XXXI.

Über die Permutationen des Körpers aller algebraischen Zahlen.

[Festschrift zur Feier des hundertfünfzigjährigen Bestehens der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Abhandlungen der mathematisch-physikalischen Klasse, S. 1—17 (1901).]

Die vorliegende, rein algebraische Untersuchung verfolgt das Ziel, gewisse Sätze, die sich auf endliche Körper beziehen, auf unendliche Körper auszudehnen; um aber ihren Gegenstand genauer zu bezeichnen, ist es nötig, an die Bedeutung der in der Überschrift gewählten Ausdrücke und an einige Sätze zu erinnern, welche sich auf dieselben beziehen. Eine ausführliche Entwicklung dieser Begriffe und der Beweise findet man in der vierten Auflage (1894) von Dirichlets Vorlesungen über Zahlentheorie (Supplement XI), die ich im folgenden mit D. zitieren werde; hier beschränke ich mich in den beiden ersten Paragraphen darauf, aus dieser Darstellung mit Übergehung der Beweise nur das zu entlehnen, was für unseren Zweck unerläßlich ist.

§ 1.

Körper und irreduzibele Systeme.

Ein System A von reellen oder komplexen Zahlen heißt ein Körper (D. § 160), wenn die Summen, Differenzen, Produkte und Quotienten von je zwei dieser Zahlen demselben System A angehören. Der kleinste Körper R besteht aus allen rationalen, der größte Körper Z aus allen komplexen Zahlen. Ein Körper A heißt Divisor eines Körpers B, und zugleich heißt B ein Multiplum von A, wenn jede in A enthaltene Zahl auch dem Körper B angehört; der Körper R ist ein gemeinsamer Divisor, der Körper Z ein gemeinsames Multiplum aller Körper A. Ist B Multiplum von A und Divisor von C, so ist A Divisor von C. Jedes bestimmte System von Körpern A, mag ihre Anzahl endlich oder unendlich sein, besitzt einen

bestimmten größten gemeinsamen Divisor D; dieser Körper besteht aus denjenigen Zahlen, welche allen diesen Körpern A gemeinsam angehören, und jeder gemeinsame Divisor dieser Körper A ist Divisor von D. Dasselbe Körpersystem besitzt ein bestimmtes kleinstes gemeinsames Multiplum M; dieser Körper M ist der größte gemeinsame Divisor aller derjenigen Körper, welche (wie z. B. Z) gemeinsame Multipla der Körper A sind.

Ein endliches System T von m Zahlen $t_1, t_2 \cdots t_m$ heißt reduzibel in bezug auf den Körper A, wenn es m Zahlen $a_1, a_2 \cdots a_m$ in A gibt, welche der Bedingung

$$a_1 t_1 + a_2 t_2 + \cdots + a_m t_m = 0$$

genügen und nicht alle verschwinden; im entgegengesetzten Falle heißt das System T irreduzibel nach A (D. § 164).

Eine Zahl t heißt algebraisch in bezug auf den Körper A, wenn es eine natürliche Zahl n gibt, für welche die $n+1$ Potenzen

$$1, t, t^2 \cdots t^{n-1}, t^n$$

ein nach A reduzibeles System bilden; die kleinste Zahl n, für welche dies eintritt, heißt der Grad von t, und wir sagen, t sei eine algebraische Zahl n^{ten} Grades in bezug auf A. Offenbar ist eine solche Zahl t die Wurzel einer (irreduzibelen) Gleichung

$$t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n = 0,$$

deren Koeffizienten $a_1, a_2 \cdots a_n$ Zahlen des Körpers A sind, während die n Potenzen

$$1, t, t^2 \cdots t^{n-1}$$

ein nach A irreduzibeles System bilden. Man überzeugt sich leicht (D. § 164, IX), daß der Inbegriff U aller Zahlen u von der Form

$$u = x_1 t^{n-1} + x_2 t^{n-2} + \cdots + x_{n-1} t + x_n,$$

wo $x_1, x_2 \cdots x_{n-1}, x_n$ willkürliche Zahlen in A bedeuten, wieder ein Körper, und zwar ein Multiplum von A ist; diesen Körper U bezeichnen wir mit $A(t)$, und wir sagen, er entstehe aus A durch Adjunktion von t. Je $n+1$ Zahlen dieses Körpers $A(t)$ bilden ein nach A reduzibeles System, mithin ist jede Zahl u algebraisch in bezug auf A, und ihr Grad nicht größer als n; ist dieser Grad $= n$, so ist $A(u)$ identisch mit $A(t)$.

Ein Körper B heißt endlich in bezug auf den Körper A und vom Grade n, wenn es in B ein aus n Zahlen bestehendes, nach A irreduzibeles System gibt, während je $n+1$ Zahlen des Körpers B

ein nach A reduzibeles System bilden; diesen Grad n, welcher immer eine natürliche Zahl ist, bezeichnen wir durch das Symbol (B, A). Dann sind alle Zahlen in B algebraisch in bezug auf A, darunter gibt es auch (unendlich viele) Zahlen t, deren Grad $= n$ ist (D. § 165, VI), und der durch Adjunktion einer solchen Zahl t aus A entstehende Körper $A(t)$ ist das kleinste gemeinsame Multiplum M der beiden Körper A, B; mithin besteht der Satz

$$(1) \qquad (B, A) = (M, A).$$

Wenn B selbst ein Multiplum von A, also $M = B$ ist, so heißt B ein endliches Multiplum von A; ist zugleich der Körper C ein endliches Multiplum von B, so ist C auch ein endliches Multiplum von A, und es gilt der Satz (D. § 164, X)

$$(2) \qquad (C, A) = (C, B)\,(B, A).$$

Daß ein Körper D Divisor eines Körpers M ist, wird durch $(D, M) = 1$ vollständig ausgedrückt.

Ist aber B nicht endlich in bezug auf A, gibt es also in B, wie groß auch die natürliche Zahl m gewählt sein mag, immer m Zahlen, die ein nach A irreduzibeles System bilden, so wollen wir $(B, A) = \infty$ setzen*), wodurch wir erreichen, daß die beiden Sätze (1) und (2) allgemein gelten, der letztere natürlich unter der früheren Annahme, daß B Multiplum von A und Divisor von C ist.

§ 2.

Permutationen eines Körpers.

Eine Abbildung φ des Körpers A, durch welche jede in A enthaltene Zahl a in eine entsprechende Zahl $a\varphi$ übergeht, heißt eine Permutation von A, wenn sie den vier Gesetzen

$$(u+v)\varphi = u\varphi + v\varphi, \quad (u-v)\varphi = u\varphi - v\varphi,$$
$$(uv)\varphi = (u\varphi)\,(v\varphi), \quad \left(\frac{u}{v}\right)\varphi = \frac{u\varphi}{v\varphi}$$

gehorcht, wo u, v willkürliche Zahlen in A bedeuten (D. § 161); wir sagen auch, die Permutation φ beziehe sich auf den Körper A, und nennen den letzteren kurz den Körper von φ, um hierdurch auszudrücken, daß die Abbildung φ auf keine außerhalb A liegende Zahl wirken soll. Ist ferner T irgendein Teil von A, d. h. ein

*) Vgl. den Schluß von D. § 164, wo für diesen Fall $(B, A) = 0$ gesetzt wird, was aber für die jetzige Untersuchung weniger vorteilhaft ist.

System von Zahlen t, die alle in A enthalten sind, so bezeichnen wir mit $T\varphi$ den Inbegriff aller Bilder $t\varphi$ dieser Zahlen t. Die Zahl $t\varphi$ heißt konjugiert mit t.

Aus dieser Definition folgt leicht, daß das Zahlensystem $A\varphi$ wieder ein Körper ist, und daß je zwei verschiedene Zahlen des Körpers A durch φ in zwei verschiedene Zahlen des konjugierten Körpers $A\varphi$ übergehen; aus diesem Grunde läßt sich die Permutation φ eindeutig umkehren, und wenn man mit φ^{-1} diejenige Abbildung des Körpers $A\varphi$ bezeichnet, durch welche jede in $A\varphi$ enthaltene Zahl $a\varphi$ in a übergeht, so leuchtet ein, daß diese Umkehrung φ^{-1} eine Permutation von $A\varphi$, und $(A\varphi)\varphi^{-1} = A$ ist.

Jeder Körper A besitzt mindestens eine, nämlich die sogenannte identische Permutation, durch welche jede seiner Zahlen in sich selbst übergeht; wir wollen sie im folgenden mit A_0 bezeichnen. Ist φ eine beliebige Permutation von A, und r eine rationale, also auch in A enthaltene Zahl, so ist $r\varphi = r$, woraus zugleich folgt, daß der Körper R der rationalen Zahlen nur eine einzige, die identische Permutation R_0 besitzt.

Ist der Körper A ein Divisor des Körpers B, so ist in jeder Permutation ψ von B eine entsprechende Permutation φ von A enthalten, welche für jede Zahl a des Körpers A durch $a\varphi = a\psi$ definiert wird, woraus zugleich folgt, daß der Körper $A\varphi = A\psi$, also ein Divisor des Körpers $B\psi$ ist. Diese Permutation φ heißt der auf A bezügliche Divisor von ψ, und umgekehrt heißt ψ ein auf B bezügliches Multiplum von φ (D. § 163). Im Falle $A = B$ ist offenbar $\varphi = \psi$; ist aber A verschieden von B, also ein sogenannter echter Divisor von B, so ist auch φ wesentlich verschieden von ψ, weil die Wirkungsgebiete beider Permutationen verschieden sind. Die einzige Permutation R_0 des Körpers R der rationalen Zahlen ist gemeinsamer Divisor aller Körperpermutationen, und jeder Divisor einer identischen Permutation ist ebenfalls eine identische Permutation. Ist die Permutation φ des Körpers A ein Divisor der Permutation ψ, und letztere ein Divisor der Permutation χ, so ist φ zugleich der auf A bezügliche Divisor von χ.

Aus der unendlichen Menge von Sätzen, zu welchen diese Begriffe führen, wollen wir hier nur zwei besonders wichtige hervorheben; um sie bequem aussprechen zu können, schicken wir noch folgende Erklärung voraus (D. § 161). Ist $\mathfrak{P}$ ein (endliches oder unendliches)

System von Permutationen ψ beliebiger Körper B, so geht eine in dem größten gemeinsamen Divisor dieser Körper B enthaltene Zahl t durch jede Permutation ψ in eine entsprechende Zahl $t\psi$ über, und sie heißt n-wertig zu $\mathfrak{P}$, wenn n die Anzahl der voneinander verschiedenen Werte ist, welche sich unter diesen Zahlen $t\psi$ finden; offenbar ist jede rationale Zahl einwertig zu $\mathfrak{P}$. Hiernach lautet unser erster, leicht zu beweisender Satz (D. § 163) so:

I. Ist $\mathfrak{P}$ ein System von Körper-Permutationen ψ, so bildet die Gesamtheit aller zu $\mathfrak{P}$ einwertigen Zahlen einen Körper A; die Permutationen ψ haben alle einen und denselben auf A bezüglichen Divisor φ, und jeder gemeinsame Divisor der Permutationen ψ ist Divisor dieser Permutation φ.

Diesen Körper A, welcher durch das System $\mathfrak{P}$ vollständig bestimmt ist, wollen wir kurz den Körper von $\mathfrak{P}$ nennen, und seine Permutation φ soll der größte gemeinsame Divisor der Permutationen ψ oder kürzer der Rest von $\mathfrak{P}$ heißen; besteht das System $\mathfrak{P}$ nur aus einer einzigen Permutation ψ, so ist offenbar auch im früheren Sinne A der Körper von ψ, und $\varphi = \psi$.

Während die Existenz der Divisoren einer gegebenen Körper-Permutation unmittelbar einleuchtet, so liegt die umgekehrte Frage viel tiefer; sie wird wenigstens teilweise durch den folgenden zweiten Satz (D. § 165, III) beantwortet:

II. Ist der Körper B ein endliches Multiplum des Körpers A, und φ eine Permutation von A, so ist der Grad (B, A) auch die Anzahl aller verschiedenen Permutationen ψ von B, welche Multipla von φ sind; zugleich ist A der Körper, und φ der Rest des Systems $\mathfrak{P}$ dieser Permutationen ψ.

Das bekannteste Beispiel zu diesem Satze ergibt sich aus der Betrachtung des Körpers Z aller Zahlen und des Körpers X aller reellen Zahlen. Offenbar ist $Z = X(i)$, wo i eine Wurzel der quadratischen Gleichung $i^2 + 1 = 0$ bedeutet; die beiden Zahlen 1, i bilden ein nach X irreduzibeles System, jede Zahl in Z ist auf eine einzige Weise in der Form $x_1 + i x_2$ darstellbar, wo x_1, x_2 in X enthalten sind, und folglich ist $(Z, X) = 2$. Bedeutet nun φ die identische Permutation von X, so gibt es wirklich zwei und nur zwei verschiedene Permutationen ψ von Z, die Multipla von φ sind; die eine ist die identische Permutation von Z, während die andere durch $(x_1 + i x_2)\psi = x_1 - i x_2$ definiert ist.

§ 3.

Permutationen des Körpers aller algebraischen Zahlen.

Der zuletzt hervorgehobene Hauptsatz II setzt voraus, daß der Körper B ein endliches Multiplum des Körpers A ist; läßt man diese Voraussetzung fallen, so scheint mir die Beantwortung der Frage, ob jede Permutation φ von A mindestens ein auf B bezügliches Multiplum ψ besitzt, auf die größten Schwierigkeiten zu stoßen. Nehmen wir z. B. den reellen quadratischen Körper $A = R(\sqrt{2})$, welcher aus dem rationalen Körper R durch Adjunktion von $\sqrt{2}$ entsteht, so besitzt A eine nicht identische Permutation φ, durch welche $\sqrt{2}$ in $-\sqrt{2}$ übergeht, und da A ein Divisor des Körpers X aller reellen Zahlen ist, so entsteht die Frage: gibt es ein auf X bezügliches Multiplum von φ? Ich weiß es nicht, doch glaube ich, daß diese Frage zu verneinen ist; die Zahlen des reellen Körpers X scheinen mir durch die Stetigkeit so unlöslich miteinander verbunden zu sein, daß ich vermute, er könne außer der identischen gar keine andere Permutation besitzen, und hieraus würde folgen, daß der Körper Z aller Zahlen nur die beiden, am Schlusse von § 2 genannten Permutationen besitzt. Nach einigen vergeblichen Versuchen, hierüber Gewißheit zu erlangen, habe ich diese Untersuchung aufgegeben; um so mehr würde es mich erfreuen, wenn ein anderer Mathematiker mir eine entscheidende Antwort auf diese Frage mitteilen wollte.

Dieselbe Frage kann aber vollständig beantwortet werden, wenn man sich auf das unstetige Gebiet H aller algebraischen Zahlen beschränkt. Unter einer algebraischen Zahl schlechthin wird hier jede Zahl t verstanden, welche algebraisch in bezug auf den rationalen Körper R, also die Wurzel einer Gleichung

$$t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t + a_n = 0$$

mit rationalen Koeffizienten a_1, $a_2 \cdots a_{n-1}$, a_n ist. Der Inbegriff H aller dieser Zahlen t ist bekanntlich ein Körper, und unter einem algebraischen Körper schlechthin verstehen wir jeden Divisor von H; offenbar ist H kein endliches Multiplum von R, also $(H, R) = \infty$. Wir erwähnen ferner, daß jede mit einer algebraischen Zahl t konjugierte Zahl $t\psi$ (§ 2) ebenfalls algebraisch ist; denn weil die rationalen Koeffizienten a_1, $a_2 \cdots a_n$ durch jede Permutation ψ in sich selbst übergehen, so muß $t\psi$ derselben Gleichung genügen, deren Wurzel t ist. Hierauf schreiten wir zum Beweis des folgenden Existenzsatzes:

III. Ist φ eine Permutation eines algebraischen Körpers A, so besitzt der Körper H aller algebraischen Zahlen mindestens eine Permutation ω, welche Multiplum von φ ist.

Ist H ein endliches Multiplum von A, so ist unser Satz eine unmittelbare Folge des oben (in § 2) erwähnten Hauptsatzes II; wir beschränken uns daher im folgenden auf den entgegengesetzten Fall $(H, A) = \infty$, während (A, R) endlich oder auch unendlich sein kann. Der Beweis beruht dann hauptsächlich auf einer wichtigen Eigenschaft des Körpers H, welche zuerst von G. Cantor*) hervorgehoben ist und darin besteht, daß alle Zahlen dieses Körpers H sich in eine einfach unendliche Reihe

$$h_1, h_2, h_3 \cdots h_r, h_{r+1} \cdots \qquad (h)$$

anordnen lassen, in der Art, daß jeder natürlichen Zahl r eine bestimmte algebraische Zahl h_r, und daß umgekehrt jeder algebraischen Zahl t eine (und nur eine) natürliche Zahl r entspricht, für welche $h_r = t$ wird. Eine solche Anordnung (Abbildung des Körpers H durch die Reihe der natürlichen Zahlen r) läßt sich auf unendlich viele verschiedene Arten herstellen; unserem Beweis legen wir eine bestimmte solche Anordnung (h), gleichgültig welche, zugrunde, und wir nennen die natürliche Zahl r den Index der algebraischen Zahl h_r.

Da nun $(H, A) = \infty$ vorausgesetzt wird, so ist A ein echter Divisor von H, d. h. es gibt in H, also in der Reihe (h) Zahlen, welche nicht in A enthalten sind; unter allen diesen Zahlen gibt es eine völlig bestimmte Zahl $t = h_r$, welche den kleinsten Index r hat, und wir wollen diese Zahl r auch den Index des Körpers A nennen; ist $r > 1$, so sind die der Zahl t vorausgehenden $r - 1$ Zahlen $h_1, h_2 \cdots h_{r-1}$ alle in A enthalten. Da nun die Zahl t auch algebraisch in bezug auf A ist, so entsteht (nach § 1) aus A durch Adjunktion von t ein Körper

$$A_1 = A(t),$$

welcher ein endliches Multiplum von A und zugleich ein Divisor von H ist. Der Kürze halber wollen wir diesen Körper A_1, welcher

*) Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen (Crelles Journal, Bd. 77). Diesen, auf den Körper H ausgedehnten Satz hatte ich ebenfalls gefunden, aber ich zweifelte an seiner Fruchtbarkeit, bis ich durch den schönen Beweis der Existenz von transzendenten Zahlen, den Cantor in § 2 seiner Abhandlung geführt hat, eines Besseren belehrt wurde.

durch A und die zugrunde gelegte Anordnung (h) völlig bestimmt ist, das nächste Multiplum von A nennen. Der Körper H kann aber kein endliches Multiplum von A_1 sein, weil sonst [nach (2) in § 1] H auch ein endliches Multiplum von A wäre, mithin ist $(H, A_1) = \infty$; man kann daher auf A_1 dieselbe Betrachtung anwenden wie eben auf A, und so entspringt, indem man auf dieselbe Weise fortfährt, aus dem Körper A eine offenbar unendliche Kette (A) von Körpern

$$A, A_1, A_2 \cdots A_s, A_{s+1} \cdots, \qquad (A)$$

in der jedes folgende Glied A_{s+1} das nächste Multiplum des vorhergehenden A_s ist, während sie alle zugleich Divisoren von H sind. Da ferner der Körper $A_1 = A(t)$ außer den schon in A enthaltenen Zahlen $h_1, h_2 \cdots h_{r-1}$ auch noch die neue Zahl $t = h_r$ enthält, so ist sein Index $\geqq r + 1$, und durch Wiederholung desselben Schlusses ergibt sich, daß der Körper A_s gewiß alle diejenigen Zahlen der Reihe (h) enthält, deren Index $< r + s$ ist. Da nun jede algebraische Zahl einen bestimmten endlichen Index hat, so kann man, wenn eine oder mehrere solche Zahlen $u, v \cdots$ in endlicher Anzahl gegeben sind, die natürliche Zahl s immer so groß wählen, daß alle diese Zahlen in dem Körper A_s, mithin auch in allen folgenden Körpern A_{s+1}, $A_{s+2} \cdots$ enthalten sind.

Wir nehmen jetzt an, es sei irgendeine Permutation φ des Körpers A gegeben. Da die Zahl $t = h_r$ nicht in A enthalten, also der endliche Grad $(A_1, A) \geqq 2$ ist, so gibt es nach dem für endliche Multipla geltenden Hauptsatz II (in § 2) immer mehrere verschiedene Permutationen ψ des Körpers $A_1 = A(t)$, welche Multipla von φ sind, und jede dieser Permutationen ψ ist vollständig bestimmt durch die konjugierte Zahl $t\psi$, in welche die Zahl t durch ψ übergeht. An sich wäre es für unseren Beweis ganz gleichgültig, welche von diesen Permutationen ψ, deren Anzahl $= (A_1, A)$ ist, wir auswählen wollen; um aber alles auf völlig bestimmte Regeln zu bringen, verfahren wir folgendermaßen. Da die Zahlen $t\psi$ (wie oben erwähnt ist) ebenfalls algebraisch, also in der Reihe (h) enthalten und außerdem alle voneinander verschieden sind, so setzen wir fest, daß von den Permutationen ψ immer diejenige gewählt werden soll, für welche der Index von $t\psi$ so klein wie möglich ausfällt; diese Permutation von A_1, welche durch φ und die Anordnung (h) völlig bestimmt ist, wollen wir mit φ_1 bezeichnen und das nächste Multiplum der ge-

gebenen Permutation φ nennen. Offenbar kann man nun mit dieser Permutation φ_1 des Körpers A_1 genau so verfahren, wie eben mit der Permutation φ des Körpers A, und durch beständige Fortsetzung dieser Bildung entspringt aus der gegebenen Permutation φ eine unendliche Kette

$$\varphi, \varphi_1, \varphi_2 \cdots \varphi_s, \varphi_{s+1} \cdots, \qquad (\varphi)$$

in der allgemein φ_s eine Permutation von A_s, und φ_{s+1} das nächste Multiplum von φ_s ist.

Nachdem die beiden Ketten (A) und (φ) der Körper A_s und ihrer Permutationen φ_s gebildet sind, gestaltet sich der Beweis unseres Satzes III sehr einfach. Wir definieren eine Abbildung ω des Körpers H auf folgende Weise. Ist u irgendeine algebraische Zahl, so gibt es nach einer früheren Bemerkung in der Kette (A) auch solche Körper A_s, in denen die Zahl u enthalten ist, und wenn n die kleinste Zahl s bedeutet, für welche dies eintritt, so setzen wir fest, daß u durch die Abbildung ω in das Bild

$$u\omega = u\varphi_n$$

übergehen soll; hierdurch ist die Abbildung ω des Körpers H vollständig bestimmt, und wir wollen jetzt beweisen, daß sie eine Permutation von H und zugleich ein Multiplum von φ ist. Zunächst bemerken wir, daß die Zahl u des Körpers A_n auch in allen folgenden Körpern A_{n+1}, $A_{n+2} \cdots$ der Kette (A), also allgemein in A_s enthalten ist, wenn $s \geqq n$ genommen wird, und da φ_s zugleich ein Multiplum von φ_n ist, so folgt aus der Definition von ω auch

$$u\omega = u\varphi_s.$$

Bedeutet nun v ebenfalls eine algebraische Zahl, so kann man s so groß wählen, daß beide Zahlen u, v und folglich auch deren Summe, Differenz, Produkt und Quotient demselben Körper A_s angehören, und hieraus folgt, wie eben bemerkt ist, auch

$$u\omega = u\varphi_s, \quad v\omega = v\varphi_s,$$
$$(u+v)\omega = (u+v)\varphi_s, \quad (u-v)\omega = (u-v)\varphi_s,$$
$$(uv)\omega = (uv)\varphi_s, \quad \left(\frac{u}{v}\right)\omega = \left(\frac{u}{v}\right)\varphi_s;$$

da nun φ_s eine Permutation des Körpers A_s ist, also den in § 2 angegebenen Grundgesetzen gehorcht, so ergibt sich unmittelbar, daß die Abbildung ω des Körpers H denselben Grundgesetzen gehorcht,

also eine Permutation von H ist. Bedeutet ferner a irgendeine Zahl des Körpers A, so ist zufolge der Definition von ω auch $a\omega = a\varphi$, also ist ω ein Multiplum von φ, w. z. b. w.

§ 4.

Verallgemeinerung.

Wir wollen nun den eben bewiesenen Satz III durch die folgenden Bemerkungen vervollständigen und verallgemeinern, wobei wir unter H immer den aus allen algebraischen Zahlen bestehenden Körper verstehen. Zunächst erkennt man leicht, daß der Satz bestehen bleibt, wenn der Körper H durch irgendeinen algebraischen Körper B ersetzt wird, der ein Multiplum des Körpers A ist. Wenn nämlich φ wieder eine Permutation von A ist, so gibt es, wie wir jetzt wissen, mindestens eine Permutation ω von H, welche Multiplum von φ ist; bedeutet nun ψ den auf B bezüglichen Divisor von ω, so ist φ nach einer früheren Bemerkung (§ 2) zugleich der auf A bezügliche Divisor von ψ. Es gilt daher der folgende Satz:

IV. Ist der Körper A ein Divisor des algebraischen Körpers B, so besitzt jede Permutation φ von A mindestens ein auf B bezügliches Multiplum.

Dies ist, falls B ein endliches Multiplum von A ist, offenbar nur ein spezieller Fall des Satzes II (in § 2), welcher zugleich die schärfere Bestimmung enthält, daß der Grad (B, A) die genaue Anzahl aller verschiedenen Permutationen ψ ist. Wir können nun auch leicht beweisen, daß im entgegengesetzten Falle, wenn B kein endliches Multiplum von A ist, die Anzahl der Permutationen ψ von B, welche Multipla derselben Permutation φ von A sind, unendlich groß, also wieder $= (B, A)$ ist, wenn wir die am Schlusse von § 1 festgesetzte Bedeutung des Symbols beibehalten. Hierzu führt die Betrachtung derjenigen Körper A', welche (wie z. B. A selbst) endliche Multipla von A und zugleich Divisoren von B sind. Da jeder solche Körper A' verschieden von B, also ein echter Divisor von B ist, so gibt es in B gewiß solche Zahlen t, die nicht in A' enthalten sind, und folglich entsteht aus A' durch Adjunktion einer solchen algebraischen Zahl t ein Körper $A'' = A'(t)$, der ein endliches Multiplum von A', also auch von A, und zugleich wieder ein Divisor von B ist; da ferner $(A'', A') \geqq 2$, also $(A'', A) = (A'', A')\ (A', A) \geqq 2\,(A', A)$

ist, so leuchtet ein, daß, wenn m eine gegebene, beliebig große natürliche Zahl bedeutet, unter allen Körpern A' es auch solche gibt, für welche $(A', A) \geqq m$ ist. Nach dem Satze II (in § 2) besitzt ein solcher Körper A' gewiß mindestens m verschiedene Permutationen

$$\varphi'_1, \varphi'_2 \cdots \varphi'_m,$$

welche Multipla der gegebenen Permutation φ von A sind, und da A' ein Divisor von B ist, so besitzt nach dem eben bewiesenen Satze IV jede dieser m Permutationen φ' mindestens ein auf B bezügliches Multiplum ψ; die so erhaltenen m Permutationen

$$\psi_1, \psi_2 \cdots \psi_m$$

sind folglich auch Multipla von φ, und sie sind alle voneinander verschieden, weil jede Permutation ψ von B nur einen einzigen, völlig bestimmten, auf A' bezüglichen Divisor φ' besitzt. Da m beliebig groß genommen werden kann, so ergibt sich, daß die Anzahl aller verschiedenen Permutationen ψ von B, welche Multipla derselben Permutation φ von A sind, unendlich groß, also $= (B, A)$ ist, w. z. b. w.

Unter derselben Voraussetzung wollen wir endlich noch zeigen, daß auch der letzte Teil des Satzes II (in § 2) bestehen bleibt. Das System $\mathfrak{P}$ aller Permutationen ψ von B, welche Multipla der Permutation φ von A sind, besitzt (nach dem Satze I in § 2) einen bestimmten größten gemeinsamen Divisor oder Rest χ, und da φ ein gemeinsamer Divisor aller Permutationen ψ, also auch Divisor von χ ist, so ist der Körper C dieser Permutation χ ein Multiplum von A und zugleich Divisor von B. Machen wir nun die Annahme, C sei verschieden von A, also $(C, A) \geqq 2$, so besitzt C, wie eben bewiesen ist, mindestens eine von χ verschiedene Permutation χ', welche ebenfalls Multiplum von φ ist; da ferner C Divisor von B ist, so hat B mindestens eine Permutation ψ', welche Multiplum von χ', also auch von φ ist und folglich auch dem System $\mathfrak{P}$ angehört; mithin muß χ als Rest von $\mathfrak{P}$ auch Divisor von ψ' sein; es besäße daher ψ' zwei verschiedene, auf denselben Körper C bezügliche Divisoren χ, χ', was unmöglich ist. Unsere obige Annahme, die Körper A, C seien verschieden, ist daher unzulässig, und hieraus folgt offenbar, daß $\chi = \varphi$ ist. Hiernach können wir den obigen Satz IV in folgender Weise vervollständigen:

V. Ist der Körper A ein Divisor des algebraischen Körpers B, und φ eine Permutation von A, so ist der Grad (B, A), mag er

endlich oder unendlich sein, die Anzahl aller verschiedenen Permutationen ψ von B, welche Multipla von φ sind; zugleich ist A der Körper, und φ der Rest des Systems $\mathfrak{P}$ dieser Permutationen ψ.

§ 5.

Gruppen von Permutationen.

Aus dem Vorhergehenden folgt unmittelbar, daß der Körper H, welcher aus allen algebraischen Zahlen besteht, unendlich viele verschiedene Permutationen ω besitzt. Da nun jede in H enthaltene Zahl t durch eine Permutation ω wieder in eine algebraische Zahl $t\omega$ übergeht, so ist der mit H konjugierte Körper $H\omega$ gewiß ein Divisor von H, aber wir können leicht zeigen, daß immer $H\omega = H$ ist. Denn betrachtet man wieder irgendeine mit rationalen Koeffizienten behaftete Gleichung, deren Wurzel eine gegebene algebraische Zahl t ist, und bezeichnet mit $t_1, t_2 \cdots t_m$ alle diejenigen m Wurzeln dieser Gleichung, die voneinander verschieden sind, so gehören dieselben auch dem Körper H an, und sie gehen (wie in § 2 erwähnt ist) durch ω in ebenso viele verschiedene Zahlen $t_1\omega, t_2\omega \cdots t_m\omega$ über; da die letzteren aber derselben Gleichung genügen, so muß eine von ihnen mit der gegebenen Zahl t übereinstimmen, mithin ist jede Zahl t des Körpers H auch in $H\omega$ enthalten, woraus offenbar die obige Behauptung $H\omega = H$ folgt. Diese Eigenschaft des Körpers H, durch jede seiner Permutationen in sich selbst überzugehen, bezeichnen wir dadurch, daß wir ihn einen Normalkörper nennen (vgl. D. § 166). Eine unmittelbare Folge, oder vielmehr nur eine andere Ausdrucksform dieser Eigenschaft besteht darin, daß die Umkehrung ω^{-1} einer jeden Permutation ω von H ebenfalls eine Permutation von H ist (§ 2).

Es ist nun an der Zeit, noch einen Begriff aus der allgemeinen Theorie der Körper-Permutationen in Erinnerung zu bringen, nämlich den ihrer Zusammensetzung (D. § 162). Hierbei beschränken wir uns der Kürze halber auf den folgenden speziellen Fall*). Es sei M

*) Ich will hier beiläufig bemerken, daß man die Resultante $\varphi\psi$ auch ganz allgemein erklären kann, wenn φ, ψ Permutationen von zwei beliebigen Körpern A, B sind; es gibt einen und nur einen Divisor A' von A, welcher durch φ in den größten gemeinsamen Divisor von $A\varphi$ und B übergeht, und die Resultante $\varphi\psi$ wird als Permutation dieses Körpers A' durch $x(\varphi\psi) = (x\varphi)\psi$ definiert, wo x jede Zahl in A' bedeutet. Die beiden Sätze $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}$ und $(\varphi\psi)\chi = \varphi(\psi\chi)$ behalten ihre Gültigkeit, während andere Sätze gewisse Modifikationen erfordern.

ein beliebiger Körper, und $\mathfrak{E}$ der Inbegriff aller derjenigen Permutationen ε von M, durch welche M in sich selbst übergeht, welche also der Bedingung $M\varepsilon = M$ genügen; es gibt immer wenigstens eine solche, nämlich die identische Permutation M_0 von M, und jede Umkehrung ε^{-1} ist ebenfalls in $\mathfrak{E}$ enthalten. Je zwei (gleiche oder verschiedene) solche Permutationen φ, ψ erzeugen eine Resultante $\varphi\psi$, welche für jede in M enthaltene Zahl x durch

$$x(\varphi\psi) = (x\varphi)\psi$$

definiert wird und ebenfalls eine in $\mathfrak{E}$ enthaltene Permutation von M ist. Hieraus folgen die beiden Sätze

$$(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1},\ (\varphi\psi)\chi = \varphi(\psi\chi),$$

wo χ ebenfalls jede in $\mathfrak{E}$ enthaltene Permutation bedeutet, und die Resultante $\varphi\varphi^{-1}$ ist die identische Permutation M_0. Ein in $\mathfrak{E}$ enthaltenes System $\mathfrak{A}$ von Permutationen α heißt eine Gruppe, wenn 1. die Resultanten von je zwei Permutationen α und 2. alle Umkehrungen α^{-1} demselben System $\mathfrak{A}$ angehören, und sie heißt endlich oder unendlich, je nachdem die Anzahl der Permutationen α endlich oder unendlich ist; im ersteren Falle findet man leicht, daß die Bedingung 2. schon eine notwendige Folge der Bedingung 1. ist. Der Inbegriff $\mathfrak{E}$ ist selbst eine Gruppe, und ebenso bildet die identische Permutation M_0 für sich allein eine Gruppe, welche in jeder Gruppe $\mathfrak{A}$ enthalten ist. Für endliche Gruppen gilt nun der folgende Fundamentalsatz (D. § 166, I):

VI. Besteht eine endliche Gruppe $\mathfrak{A}$ aus n Permutationen des Körpers M, und ist A der Körper von $\mathfrak{A}$, so ist $(M, A) = n$, also M ein endliches Multiplum von A, und der Rest von $\mathfrak{A}$ ist die identische Permutation A_0 von A. Zugleich folgt aus dem Satze II (in § 2), daß die Gruppe $\mathfrak{A}$ auch der Inbegriff aller auf M bezüglichen Multipla von A_0 ist.

