichlets Zahlentheorie, Aufl. 2 und 3, § 160). Hieraus ergeben sich sofort die a. a. O. bewiesenen Sätze:

1. Die Summen, Differenzen, Produkte von je zwei ganzen Zahlen sind ganze Zahlen.

2. Jede Wurzel einer Gleichung, deren höchster Koeffizient $= 1$ und deren übrige Koeffizienten ganze Zahlen sind, ist eine ganze Zahl.

Aus diesen beiden Sätzen leiten wir leicht noch den folgenden ab:

3. Eine Zahl α ist gewiß eine ganze Zahl, wenn es ein endliches System von Zahlen $\mu_1, \mu_2 \dots \mu_n$ gibt, die nicht sämtlich verschwinden und deren jede (μ_r) durch Multiplikation mit α ein Produkt von der Form

$$\alpha \mu_r = z_1^{(r)} \mu_1 + z_2^{(r)} \mu_2 + \cdots + z_n^{(r)} \mu_n$$

gibt, wo alle mit z bezeichneten Koeffizienten ganze Zahlen sind.

Denn durch Elimination der n Größen μ_r aus diesen n homogenen linearen Gleichungen ergibt sich bekanntlich die Gleichung

$$\begin{vmatrix} z_1' - \alpha, & z_2' & \dots & z_n' \\ z_1'' & , z_2'' - \alpha & \dots & z_n'' \\ \dots & \dots & \dots & \dots \\ z_1^{(n)} & , z_2^{(n)} & \dots & z_n^{(n)} - \alpha \end{vmatrix} = 0;$$

entwickelt man die Determinante nach Potenzen von α, so erhält man eine Gleichung von der Form

$$\alpha^n + y_1 \alpha^{n-1} + y_2 \alpha^{n-2} + \cdots + y_n = 0,$$

deren Koeffizienten $y_1, y_2 \dots y_n$ durch Addition, Subtraktion, Multiplikation aus den ganzen Zahlen z entstehen und folglich (nach 1.) ebenfalls ganze Zahlen sind, und hieraus folgt (nach 2.), daß auch α eine ganze Zahl ist, w. z. b. w.

Mit Hilfe der in dem genannten Werke begründeten allgemeinen Zahlentheorie, die sich auf die Begriffe des endlichen Zahlenkörpers und der ihm angehörenden Ideale stützt, ist es nun leicht, den obigen Satz III auf Funktionen mit beliebigen algebraischen Koeffizienten zu übertragen. Sind nämlich die Koeffizienten der beiden Funktionen

$$A = a_0 x^m + a_1 x^{m-1} + \cdots + a_m,$$
$$B = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$$

und folglich auch diejenigen ihres Produktes

$$AB = c_0 x^{m+n} + c_1 x^{m+n-1} + \cdots + c_{m+n}$$

ganze Zahlen eines endlichen Körpers Ω, und bedeutet $\mathfrak{p}$ irgendein Primideal in Ω, so ergibt sich in ganz ähnlicher Art wie bei dem Beweise von Gauß, daß die höchste in allen Koeffizienten c aufgehende Potenz von $\mathfrak{p}$ gleich $\mathfrak{p}^{\mu+\nu}$ ist, wo $\mathfrak{p}^\mu$ die höchste in allen Zahlen a, und $\mathfrak{p}^\nu$ die höchste in allen Zahlen b enthaltene Potenz ist; sind nämlich r, s die kleinsten Indizes, für welche a_r nicht durch $\mathfrak{p}^{\mu+1}$ und b_s nicht durch $\mathfrak{p}^{\nu+1}$ teilbar ist, so kann der Koeffizient c_{r+s} gewiß nicht durch $\mathfrak{p}^{\mu+\nu+1}$ teilbar sein, weil er ein Aggregat von Produkten ab ist, die alle, mit Ausnahme des einzigen Gliedes $a_r b_s$, durch $\mathfrak{p}^{\mu+\nu+1}$ teilbar sind. Hiermit ist aber nach den Prinzipien der Idealtheorie wirklich bewiesen, daß der Teiler des Produktes AB d. h. der größte gemeinsame Idealteiler aller Koeffizienten c, das Produkt aus den Teilern von A und B ist.

Aber welche weit ausgedehnte Theorie gehört dazu, um diesen Satz beweisen, ja um ihn nur mit Verständnis aussprechen zu können! Ganz anders verhält es sich mit der folgenden Verallgemeinerung des Satzes IV, die nur den obigen einfachen Begriff der ganzen Zahl aber gar nichts von Körpern oder Idealen voraussetzt:

V. Wenn das Produkt aus zwei Funktionen A, B lauter ganze Koeffizienten besitzt, so ist jedes aus einem Koeffizienten von A und einem Koeffizienten von B gebildete Produkt eine ganze Zahl.

Dieser Satz ist zwar für den Kenner der Idealtheorie wieder gleichwertig mit der eben besprochenen Verallgemeinerung des Satzes III, aber seine viel einfachere Form läßt auch die Möglichkeit eines einfacheren Beweises vermuten. Die Herstellung eines solchen

Beweises bildet den eigentlichen Gegenstand der vorliegenden Abhandlung, und dies wird wohl im Hinblick auf die zahlreichen Anwendungen, welche der Satz V gestattet, hinreichend gerechtfertigt erscheinen.

§ 3.

Am kürzesten gelangt man zu dem gewünschten Ziele, indem man sich auf den folgenden speziellen Fall stützt:

VI. Wenn die ganze Funktion $f(x)$ lauter ganze Koeffizienten hat, und wenn ω irgendeine Wurzel der Gleichung $f(\omega) = 0$ bedeutet, so hat auch die ganze Funktion

$$f_1(x) = \frac{f(x)}{x - \omega}$$

lauter ganze Koeffizienten.

Um dies zu beweisen, setzen wir

$$f(x) = c_0 x^k + c_1 x^{k-1} + \cdots + c_k,$$
$$f_1(x) = a_0 x^{k-1} + a_1 x^{k-2} + \cdots + a_{k-1},$$

woraus

$$a_r = c_0 \omega^r + c_1 \omega^{r-1} + \cdots + c_r$$

folgt. Multipliziert man nun einen bestimmten solchen Koeffizienten a_r mit jeder der k Potenzen $1, \omega, \omega^2 \ldots \omega^{k-1}$, so erhält man

$$a_r \omega^s = c_0 \omega^{r+s} + c_1 \omega^{r+s-1} + \cdots + c_r \omega^s;$$

ist der Exponent s eine der $k - r$ Zahlen $0, 1, 2 \ldots k - r - 1$, also $r + s < k$, so behalten wir diese Form des Produktes bei; ist aber der Exponent s eine der r Zahlen $k - r, k - r + 1 \ldots k - 1$, so multiplizieren wir die Gleichung

$$f(\omega) = c_0 \omega^k + c_1 \omega^{k-1} + \cdots + c_k = 0$$

mit ω^{r+s-k}, wodurch sich die andere Form

$$a_r \omega^s = -c_{r+1} \omega^{s-1} - c_{r+2} \omega^{s-2} - \cdots - c_k \omega^{s+r-k}$$

ergibt; da mithin alle diese Produkte $a_r \omega^s$ in der Form

$$z_1 \omega^{k-1} + z_2 \omega^{k-2} + \cdots + z_k$$

darstellbar sind, wo die Koeffizienten z ganze Zahlen bedeuten, so ist (nach 3. in § 2) auch jeder Koeffizient a_r eine ganze Zahl, w. z. b. w.

Durch wiederholte Anwendung dieses Satzes ergibt sich offenbar folgendes. Wenn die Funktion

$$f(x) = c_0 (x - \omega_1)(x - \omega_2) \ldots (x - \omega_k)$$

lauter ganze Koeffizienten hat, so behält sie diese Eigenschaft nach Division durch beliebig viele der Faktoren ersten Grades $(x - \omega)$; der letzte Koeffizient einer so erhaltenen Funktion ist (abgesehen vom Vorzeichen) immer von der Form $c_0 \omega' = c_0 \omega_r \omega_s \omega_t \ldots$, wo $r, s, t \ldots$ irgendwelche voneinander verschiedene Indizes aus der Reihe 1, 2 ... k bedeuten, also ω' jedes beliebige Glied des entwickelten Produktes

$$(1 + \omega_1)(1 + \omega_2) \ldots (1 + \omega_k)$$

sein kann. Alle Produkte von der Form $c_0 \omega'$ sind also ganze Zahlen.