Man überzeugt sich leicht, daß dieser Satz VI in Verbindung mit dem Satze II (in § 2) die Theorie von Galois vollständig in sich schließt. Um dies etwas näher auszuführen, nehmen wir an, die obige Gruppe $\mathfrak{E}$ sei endlich, woraus natürlich auch die Endlichkeit jeder in $\mathfrak{E}$ enthaltenen Gruppe $\mathfrak{A}$ folgt. Bedeutet E den Körper der Gruppe $\mathfrak{E}$, und E_0 seine identische Permutation, so ist M nach VI

ein endliches Multiplum von E, der Rest von $\mathfrak{E}$ ist E_0, und umgekehrt ist $\mathfrak{E}$ der Inbegriff aller auf M bezüglichen Multipla von E_0. Der Kern der Theorie von Galois besteht nun darin, daß einerseits die Körper A, welche Divisoren von M und zugleich Multipla von E sind, und andererseits die in $\mathfrak{E}$ enthaltenen Gruppen $\mathfrak{A}$ sich gegenseitig eindeutig entsprechen. Erstens besitzt jede solche Gruppe $\mathfrak{A}$ einen bestimmten Körper A, welcher aus allen zu $\mathfrak{A}$ einwertigen Zahlen des Körpers M besteht, also ein Divisor von M ist, und da jede in E enthaltene, also zu $\mathfrak{E}$ einwertige Zahl auch einwertig zu $\mathfrak{A}$ ist, so ist A auch Multiplum von E. Da ferner $\mathfrak{A}$ nach VI der Inbegriff aller auf M bezüglichen Multipla der identischen Permutation A_0 von A ist, so haben zwei verschiedene Gruppen $\mathfrak{A}$ auch zwei verschiedene Körper A. Wir haben daher zweitens nur noch zu zeigen, daß umgekehrt jeder Körper A, welcher Divisor von M und Multiplum von E ist, auch wirklich der Körper einer in $\mathfrak{E}$ enthaltenen Gruppe $\mathfrak{A}$ ist. Zunächst folgt aus dem in § 1 erwähnten Satze $(M, E) = (M, A)(A, E)$, daß M ein endliches Multiplum von A ist; mithin ist der Grad (M, A) nach dem Satze II (in § 2) auch die Anzahl aller derjenigen Permutationen α von M, welche Multipla der identischen Permutation A_0 von A sind, und zugleich ist A der Körper, A_0 der Rest des Systems $\mathfrak{A}$ dieser Permutationen α. Wir brauchen also nur noch zu beweisen, daß dieses System $\mathfrak{A}$ eine in $\mathfrak{E}$ enthaltene Gruppe ist. Da A Multiplum von E, also E_0 der auf E bezügliche Divisor von A_0 ist, so ist jede Permutation α auch Multiplum von E_0 und folglich in der Gruppe $\mathfrak{E}$ enthalten. Bedeutet ferner x jede Zahl des Körpers A, so ist $x = xA_0 = x\alpha$, also auch $x\alpha^{-1} = x$, und wenn α_1, α_2 zwei solche Permutationen α sind, so folgt hieraus auch $x(\alpha_1\alpha_2) = (x\alpha_1)\alpha_2 = x\alpha_2 = x$, also gehört die Resultante $\alpha_1\alpha_2$ demselben System $\mathfrak{A}$ an, welches folglich eine Gruppe ist, w. z. b. w.

Aus der hiermit nachgewiesenen Korrespondenz zwischen den Körpern A und den Gruppen $\mathfrak{A}$ fließen unmittelbar die übrigen Sätze der Theorie von Galois, welche von den Beziehungen zwischen mehreren solchen Körpern A und von den entsprechenden Beziehungen zwischen den zugehörigen Gruppen $\mathfrak{A}$ handeln (D. § 166). Auf alles dies brauchen wir, weil es hinreichend bekannt ist, hier nicht einzugehen, und wir haben auch das Vorstehende nur deshalb wieder in Erinnerung gebracht, um jetzt auf das abweichende Verhalten unendlicher Permutationsgruppen aufmerksam zu machen.

§ 6.

Unendliche Gruppen von Permutationen.

Wir haben gesehen, daß der aus allen algebraischen Zahlen bestehende Körper H unendlich viele Permutationen ω besitzt, und daß er durch jede von ihnen in sich selbst übergeht; diese Permutationen ω bilden daher eine unendliche Gruppe, die wir mit $\mathfrak{G}$ bezeichnen wollen, und wir fragen, ob wohl auch hier eine gegenseitig eindeutige Korrespondenz zwischen den algebraischen Körpern A (den Divisoren von H) und den in $\mathfrak{G}$ enthaltenen Gruppen $\mathfrak{A}$ besteht.

Geht man von irgendeinem algebraischen Körper A aus, und bezeichnet mit A_0 dessen identische Permutation, so gibt es nach dem Satze V (in § 4), welcher hier den Satz II (in § 2) vollständig ersetzt, immer Permutationen α des Körpers H, welche Multipla von A_0 sind; mag ihre Anzahl (H, A) endlich oder unendlich sein, immer ist A der Körper, und A_0 der Rest des Systems $\mathfrak{A}$ dieser Permutationen α. Da ferner A_0 eine identische Permutation ist, so findet man leicht (wie zuletzt in § 5), daß dieses in $\mathfrak{G}$ enthaltene System $\mathfrak{A}$ eine Gruppe ist; wir wollen sie die Identitätsgruppe des Körpers A nennen. Da ferner, wie schon bemerkt, A der Körper von $\mathfrak{A}$ ist, so folgt, daß zwei verschiedene Körper A auch zwei verschiedene Identitätsgruppen $\mathfrak{A}$ haben. Die oben aufgeworfene Frage würde daher zu bejahen sein, wenn man beweisen könnte, daß jede in $\mathfrak{G}$ enthaltene Gruppe $\mathfrak{A}$ die Identitätsgruppe eines Körpers A ist, was ja für endliche Gruppen $\mathfrak{A}$ nach dem Satze VI (in § 5) wirklich der Fall ist. Nun hat zwar auch jede unendliche Gruppe $\mathfrak{A}$ einen bestimmten Körper A, der Divisor von H, also algebraisch ist, und da in $\mathfrak{A}$ immer die identische Permutation von H enthalten ist, so ist der Rest von $\mathfrak{A}$ gewiß die identische Permutation A_0 dieses Körpers A, also enthält $\mathfrak{A}$ nur solche Permutationen α von H, welche auch in der Identitätsgruppe $\mathfrak{A}'$ des Körpers A enthalten sind; aber es fehlt der Nachweis, daß umgekehrt jede in $\mathfrak{A}'$ enthaltene Permutation α', d. h. jedes auf H bezügliche Multiplum von A_0 auch in der gegebenen Gruppe $\mathfrak{A}$ enthalten ist, oder anders ausgedrückt, daß die Körper zweier verschiedener Gruppen auch verschieden sind. Dies habe ich anfangs für sehr wahrscheinlich gehalten, und erst nach mehreren vergeblichen Versuchen, es zu beweisen, ist es mir gelungen, mich von der Unrichtigkeit dieser Vermutung durch ein Beispiel zu

überzeugen, welches ich zum Schluß dieser Arbeit jetzt noch mitteilen will.

Dieses Beispiel bezieht sich nicht auf den vollen Körper H, sondern auf die einfachste Klasse unendlicher Kreiskörper. Ist p eine bestimmte natürliche Primzahl, so entspricht jeder natürlichen Zahl n eine bestimmte Einheitswurzel

$$u_n = \cos\frac{2\pi}{p^n} + i\sin\frac{2\pi}{p^n}, \tag{1}$$

und wir wollen mit P_n den durch sie erzeugten Kreiskörper $R(u_n)$ vom Grade $\varphi(p^n) = (p-1)p^{n-1}$ bezeichnen, während P_0 der Körper R der rationalen Zahlen ist. Aus

$$u_n = u_{n+1}^p \tag{2}$$

folgt, daß in der unendlichen Kette von Körpern

$$P_0, P_1, P_2, P_3 \cdots$$

jedes Glied P_n Divisor des nächstfolgenden P_{n+1}, also auch jedes folgenden Gliedes P_{n+s} ist.

Wenn irgendeine Kette von Körpern P_n vorliegt, welche diese letztere Eigenschaft besitzt, so kann ihr kleinstes gemeinsames Multiplum M keine anderen als solche Zahlen t enthalten, die schon mindestens einem Körper P_n und also auch allen folgenden Körpern P_{n+s} angehören; denn der Inbegriff aller dieser Zahlen t bildet, wie man leicht findet, wirklich einen Körper, welcher offenbar ein Divisor von M, zugleich aber auch Multiplum aller P_n, also auch Multiplum von M, mithin $= M$ ist; man kann daher dieses Multiplum M zweckmäßig auch mit P_∞ bezeichnen. Ist nun ε irgendeine Permutation von M und ε_n der auf P_n bezügliche Divisor von ε, so entsteht eine unendliche Kette von Permutationen

$$\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3 \cdots,$$

in der jedes Glied ε_n Divisor aller folgenden Glieder ε_{n+s} ist. Umgekehrt, wenn eine bestimmte Kette von Permutationen ε_n der Körper P_n vorliegt, welche diese letztere Eigenschaft besitzt, so folgt aus der oben besprochenen Konstitution des Körpers M leicht (wie in § 3), daß es eine und nur eine Permutation ε von M gibt, welche Multiplum aller dieser Permutationen ε_n ist.

Wenden wir dies auf unseren Fall der Kreiskörper $P_n = R(u_n)$ an, und bezeichnen mit $\mathfrak{E}$ den Inbegriff aller Permutationen ε ihres

kleinsten Multiplums $M = P_\infty$, so ist der auf P_n bezügliche Divisor ε_n von ε völlig bestimmt durch die mit u_n konjugierte Zahl $u_n\varepsilon_n = u_n\varepsilon$, und diese ist bekanntlich immer eine Potenz von u_n, deren Exponent eine durch p nicht teilbare Zahl ist und durch jede nach dem Modul p^n kongruente Zahl ersetzt werden darf; bezeichnen wir diese Zahl mit (n, ε), so wird daher

$$u_n\varepsilon_n = u_n\varepsilon = u_n^{(n,\,\varepsilon)}, \tag{3}$$

und da aus (2) auch

$$u_n\varepsilon = (u_{n+1}\varepsilon)^p,$$

also

$$u_n^{(n,\,\varepsilon)} = u_{n+1}^{p\,(n+1,\,\varepsilon)} = u_n^{(n+1,\,\varepsilon)}$$

folgt, so ist

$$(n, \varepsilon) \equiv (n+1, \varepsilon) \pmod{p^n}, \tag{4}$$

und diese Kongruenz drückt aus, daß ε_n Divisor von ε_{n+1} ist. Umgekehrt, wenn eine Kette von solchen, durch p nicht teilbaren Zahlen (n, ε) vorliegt, welche den Bedingungen (4) genügen, so folgt aus den obigen allgemeinen Bemerkungen, daß ihr eine und nur eine Permutation ε von M entspricht, welche durch (3) bestimmt ist. Hierbei darf man festsetzen, daß (n, ε) positiv und kleiner als p^n sein soll, und wenn man $(n+1, \varepsilon) = (n, \varepsilon) + c_n p^n$ setzt, so wird $0 \leqq c_n < p$; jede willkürlich gewählte unendliche Reihe von solchen Zahlen $c_1, c_2, c_3 \cdots$ liefert in Verbindung mit jeder der $p-1$ Zahlen $(1, \varepsilon)$ eine bestimmte Permutation ε, und hieraus folgt, daß der Inbegriff $\mathfrak{E}$ aller ε in gewissem Sinne eine stetige Mannigfaltigkeit bildet, worauf wir hier nicht weiter eingehen.

Bekanntlich geht der Körper P_n durch jede Permutation in sich selbst über, es ist also $P_n\varepsilon = P_n\varepsilon_n = P_n$, und hieraus folgt offenbar auch $M\varepsilon = M$, mithin bildet der Inbegriff $\mathfrak{E}$ (nach § 5) eine Gruppe. Sind ε, ε', also auch $\varepsilon\varepsilon'$ in $\mathfrak{E}$ enthalten, so folgt aus (3)

$$u_n(\varepsilon\varepsilon') = (u_n\varepsilon)\varepsilon' = (u_n\varepsilon')^{(n,\,\varepsilon)} = u_n^{(n,\,\varepsilon)\,(n,\,\varepsilon')},$$

also

$$(n, \varepsilon\varepsilon') \equiv (n, \varepsilon)\ (n, \varepsilon') \pmod{p^n}, \tag{5}$$

und da die rechte Seite sich durch Vertauschung von ε, ε' nicht ändert, so folgt, daß

$$\varepsilon\varepsilon' = \varepsilon'\varepsilon, \tag{6}$$

also $\mathfrak{E}$ eine Abelsche Gruppe ist.

Jede Permutation ε erzeugt durch wiederholte Zusammensetzung mit sich selbst und ihrer Umkehrung ε^{-1} die Reihe aller Potenzen ε^r,

welche eine Gruppe bilden, die wir mit $[\varepsilon]$ bezeichnen wollen. Von einigem Interesse ist nun die Frage, ob es außer der identischen Permutation M_0 von M, welche für sich allein eine Gruppe bildet, noch andere endliche, d. h. solche Permutationen α gibt, die eine endliche Gruppe $[\alpha]$ erzeugen. Bedeutet m die Anzahl der in einer solchen Gruppe $[\alpha]$ enthaltenen verschiedenen Permutationen α^r, so ist bekanntlich $\alpha^m = M_0$, und umgekehrt, wenn eine natürliche Zahl m diese Bedingung erfüllt, so folgt hieraus, daß α endlich ist. Diese Forderung drückt sich nach (3), (4), (5) dadurch aus, daß α für jede natürliche Zahl n den Bedingungen

$$(n, \alpha)^m \equiv 1,\ (n, \alpha) \equiv (n+1, \alpha) \pmod{p^n} \tag{7}$$

genügen muß. Schließt man den Fall $p = 2$ aus, so ergibt die genaue Untersuchung, welche keine erheblichen Schwierigkeiten darbietet, daß es nur $p-1$ endliche Permutationen α gibt; diese sind durch

$$(n, \alpha) \equiv (1, \alpha)^{p^{n-1}} \pmod{p^n} \tag{8}$$

bestimmt, und man erhält sie alle, wenn man $(1, \alpha)$ irgendein vollständiges System nach p inkongruenter Zahlen durchlaufen läßt, welche nicht durch p teilbar sind; die entsprechenden Zahlen (n, α) bilden alle $p-1$ Wurzeln x_n der Kongruenz

$$x_n^{p-1} \equiv 1 \pmod{p^n}, \tag{9}$$

und hieraus folgt, daß diese $p-1$ Permutationen α die Bedingung

$$\alpha^{p-1} = M_0 \tag{10}$$

erfüllen. Sie bilden eine Gruppe $\mathfrak{A}$, und wenn man für $(1, \alpha)$ eine primitive Wurzel der Primzahl p wählt, so ist diese Gruppe $\mathfrak{A} = [\alpha]$. Bedeutet ferner A den Körper von $\mathfrak{A}$, so folgt aus dem Satze VI (in § 5), daß $(M, A) = p-1$, also M ein endliches Multiplum von A ist*).

Es ist nun auch nicht schwer, alle endlichen und unendlichen Divisoren des Körpers M aufzufinden und die zugehörigen, in $\mathfrak{E}$ enthaltenen Identitätsgruppen zu bestimmen. Der Kürze wegen verzichten wir hierauf, und wir wollen nur noch zum Schluß an einem Beispiel den oben versprochenen Nachweis liefern, daß nicht jede in $\mathfrak{E}$

*) In dem oben ausgeschlossenen Falle $p = 2$ findet man leicht, daß es zwei endliche Permutationen von M gibt, nämlich die identische und eine andere, durch welche jede Einheitswurzel u_n in u_n^{-1} übergeht.

enthaltene Gruppe eine Identitätsgruppe ist, oder anders ausgedrückt, daß zwei verschiedene Gruppen denselben Körper haben können.

Wir bezeichnen mit g eine bestimmt gewählte primitive Wurzel aller Potenzen der (ungeraden) Primzahl p und definieren eine Permutation β unseres Körpers M durch die für jede natürliche Zahl n geltende Kongruenz

$$(n, \beta) \equiv g \pmod{p^n},$$

wodurch die Existenz-Bedingung (4) erfüllt ist. Bedeutet β_n wieder den auf P_n bezüglichen Divisor von β, so ist also

$$u_n \beta_n = u_n^g, \quad u_n \beta_n^r = u_n^{g^r},$$

und da die Potenzen

$$g, g^2, g^3 \cdots g^{\varphi(p^n)}$$

nach dem Modul p^n ein vollständiges System inkongruenter, durch p nicht teilbarer Zahlen bilden, so erschöpfen die Potenzen

$$\beta_n, \beta_n^2, \beta_n^3 \cdots \beta_n^{\varphi(p^n)}$$

alle Permutationen des endlichen Körpers P_n; mithin muß nach einem bekannten Satze (oder nach II in § 2) jede in P_n enthaltene Zahl t, welche der Bedingung $t\beta = t$, also auch den Bedingungen $t\beta^r = t$ genügt, rational sein, also dem Körper R angehören. Wir kehren nun zu der Permutation β des Körpers M zurück, betrachten die aus allen Potenzen von β bestehende Gruppe $\mathfrak{B} = [\beta]$ und suchen deren Körper, d. h. den Inbegriff B aller zu $\mathfrak{B}$ einwertigen Zahlen t des Körpers M; diese Einwertigkeit wird schon vollständig durch die Forderung $t\beta = t$ ausgedrückt, weil hieraus auch $t\beta^{-1} = t$ und allgemein $t\beta^r = t$ folgt. Da nun, wie früher bemerkt, jede Zahl t des unendlichen Körpers M gewiß auch einem endlichen Körper P_n angehört, woraus $t\beta = t\beta_n$ folgt, so muß t auch der Bedingung $t\beta_n = t$ genügen und folglich rational sein, mithin ist $B = R$. Andererseits leuchtet aber ein, daß die Identitätsgruppe von R, d. h. der Inbegriff aller auf M bezüglichen Multipla der identischen Permutation R_0 die volle Gruppe $\mathfrak{E}$ aller Permutationen ε von M, und daß R der Körper dieser Gruppe $\mathfrak{E}$ ist, weil jede zu $\mathfrak{E}$ einwertige Zahl auch einwertig zu $\mathfrak{B}$ sein muß. Daß endlich die in $\mathfrak{E}$ enthaltene Gruppe $\mathfrak{B}$ verschieden von $\mathfrak{E}$ ist, ergibt sich schon daraus, daß von den oben gefundenen $p-1$ endlichen Permutationen α nur eine einzige, nämlich die identische Permutation M_0 in $\mathfrak{B}$ enthalten ist. Also haben die beiden verschiedenen Gruppen $\mathfrak{B}$ und $\mathfrak{E}$ denselben Körper R, w. z. b. w.

Zusatz aus dem Nachlaß:

Bestimmung der Divisoren von M und ihrer Identitätsgruppen.

Wir suchen jetzt alle Divisoren D von M. Enthält D eine Zahl μ vom Exponenten p^s (wo $s \geqq 1$)*), so ist D als Multiplum von $R(\mu) = A_s \cdot Q_e$**) auch Multiplum von A_s. Gibt es daher in D Zahlen μ, deren Exponent p^s jeden gegebenen Wert übertrifft, so ist D gemeinsames Multiplum aller A_s und folglich auch ein Multiplum von A, mithin

$$(M, A) = (M, D) \cdot (D, A) = p - 1,$$
$$(D, A) = e, \quad (M, D) = f; \quad p - 1 = e \cdot f$$

und folglich (leicht)

$$D = A \cdot Q_e.$$

Im entgegengesetzten Fall ist D kein Multiplum von A; dann gibt es eine Zahl s von der Art, daß A_s Divisor von D, aber A_{s+1} nicht Divisor von D ist; mithin sind die Exponenten aller in D enthaltenen Zahlen $\leqq p^s$, d. h. D ist Divisor von $P_s = A_s \cdot P_1$, also D ein endlicher Körper,

$$D = A_s \cdot Q_e. \quad [\text{Im Falle } s = 0 \text{ ist } D = R.]$$

Identitätsgruppen der Unterkörper von M.

Körper $M_{s,e} = A_s \cdot Q_e$; $\quad p - 1 = e \cdot f$.

Identitätsgruppe $\mathfrak{E}_{s,e}$: Alle Permutationen ε von M, die Multipla der identischen Permutation von $A_s \cdot Q_e$ sind.

$$u_n \varepsilon = u_n^{(n,\varepsilon)}; \quad (n, \varepsilon) \equiv (1, \varepsilon)^{p^n - 1} \pmod{p^n},$$
$$(s, \varepsilon)^f \equiv 1 \pmod{p^s}.$$

Körper $A \cdot Q_e$; Identitätsgruppe $\mathfrak{E}_{\infty,e}$:

$$u_n \varepsilon = u_n^{(n,\varepsilon)}; \quad (n, \varepsilon) \equiv (1, \varepsilon)^{p^n - 1} \pmod{p^n},$$
$$(1, \varepsilon)^f \equiv 1 \pmod{p}.$$

*) Jede Zahl μ in M hat einen bestimmten Exponenten p^s, d. h. sie ist in P_s, aber nicht in P_{s-1} enthalten.

**) Bezeichnet man, wenn e jeden Divisor von $p - 1 = e \cdot f$ bedeutet, mit Q_e den in P_1 enthaltenen Körper vom Grade e, so sind alle endlichen Körper, die in M enthalten sind, von der Form

$$A_s \cdot Q_e \quad [s = 1, 2, \cdots],$$

wo A_s der Durchschnitt des Körpers A mit P_s ist.

Erläuterungen zur vorstehenden Abhandlung.

In einem Brief an Frobenius (18. April 1897) schreibt Dedekind, nachdem er einen kurzen Überblick über den Inhalt der Arbeit gegeben hatte: „Für die unendlichen Körper hat bisher ein Noli me tangere gegolten; nur deshalb möchte ich gern einmal von ihnen sprechen."

Seitdem hat die Entwicklung der Algebra dieses „Noli me tangere" überwunden: Auf Grund der Steinitzschen Theorie der Körper konnte für beliebige unendliche Körper die volle Automorphismengruppe aufgestellt werden, im wesentlichen nach der Dedekindschen Methode; nur daß eine beliebige Wohlordnung zugrunde gelegt werden muß, und neben der algebraischen noch eine vorher abzuspaltende rein transzendente Erweiterung zu berücksichtigen ist. Dabei treten im Fall der komplexen Zahlen neben dem Übergang zum konjugiert Komplexen noch beliebig viele, allerdings „extrem unstetige" Abbildungen auf, entgegen der von Dedekind am Anfang von § 3 ausgesprochenen Vermutung [vgl. dazu A. Ostrowski, Journ. f. Math. **143** (1913); E. Noether, Math. Ann. **77** (1916); in geometrischer Einkleidung der Fragestellung: H. Lebesgue, Atti Torino **42** (1907); E. Kamke, Jahresber. d. d. Math.-Ver. **36** (1927)].

Die Galoissche Theorie der unendlichen Körper ist von W. Krull im engen Anschluß an Dedekind entwickelt [Math. Ann. **100** (1928)]. Bei geeigneter Topologisierung — die sich im abzählbaren Fall direkt aus den Dedekindschen Fundamentalfolgen ergibt — zeigt sich, daß alle und nur die abgeschlossenen Untergruppen „Identitätsgruppen" sind, und daß bei jedem unendlichen Körper (erster Art) auch Nicht-Identitätsgruppen auftreten, entsprechend dem Dedekindschen Beispiel. Auch der Zusammenhang mit den p-adischen Zahlen, der sich schon deutlich bei Dedekind zeigt, kehrt allgemein bei allen „idealzyklischen" Gruppen wieder.

Die von Dedekind selbst noch nicht betrachtete Idealtheorie der unendlichen Körper ist seither ebenfalls entwickelt: in den Grundzügen durch E. Stiemke [Math. Zeitschr. **25** (1926)], unter ausdrücklicher Berufung auf die Methoden der vorliegenden Abhandlung, und weitergehend durch W. Krull [Math. Zeitschr. 29 (1928) und **31** (1930)].

Noether.

XXXII.

Gauß in seiner Vorlesung über die Methode der kleinsten Quadrate.

[Festschrift zur Feier des hundertfünfzigjährigen Bestehens der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Beiträge zur Gelehrtengeschichte Göttingens. S. 45—59 (1901).]

Als geborener Braunschweiger habe ich schon früh von Gauß sprechen hören, und ich glaubte gern an seine Größe, ohne zu wissen, worin sie bestand. Um so tieferen Eindruck machte es auf mich, als ich zuerst von seiner geometrischen Darstellung der imaginären oder, wie man zu jener Zeit wohl noch sagte, der unmöglichen Größen hörte. Ich war damals als Student auf dem Collegium Carolinum (der heutigen Technischen Hochschule) ein wenig in die höhere Mathematik eingedrungen, und bald darauf, als Gauß im Juli 1849 sein 50jähriges Doktor-Jubiläum feierte, sandte unser Lehrkörper einen von dem geistreichen Philologen Petri verfaßten Glückwunsch an ihn, worin mir der Passus, er habe das Unmögliche möglich gemacht, ganz besonders gefiel. Zu Ostern 1850 kam ich nach Göttingen, und hier wuchs mein Verständnis schon etwas mehr, als ich im Seminar durch eine kurze, aber sehr interessante Vorlesung von Stern in die Elemente der Zahlentheorie eingeführt wurde und den Reziprozitätssatz kennen lernte. Auf meinen Wegen nach oder von der Sternwarte, wo ich eine Vorlesung des trefflichen Professors Goldschmidt über populäre Astronomie hörte, begegnete ich zuweilen Gauß und erfreute mich des Anblicks seiner stattlichen, Ehrfurcht gebietenden Erscheinung, und sehr oft sah ich ihn in größter Nähe auf seinem festen Platze im Literarischen Museum, das er regelmäßig besuchte, um Zeitungen zu lesen.

Zu Anfang des folgenden Wintersemesters hielt ich mich für reif, seine Vorlesung über die Methode der kleinsten Quadrate zu hören, und so betrat ich, mit dem Testierbuch ausgerüstet und nicht ohne

Herzklopfen, zum ersten Male sein Wohnzimmer, wo ich ihn an seinem Schreibtisch sitzend fand. Meine Meldung schien ihn wenig zu erfreuen, ich hatte auch wohl gehört, daß er sich ungern entschloß, Vorlesungen zu halten; nachdem er seinen Namen in das Buch eingetragen hatte, sagte er nach kurzem Schweigen: „Sie wissen vielleicht, daß es immer sehr zweifelhaft ist, ob meine Vorlesungen zustande kommen; wo wohnen Sie? bei dem Barbier Vogel? Nun, das trifft sich ja glücklich, denn der ist auch mein Barbier, durch ihn werde ich Sie benachrichtigen."

Einige Tage darauf trat dann Vogel, eine stadtbekannte Persönlichkeit, ganz erfüllt von der Wichtigkeit seiner Mission, bei mir ein, um zu bestellen, daß sich noch mehrere Zuhörer gemeldet hätten, und daß Herr Geh. Hofrat Gauß die Vorlesung halten würde.

Wir waren neun Studenten, von denen ich A. Ritter (später Professor der Mechanik in Hannover und Aachen) und Moritz Cantor (später Professor in Heidelberg) nach und nach näher kennen lernte; wir alle kamen sehr regelmäßig, es hat wohl selten einer von uns gefehlt, obgleich der Weg nach der Sternwarte im Winter bisweilen nicht angenehm war. Das Auditorium war durch ein Vorzimmer von Gauß' Arbeitszimmer getrennt und ziemlich klein. Wir saßen an einem Tisch, dessen Längsseiten für je drei, aber nicht für vier Personen bequemen Platz darboten. Der Tür gegenüber am oberen Ende saß Gauß in mäßiger Entfernung vom Tische, und wenn wir vollzählig waren, so mußten zwei von uns, die zuletzt kamen, ganz in seine Nähe rücken und ihr Heft auf den Schoß nehmen. Gauß trug ein leichtes schwarzes Käppchen, einen ziemlich langen braunen Gehrock, graue Beinkleider; er saß meist in bequemer Haltung, etwas gebeugt vor sich niedersehend, mit über dem Leib gefalteten Händen. Er sprach ganz frei, sehr deutlich, einfach und schlicht; wenn er aber einen neuen Gesichtspunkt hervorheben wollte, wobei er ein besonders charakteristisches Wort gebrauchte, so erhob er wohl plötzlich den Kopf, wandte sich zu einem seiner Nachbarn und blickte ihn während der nachdrücklichen Rede ernst mit seinen schönen, durchdringenden blauen Augen an. Das war unvergeßlich. Seine Sprache war fast ganz dialektfrei, nur bisweilen kamen Anklänge an unsere stadt-braunschweigische Mundart; beim Zählen z. B., wobei er auch den Gebrauch der Finger nicht verschmähte, sagte er nicht eins, zwei, drei, sondern eine, zweie, dreie usf., wie man es

noch jetzt bei uns auf dem Markte hören kann. Ging er von einer prinzipiellen Erörterung zur Entwicklung mathematischer Formeln über, so erhob er sich, und in stattlicher, ganz aufrechter Haltung schrieb er an einer neben ihm stehenden Tafel mit der ihm eigenen schönen Handschrift, wobei es ihm immer durch Sparsamkeit und zweckmäßige Anordnung gelang, mit dem ziemlich kleinen Raume auszukommen. Für die Zahlenbeispiele, auf deren sorgfältige Durchführung er besonderen Wert legte, brachte er die erforderlichen Data auf kleinen Zetteln mit.

Indem ich nun zu dem Inhalt der (wöchentlich dreistündigen) Vorlesung übergehe, beziehe ich mich auf einen Brief von Gauß an Schumacher aus dem Jahre 1844, welcher im Band VIII von Gauß' Werken (S. 147—148) abgedruckt ist; er berichtet dort, daß seine Vorlesung aus drei Teilen besteht, von denen der erste eine nur auf Prinzipien der Zweckmäßigkeit basierte Begründungsart und die eigentliche praktische Anwendung der Methode der kleinsten Quadrate gibt, während der zweite und dritte Teil die beiden wesentlich verschiedenen Begründungsarten der Methode durch die Wahrscheinlichkeitsrechnung behandelt, wie sie in der Theoria motus corporum coelestium und in der Theoria combinationis observationum dargestellt sind. Denselben Weg schlug Gauß auch zu meiner Zeit ein, und ich möchte hier einiges aus dem ersten Teile mitteilen, was, wie ich glaube, weniger bekannt ist als der Inhalt der anderen Teile; freilich kann ich es auch hierbei nicht vermeiden, sehr bekannte Dinge mit einzuflechten. Den Zweck der Methode der kleinsten Quadrate und ihre elementare Begründung stellte Gauß ungefähr so dar:

Es liegt eine Reihe von Beobachtungen (Messungen) vor, die dazu dienen sollen, gewisse unbekannte Größen $x, y, z \cdots$ zahlenmäßig zu bestimmen; die unmittelbaren Gegenstände dieser Beobachtungen können diese Unbekannten selbst, allgemeiner aber gewisse Funktionen von ihnen sein, d. h. Größen $V, V', V'' \cdots$, welche sich streng berechnen lassen würden, wenn die Werte von $x, y, z \cdots$ schon bekannt wären. Werden nun für diese Funktionen durch unmittelbare Beobachtungen die Werte $M, M', M'' \cdots$ gefunden, so erhält man ein entsprechendes System von sogenannten Beobachtungsgleichungen $V = M, V' = M', V'' = M'' \cdots$, aus denen die unbekannten Elemente $x, y, z \cdots$ ermittelt werden sollen; dies ist natürlich nur dann möglich, wenn die Anzahl der Beobachtungen mindestens ebenso

groß ist, wie die der unbekannten Elemente. Da aber alle unsere Messungen nur einen begrenzten Genauigkeitsgrad besitzen, also Fehlern unterworfen sind, so sucht man deren schädlichen Einfluß durch Vermehrung der Anzahl der Beobachtungen zu bekämpfen, und dann fragt sich, wie soll man ein solches, mit unbekannten Fehlern $M - V$, $M' - V'$, $M'' - V'' \cdots$ behaftetes, überzähliges System von Beobachtungsgleichungen $V = M$, $V' = M'$, $V'' = M'' \cdots$ behandeln, um die unvermeidlichen Widersprüche zwischen ihnen auszugleichen und so die plausibelsten Werte der unbekannten Elemente $x, y, z \cdots$ zu finden? Hierbei wird vorausgesetzt, daß diese Beobachtungen gleiche Zuverlässigkeit besitzen, d. h., daß wir keinen Grund haben, einer von ihnen größeres Zutrauen zu schenken als den übrigen. Macht man eine bestimmte Hypothese über die Werte $x, y, z \cdots$ und berechnet daraus die entsprechenden Werte der Funktionen $V, V', V'' \cdots$, so erhält man ein entsprechendes System von Fehlern $M - V$, $M' - V'$, $M'' - V'' \cdots$, aber es fragt sich, welchen Maßstab soll man zugrunde legen, um nach Beschaffenheit dieser Fehler einer solchen Hypothese den Vorzug vor einer anderen zuzuerkennen?

Hier könnte man, da die Beobachtungen wegen ihrer gleichen Zuverlässigkeit eine gleichmäßige Behandlung verdienen, zunächst an die algebraische Summe der Fehler denken, um nach ihrer Kleinheit die Brauchbarkeit einer Hypothese zu beurteilen, und dies würde geradezu dahin führen, die Hypothese für die beste zu erklären, für welche diese Summe gleich Null wird. Allein man sieht sofort, daß dies nicht als allgemeines Prinzip gelten kann, weil, sobald die Anzahl der unbekannten Elemente mindestens gleich zwei ist, unendlich viele verschiedene Hypothesen dieser Forderung genügen würden, und außerdem würde eine Hypothese, bei welcher große Fehler durch die entgegengesetzten Vorzeichen sich in der Summe aufheben, für ebenso gut gelten, als eine andere, in welcher die einzelnen Fehler absolut genommen kleiner sind.

Dies kann uns veranlassen, nur die absoluten Werte der Fehler zu betrachten und die Hypothese für die beste zu erklären, für welche deren Summe so klein wie möglich ausfällt. Allein auch gegen dieses Prinzip lassen sich mehrere triftige Einwände erheben, nämlich:

a) Es verstößt gegen den mathematischen Sinn, daß hierbei die negativen Fehler auf andere Weise in die Rechnung eintreten sollen als die positiven.

b) Die Behandlung wird bei einer größeren Anzahl unbekannter Elemente $x, y, z \cdots$ bald sehr verwickelt.

c) Selbst im einfachsten Falle, wo nur eine einzige unbekannte Größe auftritt, und diese zugleich der unmittelbare Gegenstand der sämtlichen Beobachtungen ist, führt dieses Prinzip zu Resultaten, denen wir unseren Beifall nicht schenken können. Hätte man z. B. vier Beobachtungen $x = 900$, $x = 903$, $x = 917$, $x = 921$ gemacht, so würde jeder zwischen 903 und 917 liegende Wert x für gleich brauchbar gelten müssen, weil für alle diese Werte x die Summe der absoluten Fehler denselben kleinsten Wert $(x - 900) + (x - 903) + (917 - x) + (921 - x) = 35$ erhalten würde; dieselbe Erscheinung tritt immer auf, wenn die Anzahl der Beobachtungen gerade ist, während bei einer ungeraden Anzahl immer der in der Mitte liegende Wert x für den besten gelten müßte, so daß die übrigen Beobachtungen auch hier gar keinen Einfluß auf die Bestimmung von x ausüben würden.

d) Von besonderem Gewicht ist endlich der Einwand, daß nach diesem Prinzip bei einer größeren Anzahl von Beobachtungen ein großer Fehler keinen stärkeren Einfluß auf das Resultat ausüben würde, als eine Reihe kleiner Fehler, deren absolute Werte dieselbe Summe besitzen, während doch die Hypothese, welcher die letztere Erscheinung entspricht, nach unserem Gefühl gewiß den Vorzug vor der ersteren verdient.

Aus allen diesen Gründen ist dieses Prinzip zu verwerfen, und wir müssen einen anderen Maßstab suchen, durch welchen diese Mängel beseitigt werden, zumal die Wahl dieses Maßstabes ganz unserer Willkür überlassen ist. Hierzu führt uns von selbst der letztgenannte Einwand; die Rücksicht darauf, daß ein Fehler, welcher a-mal so groß ist als ein Fehler, der a-mal vorkommt, stärker ins Gewicht fallen muß, als diese a einzelnen Fehler, veranlaßt uns, statt der Fehler selbst ihre Quadrate zu nehmen und die Brauchbarkeit einer Hypothese nach der Kleinheit der ihr entsprechenden Summe der Fehlerquadrate zu schätzen. So gewinnen wir den Grundsatz der sogenannten Methode der kleinsten Quadrate, nach welchem diejenige Hypothese über die Werte der unbekannten Größen $x, y, z \cdots$ als die beste gelten soll, für welche die Summe der Fehlerquadrate so klein wie möglich wird. Durch die Wahl dieses Maßstabes weichen wir den obigen Einwänden a) und d) aus, ebenso gestaltet sich der unter b) erwähnte Übelstand weit besser, und die

unter c) bemerkte Erscheinung wird ganz unmöglich. Wollte man, um den Einwand d) zu beseitigen, eine noch höhere Potenz der Fehler einführen, so müßte dieselbe jedenfalls eine paare sein, um dem ersten Vorwurf zu begegnen; aber dann werden die Rechnungen so außerordentlich verwickelt, daß diese Behandlung die Mühe nicht lohnen würde.

Nach dieser sehr einleuchtenden, nur auf Prinzipien der Zweckmäßigkeit beruhenden Begründung der Methode ging Gauß sofort zur Bildung der sogenannten Normalgleichungen über, die durch partielle Differentiation der Summe

$$\Omega = (V - M)^2 + (V' - M')^2 + (V'' - M'')^2 + \cdots$$

der Fehlerquadrate in bezug auf jede der unbekannten Größen x, $y, z \cdots$ gewonnen werden. Der Kürze wegen will ich hier

$$d\Omega = 2(X\,dx + Y\,dy + Z\,dz + \cdots)$$

setzen, dann gibt die Forderung des Minimums von Ω die auf x, $y, z \cdots$ bezüglichen Normalgleichungen

$$X = 0, \quad Y = 0, \quad Z = 0 \cdots,$$

die von Gauß vollständig entwickelt dargestellt wurden.

Der zunächst behandelte und wichtigste Hauptfall ist der, wo die Größen $V, V', V'' \cdots$, also auch $X, Y, Z \cdots$ lineare Funktionen von $x, y, z \cdots$ sind. Zuerst wurde natürlich der spezielle Fall vorgeführt, wo eine einzige unbekannte Größe x durch wiederholte unmittelbare Messungen bestimmt werden soll, und wo die entsprechende Normalgleichung zu der altbekannten Regel des arithmetischen Mittels führt. Ein dazugehöriges Zahlenbeispiel — Bestimmung der Polhöhe von Lauenburg aus 11 Beobachtungen — benutzte Gauß, um uns auf gewisse Rechnungsvorteile aufmerksam zu machen. Da alle beobachteten Werte natürlich dieselbe Anzahl 53 der Grade aufwiesen und erst in den Minuten zwischen 21 und 22 schwankten, so wäre es ja töricht, bei der Bildung des arithmetischen Mittels diese so weit miteinander übereinstimmenden Werte wirklich zu addieren und ihre Summe nachher durch ihre Anzahl zu dividieren; statt dessen ist es offenbar vorteilhafter, etwa $53^0\,21'$ oder $53^0\,22'$ als genäherten Wert von x anzusehen, also $x = 53^0\,21' + t''$ oder $x = 53^0\,22' + u''$ zu setzen, und nur das arithmetische Mittel dieser Korrektionen t oder u

in Sekunden zu berechnen. Das war freilich sehr einleuchtend, aber Gauß verschmähte es nicht, eine solche scheinbare Kleinigkeit hervorzuheben, weil in ihr der Keim eines allgemeinen Prinzips enthalten war, und ebenso verfuhr er in den folgenden Aufgaben mit einer oder mehreren Unbekannten; immer wurde die allgemeine Regel an bestimmten Zahlenbeispielen durchgeführt, die zu ähnlichen Bemerkungen Veranlassung gaben. Von allen diesen Aufgaben glaube ich hier die letzte (fünfte) mitteilen zu dürfen, weil sie wohl auch heute noch einiges Interesse darbietet.

Es handelt sich um die als nahezu gleich zuverlässig anzusehenden Messungen der Höhendifferenzen (in Metern) von den folgenden fünf Punkten: P (Boden der Göttinger Sternwarte), Q (Meridianzeichen der Wehnder Papiermühle), R (Fläche des Postamentes auf dem Hohenhagen), S (östlicher Abhang des Hils, eine Viertelstunde von Ammensen), T (Brocken, Marmorplatte des vormaligen, im Hause gelegenen Turms). Bedeuten diese Zeichen zugleich die Höhen der entsprechenden Punkte, so liegen folgende sieben Beobachtungen vor:

$$\begin{aligned}
Q &= P + 64{,}334 \\
R &= P + 349{,}366 \\
R &= Q + 283{,}596 \\
S &= Q + 206{,}580 \\
S &= R - 76{,}108 \\
T &= R + 648{,}427 \\
T &= S + 719{,}612
\end{aligned}$$

In diesen Gleichungen treten tatsächlich nur vier Unbekannte auf, nämlich die relativen Höhen $Q-P$, $R-P$, $S-P$, $T-P$ über Göttingen; denn absolute Höhen können natürlich hieraus nicht gefunden werden. Nun wird man sich zunächst durch geschickte Kombinationen genäherte Werte für diese Unbekannten verschaffen und hierauf

$$\begin{aligned}
Q &= P + 64{,}334 + q \\
R &= P + 348{,}648 + r \\
S &= P + 271{,}727 + s \\
T &= P + 994{,}207 + t
\end{aligned}$$

setzen, wo q, r, s, t die Korrektionen dieser Näherungswerte bedeuten. Führt man sie als neue Unbekannte ein und drückt sie in Millimetern

aus, so nehmen die obigen sieben Beobachtungsgleichungen folgende Form an:

$$\begin{aligned}
0 &= 0 + q \\
0 &= -718 + r \\
0 &= +718 - q + r \\
0 &= +813 - q + s \\
0 &= -813 - r + s \\
0 &= -2868 - r + t \\
0 &= +2868 - s + t
\end{aligned}$$

und die vier Normalgleichungen lauten:

$$\begin{aligned}
0 &= -1531 + 3q - r - s \\
0 &= +3681 - q + 4r - s - t \\
0 &= -2868 - q - r + 3s - t \\
0 &= \quad - r - s + 2t
\end{aligned}$$

Nach einigen Bemerkungen über die direkte Auflösung dieser Gleichungen durch zweckmäßige Anordnung der sukzessiven Eliminationen teilte uns Gauß eine indirekte Auflösungsmethode mit, einen Kunstgriff, durch den man sich die beschwerliche Eliminationsarbeit, wie er sagte, oft erleichtern könne. Derselbe besteht wesentlich darin, die konstanten Glieder durch fortgesetzte Substitutionen auf immer kleinere absolute Werte herabzudrücken, und dieser Prozeß beginnt in unserem Beispiel auf folgende Weise. Ignoriert man in der zweiten Gleichung, welche das größte konstante Glied (3681) enthält, die Unbekannten q, s, t neben dem Gliede $4r$, welches den größten Koeffizienten (4) hat, und vernachlässigt Bruchteile, so erhält man für r den Wert -920; man betrachtet ihn als eine Annäherung und führt eine Korrektion r' als neue Unbekannte ein, indem man $r = -920 + r'$ setzt; die unbekannten Glieder werden hierdurch nur insofern berührt, daß r' an Stelle von r tritt, während die konstanten Glieder in $-611, +1, -1948, +920$ übergehen. Indem man nach derselben Regel fortfährt, wird man in der dritten Gleichung die Unbekannten q, r', t ignorieren und $s = +649 + s'$ setzen, wodurch die konstanten Glieder in $-1260, -648, -1, +271$ übergehen. Offenbar kommt es immer nur darauf an, die neue Substitution zu notieren, wobei man die Akzente der neuen Unbekannten füglich unterdrücken darf, und die neuen Werte der konstanten Glieder zu berechnen; den ganzen

Mechanismus kann man in leicht verständlicher Weise durch eine Tabelle darstellen, deren Anfang hier folgen mag:

	r -920	s $+649$	q $+420$	r $+267$	s $+229$
-1531	-611	-1260	0	-267	-496
$+3681$	$+1$	-648	-1068	0	-229
-2868	-1948	-1	-421	-688	-1
0	$+920$	$+271$	$+221$	$+4$	-225

Hat man 73 solche Operationen gemacht, so sind die konstanten Teile so klein geworden, daß sie durch eine neue Substitution nicht mehr vermindert werden können, und es genügt dann, jede der ursprünglichen Unbekannten durch Addition ihrer sukzessiven Näherungswerte zu berechnen:

$$\begin{aligned}
q &= +420\cdots \\
r &= -920 + 267\cdots \\
s &= +649 + 229\cdots \\
t &= \cdots
\end{aligned}$$

Noch viel kürzer wird die Arbeit, wenn man mit diesem Kunstgriff einen zweiten verbindet, welcher im folgenden besteht. Man führt noch eine neue Unbekannte p ein, indem man den Anfangspunkt verlegt und q, r, s, t durch $q - p$, $r - p$, $s - p$, $t - p$ ersetzt; behandelt man die hierdurch umgeformten Beobachtungsgleichungen wieder nach der Methode der kleinsten Quadrate, so erhält man die folgenden fünf Normalgleichungen:

$$\begin{aligned}
0 &= +718 + 2p - q - r \\
0 &= -1531 - p + 3q - r - s \\
0 &= +3681 - p - q + 4r - s - t \\
0 &= -2868 \quad - q - r + 3s - t \\
0 &= \quad - r - s + 2t,
\end{aligned}$$

von denen die vier letzten in die früheren übergehen, wenn $p = 0$ gesetzt wird. Sie haben zwei merkwürdige Eigenschaften, deren Grund man leicht erkennt: erstens ist die Summe der konstanten Glieder, und

ebenso die Summe der Koeffizienten jeder einzelnen Unbekannten gleich Null, und zweitens ist auch die Summe der Koeffizienten aller Unbekannten in jeder einzelnen Gleichung gleich Null. Zufolge der ersten Eigenschaft ist jede Gleichung eine identische Folge der vier anderen, und es ist daher unmöglich, bestimmte Werte der fünf Unbekannten aus ihnen abzuleiten. Wendet man aber die oben beschriebene indirekte Auflösungsmethode an, so wird man finden, daß dieselbe jetzt viel schneller zum Abschluß kommt, und außerdem ergibt sich aus dem Umstande, daß die Summe der konstanten Glieder stets gleich Null bleiben muß, eine überaus angenehme Kontrolle der fortlaufenden Rechnung, deren Anfang wieder durch die folgende Tabelle dargestellt werden mag:

	r	s	p	q
	− 920	+ 649	− 819	+ 147
+ 718	+ 1638	+ 1638	0	− 147
− 1531	− 611	− 1260	− 441	0
+ 3681	+ 1	− 648	+ 171	+ 24
− 2868	− 1948	− 1	− 1	− 148
0	+ 920	+ 271	+ 271	+ 271

Nach etwa 20 Operationen schließt diese Rechnung ab und liefert bestimmte Werte der fünf Unbekannten, aus denen sich schließlich die eigentlichen Unbekannten $q - p$, $r - p$, $s - p$, $t - p$ ergeben. In der Vorlesung wurden natürlich nur die ersten Schritte dieses wie des früheren Prozesses wirklich ausgeführt. Über die Vorzüge und Nachteile dieser indirekten Auflösungsmethode gegenüber der gewöhnlichen durch sukzessive Elimination der Unbekannten muß ich mich jeder Bemerkung enthalten; es genügt mir, durch die Mitteilung dieses Beispiels wieder darauf hinzuweisen, wie unablässig Gauß bemüht war, auch bei dem praktischen Rechnen sinnreiche Kunstgriffe zu erfinden.

Hierauf folgte die Behandlung des Falles, wo die Beobachtungsgleichungen $V = M \cdots$ die Unbekannten nicht mehr, wie bisher, in linearer Form enthalten. Die Einführung genäherter Werte, welche früher nur als ein die Zahlenrechnungen vereinfachender Kunstgriff

auftrat, wird hier zu dem Prinzip ausgebildet, durch welches dieser Fall auf den früheren der linearen Gleichungen zurückzuführen ist, indem man die kleinen Korrektionen als neue Unbekannte behandelt und deren Produkte bei der Entwicklung nach dem Satze von Taylor vernachlässigt. Als Beispiel diente die Pothenot'sche Aufgabe in der praktischen Geometrie, speziell die Ortsbestimmung von Rosdorf bei Göttingen aus sechs Einschnitten.

Nun ging Gauß zu einer ebenfalls elementar gehaltenen Entwicklung des Begriffs der Präzision einer Beobachtungsmethode über. Wenn die vorliegenden Beobachtungen $V = M$, $V' = M' \cdots$ nicht mehr, wie bisher vorausgesetzt wurde, gleiche Zuverlässigkeit besitzen, so muß man sie als auf verschiedene Maßstäbe bezogen ansehen und jede Gleichung mit einem entsprechenden, die gleiche Zuverlässigkeit wiederherstellenden Koeffizienten k multiplizieren. Die hieraus nach der Methode der kleinsten Quadrate abgeleiteten Normalgleichungen enthalten diese (relativen) Präzisionen k nur in ihren Quadraten, und diese heißen die entsprechenden Gewichte p der Beobachtungen.

Diese Betrachtung gibt zugleich ein Mittel an die Hand, die Zuverlässigkeit der durch die Methode der kleinsten Quadrate gewonnenen Resultate im Vergleich mit der Zuverlässigkeit der gegebenen Beobachtungen zu bestimmen. Das Prinzip, auf welches sich diese Ableitung gründet, ist das der Konsequenz. Man denkt sich zu der ursprünglich vorhandenen Gruppe von Beobachtungen, die wieder als gleich zuverlässig vorausgesetzt werden, und deren Präzision $= 1$ angenommen wird, eine beliebige Anzahl anderer Beobachtungen von derselben Präzision hinzu, wodurch die zuerst gefundenen plausibelsten Werte der Unbekannten x, y, $z \cdots$ in andere Werte übergehen werden. Um diese zu finden, kann man nun zwei verschiedene Wege einschlagen, welche aber notwendig zu denselben Resultaten führen müssen. Der erste Weg besteht darin, daß man nach der Methode der kleinsten Quadrate sämtliche Beobachtungsgleichungen beider Gruppen gleichzeitig behandelt, der zweite darin, daß man die allein aus der ersten Gruppe (der wirklich gegebenen Beobachtungen) abgeleiteten Resultate mit gewissen, noch unbestimmt gelassenen Präzisions-Koeffizienten k multipliziert und hierauf mit der zweiten, hinzugedachten Gruppe von Beobachtungen kombiniert. Durch die Forderung, daß die auf diesen beiden verschiedenen Wegen er-

haltenen Schlußresultate miteinander übereinstimmen müssen, ergeben sich dann die Werte der Präzisionen k und ihrer Quadrate, der Gewichte p.

Diese allgemeine Anleitung zur Gewichtsbestimmung der durch die Methode der kleinsten Quadrate gewonnenen Resultate wurde zunächst an den einfachsten Fällen durchgeführt, wo die (immer als linear vorausgesetzten) Beobachtungsgleichungen nur eine Unbekannte enthalten. Um aber für eine beliebige Anzahl n von Unbekannten $x, y \cdots$, deren letzte z sein möge, die Regel allgemein auszudrücken (wobei die uns damals noch wenig geläufige Sprache der Determinanten-Theorie gänzlich vermieden wurde), beschrieb Gauß zunächst ein Verfahren zur Auflösung der auf $x, y \cdots z$ bezüglichen Normalgleichungen $X = 0$, $Y = 0 \cdots Z = 0$, welches er mit dem Namen der rechten Elimination belegte (vgl. Disquisitiones circa elementa elliptica Palladis). Man eliminiere die erste Unbekannte x aus allen n Gleichungen, indem man nur die erste, auf x bezügliche Normalgleichung $X = 0$ mit geeigneten Koeffizienten multipliziert und von den folgenden, unveränderten Normalgleichungen abzieht, welche dadurch in $Y' = 0 \cdots Z' = 0$ übergehen und frei von x sind; nun eliminiere man ebenso die zweite Unbekannte y aus allen diesen $(n-1)$ Gleichungen, indem man nur die erste Gleichung $Y' = 0$ mit geeigneten Koeffizienten multipliziert und von allen folgenden abzieht; fährt man so fort, so gelangt man schließlich zu einer Gleichung von der Form $H(z - C) = 0$, in welcher nur noch die letzte Unbekannte z auftritt, und wo H, C bekannte Werte bedeuten, die sich aus dem Verlauf dieser rechten Elimination mit Bestimmtheit ergeben. Die Auflösung der Normalgleichungen liefert also für z den plausibelsten Wert C, und die Regel von Gauß besteht darin, daß der Koeffizient H zugleich das Gewicht dieses Resultats $z = C$ darstellt, d. h. also: In der Methode der kleinsten Quadrate wird das Gewicht jedes einzelnen Resultats für eine Unbekannte durch den Koeffizienten dargestellt, welchen diese Unbekannte bei rechter Elimination in der letzten Gleichung erhält.

Bei dem Beweise dieses Satzes, den ich hier des Raumes wegen mit einer kleinen Änderung der Bezeichnung wiedergebe, beschränkte sich Gauß auf den Fall von drei Unbekannten x, y, z. Durch die rechte Elimination von x, y werden offenbar zwei Koeffizienten α, β gewonnen, welche bewirken, daß identisch

$$\alpha X + \beta Y + Z = H(z - C)$$

wird. Denkt man sich nun zu den wirklich vorhandenen m Beobachtungsgleichungen, denen die Normalgleichungen $X = 0$, $Y = 0$, $Z = 0$ mit dem Resultat $z = C$ entsprechen, noch eine Beobachtung $z = D$ von derselben Präzision hinzu und schlägt den oben beschriebenen ersten Weg ein, bei welchem alle $(m + 1)$ Beobachtungen gleichzeitig behandelt werden, so bleiben offenbar die auf x, y bezüglichen Normalgleichungen $X = 0$, $Y = 0$ ungeändert bestehen, während die dritte $Z = 0$ in $Z + (z - D) = 0$ übergeht; zufolge der obigen Identität ergibt sich daher z jetzt aus der Gleichung

$$H(z - C) + (z - D) = 0.$$

Schlägt man aber den zweiten Weg ein, indem man das aus den m wirklich vorhandenen Beobachtungen durch die Methode der kleinsten Quadrate gewonnene Resultat $z = C$ mit einer noch unbestimmten Präzision k multipliziert und nun nach derselben Methode mit der hinzugedachten Beobachtung $z = D$ kombiniert, so erhält man, wenn das unbekannte Gewicht $kk = p$ gesetzt wird, die einzige Normalgleichung

$$p(z - C) + (z - D) = 0,$$

und durch den Vergleich mit dem Resultate des ersten Weges folgt $p = H$, w. z. b. w.

In nahem Zusammenhang mit der eben beschriebenen rechten Elimination steht die sukzessive identische Umformung der Summe Ω der Fehlerquadrate in eine Reihe von Quadraten linearer Funktionen $A, B, C \cdots$, die so gewählt werden, daß x nur in A, y nur in A und B, z nur in A, B, C usf. auftritt. Der zuletzt verbleibende konstante Bestandteil stellt dann das Minimum von Ω dar, und die plausibelsten Werte der Unbekannten $x, y, z \cdots$ ergeben sich aus den Gleichungen $A = 0$, $B = 0$, $C = 0 \cdots$ in umgekehrter Folge.

Mit dieser Darstellung schloß Gauß am 24. Januar 1851 den ersten Teil seiner Vorlesung, durch den er uns mit dem Wesen der Methode der kleinsten Quadrate vollkommen vertraut gemacht hatte. Es folgte nun eine überaus klare und durch originelle Beispiele erläuterte Entwicklung der Grundbegriffe und der Hauptsätze der Wahrscheinlichkeitsrechnung, die als Einleitung zu der zweiten und dritten Begründungsart der Methode diente, worauf ich hier nicht mehr eingehen darf. Ich kann nur sagen, daß wir diesem ausgezeichneten Vortrage, in welchem auch einige Beispiele aus der Theorie der be-

stimmten Integrale behandelt wurden, mit immer steigendem Interesse gefolgt sind. Aber es schien uns auch, als ob Gauß selbst, der vorher wenig Neigung gezeigt hatte, die Vorlesung zu halten, im Laufe derselben doch einige Freude an seiner Lehrtätigkeit empfand. So kam es am 13. März zum Schluß, Gauß erhob sich, wir alle mit ihm, und er entließ uns mit den freundlichen Abschiedsworten: „Es bleibt mir nur noch übrig, Ihnen zu danken für die große Regelmäßigkeit und Aufmerksamkeit, mit der Sie meinem, doch wohl recht trocken zu nennenden Vortrage gefolgt sind.“ Seitdem ist nun ein halbes Jahrhundert verflossen, aber dieser angeblich trockene Vortrag steht mir unvergeßlich in der Erinnerung als einer der schönsten, die ich je gehört habe.

XXXIII.

Über binäre trilineare Formen und die Komposition der binären quadratischen Formen.

[Journal für reine und angewandte Mathematik, Bd. 129, S. 1—34 (1905).]

Bei der Besprechung der in lineare Faktoren zerlegbaren Formen, welche zu einem endlichen algebraischen Zahlkörper gehören, habe ich bemerkt, daß die drei Formen, deren eine durch eine bilineare Substitution in das Produkt der beiden anderen übergeht, im wesentlichen, d. h. abgesehen von konstanten Faktoren, umgekehrt durch diese Substitution bestimmt sind*). In dem einfachsten Falle der binären quadratischen Formen ist diese Tatsache zwar nicht ausdrücklich von Gauß ausgesprochen, aber sie ist vollständig in der Schlußbemerkung des Art. 235 der Disquisitiones Arithmeticae enthalten, in welchem die Transformation einer Form in ein Produkt aus zwei Formen durch eine bilineare Substitution in der allgemeinsten Weise behandelt wird. Bei meinem ersten Studium dieser Untersuchung erregte die genannte Tatsache meine besondere Aufmerksamkeit, und ich erkannte bald, daß mit einer solchen gegebenen Substitution immer zwei andere Substitutionen und drei quadratische Formen von der Art verbunden sind, daß jede der drei Formen durch eine ihr entsprechende Substitution in das Produkt der beiden anderen Formen übergeht. Hat man sich hiervon überzeugt, was bei zweckmäßiger Wahl der Bezeichnung keine Schwierigkeit darbietet, so wird die Lösung des allgemeinen von Gauß behandelten Problems in hohem Grade vereinfacht. Da dies noch nicht bekannt zu sein scheint, so wage ich es, meine Untersuchung zu veröffentlichen und dem Andenken an meinen großen Lehrer Dirichlet zu widmen, der selbst eine Ehre darein gesetzt hat, durch eine Reihe von Abhandlungen das Verständnis des von ihm am höchsten bewunderten Werkes von Gauß zu erleichtern.

*) Dirichlets Vorlesungen über Zahlentheorie, vierte Auflage, § 182, S. 586.

§ 1.

Wir betrachten im folgenden drei Paare von unabhängigen Variabeln

$$(x_1, y_1), (x_2, y_2), (x_3, y_3)$$

und zwei Reihen von je vier willkürlichen Konstanten

$$\alpha = \alpha_0, \alpha_1, \alpha_2, \alpha_3,$$
$$\beta = \beta_0, \beta_1, \beta_2, \beta_3.$$

Bedeutet r, s, t, wie immer im folgenden, irgend eine Permutation der drei Indizes 1, 2, 3 (während der Index 0 ungeändert bleibt), so dürfen wir jeden aus den Variabeln und Konstanten gebildeten Ausdruck, der in bezug auf die beiden Indizes s, t symmetrisch ist, als eine durch den Index r bestimmte Größe ansehen und demgemäß bezeichnen. In diesem Sinne bilden wir drei binäre quadratische Formen F_1, F_2, F_3 durch die gemeinsame Definition

$$(1)\quad \begin{cases} F_r = F_r(x_r, y_r) = A_r x_r^2 + B_r x_r y_r + C_r y_r^2 \\ = (\beta_s x_r + \alpha_t y_r)(\beta_t x_r + \alpha_s y_r) - (\alpha_r x_r + \beta_0 y_r)(\alpha_0 x_r + \beta_r y_r), \end{cases}$$

wo also

$$(2)\quad \begin{cases} A_r = \beta_s\beta_t - \alpha_0\alpha_r, \quad C_r = \alpha_s\alpha_t - \beta_0\beta_r, \\ B_r = \alpha_s\beta_s + \alpha_t\beta_t - \alpha_r\beta_r - \alpha_0\beta_0. \end{cases}$$

Wir wollen beweisen, daß diese drei Formen ein und dieselbe Diskriminante

$$(3)\qquad D = B_1^2 - 4A_1C_1 = B_2^2 - 4A_2C_2 = B_3^2 - 4A_3C_3$$

haben, und daß jede von ihnen durch eine entsprechende bilineare Substitution in das Produkt der beiden anderen Formen übergeht.

Das erstere folgt leicht aus einem bekannten Satz über partiale Determinanten. Bildet man aus zwei Reihen von je vier Größen

$$p, p', p'', p'''$$
$$q, q', q'', q'''$$

die sechs Determinanten

$$(4)\quad \begin{cases} P = pq' - qp', \quad Q = pq'' - qp'', \quad R = pq''' - qp''', \\ U = p''q''' - q''p''', \quad T = p'q''' - q'p''', \quad S = p'q'' - q'p'', \end{cases}$$

so genügen die drei letzteren den beiden Gleichungen

$$Up' - Tp'' + Sp''' = 0, \quad Uq' - Tq'' + Sq''' = 0;$$

multipliziert man die erste mit $-q$, die zweite mit p und addiert, so erhält man den in Rede stehenden Satz

$$(5)\qquad PU - QT + RS = 0.$$

Wenden wir ihn auf das Beispiel

$$(6)\quad \begin{cases} p = \beta_r, \quad p' = \alpha_s, \quad p'' = \alpha_t, \quad p''' = \beta_0, \\ q = -\alpha_0, \quad q' = -\beta_t, \quad q'' = -\beta_s, \quad q''' = -\alpha_r \end{cases}$$

an, so wird zufolge (2):

$$(7)\quad \begin{cases} P = -A_s, \quad Q = -A_t, \quad R = -\frac{1}{2}(B_t + B_s), \\ U = -C_s, \quad T = -C_t, \quad S = -\frac{1}{2}(B_t - B_s), \end{cases}$$

also

$$A_sC_s - A_tC_t + \tfrac{1}{4}(B_t + B_s)(B_t - B_s) = 0$$

oder

$$B_s^2 - 4A_sC_s = B_t^2 - 4A_tC_t,$$

womit unsere Behauptung über die Diskriminanten der drei Formen bewiesen ist. Wir bemerken zugleich, daß diese gemeinsame Diskriminante D, die eine homogene Funktion vierten Grades von den acht Konstanten α, β ist, nicht identisch verschwindet; denn wenn man z. B. $\alpha_0 = \beta_0 = 0$, alle anderen sechs Konstanten α, $\beta = 1$ setzt, so werden alle neun Koeffizienten A_r, B_r, C_r gleich 1, also $D = -3$.