Und hieraus folgt leicht der zu beweisende Satz V. Denken wir uns nämlich die Funktion $f(x)$ auf irgendeine Weise in zwei Faktoren A, B zerlegt, und setzen

$$A = a_0 (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_m),$$
$$B = b_0 (x - \beta_1)(x - \beta_2) \ldots (x - \beta_n),$$

so ist $a_0 b_0 = c_0$, $m + n = k$, und der Komplex der $m + n$ Zahlen α, β ist identisch mit dem Komplex der k Zahlen ω. Bezeichnen wir daher mit α' jedes Glied des entwickelten Produktes

$$(1 + \alpha_1)(1 + \alpha_2) \ldots (1 + \alpha_m),$$

ebenso mit β' jedes Glied des entwickelten Produktes

$$(1 + \beta_1)(1 + \beta_2) \ldots (1 + \beta_n),$$

so sind die Produkte $\alpha' \beta'$ identisch mit den Zahlen ω', und folglich ist jedes Produkt $a_0 \alpha' . b_0 \beta' = c_0 \omega'$, also eine ganze Zahl. Da nun jeder Koeffizient a der Funktion A (abgesehen vom Vorzeichen) ein Aggregat von Produkten $a_0 \alpha'$ und ebenso jeder Koeffizient b der Funktion B ein Aggregat von Produkten $b_0 \beta'$ ist, so ist jedes Produkt ab auch ein Aggregat von Produkten $a_0 \alpha' . b_0 \beta'$, also eine Summe von ganzen Zahlen und folglich (nach 1. in § 2) ebenfalls eine ganze Zahl, w. z. b. w.

Man sieht leicht, daß der nunmehr bewiesene Satz V auch für Produkte von beliebig vielen Faktoren gilt. Sind a, b, c die Koeffizienten der drei Funktionen A, B, C, so wird, wenn das Produkt $ABC = (AB)C$ lauter ganze Koeffizienten hat, nach V auch jede Funktion $(AB)c$, also auch jedes Produkt $A(Bc)$ ganze Koeffizienten haben, woraus nach V wieder folgt, daß die Produkte $a(bc)$ ganze Zahlen sind; und so kann man offenbar fortfahren. Übrigens leuchtet

ein, daß man den obigen Beweis auch ohne weiteres für Produkte von beliebig vielen Faktoren hätte führen können.

Ebenso würde die Übertragung des Satzes auf den Fall, wo die Koeffizienten nicht Zahlen, sondern algebraische Funktionen von veränderlichen Größen sind, keine neue Schwierigkeit darbieten, und in dieser Allgemeinheit kann der Satz sehr wohl dazu dienen, die Betrachtungen, welche Kronecker in § 14 seiner „Grundzüge einer arithmetischen Theorie der algebraischen Größen“ (1882) entwickelt hat, zu vereinfachen und zu vervollständigen. Der in dieser gedankenreichen Abhandlung herrschenden Auffassung der arithmetisch-algebraischen Probleme würde freilich der obige Beweis des Satzes V insofern wohl nicht vollkommen entsprechen, als in ihm die Zerlegbarkeit der Funktion $f(x)$ in Faktoren ersten Grades vorausgesetzt wird. Aus diesem Grunde will ich zum Schluß noch einen ganz anderen Beweis des Satzes V mitteilen, in welchem diese Zerlegbarkeit durchaus nicht benutzt wird.

§ 4.