Um auch die zweite Behauptung zu beweisen, setzen wir zur Abkürzung

$$(8)\qquad \frac{\partial F_r}{\partial x_r} = 2A_rx_r + B_ry_r = 2u_r, \quad \frac{\partial F_r}{\partial y_r} = B_rx_r + 2C_ry_r = 2v_r,$$

woraus

$$(9)\qquad u_rx_r + v_ry_r = F_r$$

folgt, und nehmen die Konstanten (6) zu Koeffizienten der beiden bilinearen, in bezug auf s, t symmetrischen Funktionen

$$(10)\quad \begin{cases} X_r = \beta_rx_sx_t + \alpha_sx_sy_t + \alpha_ty_sx_t + \beta_0y_sy_t, \\ Y_r = -\alpha_0x_sx_t - \beta_tx_sy_t - \beta_sy_sx_t - \alpha_ry_sy_t. \end{cases}$$

Eliminiert man der Reihe nach jedes der vier Produkte $x_s x_t$, $x_s y_t$, $y_s x_t$, $y_s y_t$, so erhält man mit Rücksicht auf (4), (7), (8) die Gleichungen

$$\begin{aligned}
&\alpha_0 X_r + \beta_r Y_r \\
&= -A_s x_s y_t - A_t y_s x_t - \frac{1}{2}(B_t + B_s) y_s y_t = -y_s u_t - u_s y_t, \\
&\beta_t X_r + \alpha_s Y_r \\
&= \quad A_s x_s x_t - \frac{1}{2}(B_t - B_s) y_s x_t - C_t y_s y_t = -y_s v_t + u_s x_t, \\
&\beta_s X_r + \alpha_t Y_r \\
&= \quad A_t x_s x_t + \frac{1}{2}(B_t - B_s) x_s y_t - C_s y_s y_t = \quad x_s u_t - v_s y_t, \\
&\alpha_r X_r + \beta_0 Y_r \\
&= \frac{1}{2}(B_t + B_s) x_s x_t + C_t x_s y_t + \quad C_s y_s x_t = \quad x_s v_t + v_s x_t,
\end{aligned}$$

die man mit Benutzung der bekannten Bezeichnung für die Multiplikation von zwei binären Substitutionen auch in der Form

$$\begin{pmatrix} \beta_s X_r + \alpha_t Y_r, & \alpha_r X_r + \beta_0 Y_r \\ \alpha_0 X_r + \beta_r Y_r, & \beta_t X_r + \alpha_s Y_r \end{pmatrix} = \begin{pmatrix} x_s, & v_s \\ -y_s, & u_s \end{pmatrix} \begin{pmatrix} u_t, & v_t \\ -y_t, & x_t \end{pmatrix}$$

darstellen kann, und da bekanntlich die Determinante des Produkts von zwei Substitutionen das Produkt aus deren Determinanten ist, so ergibt sich aus der Definition (1) der Formen $F_r = F_r(x_r, y_r)$ und aus (9) das Resultat

$$F_r(X_r, Y_r) = F_s F_t, \tag{11}$$

womit auch unsere zweite Behauptung bewiesen ist.

Man erkennt übrigens leicht, daß dieser zweite Satz (11) den ersten (3) über die Diskriminanten in sich schließt. Sieht man nämlich x_s, y_s als Konstanten an, so nimmt die obige bilineare Substitution (10) die Form einer einfachen binären Substitution

$$\begin{aligned}
X_r &= \quad (\beta_r x_s + \alpha_t y_s) x_t + (\alpha_s x_s + \beta_0 y_s) y_t, \\
Y_r &= -(\alpha_0 x_s + \beta_s y_s) x_t - (\beta_t x_s + \alpha_r y_s) y_t
\end{aligned}$$

an, deren Determinante zufolge (1) gleich $-F_s$ ist, und durch diese Substitution geht die Form

$$F_r(X_r, Y_r) = A_r X_r^2 + B_r X_r Y_r + C_r Y_r^2$$

nach dem Satz (11) in die Form

$$F_s F_t(x_t, y_t) = F_s A_t x_t^2 + F_s B_t x_t y_t + F_s C_t y_t^2$$

über. Nach dem bekannten Fundamentalsatz über die Transformation einer binären quadratischen Form durch eine einfache lineare Substitution ist aber die Diskriminante der neuen Form gleich der der alten, multipliziert mit dem Quadrat der Substitutionsdeterminante. Bezeichnet man nun mit D_1, D_2, D_3 die Diskriminanten der Formen F_1, F_2, F_3, so ist in unserem Falle die Diskriminante der neuen Form

$$(F_s B_t)^2 - 4(F_s A_t)(F_s C_t) = D_t F_s^2,$$

und da D_r die Diskriminante der alten Form, und $-F_s$ die Substitutionsdeterminante ist, so folgt $D_t F_s^2 = D_r(-F_s)^2$, also $D_t = D_r$, was zu beweisen war.

Die acht Konstanten α, β bilden daher immer die Koeffizienten von drei verwandten binären bilinearen Substitutionen, deren Zusammenhang wesentlich in der Identität

$$y_1 X_1 - x_1 Y_1 = y_2 X_2 - x_2 Y_2 = y_3 X_3 - x_3 Y_3 \tag{12}$$

besteht, und erzeugen zugleich drei quadratische Formen, deren jede durch eine dieser Substitutionen in das Produkt der beiden anderen übergeht.

Indem wir uns vorbehalten, auf diese Identität später (in § 4) zurückzukommen, beschließen wir diese Betrachtungen mit einer Bemerkung, die sich auf den Fall bezieht, wo die bisher willkürlichen acht Konstanten α, β ganze rationale Zahlen sind. Dann sind auch die Koeffizienten der drei Formen F_1, F_2, F_3 und deren Diskriminante D ganze Zahlen; wir wollen annehmen, daß keine dieser Formen identisch verschwindet, und wollen mit M_r den Teiler der Form F_r, d. h. den positiven größten gemeinsamen Teiler ihrer Koeffizienten A_r, B_r, C_r bezeichnen. Bedeutet ferner K_r den größten gemeinsamen Teiler von M_s, M_t, also auch den der sechs Koeffizienten A_s, B_s, C_s, A_t, B_t, C_t, so folgt aus (3) auch $B_s \equiv B_t \pmod{2K_r}$, mithin ist K_r auch gemeinsamer Teiler der sechs partialen Determinanten (7), und zwar der größte, weil umgekehrt jeder gemeinsame Teiler dieser Determinanten offenbar auch in B_s, B_t, also in M_s, M_t, K_r aufgeht.

Entwickelt man nun beide Seiten der in bezug auf die vier Variabeln x_s, y_s, x_t, y_t identischen Gleichung (11) durch Auflösung aller die Variabeln einschließenden Klammern, so leuchtet ein, daß alle Koeffizienten der linken Seite durch M_r teilbar sind, während offenbar das Produkt $M_s M_t$ der größte gemeinsame Teiler der neun

Koeffizienten der rechten Seite ist; mithin ist $M_s M_t$ teilbar durch M_r, also

(13) $M_2 M_3 = M_1 N_1, \quad M_3 M_1 = M_2 N_2, \quad M_1 M_2 = M_3 N_3,$

wo N_1, N_2, N_3 ebenfalls natürliche Zahlen bedeuten; dann ist zugleich

(14) $M_1^2 = N_2 N_3, \quad M_2^2 = N_3 N_1, \quad M_3^2 = N_1 N_2,$

und wenn z. B. M_2, M_3 relative Primzahlen sind, also $K_1 = 1$, so folgt

(15) $M_1 = M_2 M_3, \quad N_1 = 1, \quad N_2 = M_3^2, \quad N_3 = M_2^2.$

§ 2.

Nach dieser Vorbereitung wenden wir uns zu der Aufgabe, welche Gauß im Art. 235 der Disquisitiones Arithmeticae behandelt hat. Ich will aber vorher bemerken, daß ich hier wie schon früher*) statt der von Gauß zugrunde gelegten Formen $ax^2 + 2bxy + cy^2$, deren zweiter Koeffizient den Faktor 2 enthält, immer Formen $f(x, y) = ax^2 + bxy + cy^2$ betrachte, wo a, b, c beliebige Konstanten bedeuten, die nur der Beschränkung unterliegen sollen, daß die aus ihnen gebildete Diskriminante $\partial = b^2 - 4ac$ der Form $f = f(x, y)$ von Null verschieden ist.

Sind nun $f_1 = f_1(x_1, y_1)$, $f_2 = f_2(x_2, y_2)$, $f_3 = f_3(x_3, y_3)$ drei solche Formen mit den Diskriminanten ∂_1, ∂_2, ∂_3, so besteht die Untersuchung darin, alle Folgerungen aus der Annahme zu ziehen, daß die erste Form f_1 durch eine bilineare Substitution in das Produkt $f_2 f_3$ der beiden anderen Formen übergeht; bezeichnet man daher mit X_1, Y_1 zwei bilineare Funktionen der beiden Paare (x_2, y_2), (x_3, y_3), so wird diese Annahme durch die Identität

$$f_1(X_1, Y_1) = f_2 f_3$$

ausgedrückt; um aber die Symmetrie so viel wie möglich zu bewahren, fügen wir dem Produkt noch einen von Null verschiedenen konstanten Faktor k_1 hinzu und setzen also

(16) $$f_1(X_1, Y_1) = k_1 f_2 f_3.$$

Aus den acht Koeffizienten α, β der bilinearen Funktionen, die wir (gemäß (10) in § 1) in die Form

(17) $$\begin{cases} X_1 = \beta_1 x_2 x_3 + \alpha_2 x_2 y_3 + \alpha_3 y_2 x_3 + \beta_0 y_2 y_3, \\ Y_1 = -\alpha_0 x_2 x_3 - \beta_3 x_2 y_3 - \beta_2 y_2 x_3 - \alpha_1 y_2 y_3 \end{cases}$$

*) Zuerst in §§ 169, 170 der zweiten Auflage (1871) von Dirichlets Vorlesungen über Zahlentheorie.

setzen, bilden wir nach § 1 die drei Formen F_1, F_2, F_3; dann besteht das Endresultat der Untersuchung wesentlich darin, daß diese Formen sich beziehungsweise von den Formen f_1, f_2, f_3 nur um konstante, von Null verschiedene Faktoren n_1, n_2, n_3 unterscheiden, daß also identisch

(18) $$F_1 = n_1 f_1, \quad F_2 = n_2 f_2, \quad F_3 = n_3 f_3$$

ist.

Um dies in aller Kürze zu beweisen, verfahre man ebenso wie bei dem zweiten Beweise des Diskriminantensatzes (3) in § 1. Sieht man in den Gleichungen (17) erst x_2, y_2, dann x_3, y_3 als Konstanten an, so nehmen sie die Gestalt von einfachen linearen Substitutionen an, deren Determinanten bzw. $-F_2$, $-F_3$ sind, und der Fundamentalsatz über solche Transformationen einer Form f_1 ergibt zufolge der Annahme (16) die beiden Gleichungen

$$\partial_1(-F_2)^2 = \partial_3(k_1 f_2)^2, \quad \partial_1(-F_3)^2 = \partial_2(k_1 f_3)^2,$$

und da k_1, ∂_1, ∂_2, ∂_3 nach unserer Annahme von Null verschieden sind, so folgen hieraus die beiden letzten Gleichungen (18), wo n_2, n_3 von Null verschiedene Konstanten bedeuten. Multipliziert man diese beiden Gleichungen miteinander, so geht die Annahme (16) mit Rücksicht auf den Satz (11) in § 1 in die Gleichung

$$k_1 F_1(X_1, Y_1) = n_2 n_3 f_1(X_1, Y_1)$$

über, welche identisch in bezug auf die vier Variabeln x_2, y_2, x_3, y_3 bestehen muß. Da nun ∂_2 nicht Null ist, also auch die Form f_2 nicht identisch verschwindet, so gilt dasselbe auch von der Form $F_2 = n_2 f_2$; man kann daher den Variabeln x_2, y_2 in (17) solche Werte beilegen, daß F_2 einen von Null verschiedenen Wert erhält, und folglich kann man hierauf x_3, y_3 immer so wählen, daß X_1, Y_1 beliebig vorgeschriebene Werte x_1, y_1 annehmen; man darf daher in der vorstehenden Gleichung X_1, Y_1 durch die unabhängigen Variabeln x_1, y_1 ersetzen, und folglich gilt auch die erste der Identitäten (18), was zu beweisen war.

Umgekehrt, wenn zwischen drei Formen f_1, f_2, f_3 und den in § 1 definierten Formen F_1, F_2, F_3 die drei Identitäten (18) bestehen, wo n_1, n_2, n_3 von Null verschiedene Konstanten bedeuten, so folgen aus dem Satze (11) in § 1 die drei Identitäten

(19) $$f_r(X_r, Y_r) = k_r f_s f_t,$$

wo

$$k_r = \frac{n_s n_t}{n_r}, \tag{20}$$

d. h. jede der drei Formen f_1, f_2, f_3 geht durch eine bilineare Substitution in das mit einer Konstanten multiplizierte Produkt der beiden anderen Formen über.

Die drei Gleichungen (18), aus denen unmittelbar die Relationen

$$D = \partial_1 n_1^2 = \partial_2 n_2^2 = \partial_3 n_3^2 \tag{21}$$

zwischen den Diskriminanten der sechs Formen F_r, f_r folgen, schließen diejenigen neun Gleichungen in sich, welche Gauß in der Schlußbemerkung des Art. 235 mit Ω bezeichnet, und die als Grundlage für die in den Artikeln 236—241 folgenden Untersuchungen dienen. Die Gleichungen (18), bei deren Ableitung wir gar keine Voraussetzung über die besondere Natur der Koeffizienten der Formen f_1, f_2, f_3 und der bilinearen Funktionen X_1, Y_1 gemacht haben, enthalten den algebraischen Teil der Untersuchung; wir wollen jetzt annehmen, alle diese Koeffizienten seien ganze rationale Zahlen, und wollen die zahlentheoretischen Folgerungen aus der Annahme (16) ziehen, die bei Gauß schon im Laufe seiner Untersuchung auftreten.

Aus (18) folgt zunächst, daß n_1, n_2, n_3 ganze oder gebrochene rationale Zahlen sind, mithin haben zufolge (21) die Diskriminanten D, ∂_1, ∂_2, ∂_3 dasselbe Vorzeichen, und sie verhalten sich wie Quadrate von ganzen Zahlen (Conclusio prima bei Gauß). Bezeichnen wir ferner mit m_r den Teiler der Form f_r und (wie in § 1) mit M_r den der Form F_r, so ist zufolge (18)

$$M_1 = \varepsilon_1 m_1 n_1, \quad M_2 = \varepsilon_2 m_2 n_2, \quad M_3 = \varepsilon_3 m_3 n_3, \tag{22}$$

wo

$$\varepsilon_1^2 = \varepsilon_2^2 = \varepsilon_3^2 = 1, \tag{23}$$

also $\varepsilon_1 n_1$, $\varepsilon_2 n_2$, $\varepsilon_3 n_3$ positiv sind.

Jetzt kehren wir, indem wir die Symmetrie aufgeben, zu der eigentlichen Annahme von Gauß zurück, daß nämlich f_1 durch die bilineare Substitution (17) in das Produkt $f_2 f_3$ selbst übergeht, daß also

$$f_1(X_1, Y_1) = f_2 f_3, \tag{24}$$

mithin

$$k_1 = 1, \quad n_1 = n_2 n_3, \quad \varepsilon_1 = \varepsilon_2 \varepsilon_3 \tag{25}$$

ist, woraus nach (21), (22) auch

$$\partial_2 = \partial_1 n_3^2, \quad \partial_3 = \partial_1 n_2^2, \tag{26}$$

$$\partial_2 m_3^2 = \partial_1 M_3^2, \quad \partial_3 m_2^2 = \partial_1 M_2^2 \tag{27}$$

folgt. Bedeutet daher K_1 wieder den größten gemeinsamen Teiler von M_2, M_3 (wie in § 1), so ist $\partial_1 K_1^2$ der größte gemeinsame Teiler der beiden Produkte $\partial_2 m_3^2$, $\partial_3 m_2^2$ (Conclusio secunda et quarta bei Gauß).

Nach der Definition von Gauß heißt nun die Form f_1 zusammengesetzt (composita) aus den beiden Formen f_2, f_3, wenn $K_1 = 1$ ist, also M_2, M_3 relative Primzahlen sind. Beschränken wir uns jetzt auf diesen Fall, so folgt aus (27), daß die Diskriminante ∂_1 der aus f_2, f_3 zusammengesetzten Form f_1 der größte gemeinsame Teiler von $\partial_2 m_3^2$, $\partial_3 m_2^2$ ist. Da ferner nach (15) in § 1 aus der jetzigen Annahme auch $M_1 = M_2 M_3$ folgt, so ergibt sich aus (22), (25) auch $m_1 = m_2 m_3$, d. h. der Teiler m_1 der zusammengesetzten Form f_1 ist das Produkt aus den Teilern m_2, m_3 der Formen f_2, f_3 (Conclusio quinta bei Gauß).

Hiermit ist der wesentliche Inhalt des Art. 235 der Disquisitiones Arithmeticae erschöpft. Die daselbst zum Ziele führenden Rechnungen, die zum großen Teil nur angedeutet sind, und deren wirkliche Ausführung dem Leser überlassen ist, glaube ich in der hier vorliegenden Darstellung erheblich vereinfacht zu haben. Da diese Vereinfachung hauptsächlich auf der in § 1 vorausgeschickten Einführung der mit einer jeden bilinearen Substitution verbundenen drei Formen F_1, F_2, F_3 und auf deren symmetrischer Behandlung beruht, welche mit geringer Rechnung zu dem Hauptsatz (11) führt, so war es eben wegen dieser Symmetrie nicht möglich, die Bezeichnungen von Gauß beizubehalten. Zur Erleichterung einer Vergleichung bemerke ich folgendes. Gauß untersucht die Transformation einer Form F in das Produkt von zwei Formen f, f', deren Variable entsprechend bezeichnet sind, durch die bilineare Substitution

$$X = pxx' + p'xy' + p''yx' + p'''yy',$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

und gebraucht die Zeichen P, Q, R, S, T, U in derselben Bedeutung wie in Gleichung (4). Um daher von dieser Bezeichnung zu der meinigen in (24) überzugehen, hat man F, f, f' bzw. durch f_1, f_2, f_3

zu ersetzen, und die vorstehende bilineare Substitution geht in (17) über, wenn die Koeffizienten p, $p' \cdots q'''$ wie in (6) ausgedrückt werden, wobei die Indizes r, s, t bzw. durch 1, 2, 3 zu ersetzen sind. Beachtet man nun die Vorzeichen der hieraus entspringenden Ausdrücke (7), so erkennt man, daß man die in den neun Schlußgleichungen Ω bei Gauß auftretenden beiden Zahlen n, n' bzw. durch $-n_3$, $-n_2$ zu ersetzen hat, um diese Gleichungen Ω in Übereinstimmung mit unseren Gleichungen (18) zu bringen, in denen zufolge (25) $n_1 = n_2 n_3$ ist. Dies ist deshalb erwähnenswert, weil Gauß auf die Vorzeichen der Zahlen n, n' eine wichtige Unterscheidung hinsichtlich der Art gründet, wie die Formen f, f' in die Transformation oder Komposition $F = ff'$ eintreten, worauf wir hier aber nicht näher eingehen können.

§ 3.

Der Satz (11) in § 1, auf welchem alles andere beruht, ist dort wohl auf dem kürzesten Wege hergeleitet, nämlich durch unmittelbare Rechnung mit den acht Konstanten α, β, aus denen die Koeffizienten der sechs bilinearen Funktionen (10) und die der drei quadratischen Formen (1) gebildet sind. Man kann aber zu demselben Resultat und zu einem tieferen Einblick in den Gegenstand der Untersuchung auf einem ganz anderen Wege gelangen, wobei diese Konstanten α, β gar nicht explizite in die Rechnung eintreten, sondern die in (12) angeführte binäre trilineare Form als alleiniger Ausgangspunkt der Untersuchung dient. Der Weg, den ich hierbei einschlage, beruht auf der freiesten Ausnutzung der totalen Differentiation in der Auffassung, wie ich sie mir seit vielen Jahren gebildet und gelegentlich auch befreundeten Mathematikern mitgeteilt habe*). Da dieselbe nicht nur in der reinen Analysis, sondern auch in der Geometrie, Mechanik, in der mathematischen Physik nützlich verwendet werden kann und noch nicht so allgemein bekannt zu sein scheint, wie sie es wohl verdient, so will ich wenigstens das, was für unseren Zweck erforderlich ist, zunächst besprechen.

*) Vgl. § 159 der zweiten Auflage (1871) von Dirichlets Vorlesungen über Zahlentheorie und meinen Aufsatz: Zur Theorie der aus n Haupteinheiten gebildeten komplexen Größen (Göttinger Nachrichten 1885), wo von dieser Auffassung Gebrauch gemacht ist.

Ich betrachte einen analytischen Raum, in welchem jeder Punkt durch die Werte von n unabhängigen Variabeln (Koordinaten) x_1, $x_2, \cdots, x_n$ bestimmt ist, und bezeichne mit Φ den Inbegriff aller derjenigen Funktionen φ dieser Variabeln, welche partielle Derivierte von beliebig hoher Ordnung besitzen und zugleich der Bedingung

$$\frac{\partial}{\partial x_r}\left(\frac{\partial \varphi}{\partial x_s}\right) = \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) \tag{28}$$

genügen. Dann soll das Zeichen d eine Operation bedeuten, welche aus jeder solchen Funktion φ eine entsprechende, ebenfalls in Φ enthaltene Funktion $d\varphi$ in der Weise erzeugt, daß das bekannte Grundgesetz der totalen Differentiation erfüllt wird, d. h. jede zwischen m solchen Funktionen $\varphi_1, \varphi_2, \cdots, \varphi_m$ bestehende Identität

$$F(\varphi_1, \varphi_2, \cdots, \varphi_m) = 0 \tag{29}$$

soll die Identität

$$\frac{\partial F}{\partial \varphi_1} d\varphi_1 + \frac{\partial F}{\partial \varphi_2} d\varphi_2 + \cdots + \frac{\partial F}{\partial \varphi_m} d\varphi_m = 0 \tag{30}$$

zur Folge haben.

Daß solche Operationen d überhaupt möglich sind, geht aus der gewöhnlichen Auffassung der Differentiale als unendlich kleiner Änderungen der Variablen hervor; wir müssen aber jetzt feststellen, in welchem Umfange solche Operationen d in der obigen allgemeinsten Auffassung existieren, und wodurch sie vollständig bestimmt werden. Die letztere Frage läßt sich sofort beantworten; denn wenn φ irgend eine in dem System Φ enthaltene Funktion ist, so besteht zwischen ihr und den n unabhängigen Variablen $x_1, x_2, \cdots, x_n$ eine Identität, die wir in der Form

$$\varphi = f(x_1, x_2, \cdots, x_n) \tag{31}$$

darstellen dürfen, und hieraus soll nach der obigen Definition der Operation d die Identität

$$d\varphi = \frac{\partial \varphi}{\partial x_1} dx_1 + \frac{\partial \varphi}{\partial x_2} dx_2 + \cdots + \frac{\partial \varphi}{\partial x_n} dx_n = \sum^{r} \frac{\partial \varphi}{\partial x_r} dx_r \tag{32}$$

folgen; mithin ist die Operation d vollständig bestimmt, sobald in jedem Punkte unseres Raumes die Werte der n Funktionen

$$dx_1, dx_2, \cdots, dx_n \tag{33}$$

gegeben sind. Umgekehrt, hat man diese n Funktionen willkürlich aus Φ gewählt, und bildet man daraus nach (32) für jede Funk-

tion φ eine zugehörige Funktion $d\varphi$ (welche für $\varphi = x_r$ offenbar mit der gewählten Funktion dx_r übereinstimmt), so ist leicht zu zeigen, daß die hierdurch bestimmte Operation d wirklich der obigen Grundforderung genügt. Denn durch partielle Derivation in bezug auf die Variable x_r ergibt sich aus der oben angenommenen Identität (29) bekanntlich

$$\frac{\partial F}{\partial \varphi_1}\frac{\partial \varphi_1}{\partial x_r} + \frac{\partial F}{\partial \varphi_2}\frac{\partial \varphi_2}{\partial x_r} + \cdots + \frac{\partial F}{\partial \varphi_m}\frac{\partial \varphi_m}{\partial x_r} = 0;$$

multipliziert man mit dx_r und summiert, indem man r die Indizes $1, 2, \cdots, n$ durchlaufen läßt, so ergibt sich mit Rücksicht auf (32) die zu beweisende Gleichung (30).

Aus dem in (29), (30) ausgedrückten Grundgesetz einer solchen Operation d leuchtet auch unmittelbar ihre Invarianz ein, d. h. sie bleibt dieselbe, wenn statt der Koordinaten x ein anderes System von n voneinander unabhängigen Funktionen y zur Ortsbestimmung gewählt wird, wobei die ihnen entsprechenden Funktionen dy gemäß (32) aus den Funktionen dx zu bestimmen sind. Auch versteht sich von selbst, daß zufolge desselben Gesetzes alle Regeln der gewöhnlichen Differentiation, wie

$$d(\varphi_1 \pm \varphi_2) = d\varphi_1 \pm d\varphi_2, \quad d(\varphi_1\varphi_2) = \varphi_2 d\varphi_1 + \varphi_1 d\varphi_2$$

ihre volle Geltung behalten.

Unter den vielen verschiedenen Namen, welche man je nach der Beschaffenheit des Anwendungsgebietes einer solchen Operation d beilegen möchte*), will ich hier den in einem solchen Gebiet eingebürgerten, freilich in viel speziellerer Bedeutung gebrauchten Namen Vektor wählen, während die durch d erzeugten Funktionen $d\varphi$ unbedenklich Differentiale genannt werden können. Die partielle Derivation $\dfrac{\partial}{\partial x_r}$ in bezug auf die Variable x_r ist offenbar der spezielle Vektor d, für welchen die Differentiale (33) mit Ausnahme von dx_r, welches $= 1$ ist, identisch verschwinden. Es ist auch zweckmäßig, den Vektor Null einzuführen, und durch $d = 0$ anzudeuten, daß alle n Funktionen (33), also auch alle $d\varphi$ identisch verschwinden;

*) Immer von einer Differentiation erster Ordnung oder Variation erster Ordnung zu sprechen, ist zu unbequem. Sophus Lie gebraucht für seine Symbole $X(f)$, die mit den Vektoren identisch sind, den Namen infinitesimale Transformation (Theorie der Transformationsgruppen; Abschnitt 1, Kapitel 3, § 13, S. 54).

eine Verwirrung ist hierbei nicht zu befürchten, weil aus dem Zusammenhang sich immer ergeben wird, ob von der Zahl oder dem Vektor Null die Rede ist.

Da ein Vektor d aus jedem Element φ des Systems Φ ein ebenfalls in Φ enthaltenes Element $d\varphi$ erzeugt, so fällt diese Operation unter den viel allgemeineren Begriff einer Abbildung des Systems Φ in sich selbst. Solche Abbildungen, die im folgenden ausschließlich durch Buchstaben e (mit Akzenten oder Indizes) bezeichnet werden sollen, gestatten sehr mannigfaltige Verbindungen und symbolische Rechnungen, die ich jetzt erkläre, um sie später auf unsere Vektoren anzuwenden. Eine Abbildung e von Φ in sich selbst erzeugt aus jedem Element φ des Systems Φ ein mit $e\varphi$ zu bezeichnendes Bild, welches wieder eine in Φ enthaltene Funktion ist, und die Abbildungen e, e' gelten stets und nur dann für eine und dieselbe — was durch $e = e'$ ausgedrückt wird —, wenn für jede Funktion φ die Identität $e\varphi = e'\varphi$ besteht. Aus je zwei Abbildungen e_1, e_2 entspringt eine als Produkt e_1e_2 zu bezeichnende Abbildung, welche durch die für jede Funktion φ geltende Identität $(e_1e_2)\varphi = e_1(e_2\varphi) = e_1e_2\varphi$ erklärt wird und von dem Produkt e_2e_1 wohl zu unterscheiden ist; ersetzt man aber in dieser Definition die willkürliche Funktion φ durch $e_3\varphi$, wo e_3 eine beliebige Abbildung bedeutet, so ergibt sich unmittelbar die Geltung des Assoziationsgesetzes

$$(e_1e_2)e_3 = e_1(e_2e_3) = e_1e_2e_3,$$

und hieraus folgt in bekannter Weise die bestimmte Bedeutung eines aus m Abbildungen in vorgeschriebener Folge gebildeten Produkts $e_1e_2\cdots e_m$. Zwei Abbildungen e_1, e_2 heißen permutabel, wenn $e_1e_2 = e_2e_1$ ist.

Ebenso sollen Summe und Differenz $(e_1 \pm e_2)$ und, wenn λ eine Funktion in Φ ist, das Produkt λe durch

$$(e_1 \pm e_2)\varphi = e_1\varphi \pm e_2\varphi \quad \text{und} \quad (\lambda e)\varphi = \lambda(e\varphi) = \lambda e\varphi$$

erklärt werden, und eine symbolische Gleichung von der Form

$$e = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_m e_m = \sum_{\iota}^{} \lambda_\iota e_\iota, \tag{34}$$

wo die λ_ι Funktionen in Φ sind, soll bedeuten, daß für jede Funktion φ die Identität

$$e\varphi = \sum_{\iota}^{} \lambda_\iota e_\iota \varphi \tag{35}$$

besteht. Ersetzt man φ durch $e'\varphi$, wo e' eine beliebige Abbildung bedeutet, so ergibt sich, daß die symbolische Gleichung

$$\lambda e e' = \sum_{\iota} \lambda \lambda_\iota e_\iota e', \tag{36}$$

wo λ eine Funktion bedeutet, eine notwendige Folge der Gleichung (34) ist, d. h. man darf eine solche Gleichung gliedweise von links mit einer Funktion λ, von rechts mit einer Funktion φ oder einer Abbildung e' multiplizieren; ebenso darf man solche Gleichungen addieren und subtrahieren, wie wenn die Abbildungen e Größen wären. Da ferner ein Vektor d alle Regeln der gewöhnlichen Differentiation befolgt, so ergibt sich aus (35) ebenso, daß auch die symbolische Gleichung

$$de = \sum_{\iota} \lambda_\iota de_\iota + \sum_{\iota} d\lambda_\iota e_\iota \tag{37}$$

eine Folge von (34) ist.

Wir betrachten im folgenden nur solche Abbildungen e, welche entweder selbst Vektoren oder Produkte von mehreren Vektoren sind. Hat man ein System von m Vektoren $d_1, d_2, \cdots, d_m$ und ebenso vielen Funktionen $\lambda_1, \lambda_2, \cdots, \lambda_m$, so ergibt sich aus der Gleichung (32), wenn man sie für jeden Vektor d_ι in Anspruch nimmt und von links mit λ_ι multipliziert, daß jede Abbildung von der Form

$$d = \lambda_1 d_1 + \lambda_2 d_2 + \cdots + \lambda_m d_m = \sum_{\iota} \lambda_\iota d_\iota \tag{38}$$

wieder ein Vektor ist; einen solchen Vektor d nennen wir abhängig von den m Vektoren d_ι, und ebenso sagen wir, daß diese m Vektoren d_ι voneinander abhängig seien oder ein reduzibles System bilden, falls es m Funktionen λ_ι gibt, die nicht alle identisch verschwinden, und für welche der vorstehende Vektor $d = 0$ wird. Offenbar tritt dieser Fall immer ein, wenn $m > n$ ist; ist aber $m \leqq n$, so wird er dadurch charakterisiert, daß alle Determinanten m-ten Grades, die man aus den m Zeilen und aus m Spalten des Systems

$$\begin{array}{llll} d_1x_1, & d_1x_2, & \cdots, & d_1x_n \\ d_2x_1, & d_2x_2, & \cdots, & d_2x_n \\ \cdots & \cdots & \cdots & \cdots \\ d_mx_1, & d_mx_2, & \cdots, & d_mx_n \end{array}$$

bilden kann, identisch verschwinden. Wir sagen ferner, die m Vektoren d_ι in (38) seien voneinander unabhängig oder sie bilden ein irreduzibles System, wenn die Forderung $d = 0$ nur durch das identische Verschwinden aller m Funktionen λ_ι erfüllt wird. Bilden n Vektoren $d_1, d_2, \cdots, d_n$ ein solches irreduzibles System, so läßt sich jeder Vektor d in der Form

$$d = \lambda_1 d_1 + \lambda_2 d_2 + \cdots + \lambda_n d_n = \sum_{r}^{r} \lambda_r d_r \tag{39}$$

darstellen, wo die n Funktionen λ_r durch d vollständig bestimmt sind. Ein solches System bilden offenbar die n partiellen Derivationen $\frac{\partial}{\partial x_r}$, und die vorstehende Gleichung geht dann in

$$d = \sum_{r}^{r} dx_r \frac{\partial}{\partial x_r}$$

über, die mit (32) übereinstimmt.

Wir wollen jetzt zwei beliebige Vektoren d_1, d_2 betrachten und die daraus entspringenden Produkte d_1d_2 und d_2d_1 miteinander vergleichen. Zufolge (32) ist

$$d_2\varphi = \sum_{r}^{r} \frac{\partial \varphi}{\partial x_r} d_2x_r, \quad d_1 \frac{\partial \varphi}{\partial x_r} = \sum_{s}^{s} \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) d_1x_s,$$

wo r, s die Indizes $1, 2, \cdots, n$ durchlaufen, und da jeder Vektor die Regeln der totalen Differentiation befolgt, so wird

$$d_1d_2\varphi = \sum_{r}^{r} \frac{\partial \varphi}{\partial x_r} d_1d_2x_r + \sum_{r,s}^{r,s} \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) d_1x_s d_2x_r$$

und ebenso durch Vertauschung von d_1, d_2

$$d_2d_1\varphi = \sum_{r}^{r} \frac{\partial \varphi}{\partial x_r} d_2d_1x_r + \sum_{r,s}^{r,s} \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) d_2x_s d_1x_r;$$

vertauscht man in der letzten Doppelsumme die beiden voneinander unabhängigen Summationsbuchstaben r, s miteinander, so ergibt sich aus der Annahme (28) ihre Identität mit der Doppelsumme, welche in der Darstellung von $d_1d_2\varphi$ auftritt; durch Subtraktion erhält man daher die Gleichung

$$(d_1d_2 - d_2d_1)\varphi = \sum_{r}^{r} \frac{\partial \varphi}{\partial x_r}(d_1d_2 - d_2d_1)x_r,$$

in welcher nur die Derivierten erster Ordnung der willkürlichen Funktion φ auftreten. Definiert man daher eine neue Operation oder Abbildung (d_1, d_2) durch

$$(40) \qquad (d_1, d_2) = d_1 d_2 - d_2 d_1 = -(d_2, d_1),$$

so wird

$$(41) \qquad (d_1, d_2)\varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r}(d_1, d_2) x_r,$$

und durch Vergleichung mit (32) ergibt sich der wichtige Satz, daß diese Abbildung (d_1, d_2) wieder ein Vektor ist. Dieser Satz ist meines Wissens zuerst von Jacobi gefunden (in § 23 der nachgelassenen Abhandlung Nova methodus, aequationes differentiales partiales primi ordinis inter numerum variabilium quemcunque propositas integrandi, dieses Journal Bd. 60) und bildet eine wesentliche Grundlage seiner Untersuchungen über die partiellen Differentialgleichungen. Ich bemerke ausdrücklich, daß die von ihm mit A, B bezeichneten Operationen vollständig identisch mit unseren Vektoren sind; daß aber diese Operationen nicht nur die Gesetze der totalen Differentiation befolgen, sondern daß gerade in dieser, alles andere einschließenden Eigenschaft ihr ganzes Wesen besteht, scheint nirgends deutlich erkannt und in aller Schärfe ausgesprochen zu sein.

Daß zwei Vektoren d_1, d_2 permutabel sind, daß also $d_1 d_2 = d_2 d_1$ ist, wird jetzt durch $(d_1, d_2) = 0$ ausgedrückt. Wir betrachten nun drei beliebige Vektoren d_1, d_2, d_3 und bilden daraus die Abbildung

$$(42) \qquad (d_1; d_2, d_3) = d_1(d_2, d_3) - (d_2, d_3) d_1 = -(d_1; d_3, d_2),$$

welche zufolge des eben erhaltenen Fundamentalsatzes ebenfalls ein Vektor ist; verfährt man nach den bei (34), (36), (37) angegebenen Regeln, so erhält man

$$(d_1; d_2, d_3) = (d_1 d_2 d_3 + d_3 d_2 d_1) - (d_2 d_3 d_1 + d_1 d_3 d_2),$$

und hieraus ergibt sich durch zyklische Vertauschung und Addition der Satz*)

$$(43) \qquad (d_1; d_2, d_3) + (d_2; d_3, d_1) + (d_3; d_1, d_2) = 0.$$

Wenden wir dieselben Regeln auf die Gleichung (38) an, die wir wieder in der Form

$$(44) \qquad d = \sum^{\iota} \lambda_\iota d_\iota$$

darstellen, und bezeichnen wir mit d' einen beliebigen Vektor, so erhalten wir

$$dd' = \sum^{\iota} \lambda_\iota d_\iota d', \quad d'd = \sum \lambda_\iota d' d_\iota + \sum d' \lambda_\iota d_\iota;$$

subtrahiert man die erste Gleichung von der zweiten und wendet die Symbolik (40) an, so ergibt sich die Vektorgleichung

$$(45) \qquad (d', d) = \sum^{\iota} \lambda_\iota (d', d_\iota) + \sum^{\iota} d' \lambda_\iota d_\iota$$

als eine notwendige Folge von (44).

Bezeichnet man die aus einem Vektor d durch Wiederholung entspringenden Abbildungen dd, $ddd \cdots$ bzw. mit d^2, $d^3 \cdots$, so gelten auch für diese Operationen die gewöhnlichen Regeln der Differentiation, z. B.

$$d^2\varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r} d^2 x_r + \sum^{r,s} \frac{\partial^2 \varphi}{\partial x_r \partial x_s} dx_r dx_s.$$

Genügen die n Differentiale dx_r den partiellen Differentialgleichungen $d^2 x_r = 0$ (was z. B. immer dann eintritt, wenn sie konstant sind), so folgt

$$d^2\varphi = \sum^{r,s} \frac{\partial^2 \varphi}{\partial x_r \partial x_s} dx_r dx_s,$$

und wenn man für φ eine ganze homogene Funktion zweiten Grades $F = F(x_1, x_2, \cdots, x_n)$ wählt, so wird

$$(46) \qquad d^2 F = 2F(dx_1, dx_2, \cdots, dx_n).$$

Im Falle $n = 2$ wollen wir mit x, y die unabhängigen Variabeln und mit d einen Vektor bezeichnen, der den Bedingungen $d^2 x = d^2 y = 0$ genügt. Betrachten wir nun eine binäre quadratische Form

$$(47) \qquad F = F(x, y) = Ax^2 + Bxy + Cy^2$$

und setzen deren Diskriminante

$$(48) \qquad B^2 - 4AC = D,$$

so wird

$$(49) \qquad \begin{cases} dF = (2Ax + By)dx + (Bx + 2Cy)dy \\ \qquad\quad = x(2Adx + Bdy) + y(Bdx + 2Cdy) \end{cases}$$

und

$$(50) \qquad \tfrac{1}{2} d^2 F = Adx^2 + Bdxdy + Cdy^2 = F(dx, dy).$$

*) Derselbe Satz findet sich in dem angeführten Werke von Lie (Abschnitt 1, Kapitel 5, § 26).

Diese Gleichungen lassen sich, wenn man die Multiplikation der binären Substitutionen benutzt, auch in der Form

$$\begin{pmatrix} 2F, & dF \\ dF, & d^2F \end{pmatrix} = \begin{pmatrix} x, & y \\ dx, & dy \end{pmatrix} \begin{pmatrix} 2A, & B \\ B, & 2C \end{pmatrix} \begin{pmatrix} x, & dx \\ y, & dy \end{pmatrix} \tag{51}$$

darstellen, und aus dem Satze über die Determinante eines Produkts von Substitutionen ergibt sich

$$dF^2 - 2Fd^2F = D(x\,dy - y\,dx)^2. \tag{52}$$

Es braucht aber kaum gesagt zu werden, daß dies nichts anderes ist als der bekannte, auch in § 1 benutzte Fundamentalsatz für die Transformation einer binären quadratischen Form F von der Diskriminante D durch eine binäre Substitution $\begin{pmatrix} x, & dx \\ y, & dy \end{pmatrix}$, und daß der vorstehende Beweis ganz unabhängig von der hier vorgetragenen Theorie der Vektoren ist; der Satz sollte nur im Anschluß an diese Theorie in einer solchen Form dargestellt werden, wie wir ihn demnächst gebrauchen werden.

§ 4.

Wir kehren jetzt zu der in § 1 geführten Untersuchung zurück, um sie in anderer Form zu wiederholen und fortzusetzen. Wir betrachten, wie dort, drei Paare von unabhängigen Variabeln (x_1, y_1), (x_2, y_2), (x_3, y_3), die wir kurz die Paare z_1, z_2, z_3 nennen, und wollen in diesem sechsfach ausgedehnten analytischen Raume die Eigenschaften einer binären trilinearen Form H untersuchen, d. h. einer ganzen Funktion, welche in bezug auf jedes der drei Paare homogen vom ersten Grade ist. Hieraus folgt zunächst

$$H = x_1\frac{\partial H}{\partial x_1} + y_1\frac{\partial H}{\partial y_1} = x_2\frac{\partial H}{\partial x_2} + y_2\frac{\partial H}{\partial y_2} = x_3\frac{\partial H}{\partial x_3} + y_3\frac{\partial H}{\partial y_3}. \tag{53}$$

Bezeichnen wir (wie in § 1) mit r, s, t irgendeine Permutation der drei Indizes 1, 2, 3, so können wir drei Vektoren d_1, d_2, d_3 durch die gemeinsame Definition

$$d_r\varphi = \frac{\partial\varphi}{\partial x_r}\frac{\partial H}{\partial y_r} - \frac{\partial\varphi}{\partial y_r}\frac{\partial H}{\partial x_r} \tag{54}$$

einführen, wo φ, wie immer im folgenden, jede willkürliche Funktion der sechs Variabeln bedeuten soll. Zufolge (32) ist daher

$$d_r x_r = \frac{\partial H}{\partial y_r}, \quad d_r y_r = -\frac{\partial H}{\partial x_r} \tag{55}$$

und

$$d_r x_s = d_r y_s = d_r x_t = d_r y_t = 0; \tag{56}$$

für den Vektor d_r verhalten sich daher die Paare z_s, z_t wie Konstanten, während $d_r x_r$, $d_r y_r$ bilineare Funktionen dieser beiden Paare, also konstant in bezug auf das Paar z_r sind. Ist daher φ homogen in bezug auf jedes einzelne Paar, und zwar vom Grade m_r in bezug auf z_r, so ist $d_r\varphi$ homogen von den Graden $m_r - 1$, $m_s + 1$, $m_t + 1$ in bezug auf die Paare z_r, z_s, z_t. Aus (54) folgt zunächst

$$d_r H = 0, \tag{57}$$

und zufolge (55) nehmen die Gleichungen (53) die Form

$$H = y_s d_s x_s - x_s d_s y_s \tag{58}$$

an.

Um nun den in (40) erklärten Vektor $(d_r, d_s) = -(d_s, d_r)$ zu bilden, entwickeln wir die Gleichung (57), indem wir die Operation d_r an dem Ausdruck (58) mit Rücksicht auf (56) vollziehen, woraus $y_s d_r d_s x_s = x_s d_r d_s y_s$ folgt; setzt man diese durch x_s und y_s, also auch durch $x_s y_s$ teilbare ganze Funktion $= x_s y_s F_{r,s}$, so wird

$$d_r d_s x_s = x_s F_{r,s}, \quad d_r d_s y_s = y_s F_{r,s}. \tag{59}$$

Da nun $d_s x_s$, $d_s y_s$ bilineare Funktionen von z_r, z_t, also $d_r d_s x_s$ und $d_r d_s y_s$ homogen vom ersten Grade in bezug auf z_s, vom zweiten Grade in bezug auf z_t und frei von z_r sind, so ist $F_{r,s}$ eine binäre quadratische Form des Paares z_t mit konstanten Koeffizienten. Zufolge (56) ist nun

$$d_s d_r x_s = d_s d_r y_s = 0,$$

mithin können wir die Gleichungen (59) durch

$$(d_r, d_s)x_s = x_s F_{r,s}, \quad (d_r, d_s)y_s = y_s F_{r,s}$$

ersetzen; vertauscht man r mit s, wodurch (d_r, d_s) in $(d_s, d_r) = -(d_r, d_s)$ übergeht, so folgt hieraus

$$(d_r, d_s)x_r = -x_r F_{s,r}, \quad (d_r, d_s)y_r = -y_r F_{s,r},$$

wo $F_{s,r}$ ebenfalls eine quadratische Form des Paares z_t bedeutet. Da ferner die Variabeln x_t, y_t sich für beide Vektoren d_r, d_s wie Konstanten verhalten, so ist $(d_r, d_s)x_t = 0$, $(d_r, d_s)y_t = 0$.

Hiermit ist der Vektor (d_r, d_s) vollständig bestimmt, und zufolge (32) wird

$$(d_r, d_s)\varphi = F_{r,s}\left(x_s\frac{\partial\varphi}{\partial x_s} + y_s\frac{\partial\varphi}{\partial y_s}\right) - F_{s,r}\left(x_r\frac{\partial\varphi}{\partial x_r} + y_r\frac{\partial\varphi}{\partial y_r}\right). \tag{60}$$

Dies Resultat gibt Veranlassung, drei neue, von der Form H ganz unabhängige Vektoren e_1, e_2, e_3 durch die gemeinsame Erklärung

$$e_r\varphi = x_r\frac{\partial\varphi}{\partial x_r} + y_r\frac{\partial\varphi}{\partial y_r} \tag{61}$$

einzuführen, woraus

$$e_r x_r = x_r, \quad e_r y_r = y_r \tag{62}$$

und

$$e_r x_s = e_r y_s = e_r x_t = e_r y_t = 0 \tag{63}$$

folgt. Daß eine Funktion φ homogen in bezug auf das Paar z_r und zwar vom Grade m_r ist, wird jetzt durch $e_r\varphi = m_r\varphi$ ausgedrückt; die Gleichungen (53) lauten daher

$$e_r H = H, \tag{64}$$

und die Gleichung (60) geht über in

$$(d_r, d_s)\varphi = F_{r,s}e_s\varphi - F_{s,r}e_r\varphi.$$

Setzt man nun $\varphi = H$ und bedenkt, daß zufolge (57) auch $(d_r, d_s)H = 0$ ist, so erhält man $(F_{r,s} - F_{s,r})H = 0$, und da wir annehmen, daß die Form H nicht identisch verschwindet, so ergibt sich $F_{r,s} = F_{s,r}$ (was übrigens auch in dem ausgeschlossenen Falle $H = 0$ gelten würde, weil zufolge (55), (59) dann beide Formen $F_{r,s}, F_{s,r}$ identisch verschwinden); wir dürfen daher diese quadratische Form des Paares z_t einfacher durch $F_t = F_t(x_t, y_t)$ bezeichnen, und zugleich nimmt die vorhergehende Gleichung die Form

$$(d_r, d_s)\varphi = F_t(e_s\varphi - e_r\varphi) \tag{65}$$

an, welche nach (34) symbolisch auch durch

$$(d_r, d_s) = F_t(e_s - e_r) \tag{66}$$

ausgedrückt werden kann, und die Gleichungen (59) lauten jetzt

$$d_r d_s x_s = x_s F_t, \quad d_r d_s y_s = y_s F_t. \tag{67}$$

Daß übrigens die durch die erste Gleichung (59) vollständig definierte Größe $F_{r,s}$ symmetrisch in bezug auf r, s ist, hätte man schon dort leicht zeigen können; denn setzt man in (54) die willkürliche Funktion

$$\varphi = d_s x_s = \frac{\partial H}{\partial y_s},$$

so erhält man

$$x_s F_{r,s} = \frac{\partial^2 H}{\partial x_r \partial y_s}\frac{\partial H}{\partial y_r} - \frac{\partial^2 H}{\partial y_r \partial y_s}\frac{\partial H}{\partial x_r},$$

und da die hier auftretenden Derivierten zweiter Ordnung ebenso wie $F_{r,s}$ nur noch die beiden Variabeln x_t, y_t enthalten, so ergibt sich die genannte Symmetrie durch partielle Derivation nach x_s, und wir erhalten für die Form $F_{r,s} = F_{s,r} = F_t$ den Ausdruck

$$F_t = \frac{\partial^2 H}{\partial x_r \partial y_s}\frac{\partial^2 H}{\partial y_r \partial x_s} - \frac{\partial^2 H}{\partial y_r \partial y_s}\frac{\partial^2 H}{\partial x_r \partial x_s}. \tag{68}$$

Um jetzt den Zusammenhang der gegenwärtigen Untersuchung mit der in § 1 deutlich zu machen, bemerke ich folgendes. Identifiziert man die Form H mit der dort in (12) dargestellten Funktion, so sind die Konstanten α_0, β_0, α_r, β_r bzw. die Koeffizienten von $x_1x_2x_3$, $y_1y_2y_3$, $x_ry_sy_t$, $y_rx_sx_t$; die in (55) erklärten Größen d_rx_r, d_ry_r sind identisch mit den Funktionen X_r, Y_r in (10), und der vorstehende Ausdruck für F_t stimmt vollständig mit der dortigen Definition (1) der drei Formen F_1, F_2, F_3 überein.

Den Satz (65) wenden wir jetzt auf zwei Beispiele an. Setzt man zuerst $\varphi = F_s$, so folgt

$$d_r d_s F_s = 2F_s F_t, \tag{69}$$

weil $d_rF_s = 0$, $e_sF_s = 2F_s$, $e_rF_s = 0$ ist. Setzt man zweitens $\varphi = d_tx_t$ und bedenkt, daß diese Funktion bilinear in bezug auf die beiden Paare z_r, z_s, daß also

$$e_s d_t x_t = e_r d_t x_t = d_t x_t \tag{70}$$

ist, so erhält man $d_rd_sd_tx_t = d_sd_rd_tx_t$; zufolge (67) ist aber $d_sd_tx_t = x_tF_r$, und $d_rd_tx_t = x_tF_s$, mithin wird $d_r(x_tF_r) = d_s(x_tF_s)$, und da x_t für beide Vektoren d_r, d_s konstant ist, so folgt der wichtige Satz

$$d_rF_r = d_sF_s. \tag{71}$$

Diese Funktion ist also symmetrisch in bezug auf alle drei Indizes 1, 2, 3 und offenbar eine neue trilineare Form, die wir mit H' bezeichnen und die zu H adjungierte Form nennen wollen; es ist also

$$H' = d_1F_1 = d_2F_2 = d_3F_3, \tag{72}$$

und der Satz (69) geht in

$$d_rH' = d_r^2F_r = 2F_sF_t \tag{73}$$

über. Da zufolge (55) der Vektor d_r den Bedingungen $d_r^2x_r = d_r^2y_r = 0$ genügt, so können wir hier die am Schlusse von § 3 bewiesenen Sätze

(50), (52) anwenden. Zufolge (50) läßt sich die Gleichung (73) auch in der Form

(74) $$F_r(d_r x_r,\ d_r y_r) = F_s F_t$$

darstellen, und dies Resultat ist offenbar vollständig identisch mit dem Hauptsatz (11) in § 1, welcher dort auf ganz anderem Wege bewiesen ist. Bezeichnet man ferner mit D_r die Diskriminante der Form F_r, so folgt aus (52) die Gleichung

$$d_r F_r^2 - 2F_r d_r^2 F_r = D_r(x_r d_r y_r - y_r d_r x_r)^2,$$

welche zufolge (72), (73), (58) die Form

$$H'^2 - 4F_r F_s F_t = D_r H^2$$

annimmt; da $F_r F_s F_t = F_1 F_2 F_3$ und H, H' symmetrisch in bezug auf die Indizes 1, 2, 3 sind, so folgt hieraus, daß die Formen F_1, F_2, F_3 dieselbe Diskriminante

(75) $$D = D_1 = D_2 = D_3$$

besitzen, was mit dem Satze (3) in § 1 übereinstimmt, und zugleich ergibt sich, daß zwischen den beiden trilinearen Formen H, H' und den drei quadratischen Formen F_1, F_2, F_3 die Identität

(76) $$H'^2 - DH^2 = 4F_1 F_2 F_3$$

besteht.

Der Satz (71), auf welchem die Einführung der zu H adjungierten Form H' beruht, läßt sich auf einem zwar nicht kürzeren, aber mehr symmetrischen Wege beweisen, den ich hier noch andeuten will. Aus den Definitionen (55), (56), (62), (63) ergibt sich leicht die Vektoridentität

(77) $$(d_t,\ e_r) = -d_t;$$

vertauscht man r mit s und subtrahiert, so folgt $(d_t,\ e_s - e_r) = 0$, d. h. die beiden Vektoren d_t und $(e_s - e_r)$ sind permutabel. Unterwirft man daher die Gleichung (66) nach der in (45) angegebenen Regel dem Vektor d_t und benutzt das in (42) erklärte Symbol, so erhält man

(78) $$(d_t;\ d_r,\ d_s) = d_t F_t(e_s - e_r),$$

und aus dem Satze (43) folgt

$$(d_2 F_3 - d_3 F_3)e_1 + (d_3 F_3 - d_1 F_1)e_2 + (d_1 F_1 - d_2 F_2)e_3 = 0;$$

da aber die drei Vektoren e_1, e_2, e_3 zufolge ihrer Definition (62), (63) offenbar ein irreduzibles System bilden, so müssen die drei Differenzen $(d_r F_r - d_s F_s)$ identisch verschwinden, wie zu beweisen war.

Ich bemerke endlich noch folgendes. Wenn für eine partikuläre Form H die Form F_1 identisch verschwindet, so muß zufolge (72), (74) auch H' und mindestens eine der beiden Formen F_2, F_3 identisch verschwinden. Man findet leicht, daß das Verschwinden der beiden Formen F_1, F_2 stets und nur dann eintritt, wenn $H = h_{1,2} h_3$ ist, wo $h_{1,2}$ eine bilineare Funktion der Paare z_1, z_2, und h_3 eine lineare Funktion des Paares z_3 bedeutet. Verschwinden alle drei Formen F_1, F_2, F_3, so ist $H = h_1 h_2 h_3$ ein Produkt von drei linearen Faktoren, und umgekehrt.

§ 5.

Es liegt nahe, die eben geführte Untersuchung von der Form H auf die zu ihr adjungierte Form H' zu übertragen. Bezeichnet man mit d'_r, F'_r die Vektoren und quadratischen Formen, die hierbei aus den auf H bezüglichen Vektoren und Formen d_r, F_r hervorgehen, während die in (61) erklärten Vektoren e_r ihre von H gänzlich unabhängige Bedeutung behalten, so ist

(79) $$d'_r \varphi = \frac{\partial \varphi}{\partial x_r}\frac{\partial H'}{\partial y_r} - \frac{\partial \varphi}{\partial y_r}\frac{\partial H'}{\partial x_r};$$

hieraus folgt zunächst die mit (57) analoge Gleichung

(80) $$d'_r H' = 0,$$

und durch den Vergleich mit (54), (73) ergibt sich

(81) $$d'_r H = -d_r H' = -2F_s F_t;$$

ebenso entspricht der Gleichung (64) die Gleichung

(82) $$e_r H' = H'.$$

Sodann bemerken wir, daß die drei Vektoren d_r, e_r, d'_r gewiß ein reduzibles System bilden, weil die beiden Paare z_s, z_t sich gegen sie wie Konstanten verhalten; es muß also eine Identität von der Form

$$\lambda d_r + \lambda' d'_r + \mu e_r = 0$$

bestehen, wo λ, λ', μ Funktionen bedeuten, die nicht alle verschwinden; unterwirft man dieser Identität die beiden Formen H, H' und berücksichtigt (57), (64), (80), (81), (82), so folgt

$$\lambda'(-2F_s F_t) + \mu H = 0, \quad \lambda(2F_s F_t) + \mu H' = 0,$$

mithin wird

(83) $$-H' d_r + H d'_r + 2F_s F_t e_r = 0.$$

Wendet man dieses Resultat auf die Funktion F_r an und bedenkt, daß $d_r F_r = H'$, $e_r F_r = 2F_r$ ist, so folgt

$$-H'^2 + H d_r' F_r + 4 F_r F_s F_t = 0,$$

und zufolge (76) ergibt sich

(84) $$d_r' F_r = DH.$$

Überträgt man jetzt den Satz (66) auf die Form H', so erhält man

$$(d_r', d_s') = F_t'(e_s - e_r),$$

was als Definition der quadratischen Form F_t' angesehen werden kann. Läßt man diesen Vektor auf die Form F_s wirken, so wird die rechte Seite $= 2F_s F_t'$; da ferner $d_r' F_s = 0$, $d_s' F_s = DH$, also $(d_r', d_s') F_s = d_r' d_s' F_s = D d_r' H = D(-F_s F_t)$ ist, so folgt

(85) $$F_t' = -DF_t;$$

die gemeinsame Diskriminante D' der drei Formen F_1', F_2', F_3' ist daher

(86) $$D' = D^3,$$

und die vorhergehende Vektoridentität wird

(87) $$(d_r', d_s') = -DF_t(e_s - e_r) = -D(d_r, d_s).$$

Endlich folgt aus der Definition (72) der zu H adjungierten Form H', daß die zu H' adjungierte Form $= d_t' F_t' = -D d_t' F_t = -D^2 H$, also die mit $(-D^2)$ multiplizierte erste Form H ist, und hiermit leuchtet ein, daß die Identität (76) bei dem Übergang von H zu H' sich nur mit $(-D^3)$ multipliziert. —

Die Form H und ihre Adjungierte H' bilden die Basis einer Schar von unendlich vielen trilinearen Formen

(88) $$H'' = Hp + H'q,$$

wo p, q zwei willkürliche Konstanten bedeuten. Behandelt man eine solche Form H'' ebenso wie H in § 4 und definiert drei ihr entsprechende Vektoren d_r'' durch

(89) $$d_r'' \varphi = \frac{\partial \varphi}{\partial x_r}\frac{\partial H''}{\partial y_r} - \frac{\partial \varphi}{\partial y_r}\frac{\partial H''}{\partial x_r},$$

so wird offenbar

(90) $$d_r'' H_r'' = 0, \quad d_r'' = p d_r + q d_r',$$

und aus den für die Vektoren d_r, d_r' gefundenen Resultaten ergibt sich

(91) $$d_r'' H = -2F_s F_t q, \quad d_r'' H' = +2F_s F_t p,$$

(92) $$d_r'' F_r = H'p + DHq,$$

also

(93) $$(d_r'', d_s'') F_s = d_r'' d_s'' F_s = 2F_s F_t m,$$

wo

(94) $$m = p^2 - Dq^2.$$

Die aus der Form H'' entspringenden quadratischen Formen F_1'', F_2'', F_3'' sind nach (66) durch die Vektoridentität

$$(d_r'', d_s'') = F_t''(e_s - e_r)$$

zu erklären, und aus (93) folgt

(95) $$F_t'' = mF_t,$$

(96) $$(d_r'', d_s'') = mF_t(e_s - e_r) = m(d_r, d_s).$$

Die Trias der zu den trilinearen Formen H'' der Schar (88) gehörenden quadratischen Formen ist daher **invariant**, wenn man von gemeinsamen konstanten Faktoren m absieht. Drei solche Formen (95) besitzen die gemeinsame Diskriminante

$$D'' = Dm^2,$$

und für die zu H'' adjungierte Form $H''' = d_r'' F_r''$ findet man nach (95), (92) den Ausdruck

(97) $$H''' = m(H'p + DHq);$$

diese Form ist daher ebenfalls in der Schar (88) enthalten.

Um endlich die aus (76) hervorgehende Identität

(98) $$H'''^2 - D'' H''^2 = 4 F_1'' F_2'' F_3''$$

zu bestätigen, wollen wir die **Quadratwurzeln** aus den Diskriminanten D und $D'' = Dm^2$ einführen und ihren Zusammenhang immer so bestimmen, daß

(99) $$\sqrt{D''} = m\sqrt{D}$$

wird; dann folgt aus (88), (97) die Gleichung

(100) $$H''' + H''\sqrt{D''} = m(p + q\sqrt{D})(H' + H\sqrt{D});$$

ersetzt man hierin $\sqrt{D}$ durch $-\sqrt{D}$, also auch $\sqrt{D''}$ durch $-\sqrt{D''}$, und multipliziert beide Gleichungen miteinander, so folgt

$$H'''^2 - D'' H''^2 = m^3(H'^2 - DH^2),$$

was zufolge (76), (95) mit der zu beweisenden Gleichung (98) übereinstimmt. —

Der in (96) erhaltene Satz gibt noch zu folgenden Bemerkungen Veranlassung. Entwickelt man den Vektor (d_r'', d_s'') nach den in § 3 angegebenen Regeln aus der Definition (90), so wird

$$(d_r'', d_s'') = p^2(d_r, d_s) + pq\{(d_r, d_s') + (d_r', d_s)\} + q^2(d_r', d_s');$$

die Vergleichung mit (96), wo $m = p^2 - Dq^2$, ergibt daher wieder den Satz (87), und da der mit pq multiplizierte Vektor verschwinden muß, so erhält man den neuen Satz, daß der Vektor

$$(d_r, d_s') = (d_s, d_r'), \tag{101}$$

also symmetrisch in bezug auf die beiden Indizes r, s ist. Dasselbe Resultat ergibt sich auch, wenn man nach der in § 3 angegebenen Regel (45) die Identität (83) dem Vektor d_s unterwirft und hierbei die Sätze (66), (77) benutzt; auf diese Weise erhält man den symmetrischen Ausdruck

$$H(d_s, d_r') = F_t\{2F_r d_r - H' e_r + 2F_s d_s - H' e_s\}, \tag{102}$$

der sich aber noch einfacher darstellen läßt.

Führt man nämlich noch drei Vektoren δ_1, δ_2, δ_3 durch die gemeinsame Erklärung

$$\delta_r \varphi = \frac{\partial \varphi}{\partial x_r}\frac{\partial F_r}{\partial y_r} - \frac{\partial \varphi}{\partial y_r}\frac{\partial F_r}{\partial x_r} \tag{103}$$

ein*), so folgt unmittelbar

$$\delta_r F_r = 0; \tag{104}$$

vergleicht man ferner (103) mit den Definitionen (54), (79) und berücksichtigt (72), (84), so erhält man

$$\delta_r H = -d_r F_r = -H', \quad \delta_r H' = -d_r' F_r = -DH. \tag{105}$$

Die drei Vektoren δ_r, d_r, e_r bilden offenbar wieder ein reduzibles System, und wenn man ähnlich verfährt, wie bei der Herleitung des Satzes (83), indem man die beiden vorstehenden Ausdrücke für $\delta_r F_r$, $\delta_r H$ benutzt, so ergibt sich

$$H\delta_r = 2F_r d_r - H' e_r, \tag{106}$$

wodurch die Gleichung (102) in

$$(d_s, d_r') = F_t(\delta_r + \delta_s) = (d_r, d_s') \tag{107}$$

übergeht. Eliminiert man aus den beiden Gleichungen (83), (106) einmal d_r, dann e_r, mit Rücksicht auf (76), so erhält man noch zwei ähnliche Relationen, die sich aber auch aus (104), (105) ableiten

*) Ich bemerke beiläufig, daß hieraus $\delta_r^2 x_r = Dx_r$, $\delta_r^2 y_r = Dy_r$ folgt.

ließen; das System dieser vier Gleichungen, durch welche die Abhängigkeit von je drei der vier Vektoren e_r, d_r, d_r', δ_r ausgedrückt wird, ist das folgende:

$$\begin{cases} * & DHd_r - & H'd_r' + 2F_sF_t\delta_r = 0, \\ -DHe_r & * & + 2F_r d_r' - & H'\delta_r = 0, \\ H'e_r & - 2F_r d_r & * & + & H\delta_r = 0, \\ -2F_sF_t e_r + & H'd_r - & H d_r' & * & = 0. \end{cases} \tag{108}$$

§ 6.

Da jede binäre quadratische Form ein Produkt von zwei linearen Faktoren ist, so folgt aus (76), daß jede der beiden konjugierten trilinearen Formen

$$U = \tfrac{1}{2}(H' + H\sqrt{D}), \quad V = \tfrac{1}{2}(H' - H\sqrt{D}), \tag{109}$$

deren Produkt

$$UV = F_1F_2F_3 \tag{110}$$

ist, und welche als spezielle Fälle in der Schar der Formen (88) enthalten sind, ein Produkt von drei linearen Faktoren ist. Wir nehmen im folgenden an, daß H eine allgemeine Form ist, d. h. daß ihre acht Koeffizienten α, β willkürliche Konstanten sind, und bezeichnen mit

$$\lambda_r = x_r + \omega_r y_r, \quad \mu_r = x_r + \omega_r' y_r \tag{111}$$

lineare Funktionen des Paares z_r, in denen die Variable x_r den Koeffizient 1 hat. Bezeichnet man ferner die Koeffizienten der Formen F_r wie in (1), so kann man zufolge (110) gleichzeitig

$$U = L\lambda_1\lambda_2\lambda_3, \quad V = M\mu_1\mu_2\mu_3 \tag{112}$$

und

$$F_r = A_r\lambda_r\mu_r \tag{113}$$

setzen, wo L, M Konstanten sind, die der Bedingung

$$LM = A_1A_2A_3 \tag{114}$$

genügen*), und die Konstanten ω_r, ω_r' sind als Wurzeln einer quadratischen Gleichung in ihrem Komplex durch

$$A_r(\omega_r + \omega_r') = B_r, \quad A_r\omega_r\omega_r' = C_r \tag{115}$$

bestimmt; es kommt darauf an, sie genau voneinander zu unterscheiden.

*) Bezeichnet man die den Koeffizienten α, β der Form H entsprechenden Koeffizienten von H' mit α', β', so ist offenbar

$$2L = \alpha_0' + \alpha_0\sqrt{D}, \quad 2M = \alpha_0' - \alpha_0\sqrt{D}.$$

Läßt man die Form H'' in (88) mit der Form U in (109) zusammenfallen, indem man $2p = \sqrt{D}$, $2q = 1$ setzt, und behält für diese spezielle Form $H'' = U$ die Vektorbezeichnung d_r'' bei, so verschwindet die Konstante m in (94), mithin verschwinden zufolge (95) auch die drei quadratischen Formen F_r'' identisch, was mit den am Schluß von § 4 gemachten Bemerkungen vollständig übereinstimmt. Aus der Definition von d_r'' und aus (112) ergibt sich sodann

$$d_r'' x_r = \frac{\partial U}{\partial y_r} = L\lambda_s\lambda_t\omega_r, \quad d_r'' y_r = -\frac{\partial U}{\partial x_r} = -L\lambda_s\lambda_t,$$

und hieraus folgen die beiden Gleichungen

$$d_r''\lambda_r = 0, \quad d_r''\mu_r = L\lambda_s\lambda_t(\omega_r - \omega_r'),$$

deren erste auch eine unmittelbare Folge der Gleichung $d_r''H'' = d_r''U = 0$ ist. Zufolge (113) wird daher

$$d_r''F_r = A_r\lambda_r d_r''\mu_r = A_r U(\omega_r - \omega_r'),$$

und da andererseits die Gleichung (92) in

$$d_r''F_r = \tfrac{1}{2}(H'\sqrt{D} + DH) = U\sqrt{D}$$

übergeht, so ergibt die Vergleichung beider Ausdrücke das unterscheidende Resultat

$$A_r(\omega_r - \omega_r') = \sqrt{D}. \tag{116}$$

Verbindet man dasselbe mit (115), so folgt

$$\omega_r = \frac{B_r + \sqrt{D}}{2A_r}, \quad \omega_r' = \frac{B_r - \sqrt{D}}{2A_r}, \tag{117}$$

und hierdurch sind die sechs linearen Funktionen λ_r, μ_r vollständig bestimmt.