Der Gang des neuen Beweises läßt sich am einfachsten darstellen, wenn man einige wenige Begriffe aus der Theorie der Moduln entlehnt. Ein System $\mathfrak{a}$ von Zahlen α nenne ich einen Modul*), wenn die Summen und Differenzen von je zwei solchen Zahlen α wieder demselben System $\mathfrak{a}$ angehören. Sind alle diese Zahlen α auch in dem Modul $\mathfrak{b}$ enthalten, so heißt $\mathfrak{a}$ teilbar durch $\mathfrak{b}$; sind zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ gegenseitig durch einander teilbar, so sind sie identisch, was durch $\mathfrak{a} = \mathfrak{b}$ bezeichnet wird. Bedeutet α jede Zahl des Moduls $\mathfrak{a}$, ebenso β jede Zahl des Moduls $\mathfrak{b}$, so bilden alle Produkte $\alpha\beta$ und alle Summen solcher Produkte wieder einen Modul, welcher das Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ heißt und mit $\mathfrak{ab}$ bezeichnet wird. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, so ist offenbar $\mathfrak{ab}$ teilbar durch $\mathfrak{bb}$ Ebenso kann man Produkte von beliebig vielen Moduln und Potenzen von Moduln bilden, und es gelten hierbei dieselben Multiplikationsgesetze wie bei Produkten von Zahlen.

Wir brauchen uns hier nur mit sogenannten endlichen Moduln zu beschäftigen. Sind $a_0, a_1, a_2 \ldots a_m$ irgendwelche bestimmte Zahlen,

*) Dirichlets Zahlentheorie, Aufl. 2, § 161.

während $x_0, x_1, x_2 \ldots x_m$ willkürliche rationale ganze Zahlen bedeuten, so bilden alle in der Form

$$\alpha = a_0 x_0 + a_1 x_1 + a_2 x_2 + \cdots + a_m x_m \tag{1}$$

darstellbaren Zahlen α einen solchen endlichen Modul $\mathfrak{a}$, der durch das Symbol

$$\mathfrak{a} = [a_0, a_1, a_2 \ldots a_m] \tag{2}$$

bezeichnet wird; das System der Zahlen $a_0, a_1 \ldots a_m$ heißt eine Basis von $\mathfrak{a}$, und diese Zahlen selbst heißen die Glieder oder Elemente dieser Basis. Offenbar kann die Basis eines endlichen Moduls $\mathfrak{a}$ in unendlich viele, äußerlich verschiedene Formen gebracht werden, ohne die geringste Änderung des gesamten Zahleninhalts von $\mathfrak{a}$; z. B. darf man das erste Glied a_0, indem man alle anderen beibehält, durch jede Zahl von der Form (1) ersetzen, in welcher $x_0 = \pm 1$ ist. Wenn nun

$$\mathfrak{b} = [b_0, b_1 \ldots b_n] \tag{3}$$

ebenfalls ein endlicher Modul ist, so gilt dasselbe offenbar auch von dem Produkt $\mathfrak{a}\mathfrak{b}$, und zwar ist

$$\mathfrak{a}\mathfrak{b} = [p_0, p_1 \ldots], \tag{4}$$

wo die Zahlen $p_0, p_1 \ldots$ alle Produkte von der Form $a_r b_s$ bedeuten.

Ebenso leuchtet ein, daß auch jede Potenz des endlichen Moduls (2) wieder ein endlicher Modul ist; die Basis einer solchen Potenz

$$\mathfrak{a}^{n+1} = [\alpha_0, \alpha_1, \alpha_2 \ldots]$$

besteht aus allen Produkten α von $n+1$ gleichen oder verschiedenen Faktoren aus der Reihe $a_0, a_1 \ldots a_m$; die Anzahl dieser Produkte α ist bekanntlich

$$\frac{\Pi(m+n+1)}{\Pi(m)\,\Pi(n+1)}.$$

Für unseren Zweck ist aber eine Transformation dieser Basis in eine andere erforderlich, deren Glieder gewisse aus den Größen $a_0, a_1 \ldots a_m$ gebildete Determinanten sind. Der Kürze halber wollen wir mit r irgendeine Kombination von $n+1$ verschiedenen, der Größe nach geordneten Indizes