Wir kehren nun noch einmal zu den durch die Form H gegebenen Vektoren d_r zurück, um ihnen die Funktionen U, V, λ_r, μ_r zu unterwerfen. Da $d_r H = 0$ und $d_r H' = 2F_s F_t$ ist, so folgt aus den Definitionen (109)

$$d_r U = d_r V = F_s F_t;$$

andererseits ergibt sich aus den Darstellungen (112)

$$d_r U = L\lambda_s\lambda_t d_r\lambda_r, \quad d_r V = M\mu_s\mu_t d_r\mu_r;$$

vergleicht man diese Ausdrücke mit einander und berücksichtigt (113), (114), so folgt

$$A_r d_r\lambda_r = M\mu_s\mu_t, \quad A_r d_r\mu_r = L\lambda_s\lambda_t, \tag{118}$$

und die vorhergehenden Ausdrücke vereinigen sich in

$$d_r U = d_r V = F_s F_t = A_r d_r\lambda_r d_r\mu_r. \tag{119}$$

Bedenkt man nun, daß die homogenen linearen Funktionen λ_r, μ_r, wenn x_r, y_r durch $d_r x_r$, $d_r y_r$ ersetzt werden, in $d_r\lambda_r$, $d_r\mu_r$ übergehen, so läßt sich diese letzte Gleichung zufolge (113) auch in der Form

$$F_r(d_r x_r,\ d_r y_r) = F_s F_t$$

darstellen, die wir früher in (74) erhalten haben, und die, wie schon bemerkt, mit dem Hauptsatze (11) in § 1 übereinstimmt. Die Gleichungen (118) dagegen enthalten eine wichtige Ergänzung zu diesem Transformationssatz, weil sie lehren, in welcher Weise hierbei die beiden Linearfaktoren von F_r sich transformieren, und dies ist von Bedeutung für die Art, in welcher nach Gauß die Formen F_s, F_t in die Transformation eintreten (vgl. den Schluß von § 2).

In ähnlicher Weise folgt aus (105), wenn man den Vektor δ_r auf die Darstellungen (109), (112) wirken läßt,

$$\begin{cases} \delta_r U = -U\sqrt{D}, & \delta_r V = V\sqrt{D}, \\ \delta_r\lambda_r = -\lambda_r\sqrt{D}, & \delta_r\mu_r = \mu_r\sqrt{D}, \end{cases} \tag{120}$$

und hieraus nach (113) wieder die Gleichung (104).

§ 7.

Es ist schon in § 1 bemerkt, daß die Diskriminante D der drei Formen F_1, F_2, F_3 eine homogene Funktion vierten Grades von den acht Konstanten α, β ist, welche nach § 4 zugleich die Koeffizienten der Form H sind. Ich will jetzt zum Schluß noch auf die beherrschende Stellung aufmerksam machen, welche diese Funktion D einnimmt, indem ich nachweise, daß aus ihren partiellen Derivierten auch die Koeffizienten der zu H adjungierten Form H' und die der drei Formen F_1, F_2, F_3 sich bilden lassen.

Nach § 4 sind α_0, β_0, α_r, β_r bzw. die Koeffizienten der Produkte $x_1x_2x_3$, $y_1y_2y_3$, $x_r y_s y_t$, $y_r x_s x_t$ in H, d. h. es ist

$$\alpha_0 = \frac{\partial^3 H}{\partial x_1\partial x_2\partial x_3}, \quad \beta_0 = \frac{\partial^3 H}{\partial y_1\partial y_2\partial y_3},$$

$$\alpha_r = \frac{\partial^3 H}{\partial x_r\partial y_s\partial y_t}, \quad \beta_r = \frac{\partial^3 H}{\partial y_r\partial x_s\partial x_t},$$

und wir wollen mit α_0', β_0', α_r', β_r' die entsprechenden Koeffizienten in der adjungierten Form H' bezeichnen. Für die letztere ergibt sich aus ihrer Definition (72) der Ausdruck

$$H' = d_r F_r = \frac{\partial F_r}{\partial x_r}\frac{\partial H}{\partial y_r} - \frac{\partial F_r}{\partial y_r}\frac{\partial H}{\partial x_r}$$

$$= (2A_r x_r + B_r y_r)\frac{\partial H}{\partial y_r} - (B_r x_r + 2C_r y_r)\frac{\partial H}{\partial x_r},$$

mithin wird

$$\frac{\partial H'}{\partial x_r} = 2A_r\frac{\partial H}{\partial y_r} - B_r\frac{\partial H}{\partial x_r}, \quad \frac{\partial H'}{\partial y_r} = B_r\frac{\partial H}{\partial y_r} - 2C_r\frac{\partial H}{\partial x_r},$$

und durch fortgesetzte Derivationen erhält man daher

$$(121)\qquad \begin{cases} \alpha_0' = 2A_r\beta_r - B_r\alpha_0, & \beta_0' = B_r\beta_0 - 2C_r\alpha_r, \\ \alpha_r' = 2A_r\beta_0 - B_r\alpha_r, & \beta_r' = B_r\beta_r - 2C_r\alpha_0. \end{cases}$$

Aus den in (2) angegebenen Ausdrücken für die Koeffizienten A_r, B_r, C_r der Form F_r folgt nun

$$\frac{\partial C_r}{\partial \alpha_0} = \frac{\partial A_r}{\partial \beta_0} = \frac{\partial C_r}{\partial \alpha_r} = \frac{\partial A_r}{\partial \beta_r} = 0,$$

$$\frac{\partial B_r}{\partial \beta_0} = \frac{\partial A_r}{\partial \alpha_r} = -\alpha_0, \quad \frac{\partial B_r}{\partial \alpha_0} = \frac{\partial C_r}{\partial \beta_r} = -\beta_0,$$

$$\frac{\partial A_r}{\partial \alpha_0} = \frac{\partial B_r}{\partial \beta_r} = -\alpha_r, \quad \frac{\partial C_r}{\partial \beta_0} = \frac{\partial B_r}{\partial \alpha_r} = -\beta_r,$$

mithin erhält man mit Rücksicht auf $D = B_r^2 - 4A_rC_r$ für die Koeffizienten von H' die Formeln

$$\alpha_0' = -2A_r\frac{\partial C_r}{\partial \beta_0} + B_r\frac{\partial B_r}{\partial \beta_0} = \frac{1}{2}\frac{\partial D}{\partial \beta_0},$$

$$\beta_0' = -B_r\frac{\partial B_r}{\partial \alpha_0} + 2C_r\frac{\partial A_r}{\partial \alpha_0} = -\frac{1}{2}\frac{\partial D}{\partial \alpha_0},$$

$$\alpha_r' = -2A_r\frac{\partial C_r}{\partial \beta_r} + B_r\frac{\partial B_r}{\partial \beta_r} = \frac{1}{2}\frac{\partial D}{\partial \beta_r},$$

$$\beta_r' = -B_r\frac{\partial B_r}{\partial \alpha_r} + 2C_r\frac{\partial A_r}{\partial \alpha_r} = -\frac{1}{2}\frac{\partial D}{\partial \alpha_r}.$$

Bezeichnet man daher mit (α, β) jedes der vier Paare (α_0, β_0), (α_1, β_1), (α_2, β_2), (α_3, β_3) und mit (α', β') das entsprechende Paar für die Form H', so wird

$$(122)\qquad \alpha' = \frac{1}{2}\frac{\partial D}{\partial \beta}, \quad \beta' = -\frac{1}{2}\frac{\partial D}{\partial \alpha}.$$

Hieraus erhält man für die beiden Paare (α_s', β_s'), (α_t', β_t'), indem man den Ausdruck $D = B_r^2 - 4A_rC_r$ beibehält und die Derivierten von A_r, B_r, C_r gemäß (2) bildet, die Ausdrücke

$$(123)\qquad \begin{cases} \alpha_s' = B_r\alpha_s - 2C_r\beta_t, & \beta_s' = 2A_r\alpha_t - B_r\beta_s, \\ \alpha_t' = B_r\alpha_t - 2C_r\beta_s, & \beta_t' = 2A_r\alpha_s - B_r\beta_t. \end{cases}$$

Bedient man sich der Bezeichnung für die allgemeine Komposition von rechteckigen, nach Zeilen und Spalten geordneten Größensystemen (Matrizen), so kann man die acht Gleichungen (121), (123) in

$$(124)\qquad \begin{pmatrix} B_r, & -2C_r \\ 2A_r, & -B_r \end{pmatrix}\begin{pmatrix} \beta_r, & \alpha_s, & \alpha_t, & \beta_0 \\ \alpha_0, & \beta_t, & \beta_s, & \alpha_r \end{pmatrix} = \begin{pmatrix} \beta_r', & \alpha_s', & \alpha_t', & \beta_0' \\ \alpha_0', & \beta_t', & \beta_s', & \alpha_r' \end{pmatrix}$$

zusammenfassen; permutiert man die Indizes r, s, t, so erhält man für jeden der acht Koeffizienten α', β' drei äußerlich verschiedene Ausdrücke, die alle aus (122) entspringen, wenn man D wie in (3) durch die Koeffizienten der Formen F_1 oder F_2 oder F_3 darstellt.

Hiermit ist gezeigt, daß die Koeffizienten der zu H adjungierten Form H' durch Derivierte erster Ordnung von D dargestellt werden; durch fortgesetzte Derivation erhält man für die Koeffizienten der quadratischen Formen F_1, F_2, F_3 die folgenden Ausdrücke

$$(125)\qquad \begin{cases} 6A_r = \dfrac{\partial^2 D}{\partial \beta_0 \partial \beta_r} - \dfrac{\partial^2 D}{\partial \alpha_s \partial \alpha_t}, & 6C_r = \dfrac{\partial^2 D}{\partial \alpha_0 \partial \alpha_r} - \dfrac{\partial^2 D}{\partial \beta_s \partial \beta_t}, \\ 6B_r = \dfrac{\partial^2 D}{\partial \alpha_s \partial \beta_s} + \dfrac{\partial^2 D}{\partial \alpha_t \partial \beta_t} - \dfrac{\partial^2 D}{\partial \alpha_r \partial \beta_r} - \dfrac{\partial^2 D}{\partial \alpha_0 \partial \beta_0}, \end{cases}$$

deren Analogie mit den Darstellungen (2) von $-C_r$, $-A_r$, $+B_r$ ersichtlich ist; die Ausführung der Rechnung mag aber dem Leser überlassen bleiben.

Das in (122) erhaltene Resultat reizt dazu, in dem von den sieben Paaren (α, β), (x_r, y_r) gebildeten, vierzehnfach ausgedehnten Raume einen Vektor δ einzuführen, welcher durch

$$(126)\qquad \delta\alpha = \alpha', \quad \delta\beta = \beta', \quad \delta x_r = \delta y_r = 0,$$

also durch

$$(127)\qquad \delta\varphi = \frac{1}{2}\sum^{(\alpha,\beta)}\left(\frac{\partial\varphi}{\partial\alpha}\frac{\partial D}{\partial\beta} - \frac{\partial\varphi}{\partial\beta}\frac{\partial D}{\partial\alpha}\right)$$

definiert wird, wo φ eine willkürliche Funktion bedeutet, und die Summe über alle vier Paare (α, β) auszudehnen ist. Da H eine homogene lineare Funktion der Größen α, β ist, so folgt aus (126) unmittelbar

$$(128)\qquad \delta H = H'.$$

Ersetzt man φ in (127) durch $\frac{\partial \varphi}{\partial x_r}$, $\frac{\partial \varphi}{\partial y_r}$, so folgt

$$\delta \frac{\partial \varphi}{\partial x_r} = \frac{\partial \delta \varphi}{\partial x_r}, \quad \delta \frac{\partial \varphi}{\partial y_r} = \frac{\partial \delta \varphi}{\partial y_r}, \tag{129}$$

d. h. der Vektor δ ist permutabel mit den Vektoren $\frac{\partial}{\partial x_r}$, $\frac{\partial}{\partial y_r}$; bedeutet daher ψ_r eine beliebige Funktion, welche frei von den beiden Variabeln x_r, y_r des Paares z_r ist, so hat $\delta \psi_r$ dieselbe Eigenschaft, und wenn ε_r irgend einen der vier in (54), (61), (79), (103) erklärten Vektoren d_r, e_r, d'_r, δ_r bedeutet, die alle nur auf das Paar z_r wirken, so folgt hieraus

$$(\delta, \varepsilon_r)\psi_r = \delta \varepsilon_r \psi_r - \varepsilon_r \delta \psi_r = 0,$$

weil $\varepsilon_r \psi_r = \varepsilon_r \delta \psi_r = 0$ ist. Um also einen solchen Vektor (δ, ε_r) vollständig zu bestimmen, braucht man nur noch die beiden Funktionen $(\delta, \varepsilon_r)x_r$ und $(\delta, \varepsilon_r)y_r$ zu ermitteln.

Beginnt man mit dem Vektor $\varepsilon_r = d_r$ und berücksichtigt (126), (128), (129), so erhält man

$$(\delta, d_r)x_r = \delta d_r x_r = \delta \frac{\partial H}{\partial y_r} = \frac{\partial \delta H}{\partial y_r} = \frac{\partial H'}{\partial y_r} = d'_r x_r,$$

$$(\delta, d_r)y_r = \delta d_r y_r = \delta\left(-\frac{\partial H}{\partial x_r}\right) = -\frac{\partial \delta H}{\partial x_r} = -\frac{\partial H'}{\partial x_r} = d'_r y_r,$$

und da zugleich $(\delta, d_r)\psi_r = 0 = d'_r \psi_r$ ist, so folgt

$$(\delta, d_r) = d'_r. \tag{130}$$

Verfährt man ähnlich mit dem Vektor $\varepsilon_r = e_r$, so ergibt sich, daß δ permutabel mit e_r, also auch mit $(e_s - e_r)$ ist, d. h. es ist

$$(\delta, e_r) = 0, \quad (\delta, e_s - e_r) = 0. \tag{131}$$

Wendet man nun den Satz (43) auf die drei Vektoren δ, d_r, d_s an und bedenkt, daß

$$(d_r, d_s) = F_t(e_s - e_r), \quad (d_s, \delta) = -d'_s, \quad (\delta, d_r) = d'_r$$

ist, so folgt zunächst

$$(\delta, F_t(e_s - e_r)) - (d_r, d'_s) + (d_s, d'_r) = 0;$$

zufolge (101) ist aber $(d_r, d'_s) = (d_s, d'_r)$, und da nach der in (45) angegebenen Regel

$$(\delta, F_t(e_s - e_r)) = F_t(\delta, e_s - e_r) + \delta F_t(e_s - e_r)$$

ist, wo das erste Glied rechts nach (131) verschwindet, so ist $\delta F_t(e_s - e_r) = 0$, und hieraus folgt

$$\delta F_t = 0; \quad \delta A_t = \delta B_t = \delta C_t = 0, \tag{132}$$

also auch

$$\delta D = 0, \tag{133}$$

was übrigens auch unmittelbar aus (127) folgt.

Läßt man jetzt den Vektor (130) auf F_r wirken, so wird

$$\delta d_r F_r - d_r \delta F_r = d'_r F_r, \quad \text{und da } d_r F_r = H', \ \delta F_r = 0, \ d'_r F_r = DH$$

ist, so folgt

$$\delta^2 H = \delta H' = DH, \tag{134}$$

mithin

$$\delta^2 \alpha = \delta \alpha' = D\alpha, \quad \delta^2 \beta = \delta \beta' = D\beta, \tag{135}$$

was sich auch aus (121) mit Rücksicht auf $\delta A_r = \delta B_r = \delta C_r = 0$ leicht ergeben würde.

Verfährt man endlich auf dieselbe Weise mit den Vektoren d'_r, δ_r, so erhält man, wie der Leser sofort finden wird,

$$(\delta, d'_r) = D d_r, \quad (\delta, \delta_r) = 0. \tag{136}$$

Erläuterungen zur vorstehenden Abhandlung.

Dedekind behandelt hier wieder die Komposition der quadratischen Formen, ein Problem, das er schon wiederholt in den Supplementen zu Dirichlets Zahlentheorie studiert hat. Die Bemerkung Dedekinds, daß jede bilineare Form die entsprechenden komponierbaren Formen bestimmt, hat schon Cayley (Journ. f. Math. **39** (1850), S. 14—15) gemacht. Arndt (Arch. f. Math. u. Phys. **15** (1850), S. 429—480) hat sich auch mit ähnlichen Fragen beschäftigt. L. E. Dickson (History of the theory of numbers, Bd. 3, S. 75) bemerkt: „Dedekind war offenbar nicht mit den Resultaten von Arndt und Cayley bekannt, indem er das Problem von neuem angriff und eine einfache und symmetrische Behandlungsweise entwickelte."

Eine übersichtliche Darstellung der Geschichte der Theorie der Komposition der quadratischen Formen findet man in dem eben erwähnten Buch von L. E. Dickson, Bd. 3, Kap. 3. Unter den wichtigsten neueren Arbeiten über die Komposition quadratischer Formen sollen die folgenden erwähnt werden: H. Weber, Gött. Nachr. 1907, S. 86—100. A. Speiser, Festschrift zu H. Weber, 1912, S. 375—395. H. Brandt, Journ. f. Math. **143** (1913), S. 106—127; **150** (1920), S. 1—46. Math. Zeitschr. **17** (1923), S. 153—160; Math. Ann. **91** (1924), S. 300—315.

Ore.

XXXIV.

Über den Zellerschen Beweis des quadratischen Reziprozitätssatzes.

[Festschrift Heinrich Weber zu seinem siebzigsten Geburtstag am 5. März 1912 gewidmet von Freunden und Schülern. Leipzig und Berlin 1912, S. 23—36.]

Das Lemma, auf welches Gauß seinen dritten und fünften Beweis des Reziprozitätssatzes gegründet hat, ist später der Ausgangspunkt für viele andere Beweise desselben Satzes geworden[1]). Unter allen diesen Beweisen scheint mir der einfachste der zu sein, welchen Chr. Zeller[2]) mir in einem Briefe vom 8. Juli 1872 mitgeteilt hat; dieser Brief schließt mit den durchaus zutreffenden Worten: „Man braucht also jene Hilfsgrößen nicht, welche bisher bei dem Beweise unseres Satzes verwendet worden sind und denselben umständlich gemacht haben.“ In der Tat vermeidet Zeller gänzlich die in dem dritten Beweise von Gauß eingeführten größten Ganzen $[x]$ und gelangt zum Ziele, indem er zwei neue Betrachtungen mit dem Lemma von Gauß verbindet. Einige Monate später hat Zeller (in dem Sitzungsberichte der Berliner Akademie vom 16. Dezember 1872) einen sehr ähnlichen Beweis veröffentlichen lassen, in welchem an Stelle der zweiten Betrachtung eine dritte tritt, wodurch aber die Einfachheit nach meiner Ansicht ein wenig gelitten hat. Mag nun diese Abänderung noch so geringfügig scheinen, so glaube ich doch Zellers Verdienst in ein helleres Licht zu rücken, wenn ich den wesentlichen Inhalt des genannten Briefes in freier Umarbeitung und geänderter Bezeichnung jetzt bekannt mache.

Hierzu ist es freilich nötig, die bekannten Tatsachen, auf denen das Lemma von Gauß beruht, kurz in Erinnerung zu bringen, und

[1]) Eine sehr eingehende Darstellung dieser Beweise findet man bei P. Bachmann (Niedere Zahlentheorie, erster Teil, 1902, Seite 212—286).

[2]) Damals Pfarrer und Bezirks-Schulinspektor zu Weiler bei Schorndorf (Württemberg), später Seminarrektor in Markgröningen, wo er im Jahre 1899 als Oberschulrat verstorben ist.

zwar in der Form, daß unter dem Reste einer ganzen Zahl in bezug auf einen ungeraden Modulus $p > 1$ immer ihr absolut kleinster, also zwischen den Grenzen $\pm\frac{p}{2}$ gelegener Rest verstanden werden soll.

Läßt man nun, wenn q relative Primzahl zu p ist, den Faktor h alle ganzen Zahlen

$$1, 2, \cdots, \frac{p-1}{2}$$

des Intervalles $0 < h < \frac{p}{2}$ durchlaufen, und bildet man die Reste a und die Quotienten y für die Produkte

$$hq = a + yp \equiv a \pmod{p}, \tag{1}$$

so sind diese Reste a alle von Null und auch voneinander verschieden, weil zwei verschiedene Faktoren h immer zwei inkongruente Produkte hq erzeugen; da ferner auch die Summe von zwei Produkten hq niemals durch p teilbar ist, so sind sogar die absoluten Werte aller Reste a verschieden und stimmen folglich in ihrem Komplex mit den Faktoren h völlig überein; jeder Faktor h ist auch der absolute Wert von einem und nur einem Reste a. Bedeutet daher P das Produkt aller Faktoren h, und m die Anzahl derjenigen Reste a, welche negativ sind, so ist $P(-1)^m$ das Produkt aller Reste a, und durch Multiplikation aller Kongruenzen (1) ergibt sich

$$Pq^{\frac{p-1}{2}} \equiv P(-1)^m \pmod{p}.$$

Wird jetzt angenommen, daß die ungerade Zahl p eine Primzahl ist, so ist das Produkt P nicht teilbar durch p, mithin

$$q^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}.$$

Das nach Euler benannte Kriterium besteht bekanntlich darin, daß die Potenz linker Hand $\equiv +1$ oder $\equiv -1 \pmod{p}$ ist, je nachdem q quadratischer Rest oder Nichtrest von p ist, und wenn man diese positive oder negative Einheit nach Legendre durch das Symbol $\left(\frac{q}{p}\right)$ bezeichnet, so kann das Resultat der vorhergehenden Betrachtung durch die Gleichung

$$\left(\frac{q}{p}\right) = (-1)^m$$

ausgedrückt werden[1]). Hierin besteht das obenerwähnte Lemma von Gauß.

Ist q ebenfalls eine ungerade positive Primzahl, so wird der zu beweisende Reziprozitätssatz bekanntlich durch die Gleichung

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

ausgedrückt, welche jetzt mit Hilfe des Lemma von Gauß eine einfachere Gestalt annimmt. Durchläuft nämlich der Faktor k alle ganzen Zahlen

$$1, 2, \cdots, \frac{q-1}{2}$$

des Intervalls $0 < k < \frac{q}{2}$, und bildet man wie in (1) die Reste b und die Quotienten x für die Produkte

$$kp = b + xq \equiv b \pmod{q}, \tag{2}$$

so sind die absoluten Werte der Reste b wieder alle verschieden, und ebenso wird

$$\left(\frac{p}{q}\right) = (-1)^n,$$

wo n die Anzahl derjenigen Reste b bedeutet, die negativ sind; hierdurch verwandelt sich der zu beweisende Satz offenbar in die Kongruenz

$$m + n \equiv \frac{p-1}{2}\frac{q-1}{2} \pmod{2}, \tag{3}$$

welche auch so ausgesprochen werden kann: Die Summe $m + n$ ist stets und nur dann ungerade, wenn $p \equiv q \equiv -1 \pmod{4}$ ist.

Nachdem diese Umformung des Reziprozitätssatzes, welche die Grundlage für den dritten und fünften Beweis von Gauß bildet, in Erinnerung gebracht ist, will ich jetzt die beiden Hauptpunkte hervorheben, auf denen Zellers Beweis beruht. Hierbei setze ich lediglich voraus, es seien p, q relative[2]) Primzahlen, beide ungerade, positiv

[1]) E. Schering hat bemerkt, daß dieselbe auch für das von Jacobi verallgemeinerte Symbol von Legendre gilt (Monatsbericht der Berliner Akademie vom 22. Juni 1876).

[2]) Der folgende Beweis gilt daher zufolge der vorhergehenden Anmerkung auch für den verallgemeinerten Reziprozitätssatz.

und > 1; auch soll (wie in der Berliner Darstellung) p die kleinere dieser beiden Zahlen bedeuten.

Die erste Bemerkung Zellers geht aus einer Vergleichung der beiden Reihen (1) und (2) hervor und besteht darin, daß alle Gleichungen (1) aus ebenso vielen Gleichungen (2) nur durch Umsetzung ihrer Glieder entspringen. Ist z. B. $p = 11$, $q = 27$, so erhält man die Reihe (2) und daraus die Reihe (1) in der folgenden Tabelle:

$1 \cdot p = +11 + 0 \cdot q$	
$2 \cdot p = -5 + 1 \cdot q$	$1 \cdot q = +5 + 2 \cdot p$
$3 \cdot p = +6 + 1 \cdot q$	
$4 \cdot p = -10 + 2 \cdot q$	
$5 \cdot p = +1 + 2 \cdot q$	$2 \cdot q = -1 + 5 \cdot p$
$6 \cdot p = +12 + 2 \cdot q$	
$7 \cdot p = -4 + 3 \cdot q$	$3 \cdot q = +4 + 7 \cdot p$
$8 \cdot p = +7 + 3 \cdot q$	
$9 \cdot p = -9 + 4 \cdot q$	
$10 \cdot p = +2 + 4 \cdot q$	$4 \cdot q = -2 + 10 \cdot p$
$11 \cdot p = +13 + 4 \cdot q$	
$12 \cdot p = -3 + 5 \cdot q$	$5 \cdot q = +3 + 12 \cdot p$
$13 \cdot p = +8 + 5 \cdot q$	

Um diese Beziehung zwischen den beiden Reihen allgemein zu beweisen, setze man jede Gleichung (1) in die Form

$$yp = -a + hq;$$

aus der Definition der Zahlen a, h und aus unserer Annahme $p < q$ folgt

$$-\frac{p}{2} < -a < +\frac{p}{2}, \quad p < hq < \frac{p}{2}q,$$

hieraus durch Addition und Division durch p

$$+\frac{1}{2} < y < \frac{q+1}{2},$$

mithin auch $0 < y < \frac{q}{2}$. Also ist jeder in der Reihe (1) auftretende Quotient y auch einer der Faktoren k in der Reihe (2), und da jede Zahl $-a$ zwischen den Grenzen $\pm\frac{p}{2}$, also gewiß auch zwischen $\pm\frac{q}{2}$ liegt, so ist $-a$ der diesem Faktor $k = y$ entsprechende Rest b des Produktes kp in (2), und der Quotient $x = h$, w. z. b. w.

Mit diesen Resten $b = -a$, deren Anzahl $= \frac{p-1}{2}$ ist, sind aber alle zwischen den Grenzen $\pm\frac{p}{2}$ liegenden Reste b in (2) erschöpft, weil, wie oben bemerkt, die absoluten Werte aller Reste b voneinander verschieden sind. Die Anzahl m der negativen Reste a in (1) ist daher zugleich die Anzahl derjenigen positiven Reste b in (2), welche $< \frac{p}{2}$ sind; fügt man zu diesen m positiven Resten b noch alle n negativen Reste b hinzu, so ist die Summe $m+n$ die Anzahl aller Reste b in (2), welche in dem Intervalle

$$(4) \qquad -\frac{q}{2} < b < +\frac{p}{2}$$

liegen.

In dem obigen Beispiel $p = 11$, $q = 27$, wo $m = 2$, $n = 5$, liegen im Intervalle (4) die sieben Reste $b = -10, -9, -5, -4, -3, +1, +2$; die übrigen sechs Reste sind $b = 6, 7, 8, 11, 12, 13$.

Nachdem hiermit die Bedeutung der Summe $m+n$ für die Reihe (2) festgestellt ist, beantwortet Zeller die Hauptfrage nach ihrer Parität, ob sie gerade oder ungerade ist, durch eine zweite Betrachtung, deren einfacher Grundgedanke in Folgendem besteht. Wenn es in einem endlichen System von Elementen b ein Gesetz gibt, das jedem b ein bestimmtes Element b' desselben Systems zuordnet, und zwar so symmetrisch, daß umgekehrt $(b')' = b$ wird, so hat die Anzahl aller b offenbar dieselbe Parität wie die Anzahl der Fälle, in denen $b' = b$ ist. Für unsere Untersuchung, wo es sich um die Reste b in der Reihe (2) handelt, gewinnt Zeller eine solche Verteilung in symmetrische Paare b, b' auf folgende Weise.

Durchläuft der Faktor k alle seine Werte, und setzt man

$$(5) \qquad k + k' = \frac{q+1}{2},$$

so durchläuft k' offenbar dieselben Werte in umgekehrter Folge, und jedem solchen Faktorenpaar k, k' entspricht ein Restepaar

$$b \equiv kp, \quad b' \equiv k'p \pmod{q}.$$

Da jeder Rest b durch einen und nur einen Faktor k erzeugt wird, so ist durch b vermöge (5) auch der Faktor k', mithin auch der zugehörige Rest b' vollständig bestimmt, und aus der Symmetrie der Gleichung (5) in bezug auf k, k' folgt, daß umgekehrt $(b')' = b$ ist.

Durch Addition der beiden vorstehenden Kongruenzen mit Rücksicht auf (5) folgt die Kongruenz

$$b + b' \equiv \frac{q+1}{2} p \pmod{q},$$

welche die gegenseitige Abhängigkeit der beiden, ein symmetrisches Paar bildenden Reste b, b' vollständig ausdrückt. Dies läßt sich aber noch genauer verfolgen. Zufolge der Definition der Reste b, b' liegt einerseits ihre Summe $b + b'$ gewiß zwischen den Grenzen $\pm q$; andererseits ist das ihr kongruente Produkt

$$(6) \qquad \frac{q+1}{2} p = \frac{p-q}{2} + \frac{p+1}{2} q = \frac{p+q}{2} + \frac{p-1}{2} q,$$

mithin

$$b + b' \equiv \frac{p-q}{2} \equiv \frac{p+q}{2} \pmod{q},$$

und da zufolge unserer Annahme $p < q$ die beiden Zahlen $\frac{p \mp q}{2}$ ebenfalls zwischen den Grenzen $\pm q$ liegen, so ist

$$\text{entweder } b + b' = \frac{p-q}{2}$$

$$\text{oder } b + b' = \frac{p+q}{2}.$$

Im ersten Fall sind beide Reste b, b' algebraisch $< \frac{p}{2}$; wäre nämlich einer derselben, z. B. $b' > \frac{p}{2}$, so wäre der andere $b < -\frac{q}{2}$, was der Definition von b widerspricht. Im zweiten Fall sind beide Reste $> \frac{p}{2}$; wäre nämlich z. B. $b' < \frac{p}{2}$, so wäre $b > \frac{q}{2}$, was abermals unmöglich ist. Mithin sondern sich die beiden Fälle in folgender Weise scharf voneinander:

$$(7) \qquad \text{I.} \quad b + b' = \frac{p-q}{2}, \; -\frac{q}{2} < b, b' < +\frac{p}{2},$$

$$(8) \qquad \text{II.} \quad b + b' = \frac{p+q}{2}, \; +\frac{p}{2} < b, b' < +\frac{q}{2},$$

und zugleich leuchtet ein, daß b' in jedem dieser beiden Intervalle dieselben Werte wie b, aber in umgekehrter Größenfolge durchläuft.

Wir betrachten jetzt nur noch das erste Intervall (7), welches identisch mit dem obigen in (4) ist und folglich genau $m+n$ Reste b enthält. Diese Summe $m+n$ wird daher immer gerade sein, wenn jedes symmetrische Restpaar in (7) aus zwei ungleichen Resten b, b' besteht. Da ferner der Fall $b = b'$ immer und nur dann eintrifft, wenn zugleich $k = k'$ ist, so geschieht dies in (7) gewiß und nur in dem einzigen Fall, wenn gleichzeitig

$$b = b' = \frac{p-q}{4},\ k = k' = \frac{q+1}{4},$$

also

$$p \equiv q \equiv -1 \pmod 4 \tag{9}$$

ist, und da alle anderen, etwa in (7) enthaltenen Restpaare aus zwei ungleichen Resten b, b' bestehen, so ist die Summe $m+n$ in diesem und nur in diesem Falle (9) ungerade.

Hiermit ist die Kongruenz (3), also auch der Reziprozitätssatz wirklich bewiesen.