$$r_0 < r_1 < r_2 \cdots < r_n \tag{r}$$

bezeichnen, welche der Reihe der $m+n+1$ Zahlen

$$0, 1, 2 \ldots (m+n)$$

angehören; dann ist zugleich

$$r_0 \leqq r_1 - 1 \leqq r_2 - 2 \cdots \leqq r_n - n,$$

und diese $n + 1$ Zahlen $r_\nu - \nu$ gehören alle der Reihe der $m + 1$ Zahlen

$$0, 1, 2 \ldots m$$

an; jeder Kombination r entspricht daher ein bestimmtes Produkt

$$\alpha_r = a_{r_0} a_{r_1 - 1} a_{r_2 - 2} \cdots a_{r_n - n},$$

und umgekehrt leuchtet ein, daß jedes Produkt α, also jedes Glied der Basis von $\mathfrak{a}^{n+1}$, aus einer und nur aus einer einzigen Kombination r entspringt. Ist ferner s eine von r verschiedene Kombination

$$s_0 < s_1 < s_2 \cdots < s_n, \qquad (s)$$

so können die Differenzen $r_0 - s_0$, $r_1 - s_1 \ldots r_n - s_n$ nicht alle verschwinden, und wir wollen von den beiden entsprechenden Gliedern α_r, α_s das erste als das höhere, das zweite als das niedrigere ansehen, wenn die erste nicht verschwindende dieser Differenzen positiv ausfällt; offenbar ordnen sich dann alle Glieder α ihrer Höhe nach in eine bestimmte Folge der Art, daß, wenn von drei Gliedern $\alpha_r, \alpha_s, \alpha$ das erste höher als das zweite und dieses höher als das dritte ist, gewiß das erste auch höher als das letzte ist; von allen Gliedern α ist a_m^{n+1} das höchste, a_0^{n+1} das niedrigste.

Indem wir ferner festsetzen, daß $a_i = 0$ sein soll, so oft der Index i nicht in der Reihe der $m + 1$ Zahlen $0, 1, 2 \ldots m$ enthalten ist, lassen wir jeder Kombination r, also jedem Produkte α_r eine bestimmte Determinante

$$\alpha_r' = \begin{vmatrix} a_{r_0} & a_{r_0 - 1} & \cdots & a_{r_0 - n} \\ a_{r_1} & a_{r_1 - 1} & \cdots & a_{r_1 - n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r_n} & a_{r_n - 1} & \cdots & a_{r_n - n} \end{vmatrix}$$

entsprechen. Dieselbe ist ein Aggregat von lauter Produkten α, unter denen sich das Hauptglied α_r befindet, und man kann beweisen — was wir der Kürze halber dem Leser überlassen müssen — daß alle anderen Glieder niedriger als α_r sind. Hieraus folgt mit Rücksicht auf eine frühere Bemerkung, daß man die aus den Produkten $\alpha_0, \alpha_1 \ldots$ bestehende Basis des Moduls $\mathfrak{a}^{n+1}$ schrittweise, indem man immer α_r durch α_r' ersetzt, in eine neue Basis transformieren kann, welche aus den sämtlichen Determinanten α_r' besteht, daß also

$$\mathfrak{a}^{n+1} = [\alpha_0', \alpha_1' \ldots]$$

ist. Mit Hilfe dieser Transformation kann man leicht den folgenden Satz beweisen:

VII. Bildet man aus den Koeffizienten der drei ganzen Funktionen

$$\begin{aligned} A &= a_0 x^m + a_1 x^{m-1} + \cdots + a_m, \\ B &= b_0 x^n + b_1 x^{n-1} + \cdots + b_n, \\ AB &= c_0 x^{m+n} + c_1 x^{m+n-1} + \cdots + c_{m+n} \end{aligned}$$

die drei endlichen Moduln

$$\begin{aligned} \mathfrak{a} &= [a_0, a_1 \ldots a_m], \\ \mathfrak{b} &= [b_0, b_1 \ldots b_n], \\ \mathfrak{c} &= [c_0, c_1 \ldots c_{m+n}], \end{aligned}$$

so ist

$$\mathfrak{a}^{n+1}\mathfrak{b} = \mathfrak{a}^n \mathfrak{c}, \quad \mathfrak{a}\mathfrak{b}^{m+1} = \mathfrak{b}^m \mathfrak{c}.$$

Beweis. Aus der Bildungsweise der Koeffizienten

$$c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_{i-n} b_n$$

geht zunächst hervor, daß der Modul $\mathfrak{c}$ durch $\mathfrak{a}\mathfrak{b}$ und folglich $\mathfrak{a}^n \mathfrak{c}$ durch $\mathfrak{a}^{n+1}\mathfrak{b}$ teilbar ist. Setzt man ferner für i die in einer bestimmten Kombination r enthaltenen Indizes $r_0, r_1 \ldots r_n$, so ergibt sich, daß alle Produkte $\alpha'_r b_\nu$ in der Form

$$\alpha'_{r,0} c_{r_0} + \alpha'_{r,1} c_{r_1} \cdots + \alpha'_{r,n} c_{r_n}$$

darstellbar sind, wo $\alpha'_{r,0}, \alpha'_{r,1} \ldots \alpha'_{r,n}$ gewisse Unterdeterminanten n^{ten} Grades von α'_r bedeuten und folglich in dem Modul $\mathfrak{a}^n$ enthalten sind. Mithin ist jedes Produkt $\alpha'_r b_\nu$ in $\mathfrak{a}^n \mathfrak{c}$ enthalten, und da die Determinanten α'_r eine Basis von $\mathfrak{a}^{n+1}$ und die Zahlen b_ν eine Basis von $\mathfrak{b}$ bilden, so ist das Produkt $\mathfrak{a}^{n+1}\mathfrak{b}$ teilbar durch $\mathfrak{a}^n \mathfrak{c}$ und folglich $\mathfrak{a}^{n+1}\mathfrak{b} = \mathfrak{a}^n \mathfrak{c}$, w. z. b. w.

Aus diesem ganz allgemeinen Satze, in welchem über die Beschaffenheit der Koeffizienten a, b, c gar nichts vorausgesetzt wird, ergibt sich nun unmittelbar unser Satz V. Bilden nämlich die Zahlen $\mu_1, \mu_2 \ldots \mu_k$ eine Basis des Moduls $\mathfrak{a}^n$, so sind alle Produkte

$$a b \mu_1, \; a b \mu_2 \ldots a b \mu_k$$

in $(\mathfrak{a}\mathfrak{b})\mathfrak{a}^n$, d. h. in $\mathfrak{a}^n \mathfrak{c}$ enthalten, also von der Form

$$z_1 \mu_1 + z_2 \mu_2 + \cdots + z_k \mu_k,$$

wo $z_1, z_2 \ldots z_k$ Zahlen des Moduls $\mathfrak{c}$ bedeuten. Setzen wir also jetzt (wie in V) voraus, daß alle Koeffizienten c ganze Zahlen sind, so gilt dasselbe (nach 1. in § 2) auch von diesen Zahlen $z_1, z_2 \ldots z_k$ und folglich (nach 3. in § 2) auch von jedem Produkt ab, w. z. b. w.

Erläuterungen zur vorstehenden Abhandlung.

In der Abhandlung Nr. XXV: Über die Begründung der Idealtheorie, bemerkt Dedekind, daß er den Beweis des Satzes V, des Hauptsatzes der vorstehenden Abhandlung, schon am 15. Februar 1887 gefunden und am 20. Februar d. J. an H. Weber mitgeteilt hat. Etwas später, aber unabhängig von Dedekind, ist der Satz von A. Hurwitz (Über die Theorie der Ideale, Göttinger Nachrichten 1894, Math.-phys. Kl., S. 291—298, vgl. Fußnote S. 292) in einer äquivalenten Form ausgesprochen worden. Aus Satz V folgt bekanntlich einfach, daß man zu einem beliebigen Ideale ein zweites so bestimmen kann, daß das Produkt ein Hauptideal wird, und diese Tatsache ist sowohl von Hurwitz als auch gelegentlich von Dedekind zum Aufbau der Idealtheorie benutzt worden. Eine eingehende Diskussion dieser Probleme gibt Dedekind in der Abhandlung Nr. XXV; man vergleiche auch die Besprechung dieser Abhandlung im Vorwort zur vierten Auflage von Dirichlets Zahlentheorie, ebenso die weiteren Literaturangaben (Kronecker, Mertens) bei A. Hurwitz: „Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Größen", Göttinger Nachrichten 1895, S. 230—240.

Ore.