Zur Erläuterung bemerke ich noch folgendes. Ist $q \equiv 1 \pmod 4$, so folgt aus (5), daß der Fall $k = k'$ niemals eintreten kann; es wird daher jedes Restpaar sowohl in (7) wie in (8) aus zwei ungleichen Resten b, b' bestehen, und folglich ist sowohl die Anzahl $m+n$ der Reste b in (7), wie die Anzahl $\frac{q-1}{2} - m - n$ der Reste b in (8) gerade. Ist dagegen $q \equiv -1 \pmod 4$, so tritt der Fall $k = k'$, also auch $b = b'$, gewiß einmal ein, nämlich in (7) oder (8), je nachdem $p \equiv -1$ oder $\equiv +1 \pmod 4$ ist.

In dem obigen Beispiel $p = 11$, $q = 27$, wo $m = 2$, $n = 5$, ordnen sich die sieben Reste des Intervalles (7) in die vier Paare

$$(b, b') = (-10, +2), (-9, +1), (-5, -3), (-4, -4)$$

mit der Summe $b + b' = -8$, und die sechs Reste des Intervalles (8) zerfallen in die drei Paare

$$(b, b') = (6, 13), (7, 12), (8, 11)$$

mit der Summe $b + b' = +19$. Da dieses Beispiel den Bedingungen (9) genügt, so entspricht dem Faktor $k = k' = 7$ das im Intervall (7) liegende, aus zwei gleichen Resten bestehende Paar $b = b' = -4$.

Im vorstehenden habe ich Zellers scharfsinnigen Beweis (auf Grund des Briefes vom 8. Juli 1872) etwas ausführlicher dargestellt, weil er mit geringstem Aufwande von Rechnung eine sehr deutliche

Einsicht in den Bau und den Zusammenhang der beiden Reihen (1), (2) gibt und deshalb besonders geeignet zum Vortrage vor Anfängern erscheint. Um ihn mit der sehr kurz gefaßten Berliner Darstellung (vom 16. Dezember 1872) bequem zu vergleichen, ändere ich die in der letzteren gewählte Bezeichnung so ab, daß sie mit unserer obigen übereinstimmt, und außerdem will ich zur Abkürzung die Anzahl der Reste b innerhalb des Intervalles

$$-\frac{q}{2} < b < -\frac{p}{2} \tag{10}$$

mit t bezeichnen. Durch eine Betrachtung, die nahezu mit dem ersten Teile des obigen Beweises übereinstimmt, ergibt sich zunächst die Zerlegung

$$m+n = \frac{p-1}{2} + t, \tag{11}$$

und handelt sich es daher jetzt noch um die Frage, wann die Anzahl t gerade oder ungerade ist. Dazu dient wieder eine Verteilung der Reste b in symmetrische Paare, die aber von der obigen, durch (5) bestimmten wesentlich abweicht und deshalb hier näher behandelt werden soll. Schließt man in (2) den größten Faktor $k = \frac{q-1}{2}$ aus, dem zufolge (6) nach Subtraktion von p der positive Rest $b = \frac{q-p}{2}$ entspricht, und setzt man

$$k + k'' = \frac{q-1}{2}, \tag{12}$$

so durchläuft k'' dieselben $\frac{q-3}{2}$ Faktoren wie k, und jedes Paar von Resten $b \equiv kp$, $b'' \equiv k''p \pmod q$ liefert eine zwischen den Grenzen $\pm q$ liegende Summe

$$b + b'' \equiv \frac{q-1}{2}\, p \equiv -\frac{p+q}{2} \equiv \frac{q-p}{2} \pmod q.$$

Verfährt man ähnlich wie oben, so erhält man wieder zwei scharf getrennte Intervalle

$$\text{III.}\quad b + b'' = -\frac{p+q}{2};\ -\frac{q}{2} < b,\ b'' < -\frac{p}{2}$$

$$\text{IV.}\quad b + b'' = +\frac{q-p}{2};\ -\frac{p}{2} < b,\ b'' < +\frac{q}{2},$$

in denen b'' immer dieselben Werte wie b durchläuft. Da das Intervall III mit dem in (10) identisch ist und folglich t Reste b enthält (weil der einzige ausgeschlossene Rest $b = \frac{q-p}{2}$ außerhalb dieses Intervalles liegt), so ergibt sich durch deren Verteilung in symmetrische Paare b, b'', daß diese Anzahl t stets und nur dann ungerade ist, wenn der Fall

$$k = k'' = \frac{q-1}{4},\ b = b'' = -\frac{p+q}{4}$$

eintritt, was immer und nur dann geschieht, wenn $q \equiv 1$, $p \equiv -1$ (mod. 4) ist. Durch Kombination dieses Resultates mit der obigen Zerlegung (11) gelangt schließlich die Berliner Darstellung, indem sie die einzelnen Fälle der Reste von p, q (mod. 4) durchgeht, ebenfalls zu dem Endergebnis, daß die Summe $m + n$ dann und nur dann ungerade ist, wenn $p \equiv q \equiv -1$ (mod. 4) ist, w. z. b. w.

Aus mehreren Gründen verdient wohl der frühere Beweis den Vorzug vor diesem zweiten. Da der Charakter der Summe $m + n$ (mod. 2) das einzige Ziel der Untersuchung bildet, so erscheint ihre Zerlegung (11) in zwei Bestandteile von vornherein als ein Umweg, der sich am Schluß nochmals fühlbar macht; außerdem ist die hier benutzte, durch (12) bestimmte Verteilung der Reste b in symmetrische Paare weniger einfach als die frühere, schon weil sie den Ausschluß eines Faktors k und des entsprechenden Restes b erfordert.

Als Zeller mir seinen Beweis mitteilte, kannte er den dritten Beweis von Gauß nur in der schon vereinfachten Darstellung, wie sie sich in §§ 43, 44 der Vorlesungen über Zahlentheorie von Dirichlet (zweite Auflage 1871) findet. In meiner Antwort (vom 13. Juli 1872) drückte ich ihm meine Freude über seinen Beweis aus, der so geradenwegs auf das Ziel zusteuert, und fügte eine kurze Darstellung des fünften Beweises von Gauß hinzu, der ihm augenscheinlich noch unbekannt war. Dies hat Zeller veranlaßt, mir noch einmal zu schreiben (am 7. Oktober 1872); auch in diesem Briefe findet sich noch keine Spur von der eben besprochenen zweiten Symmetrie der Reihe (2), die den Nerv des Beweises in der Berliner Darstellung bildet; er enthält aber noch zwölf Formeln, die von gewissen Summen der Reste a, b und der Quotienten x, y in den Reihen (1), (2) handeln und damals, wie ich glaube, noch unbekannt waren. Diese

Formeln, deren Beweise Zeller zum Teil andeutet, sind eigentlich nur Kombinationen von sechs verschiedenen Relationen, die ich jetzt im Anschluß an den ersten Beweis von Zeller noch ableiten will. Hierbei bezeichne ich die Reste a, b bzw. mit a_1, b_1 oder mit a_2, b_2, je nachdem sie negativ oder positiv sind, und die Summen der Zahlen

$$h,\ a,\ a_1,\ a_2,\ y;\ k,\ b,\ b_1,\ b_2,\ x$$

bzw. mit

$$H,\ A,\ A_1,\ A_2,\ Y;\ K,\ B,\ B_1,\ B_2,\ X.$$

Da die absoluten Werte $-a_1$, a_2 aller Reste a mit den Faktoren h, ebenso die absoluten Werte $-b_1$, b_2 aller Reste b mit den Faktoren k übereinstimmen, so erhält man zunächst

$$(13)\qquad -A_1 + A_2 = H = \frac{1}{2}\,\frac{p+1}{2}\,\frac{p-1}{2},$$

$$(14)\qquad -B_1 + B_2 = K = \frac{1}{2}\,\frac{q+1}{2}\,\frac{q-1}{2}.$$

Zwei neue Gleichungen folgen aus der Betrachtung der beiden Intervalle (7), (8). Während die $m + n$ Reste b in (7) aus den n negativen Resten b_1 und den m positiven Zahlen $-a_1$ bestehen, so verbleiben nach Entfernung der letzteren aus den Resten b_2 die $\frac{q-1}{2} - m - n$ Reste b in (8), und da b' in jedem der beiden Intervalle dieselben Werte wie b durchläuft, so folgt durch Summation

$$(15)\qquad 2\,(B_1 - A_1) = \frac{p-q}{2}\,(m+n),$$

$$(16)\qquad 2\,(B_2 + A_1) = \frac{p+q}{2}\left(\frac{q-1}{2} - m - n\right).$$

Durch Auflösung dieser vier Gleichungen ergibt sich

$$(17)\qquad -4\,A_1 = p(m+n) - \frac{p-1}{2}\,\frac{q-1}{2},$$

$$(18)\qquad -4\,B_1 = q(m+n) - \frac{p-1}{2}\,\frac{q-1}{2},$$

$$(19)\qquad +4\,A_2 = \frac{2p+q+1}{2}\,\frac{p-1}{2} - p\,(m+n),$$

$$(20)\qquad +4\,B_2 = \frac{2q+p+1}{2}\,\frac{q-1}{2} - q\,(m+n),$$

woraus auch noch

$$(21) \qquad 2A = 2(A_1 + A_2) = \frac{p+q}{2}\,\frac{p-1}{2} - p(m+n),$$

$$(22) \qquad 2B = 2(B_1 + B_2) = \frac{p+q}{2}\,\frac{q-1}{2} - q(m+n)$$

folgt.

Es leuchtet ein, daß aus jeder dieser Formeln auch die Kongruenz (3), also der Reziprozitätssatz folgt; außerdem will ich bemerken, daß diese Kongruenz durch die schärfere

$$(23) \qquad m+n \equiv -\frac{p-1}{2}\,\frac{q-1}{2} \pmod 4$$

ersetzt werden kann, die man leicht erhält, wenn man z. B. die Gleichung (17) mit p multipliziert und bedenkt, daß $p^2 \equiv 1$, also $p(p-1) \equiv -(p-1) \pmod 8$ ist.

Besonders hervorzuheben ist aber, daß alle diese Formeln, obwohl sie auf der ausdrücklichen Annahme $p < q$ beruhen, augenscheinlich auch für die entgegengesetzte Annahme $p > q$ gelten, weil die Ausdrücke für B_1, B_2 und B aus denen für A_1, A_2 und A durch gleichzeitige Vertauschung von p mit q (und von m mit n) hervorgehen.

Um endlich die Summen X, Y der Quotienten x, y ebenfalls durch p, q, m, n auszudrücken, kann man verschiedene Wege einschlagen. Da die Ausdrücke für H, A, K, B schon bekannt sind, so liegt es nahe, hierzu die beiden Gleichungen

$$(24) \qquad Hq = A + Yp, \quad Kp = B + Xq$$

zu benutzen, die aus (1), (2) durch Summation entstehen, und zufolge der eben hervorgehobenen Bemerkung genügt es, nur eine der beiden Summen, z. B. X zu berechnen, weil hieraus die andere Y durch Vertauschung von p mit q hervorgehen muß. Aus (14) und (22) folgt nun

$$2(Kp - B) = \frac{q+1}{2}\,p\,\frac{q-1}{2} - \frac{p+q}{2}\,\frac{q-1}{2} + q(m+n)$$

$$= \left(\frac{p-1}{2}\,\frac{q-1}{2} + m + n\right) q,$$

und da die in der Klammer rechts enthaltene Summe bei Vertauschung von p mit q ungeändert bleibt, so folgt aus (24) die Doppelgleichung

$$(25) \qquad 2X = 2Y = \frac{p-1}{2}\,\frac{q-1}{2} + m + n,$$

worin abermals der Reziprozitätssatz enthalten ist. Zugleich ergibt sich aus der Kongruenz (23), daß die Summe $X = Y$ stets gerade ist.

Ein anderer Weg, die Summe X zu bestimmen, ergibt sich aus der durch (5) bestimmten Verteilung der Reste b in symmetrische Paare. Bezeichnet man mit x, x' die den Faktoren k, k' entsprechenden Quotienten, so ist

$$kp = b + xq, \quad k'p = b' + x'q,$$

also

$$(b + b') + (x + x')q = \frac{q+1}{2}\,p,$$

und aus (6), (7), (8) folgt

$$x + x' = \frac{p+1}{2} \text{ im Intervalle (7)},$$

$$x + x' = \frac{p-1}{2} \text{ im Intervalle (8)}.$$

Da nun x' sowohl in (7) wie in (8) dieselben Werte wie x durchläuft, deren Anzahl bzw. $m+n$ und $\frac{q-1}{2} - m - n$ ist, so erhält man im ganzen

$$2X = \frac{p+1}{2}(m+n) + \frac{p-1}{2}\left(\frac{q-1}{2} - m - n\right),$$

was mit (25) übereinstimmt.

Hiermit ist das Wesentliche der Formeln erschöpft, die Zeller mir in seinem zweiten Briefe (vom 7. Oktober 1872) mitgeteilt hat, wo er auch beiläufig bemerkt, daß die Größen X, $X-n$, $X-m$ bzw. mit den auf ganz andere Weise definierten Anzahlen α, β, γ im fünften Beweise von Gauß übereinstimmen (wo die Zeichen m, M, n, N durch die ihnen hier entsprechenden p, q, m, n zu ersetzen sind); doch wird der Zusammenhang zwischen den beiden verschiedenen Definitionen nicht untersucht.

Die Gleichheit der beiden Quotientensummen X, Y ist hier auf einem Wege erkannt, der alle früheren Resultate voraussetzt. Diese Gleichheit besteht, wie ich noch bemerken will, selbst dann, wenn die beiden ungeraden Zahlen p, q irgendeinen gemeinsamen Teiler haben; der kürzeste Weg, sie zu beweisen, scheint der folgende zu sein, wobei es auch gleichgültig bleibt, welche der Zahlen p, q die

kleinere ist. Läßt man die Faktoren h, k alle ihre Werte durchlaufen, so kann die Anzahl α der Fälle, in denen die Produktsumme

$$hq + kp > \frac{pq}{2}$$

wird, auf zwei verschiedene Arten bestimmt werden. Wählt man zuerst einen bestimmten Faktor k und setzt $kp = b + xq$ wie in (2), so findet man leicht, daß dieser Quotient x zugleich die Anzahl aller derjenigen Faktoren h ist, welche für diesen Wert k der vorstehenden Forderung genügen, und hieraus folgt offenbar $\alpha = X$. Wählt man aber zuerst einen bestimmten Faktor h und setzt $hq = a + yp$ wie in (1), so erhält man auf dieselbe Weise die Antwort $\alpha = Y$; mithin ist $X = Y$, w. z. b. w.

Aus dem Nachlaß.

Die folgenden aus dem Nachlaß publizierten Stücke haben zum großen Teil neben dem historischen Interesse auch solches durch Auffassung und Methode, wenn auch die Resultate unterdes unabhängig wiedergefunden sind. Es handelt sich um fertige oder fast fertige Ausarbeitungen; auf die Publikation von Unausgearbeitetem konnte um so eher verzichtet werden, als Dedekind in den folgenden Briefen an Frobenius davon ein viel klareres Bild gegeben hat, als es der Nachlaß bot.

Der Nachlaß bestand aus etwa 50 Mappen, Dedekind hatte alles und jedes aufgehoben; es ist also nicht ausgeschlossen, daß sich gelegentlich noch etwas zur Publikation Geeignetes findet. Als historisch interessant ist vielleicht noch zu erwähnen eine wohl unmittelbar an die ersten Vorlesungen anschließende Darstellung der Galoisschen Theorie; oder auch eine sehr ausführliche, aus früher Zeit stammende Darstellung der Riemannschen Geometrie, aus der in die Riemann-Ausgabe (Lateinische Preisarbeit) nur kurze Auszüge durch Weber übernommen wurden. **Noether.**

XXXV.

Allgemeine Sätze über Räume.

§ 1.

Ein System von Punkten $p, p' \cdots$ bildet einen Körper, wenn für jeden Punkt p desselben sich eine Länge δ von der Beschaffenheit angeben läßt, daß alle Punkte, deren Abstand von p kleiner als δ ist, ebenfalls dem System P angehören. Die Punkte $p, p' \cdots$ liegen innerhalb P.

§ 2.

Ist P' ein Körper, dessen sämtliche Punkte auch Punkte des Körpers P sind, so heißt P' ein Teil von P.

§ 3.

Satz. Alle Punkte, deren Abstand von einem festen Punkte p kleiner als eine gegebene Länge δ ist, bilden einen Körper (der Kugel heißt; p heißt der Mittelpunkt, δ der Durchmesser desselben).

Beweis. Ist $pp' < \delta$, so wähle man $\delta' < \delta - pp'$; so sind alle Punkte p'', für welche $p'p'' < \delta'$ ist, auch solche Punkte p'', für welche $pp'' < \delta$ ist (weil $pp'' \leqq pp' + p'p''$).

§ 4.

Ist P ein Körper und m ein Punkt, um welchen sich eine Kugel beschreiben läßt, deren sämtliche Punkte nicht innerhalb P liegen, so sagt man, der Punkt m liege außerhalb P.

§ 5.

Satz. Ist P ein Körper, und existiert wenigstens ein Punkt m außerhalb P, so gibt es auch unendlich viele solche Punkte außerhalb P, und dieselben bilden einen Körper.

Beweis. Da m außerhalb P liegt, so gibt es eine um m beschriebene Kugel K, deren sämtliche Punkte m' nicht innerhalb P liegen. Alle diese Punkte m' liegen außerhalb P; denn ist δ der Halbmesser von K, und also $mm' < \delta$, so beschreibe man um m' mit einem Halbmesser $\delta' < \delta - mm'$ eine Kugel K', so bildet K' einen Teil von K; also liegt m' (nach § 4) außerhalb P. Daß das System M aller außerhalb P liegenden Punkte m einen Körper bildet, folgt auf dieselbe Weise.

§ 6.

Ist P ein Körper und π ein Punkt, welcher weder innerhalb P noch außerhalb P liegt, so heißt π ein Grenzpunkt von P.

§ 7.

Ist P ein Körper und Π das System aller Grenzpunkte π von P (wenn überhaupt solche vorhanden), so heißt Π die Begrenzung von P.

§ 8.

Satz. Liegen sämtliche Punkte eines Körpers P' nicht innerhalb eines Körpers P, so liegen sie auch sämtlich außerhalb P.

Beweis. Es sei m' ein beliebiger Punkt von P'; so läßt sich um m' eine Kugel beschreiben, deren sämtliche Punkte innerhalb P', also nicht innerhalb P liegen. Nach § 4 liegt m' außerhalb P.

§ 9.

Satz. Ein System Π' von Punkten π, welche sämtlich Grenzpunkte eines Körpers P sind, kann keinen Körper bilden.

Beweis. Die Punkte π von Π' liegen (nach § 6) sämtlich nicht innerhalb von P. Wäre Π' ein Körper, so lägen alle Punkte π von Π' (nach § 8) außerhalb P. Weil aber die Punkte π von Π' sämtlich Grenzpunkte von P sind, ist dies (nach § 6) unmöglich.

Erläuterungen zur vorstehenden Abhandlung.

Diese ersten Begriffe der Punktmengenlehre — eine Weiterführung findet sich in dem nächsten Stück — werden des historischen Interesses halber wiedergegeben. Dedekind sagt darüber in einem Brief an Cantor (vom 19. Januar 1879, über Invarianz der Dimension):

„Bei einer Publikation würde ich es für wünschenswert halten, wenn die Namen oder Kunstausdrücke der Mannigfaltigkeitslehre (beiläufig gesagt, ich würde dem ebenfalls Riemannschen Wort „Gebiet“ seiner Kürze halber entschieden den Vorzug vor dem schwerfälligen Worte „Mannigfaltigkeit“ geben) recht genau definiert würden; es wäre sehr verdienstlich, wenn diese ganze „Gebietslehre“ ab ovo dargestellt würde, ohne die geometrische Anschauung zuzuziehen; und dabei müßte z. B. der Begriff einer von dem Punkte a nach dem Punkte b innerhalb des Gebietes G stetig führenden Linie recht bestimmt und deutlich definiert werden. Die Definitionen von Netto*) (dessen Abhandlung mir sehr wohl gefällt, und dessen Beweis, wie ich glaube, mit einigen Modifikationen ganz zutreffend wird) enthalten einen guten Keim, aber sie scheinen mir der Vereinfachung und zugleich einer Vervollständigung fähig. Ich würde mir ein solches Urteil nicht erlauben, wenn ich nicht vor vielen Jahren, als ich noch die Dirichletsche Potentialvorlesung herausgeben und dabei das sogenannte Dirichletsche Prinzip strenger begründen wollte, mich schon recht viel mit solchen Fragen beschäftigt hätte. Ich habe einige solche Definitionen, die mir eine recht gute Grundlage zu geben scheinen; aber ich habe später die ganze Sache liegen lassen, und könnte für den Augenblick nur Unvollständiges geben, da ich durch die Umarbeitung der Dirichletschen Zahlentheorie ganz in Anspruch genommen bin.“

Noether.

*) Crelle 1878.

XXXVI.

Beweis und Anwendungen eines allgemeinen Satzes über mehrfach ausgedehnte stetige Gebiete.

In meiner Schrift „Stetigkeit und irrationale Zahlen“ (§ 5, IV), welche im Jahre 1872 erschienen und kürzlich unverändert wieder abgedruckt ist, habe ich den Beweis desjenigen Prinzips veröffentlicht, welches ich schon seit dem Herbst 1858 als eine sichere und zugleich einfache Grundlage für die Infinitesimal-Analysis und für die Untersuchung aller stetigen Gebiete erkannt und auf die wichtigsten dahingehörigen Fragen immer mit dem gewünschten Erfolg angewandt hatte. Das Prinzip ist auszusprechen: Zerfallen alle reellen Zahlen in zwei Klassen von der Art, daß jede Zahl der ersten Klasse algebraisch kleiner ist als jede Zahl der zweiten Klasse, so gibt es entweder in der ersten Klasse eine größte, oder in der zweiten Klasse eine kleinste Zahl.

Daß außer mir noch andere Mathematiker, insbesondere Weierstraß und G. Cantor, sich mit solchen Fragen beschäftigten, habe ich zuerst durch die Veröffentlichung einer Abhandlung von Heine (Die Elemente der Funktionenlehre, Crelles Journal, Bd. 74) im Jahre 1872 erfahren. Seitdem ist bekanntlich dieser Gegenstand in mehreren verdienstlichen Werken ausführlich und auf sehr verschiedene Art behandelt, doch scheint es mir, als ob die in denselben vorgetragenen Beweise nicht immer den kürzesten Weg einschlagen; insbesondere halte ich die oft benutzte Halbierungsmethode der Intervalle, die meines Wissens von Bolzano herrührt*), für einen zu weitläufigen Umweg, auf welchem das erstrebte Ziel nicht früh genug zum Bewußtsein kommt. Nun ist es oft nur Sache der Gewöhnung und des Geschmackes, ob man dem einen oder dem anderen Beweis den Vorzug zuerkennen will, und deshalb erlaube ich mir, als Beispiel meiner Beweismethode im folgenden einen allgemeinen Satz zu behandeln, welcher zahlreiche Anwendungen auf bekannte Fälle gestattet.

*) Sie findet sich wohl zuerst in einer kleinen Schrift aus dem Jahre 1817, deren Titel ich nicht mehr genau anzugeben weiß, in welcher Bolzano den Satz zu beweisen versucht, daß eine stetige reelle Funktion einer reellen Variabelen in einem Intervall, in welchem sie sowohl positive wie negative Werte besitzt, auch den Wert Null annehmen muß. Diese Schrift ist wegen der vortrefflich geschriebenen Einleitung sehr lesenswert, aber an einer entscheidenden Stelle (in § 7) verfällt der Verfasser in vollständige Verwirrung, und der Beweis mißlingt gänzlich, der ohne vorgängige Feststellung der Stetigkeit des reellen Zahlgebietes auch gar nicht gelingen kann.

Nach einer Mitteilung (1892, 12. 19.) von Herrn Prof. H. A. Schwarz (Villenkolonie Grunewald bei Berlin, Hubertusallee 13), der mir auch früher dies Werk von Bolzano eine zeitlang geliehen hatte, ist der Titel desselben folgender: Beweis des Lehrsatzes, dass zwischen je zwey Werthen, die ein entgegengesetztes Resultat gewähren, wenigstens eine reelle Wurzel der Gleichung liege; von Bernard Bolzano. — Für die Abhandlungen der Königl. Gesellschaft der Wissenschaften. — Prag 1817. —

Vgl. Brief von H. A. Schwarz (1888, 4. 21.) an mich, und meine Antwort (1888, 4. 25.) mit Kritik von Bolzano und einigen Beweisen. —

Ferner: Brief von H. Weber (1892, 11. 18.) mit Beweis der Existenz einer Wurzel jeder algebraischen Gleichung; zu vergleichen auch mit meinem Beweise in meinem Briefe (1878, 6. 23.) an R. Lipschitz. —

§ 1.

Ich bespreche zunächst eine Erscheinung, die bei Systemen von beliebigen Elementen eintreten kann, und benutze hierbei einige Begriffe und Kunstausdrücke in demselben Sinne wie in meiner Schrift „Was sind und was sollen die Zahlen?“ (Braunschweig, 1888); doch wird es zum Verständnis wohl genügen, wenn ich an folgendes erinnere. Ein System S ist bestimmt, wenn alle Elemente bestimmt sind, aus denen es besteht. Ein System T heißt Teil von S, wenn jedes Element von T auch Element von S ist, und zwar heißt T ein echter Teil von S, wenn T von S verschieden ist. Ein System T heißt Gemeinteil der Systeme $A, B, C \cdots$, wenn T Teil von jedem dieser Systeme ist, und unter ihrer Gemeinheit wird das System aller derjenigen Elemente verstanden, welche zugleich Elemente von jedem dieser Systeme sind; wenn es gar kein solches, allen Systemen $A, B, C \cdots$ gemeinsames Element gibt, so besitzen sie auch keinen Gemeinteil und keine Gemeinheit. Dagegen gibt es in allen Fällen ein, aus $A, B, C \cdots$ zusammengesetztes System M, welches dadurch vollständig bestimmt ist, daß jedes und nur jedes solche Ding als

Element von M gilt, welches Element von mindestens einem der Systeme $A, B, C \cdots$ ist. Statt der etwas schwerfälligen Bezeichnung, welche ich aus gewissen Gründen in der oben erwähnten Schrift gebraucht habe, will ich hier nach Schröder dieses System M mit $A + B + C + \cdots$ bezeichnen und die Summe der Systeme $A, B, C \cdots$ nennen. Jedes der letzteren ist ein Teil dieser Summe.

Hierauf gehe ich zur Erörterung eines, wie ich glaube, neuen Begriffs über, der für unsere Untersuchung von besonderer Wichtigkeit ist. Unter einem Teilschnitt φ eines Systems S verstehe ich eine Einteilung aller seiner Teile in zwei Arten, nämlich in reine und unreine Teile, welche den folgenden drei Bedingungen genügt.

1. Jeder Teil von S ist entweder rein oder unrein, aber niemals beides zugleich.

2. Jeder Teil eines reinen Teils ist rein.

3. Die Summe von je zwei reinen Teilen ist rein.

Offenbar lassen sich die beiden letzten Bedingungen auch in die folgende zusammenziehen:

4. Die Summe von zwei Teilen ist dann und nur dann rein, wenn beide Teile rein sind. Oder mit anderen Worten: die Summe von zwei Teilen ist dann und nur dann unrein, wenn mindestens einer der beiden Teile unrein ist.

Diese letzte Fassung erinnert an den Satz über das Verschwinden eines arithmetischen Produktes und führt zu der folgenden Charakterisierung des Teilschnittes φ, von der ich bisweilen Gebrauch machen werde. Belegt man jeden Teil A des Systems S mit einer Zahl $\varphi(A)$, welche $= 1$ oder $= 0$ sein soll, je nachdem A rein oder unrein ist, so ist

$$5. \qquad \varphi(A + B) = \varphi(A)\,\varphi(B),$$

wo A, B beliebige Teile von S bedeuten. Und umgekehrt, wenn jedem Teile A eines Systems S eine Zahl $\varphi(A)$ in der Weise entspricht, daß das vorstehende Gesetz 5. erfüllt wird, so ist hierdurch ein Teilschnitt φ von S bestimmt; denn aus $A + A = A$ ergibt sich zunächst, daß $\varphi(A) = 1$ oder $= 0$ sein muß, und wenn man A rein oder unrein nennt, je nachdem das Erstere oder das Letztere der Fall ist, so sind die obigen drei Bedingungen eines Teilschnittes wirklich erfüllt.

Ich füge noch die folgenden Bemerkungen hinzu. Jeder bestimmte Teil T eines Systems S erzeugt einen Teilschnitt von S,

welcher dadurch bestimmt ist, daß jeder beliebige Teil A von S als rein oder unrein gilt, je nachdem A Teil von T ist oder nicht: T selbst ist folglich ein reiner Teil. Auf den ersten Blick könnte es auch scheinen, als müßte jeder Teilschnitt φ von S auf solche Weise durch einen bestimmten Teil T von S erzeugt werden; da nämlich jedes Element von S auch ein Teil von S und folglich entweder rein oder unrein ist, so liegt es nahe, den Inbegriff T aller reinen Elemente zu betrachten und nach 3. zu glauben, der Teilschnitt φ werde durch T erzeugt. Allein dieser Schluß ist nur dann sicher, wenn T ein endliches System ist, d. h. aus einer endlichen Anzahl von Elementen besteht; in der Tat kann aus der Eigenschaft 3. durch vollständige Induktion (durch den Schluß von n auf $n + 1$) nur gefolgert werden, daß die Summe von lauter reinen Teilen $A, B, C \cdots$ gewiß rein ist, wenn ihre Anzahl endlich ist, während eine Summe von unendlich vielen reinen Teilen sehr wohl unrein sein kann. Um sich hiervon zu überzeugen, genügt es, das folgende Beispiel zu betrachten: ist S ein unendliches System, und nennt man jeden Teil A von S rein oder unrein, je nachdem A endlich oder unendlich ist, so sind die obigen drei Bedingungen eines Teilschnittes offenbar erfüllt; aber obgleich alle Elemente von S rein sind, so ist ihre Gesamtheit S doch unrein. Hieraus geht hervor, daß ein Teilschnitt durch die Einteilung aller Elemente in reine und unreine noch keineswegs bestimmt ist. Man könnte sich nun vielleicht veranlaßt fühlen, den Begriff eines Teilschnittes so abzuändern, daß die Bedingung 3. für jede Summe von lauter reinen Teilen gelten soll; allein hierdurch würde die Tragweite des Begriffs wesentlichen Schaden erleiden.

Eine zweite Bemerkung besteht in folgendem. Während die Fassung des in der Einleitung ausgesprochenen Prinzips der Stetigkeit schon die Voraussetzung enthält, daß jede der beiden dortigen Klassen mindestens eine Zahl enthält, also wirklich existiert — weil sonst von einer Vergleichung der Zahlen der einen Klasse mit denen der anderen gar keine Rede sein könnte —, so sollen hier bei dem Begriff des Teilschnittes auch die beiden Fälle zugelassen werden, daß alle Teile rein, oder daß alle Teile unrein sind. Man kann dann allgemein behaupten, daß, wenn T ein Teil von S ist, in jedem Teilschnitt φ des Systems S ein Teilschnitt ψ des Systems T enthalten ist, welcher dadurch vollständig bestimmt wird, daß jeder Teil A

von T für rein oder unrein gelten soll, je nachdem er durch den Teilschnitt φ für rein oder unrein erklärt ist; dies kann mit Benutzung der oben erwähnten Charakterisierung durch die Zahlen 1 und 0 auch so ausgesprochen werden, daß allgemein $\psi(A) = \varphi(A)$ sein soll. Für unsere Zwecke ist aber besonders wichtig, daß umgekehrt, wenn T ein echter Teil von S ist, jeder Teilschnitt ψ des Systems T zu einem Teilschnitt φ des Systems S in der Weise erweitert werden kann, daß ψ in φ enthalten ist; eine solche Erweiterung kann auf verschiedene, häufig auf unendlich viele Arten geschehen*), doch soll hier, wenn schlechthin von der Erweiterung φ des Teilschnittes ψ die Rede ist, immer nur die folgende Art gemeint sein: jeder Teil A von S soll dann und nur dann für unrein gelten, wenn es einen Gemeinteil von A und T gibt, welcher durch den Teilschnitt ψ für unrein erklärt ist. Daß diese auf ψ gegründete Einteilung φ aller Teile von S wirklich einen Teilschnitt von S bildet, ergibt sich leicht; denn von den drei obigen Bedingungen sind die beiden ersten offenbar erfüllt, und wenn weder in A noch in B ein unreiner Teil von T enthalten ist, so gilt dasselbe auch von der Summe $A + B$, weil jeder Teil der letzteren entweder Teil von A, oder Teil von B, oder von der Form $A_1 + B_1$ ist, wo A_1 Teil von A, und B_1 Teil von B ist; mithin ist auch die dritte Bedingung erfüllt, also φ ein Teilschnitt von S, und offenbar ist ψ in φ enthalten.

Eine dritte und letzte Bemerkung bezieht sich auf eine Verbindung des Teilschnittes φ eines Systems S mit irgendeiner Abbildung desselben Systems. Das Wesen einer solchen Abbildung besteht bekanntlich darin, daß jedem bestimmten Element a des Systems S ein Bild, d. h. ein bestimmtes Element entspricht, welches wir mit a' bezeichnen wollen; ist A irgend ein Teil von S, so soll der Kürze halber unter dem Bilde von A dasjenige System A' verstanden werden, dessen Elemente die Bilder aller Elemente von A sind. Vermöge einer solchen Abbildung entspringt nun aus einem Teilschnitt φ des Systems S eine bestimmte Einteilung φ' aller Teile P des Systems S' in reine und unreine Teile, wenn nämlich festgesetzt wird, daß P stets und nur dann für unrein gelten soll, wenn es einen unreinen Teil U von S gibt, dessen Bild U' Teil von P

*) Die allgemeinere Frage, wann und wie sich gegebene Teilschnitte von Systemen $A, B, C \cdots$ zu einem einzigen Teilschnitte ihrer Summe $A + B + C + \cdots$ zusammensetzen lassen, ist leicht zu beantworten.

ist; daß diese Einteilung φ' wieder einen Teilschnitt des Systems S' bildet, ergibt sich auf ähnliche Weise, wie in der vorhergehenden Bemerkung, und wir dürfen es daher dem Leser überlassen, diesen Nachweis zu führen.

§ 2.

Um diesen Begriff des Teilschnittes auf Systeme von Zahlen — und zwar immer nur von reellen Zahlen — anzuwenden, schicke ich folgende Erklärungen voraus. Ist c eine Zahl, so soll das Zeichen $[c]$ das System aller derjenigen Zahlen bedeuten, welche im algebraischen Sinne $\leqq c$ sind. Bedeutet ferner h eine positive Zahl (nicht Null), so bezeichne ich mit $(c)_h$ das System aller derjenigen Zahlen x, welche den Bedingungen $c - h \leqq x \leqq c + h$ genügen, und ich nenne jedes solche System eine Hülle von c, h ihren Halbmesser, c ihren Mittelpunkt. Zufolge der Erklärung einer Summe von Systemen (§ 1) ist dann

$$[c + h] = [c - h] + (c)_h,$$

wo selbstverständlich das Zeichen $c + h$ die arithmetische Summe der Zahlen c und h, nicht nur das aus den beiden Elementen c und h bestehende System bedeutet. Ist T irgendein System von Zahlen, so soll die Zahl c eine Beizahl von T heißen, wenn in jeder Hülle von c mindestens eine Zahl des Systems T enthalten ist; offenbar ist jede Zahl des Systems T auch eine Beizahl von T, und wenn zugleich das Umgekehrte gilt, so soll T ein selbständiges System heißen*). Man erkennt leicht, daß das System T_0 aller Beizahlen von T stets selbständig ist; denn wenn c_0 eine Beizahl von T_0 bedeutet, so ist in jeder Hülle $(c_0)_h$ mindestens eine Zahl des Systems T_0, also eine Beizahl c des Systems T enthalten, und da in der Hülle $(c)_h$, also auch in jeder Hülle $(c_0)_{2h}$ mindestens eine Zahl des Systems T enthalten ist, so ist c_0 selbst eine Beizahl von T, also in T_0 enthalten, w. z. b. w. Nennen wir ferner T ein begrenztes System, wenn es eine Zahl gibt, welche absolut größer ist, als jede Zahl in T, so besteht folgender Satz:

Werden alle Teile eines begrenzten Zahlensystems T durch einen Teilschnitt ψ in reine und unreine Teile ein-

*) Diese Begriffe einer Beizahl und eines selbständigen Systems sind wohl zu unterscheiden von dem, was G. Cantor einen Grenzpunkt eines Systems und eine perfekte Mannigfaltigkeit nennt.

geteilt, und ist T selbst unrein, so gibt es eine kleinste Zahl c von der Art, daß in jeder Hülle von c ein unreiner Teil von T enthalten ist.

Der Beweis gewinnt die einfachste Ausdrucksweise, wenn man nach der in § 1 gegebenen Vorschrift den Teilschnitt ψ zu einem Teilschnitt φ des Systems S aller Zahlen erweitert, wodurch die Behauptung des Satzes sich offenbar in die folgende verwandelt: es gibt eine kleinste Zahl c, deren Hüllen sämtlich unrein sind. Um dieselbe zu beweisen, teile man alle Zahlen x in zwei Klassen A, B ein, indem man x in A oder in B aufnimmt, je nachdem das System $[x]$ rein oder unrein ist. Da T begrenzt ist, so gibt es eine positive Zahl e, welche absolut größer ist als jede Zahl in T; dann gehört $-e$ der Klasse A an, weil das System $[-e]$ gar keine Zahl mit T gemein hat und folglich rein ist; aber $+e$ gehört zu B, weil das unreine System T ein Teil von $[e]$, also auch letzteres System unrein ist. Mithin existieren beide Klassen A, B. Jede Zahl a der Klasse A ist algebraisch kleiner als jede Zahl b in B, weil, wenn $a \geqq b$ wäre, das reine System $[a]$ einen unreinen Teil $[b]$ besäße, was dem Begriff des Teilschnittes widerspricht. Nach dem in der Einleitung ausgesprochenen Prinzip der Stetigkeit gibt es daher eine Zahl c, welche entweder die größte in A oder die kleinste in B ist, so daß, wenn h irgendeine positive Zahl bedeutet, $c-h$ in A, $c+h$ in B enthalten ist; da nun das unreine System $[c+h]$ die Summe des reinen Systems $[c-h]$ und der Hülle $(c)_h$ ist, so folgt aus dem Begriff des Teilschnittes, daß die letztere stets unrein ist. Wenn endlich $a < c$ ist, so kann man eine positive Zahl h so wählen, daß $a+h$ auch der Klasse A angehört, woraus folgt, daß die Hülle $(a)_h$ als Teil des reinen Systems $[a+h]$ ebenfalls rein ist. Mithin ist c die kleinste Zahl, deren sämtliche Hüllen unrein sind, w. z. b. w.

Die Zahl c ist offenbar eine Beizahl des Systems T; ist daher letzteres selbständig, so ist c selbst in T enthalten.

Der bewiesene Satz umfaßt sehr viele, vielleicht alle diejenigen Existenz-Sätze, welche in der Theorie der Funktionen von einer reellen Veränderlichen behandelt zu werden pflegen. Es wird aber nicht nötig sein, dies hier auszuführen, weil wir später (§ 4) dieselben Sätze für Funktionen von mehreren Veränderlichen beweisen werden.

§ 3.

Ein ganz ähnlicher Satz gilt nun auch für den n-fach ausgedehnten stetigen Zahlenraum S. Unter einem Elemente oder einem Punkte $\mathfrak{a}$ dieses Raumes verstehe ich, wie üblich, jede bestimmte Folge von n reellen Zahlen a_1, $a_2 \cdots a_{n-1}$, a_n, und diese sollen die Koordinaten von $\mathfrak{a}$ heißen. Ist h irgendeine positive Zahl (nicht Null), so soll mit $(\mathfrak{a})_h$ das System aller der Punkte bezeichnet werden, deren Koordinaten x_1, $x_2 \cdots x_n$ den Bedingungen

$$a_1-h \leqq x_1 \leqq a_1+h,\ a_2-h \leqq x_2 \leqq a_2+h,\ \cdots,\ a_n-h \leqq x_n \leqq a_n+h$$

genügen, und ich nenne jedes solche System $(\mathfrak{a})_h$ eine Hülle von $\mathfrak{a}$, h ihren Halbmesser, $\mathfrak{a}$ ihren Mittelpunkt. Ist T irgendein System von Punkten, also ein Teil von S, so soll der Punkt $\mathfrak{c}$ ein Beipunkt von T heißen, wenn in jeder Hülle von $\mathfrak{c}$ mindestens ein Punkt von T enthalten ist; offenbar ist jeder Punkt des Systems T auch ein Beipunkt von T, und wenn zugleich das Umgekehrte gilt, so soll T ein selbständiges System heißen; man überzeugt sich leicht (wie in § 2), daß das System T_0 aller Beipunkte von T stets selbständig ist. Das System T heißt begrenzt, wenn es eine Zahl gibt, welche absolut größer ist als jede Koordinate jedes in T enthaltenen Punktes.

Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei verschiedene Punkte, deren $r$te Koordinaten bzw. mit a_r, b_r bezeichnet werden, so will ich $\mathfrak{a}$ den tieferen, $\mathfrak{b}$ den höheren nennen, wenn in der Folge der Differenzen

$$b_1-a_1,\quad b_2-a_2,\quad \cdots,\quad b_n-a_n$$

die erste, welche nicht verschwindet, einen positiven Wert hat, und dies soll kurz durch die Symbole $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{b} > \mathfrak{a}$ bezeichnet werden*). Von je zwei verschiedenen Punkten ist immer einer der tiefere, der andere der höhere, und der Gebrauch des Komparativs rechtfertigt sich dadurch, daß aus $\mathfrak{a} < \mathfrak{b}$ und $\mathfrak{b} < \mathfrak{c}$ stets $\mathfrak{a} < \mathfrak{c}$ folgt. Zugleich leuchtet ein, was es heißen soll, wenn ein Punkt der tiefste oder der höchste Punkt eines Systems genannt wird.

Alle diese Namen und Bezeichnungen entsprechen, wenn $n = 1$ ist, denjenigen, welche in § 2 gebraucht sind; ist aber $n > 1$, so tritt noch folgendes hinzu. Unterdrückt man die letzte Koordinate a_n des Punktes $\mathfrak{a}$, so bildet die Folge der übrigen a_1, $a_2 \cdots a_{n-1}$ einen

*) Bei dieser Unterscheidung ist von wesentlicher Bedeutung die Reihenfolge der Koordinaten, die natürlich durch jede andere ersetzt werden kann.

Punkt $\mathfrak{a}'$ des $(n-1)$fachen Zahlenraumes; dieser Punkt $\mathfrak{a}'$ soll das Bild oder die Projektion des Punktes $\mathfrak{a}$ heißen, und wenn T irgend ein Teil von S ist, so soll unter seiner Projektion T' dasjenige System verstanden werden, dessen Elemente die Projektionen aller in T enthaltenen Punkte sind, und welches folglich ein Teil des ganzen $(n-1)$ fachen Zahlenraumes S' ist. Die Projektion der Hülle $(\mathfrak{a})_h$ ist die Hülle $(\mathfrak{a}')_h$ der Projektion $\mathfrak{a}'$. Jeder Punkt $\mathfrak{a}$ des Raumes S ist vollständig bestimmt durch Angabe seiner Projektion $\mathfrak{a}'$ und seiner letzten Koordinate a_n und kann daher durch das Symbol $(\mathfrak{a}', a_n)$ bezeichnet werden; allgemeiner, wenn P irgendein Teil von S', und Q irgendein Teil des einfachen Zahlenraumes ist, so soll mit (P, Q) das System aller derjenigen Punkte $\mathfrak{a}$ in S bezeichnet werden, deren Projektion $\mathfrak{a}'$ in P, und deren letzte Koordinate a_n in Q enthalten ist. Die Einführung der Projektionen soll dazu dienen, um mit Hilfe der vollständigen Induktion den folgenden allgemeinen Satz zu beweisen:

I. Ist T ein begrenztes System von Punkten im n-fachen Zahlenraum S, und werden alle Teile von T durch einen Teilschnitt ψ in reine und unreine Teile eingeteilt, so gibt es, wenn T selbst unrein ist, einen tiefsten Punkt $\mathfrak{c}$ von der Art, daß in jeder Hülle von $\mathfrak{c}$ ein unreiner Teil von T enthalten ist.

Auch hier erleichtern wir uns den Beweis, indem wir den Teilschnitt ψ des Systems T nach der in § 1 gegebenen Vorschrift zu einem Teilschnitt φ des ganzen n-fachen Zahlenraumes S erweitern, wodurch unser Satz sich offenbar in den folgenden verwandelt:

Ist T ein begrenzter Teil von S, und werden alle Teile von S durch einen Teilschnitt φ in reine und unreine Teile so eingeteilt, daß T für unrein, und daß jeder Teil, welcher mit T keinen Punkt gemein hat, für rein gilt, so gibt es einen tiefsten Punkt $\mathfrak{c}$, dessen Hüllen sämtlich unrein sind.

Dies ist für den Fall $n = 1$ schon in § 2 bewiesen, und wir brauchen daher nur zu zeigen, daß aus der Wahrheit dieses Satzes für den $(n-1)$fachen Raum S' auch seine Wahrheit für den n-fachen Raum S folgt. Zu diesem Zwecke leiten wir nach der am Schlusse von § 1 gegebenen Vorschrift aus dem Teilschnitt φ einen Teilschnitt φ' des Raumes S' ab, indem wir irgendeinen Teil P des letzteren dann und nur dann für unrein erklären, wenn es einen

unreinen Teil U von S gibt, dessen Projektion U' Teil von P ist. Die Projektion T' des begrenzten und unreinen Teiles T von S ist offenbar ein begrenzter und unreiner Teil von S', und jeder Teil P von S', der mit T' keinen Punkt gemein hat, ist gewiß rein; denn jeder unreine Teil U von S hat mindestens einen Punkt $\mathfrak{a}$ mit T gemein und seine Projektion U' kann daher, weil sie mindestens einen Punkt $\mathfrak{a}'$ mit T' gemein hat, nicht Teil von P sein. Nehmen wir daher an, der oben ausgesprochene Satz gelte für den $(n-1)$fachen Raum S', so gibt es in demselben einen tiefsten Punkt $\mathfrak{c}'$, dessen Hüllen sämtlich unrein sind, und folglich gibt es, wenn k irgend eine positive Zahl bedeutet, immer einen unreinen Teil U von S, dessen Projektion U' Teil der Hülle $(\mathfrak{c}')_k$ ist. Bedeutet nun Q den ganzen einfachen Zahlenraum, so ist U jedenfalls ein Teil des Systems $((\mathfrak{c}')_k, Q)$, und folglich ist auch letzteres ein unreiner Teil des Raumes S. Da ferner T begrenzt ist, so gibt es eine positive Zahl e, welche absolut größer ist, als jede Koordinate jedes Punktes in T; bezeichnet man daher mit E das System aller derjenigen Zahlen, welche algebraisch größer als e sind, so hat das System $((\mathfrak{c}')_k, E)$ keinen Punkt mit T gemein und ist folglich rein, und da das unreine System

$$((\mathfrak{c}')_k, Q) = ((\mathfrak{c}')_k, E) + ((\mathfrak{c}')_k, [e])$$

ist, so ist auch das zweite System rechter Hand unrein. Zugleich leuchtet ein, daß das System $((\mathfrak{c}')_k, [-e])$ rein ist, weil es keinen Punkt mit T gemein hat. Hierauf teilen wir alle reellen Zahlen x in zwei Klassen A, B ein; die Zahl x soll zur zweiten Klasse B gehören, wenn jeder positiven Zahl k ein unreines System $((\mathfrak{c}')_k, [x])$ entspricht; im entgegengesetzten Falle soll x zur ersten Klasse A gehören. Offenbar ist $-e$ in A, aber $+e$ in B enthalten, also existieren beide Klassen. Jede Zahl a der Klasse A ist algebraisch kleiner als jede Zahl b der Klasse B, weil, wenn $a \geqq b$ wäre, es ein reines System $((\mathfrak{c}')_k, [a])$ gäbe, welches einen unreinen Teil $((\mathfrak{c}')_k, [b])$ besäße, was dem Begriff eines Teilschnittes φ widerspricht. Nach dem in der Einleitung ausgesprochenen Stetigkeitsprinzip gibt es daher eine Zahl c, welche entweder die größte in A oder die kleinste in B ist, und wir wollen zeigen, daß der hierdurch bestimmte Punkt $\mathfrak{c} = (\mathfrak{c}', c)$ die in dem obigen Satze behauptete Eigenschaft besitzt. Bedeutet h irgendeine positive Zahl, so gehört $c - h$ zur Klasse A,

und folglich gibt es eine positive Zahl k, welche ein reines System $((\mathfrak{c}')_k, [c-h])$ erzeugt, und wenn l die kleinste der beiden Zahlen h, k bedeutet, so ist das System $((\mathfrak{c}')_l, [c-h])$ als ein Teil des vorigen ebenfalls rein. Da andererseits $c+h$ zur Klasse B gehört, so ist das System $((\mathfrak{c}')_l, [c+h])$ unrein, und da es die Summe des vorigen und des Systems $((\mathfrak{c}')_l, (\mathfrak{c})_h)$ ist, so ist letzteres ebenfalls unrein; dieses ist aber, weil $l \leqq h$ ist, ein Teil des Systems $((\mathfrak{c}')_h, (\mathfrak{c})_h) = (\mathfrak{c})_h$, und folglich ist jede Hülle des Punktes $\mathfrak{c}$ unrein. Wir haben noch zu zeigen, daß $\mathfrak{c}$ der tiefste solche Punkt ist, daß also jeder tiefere Punkt $\mathfrak{a}$ mindestens eine reine Hülle besitzt. Aus $\mathfrak{a} < \mathfrak{c}$ folgt gewiß $\mathfrak{a}' \leqq \mathfrak{c}'$; ist nun zunächst $\mathfrak{a}' < \mathfrak{c}'$, so gibt es zufolge der Definition des Punktes $\mathfrak{c}'$ und des Teilschnittes φ' mindestens eine reine Hülle $(\mathfrak{a}')_h$, und da dieselbe die Projektion der Hülle $(\mathfrak{a})_h$ ist, so muß auch letztere rein sein. Ist aber $\mathfrak{a}' = \mathfrak{c}'$, so ist die letzte Koordinate a des Punktes $\mathfrak{a}$ algebraisch kleiner als c; man kann daher eine positive Zahl l so wählen, daß auch $a+l$ zur Klasse A gehört; dann gibt es eine positive Zahl k, welche ein reines System $((\mathfrak{c}')_k, [a+l])$ erzeugt; bedeutet nun h die kleinste der beiden Zahlen k, l, so ist die Hülle $(\mathfrak{a})_h$ als Teil dieses reinen Systems ebenfalls rein, w. z. b. w.

Nachdem der Satz hiermit allgemein bewiesen ist, mag noch bemerkt werden, daß der Punkt $\mathfrak{c}$ ein Beipunkt des Systems T und folglich, falls letzteres selbständig ist, selbst in T enthalten ist.

§ 4*).

Bei den nun folgenden Anwendungen beschränke ich mich auf einige sehr bekannte Sätze; ihr Beweis kommt immer auf eine zweckmäßige, den Bedingungen 1 bis 4 genügende Definition der reinen und unreinen Systeme zurück.

II. Ist U ein bestimmter Teil von T, so gibt es einen tiefsten Punkt von der Beschaffenheit, daß jede seiner Hüllen mindestens einen Punkt von U enthält.

Dies geht unmittelbar aus dem obigen Satze I (§ 3) hervor, wenn man jeden Teil von T unrein oder rein nennt, je nachdem er mindestens einen oder keinen Punkt von U enthält; denn diese Definition genügt offenbar den Bedingungen 1 bis 4 (§ 1).

*) [In diesem der ersten Fassung entnommenen Paragraphen (vgl. die Erläuterungen) ist T als beschränkt und abgeschlossen vorausgesetzt, so daß der obige Punkt $\mathfrak{c}$ stets zu T gehört (§ 3, Schluß). E. N.]

Die folgenden Sätze beziehen sich auf irgendeine eindeutige reelle Funktion der beiden Variabelen x, y; jedem Punkte $\mathfrak{p} = (x, y)$ von T entspricht eine bestimmte reelle Zahl $\mathfrak{p}'$, die ich das Bild des Punktes $\mathfrak{p}$ nenne, und wenn U irgendein Teil von T ist, so soll U' das Bild von U, d. h. den Inbegriff der Bilder $\mathfrak{p}'$ aller in U enthaltenen Punkte $\mathfrak{p}$ bedeuten.

III. Es gibt einen tiefsten Punkt (a, b) von folgender Beschaffenheit: ist c irgendeine Zahl des Systems T', so gibt es in jeder Hülle von (a, b) mindestens einen Punkt $\mathfrak{p}$, dessen Bild $\mathfrak{p}' \leqq c$ ist.

Dies geht unmittelbar aus dem Satze I hervor, wenn man jeden Teil U von T rein oder unrein nennt, je nachdem es in T' mindestens eine oder keine Zahl gibt, die kleiner als jede Zahl in U' ist; denn diese Definition genügt den Bedingungen 1 bis 4.

IV. Ist c ein Beiwert (§ 2) des Systems T', so gibt es einen tiefsten Punkt (a, b) von folgender Beschaffenheit: ist H irgendeine Hülle von (a, b), so ist c auch Beiwert des Systems H'.

Dies geht unmittelbar aus dem Satze I hervor, wenn man jeden Teil U von T unrein oder rein nennt, je nachdem c Beiwert von U' ist oder nicht; denn diese Definition genügt den Bedingungen 1 bis 4.

Die Abbildung (Funktion) heißt stetig im Punkte $\mathfrak{p}$, wenn, wie klein auch die positive Größe k gegeben sein mag, man immer eine Hülle H von $\mathfrak{p}$ so wählen kann, daß alle Zahlen in H' um weniger als k von $\mathfrak{p}'$, also um weniger als $2k$ voneinander verschieden sind. Die Funktion heißt stetig in T, wenn sie in jedem Punkte von T stetig ist. Dann ergeben sich aus den Sätzen III und IV die folgenden Sätze:

V. Eine in T stetige Funktion besitzt einen kleinsten Wert, und es gibt einen tiefsten Punkt, in welchem die Funktion diesen Minimumwert annimmt.

Denn wenn es in T' eine Zahl c gäbe, welche kleiner als $(a, b)'$ ist, wo (a, b) den in III bestimmten Punkt bedeutet, so könnte man eine Hülle H von (a, b) so wählen, daß alle Zahlen in H' größer als c wären, was im Widerspruch mit der dort bewiesenen Eigenschaft des Punktes (a, b) steht; mithin ist $(a, b)'$ die kleinste Zahl in T'. Und es kann auch keinen tieferen Punkt (α, β) geben, in

welchem derselbe Minimumwert $(\alpha, \beta)' = (a, b)'$ auftritt, weil ein solcher Punkt (α, β) gewiß dieselbe, in III angegebene Beschaffenheit besitzt, wie (a, b).

VI. Ist die Abbildung (Funktion) stetig in T, so ist jeder Beiwert c von T' auch eine Zahl in T', und es gibt einen tiefsten Punkt (a, b), in welchem die Funktion diesen Wert $c = (a, b)'$ annimmt.

Denn wenn (a, b) den in IV bestimmten Punkt bedeutet, so kann $(a, b)'$ nicht von c verschieden sein, weil man sonst eine Hülle H von (a, b) so wählen könnte, daß alle Zahlen in H' um mehr als eine bestimmte positive Größe von c verschieden wären, also c kein Beiwert von H' wäre, was in Widerspruch mit IV steht; mithin ist $(a, b)' = c$. Und es kann auch keinen tieferen Punkt (α, β) geben, dessen Bild $(\alpha, \beta)' = c$ ist.

VII*). Besitzt eine in T stetige Funktion sowohl positive als auch negative Werte, so gibt es auch einen tiefsten Punkt, in welchem sie verschwindet.

Dies versteht sich von selbst, wenn die Funktion im Nullpunkte (0,0) verschwindet. Ist aber $(0,0)'$ positiv (auf welchen Fall wir uns beschränken dürfen), so soll ein Teil U von T rein heißen, wenn U' aus lauter positiven Zahlen besteht; im entgegengesetzten Falle heiße U unrein. Da diese Definition den Bedingungen 1. bis 4. genügt, so gibt es (nach Satz I) einen tiefsten Punkt (a, b) von der Beschaffenheit, daß jede seiner Hüllen H unrein ist.

Ich behaupte, daß $(a, b)' = 0$ ist. Denn jedenfalls kann $(a, b)'$ nicht positiv sein, weil es sonst zufolge der Stetigkeit auch reine Hüllen H gäbe. Nehmen wir ferner an, $(a, b)'$ sei negativ, so kann man zufolge der Stetigkeit eine Hülle H so wählen, daß H' aus lauter negativen Zahlen besteht; da aber (a, b) nicht der Nullpunkt ist, so gibt es in H gewiß einen Punkt (α, β), der tiefer ist als (a, b), und da $(\alpha, \beta)'$ negativ ist, so wäre auch jede Hülle von (α, β) unrein, während doch (a, b) der tiefste Punkt ist, der diese Eigenschaft besitzt. Mithin ist $(a, b)' = 0$, und es kann auch keinen tieferen Punkt als (a, b) geben, in welchem die Funktion verschwindet, weil wieder jede Hülle eines solchen Punktes unrein ist, w. z. b. w.

*) [Der Beweis gilt in der hier gegebenen Fassung nur für das Quadrat $0 \leq x \leq 1$, $0 \leq y \leq 1$. Dedekind hatte die allgemeinere Gültigkeit des Satzes bemerkt, ohne die nötigen Abänderungen hinzuschreiben. E. N.]

Ich schließe mit folgendem, für den Begriff des Doppelintegrals wichtigen Satze:

VIII. Ist z eine in T stetige Funktion, und k eine positive Größe, so kann man eine für alle Punkte $\mathfrak{p}$ gemeinsame positive Größe h so wählen, daß z in jeder Hülle $(\mathfrak{p}, h)$ sich um weniger als k ändert.

Um dies zu beweisen, bemerke ich zunächst folgendes. Ist $\mathfrak{p}$ ein bestimmter Punkt in T, so gibt es zufolge der Stetigkeit der Funktion z eine Hülle $(\mathfrak{p}, 2h)$, in welcher z sich um weniger als k ändert; betrachtet man nun alle Punkte $\mathfrak{q}$ der Hülle $(\mathfrak{p}, h)$, so ist jede Hülle $(\mathfrak{q}, h)$, deren Halbmesser $= h$, ein Teil von $(\mathfrak{p}, 2h)$, und folglich ändert sich z auch in jeder solchen Hülle $(\mathfrak{q}, h)$ um weniger als k; das Punktsystem $U = (\mathfrak{p}, h)$ hat daher die Eigenschaft, welche unser Satz dem ganzen T zuschreibt: man kann alle Punkte des Systems U in Hüllen vom gemeinsamen Halbmesser h so einschließen, daß z in jeder einzelnen solchen Hülle sich um weniger als k ändert. Nehmen wir nun an, unser Satz sei unrichtig, so nennen wir, wenn dies auch unpassend klingen mag, einen Teil von T rein oder unrein, je nachdem er die eben ausgesprochene Eigenschaft besitzt oder nicht besitzt. Diese Einteilung genügt offenbar den Bedingungen eines Teilschnittes, auch der letzten; denn wenn h_1, h_2 genügend kleine (geeignete) Halbmesser für die reinen Systeme U_1, U_2 sind, so ist die kleinste der beiden Zahlen h_1, h_2 ein genügend kleiner Halbmesser für das aus U_1 und U_2 zusammengesetzte System. Nach dem Satz I müßte es daher mindestens einen Punkt $\mathfrak{p}$ geben, dessen Hüllen sämtlich unrein sind, während doch oben gezeigt ist, daß jeder Punkt $\mathfrak{p}$ eine reine Hülle besitzt. Mithin muß auch T rein sein, w. z. b. w.

Erläuterungen zur vorstehenden Abhandlung.

Das Manuskript lag in zwei Fassungen vor, von denen die zweite von Dedekind als „sorgfältigere Fassung desselben Gegenstandes“ bezeichnet war. In dieser zweiten Fassung fehlte aber die Einleitung und der Paragraph mit den Anwendungen, die daher aus der ersten Fassung übernommen sind (wobei x, y statt $x_1, \cdots, x_n$ stehen blieb).

Zur Terminologie ist zu bemerken, daß die Dedekindschen Bezeichnungen „Beipunkt“ und „selbständiges System“ dem „Berührpunkt“ (vgl. Hausdorff, Mengenlehre) und der „abgeschlossenen Menge“ entsprechen; der Übergang von T zum „selbständigen System T_0“ ist der Übergang zur „abgeschlossenen Hülle“

(Dedekind gebraucht den Ausdruck „Hülle“ für n-dimensionale abgeschlossene Würfelumgebung eines Punktes).

Den Anwendungen kann vielleicht noch hinzugefügt werden der Heine-Borelsche Überdeckungssatz:

Es sei jedem Punkt p von T (wo T abgeschlossen und beschränkt) eine p enthaltende offene Menge δ_p zugeordnet. Man nenne eine Untermenge U von T rein oder unrein, je nachdem U durch endlich viele δ_p überdeckt wird oder nicht. Ist T unrein — d. h. der Überdeckungssatz nicht erfüllt —, so gibt es einen Punkt c von T derart, daß jede Würfelumgebung von c unrein. Das ist aber ein Widerspruch; denn ist δ_c die c zugeordnete offene Menge, $W_c \subseteq \delta_c$ eine Würfelumgebung von c (eine solche existiert, da die W eine Basis aller Umgebungen bilden), so ist W_c rein; denn es wird von einem δ_c überdeckt.

Noether.

XXXVII.

Stetiges System aller Abbildungen der natürlichen Zahlenreihe N in sich selbst.

1. Abbildung α von N in sich selbst. Ist n eine natürliche Zahl, so sei $n\alpha$ das durch α erzeugte Bild von n; $n\alpha$ ist eine natürliche Zahl.

2. Sind α, β Abbildungen von N in sich selbst und verschieden voneinander, so gibt es mindestens eine natürliche Zahl n, für welche die Differenz $n\alpha - n\beta$ von Null verschieden ist, und unter diesen Zahlen n gibt es eine kleinste r. Dann ist

$$x\alpha = x\beta, \quad \text{falls} \quad x < r,$$

und $r\alpha - r\beta$ ist entweder positiv oder negativ. Im ersten Falle

$$r\alpha > r\beta$$

heiße α größer als β, β kleiner als α, in Zeichen

$$\alpha > \beta \quad \text{und} \quad \beta < \alpha.$$

Im zweiten Falle ist $r\beta > r\alpha$, mithin $\beta > \alpha$, $\alpha < \beta$. Also: von zwei verschiedenen Abbildungen α, β ist immer eine und nur eine größer als die andere.

3. Satz: Sind α, β, γ drei verschiedene Abbildungen von N in sich selbst, und ist $\alpha > \beta$, $\beta > \gamma$, so ist auch $\alpha > \gamma$.

Beweis: Zufolge der beiden Annahmen $\alpha > \beta$, $\beta > \gamma$ gibt es zwei natürliche Zahlen r, s von folgender Beschaffenheit:

$$r\alpha > r\beta, \quad x\alpha = x\beta \quad \text{für} \quad x < r,$$
$$s\beta > s\gamma, \quad y\beta = y\gamma \quad \text{für} \quad y < s.$$

Nun sind zwei Fälle denkbar: entweder ist $r \leqq s$, oder es ist $r > s$. Im ersten Falle ist $r\alpha > r\beta$ und, je nachdem $r < s$ oder $r = s$ ist, $r\beta = r\gamma$ oder $r\beta > r\gamma$, also gewiß $r\alpha > r\gamma$, und da

jede Zahl x, welche $< r$, auch $< s$ ist, so ist $x\alpha = x\beta$ und $x\beta = x\gamma$, also auch $x\alpha = x\gamma$, mithin

$$r\alpha > r\gamma \quad \text{und} \quad x\alpha = x\gamma \quad \text{für} \quad x < r, \quad \text{also} \quad \alpha > \gamma,$$

w. z. b. w.

Im zweiten Falle $r > s$ ist $s\alpha = s\beta$ und $s\beta > s\gamma$, also auch $s\alpha > s\gamma$, und da jede Zahl y, welche $< s$, auch $< r$ ist, so folgt $y\alpha = y\beta$, und $y\beta = y\gamma$, also $y\alpha = y\gamma$, mithin

$$s\alpha > s\gamma \quad \text{und} \quad y\alpha = y\gamma \quad \text{für} \quad y < s, \quad \text{also} \quad \alpha > \gamma,$$

w. z. b. w.

[Diese kleine Bemerkung trägt das Datum 1891. 1. 2.]

XXXVIII.

Charakteristische Eigenschaft einklassiger Körper Ω.

Die erforderliche und hinreichende Bedingung dafür, daß ein endlicher Körper Ω einklassig ist, besteht darin, daß für je zwei ganze Zahlen α, β in Ω, deren letztere β von Null verschieden ist, immer zwei ganze Zahlen μ, ν in Ω gewählt werden können, deren erstere μ relative Primzahl zu β ist, und für welche die Norm $N(\alpha\mu + \beta\nu)$ absolut $< N(\beta)$ ist.

Beweis. I. Ist Ω einklassig, und $\mathfrak{o}$ die Hauptordnung, d. h. das System aller ganzen Zahlen in Ω, so ist

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}\delta \text{ (Hauptideal).}$$

Ist α teilbar durch β, so kann man $\delta = \beta$, $\alpha = \beta\gamma$, $\mu = -1$, $\nu = \gamma$ setzen, wodurch den Forderungen genügt wird, weil μ relative Primzahl zu β, wo $N(\alpha\mu + \beta\nu) = 0$ abs. $< N(\beta)$ ist. Wenn aber α nicht teilbar durch β ist, so setze man

$$\alpha = \delta\alpha_1, \ \beta = \delta\beta_1, \quad \text{also} \quad \mathfrak{o}\alpha_1 + \mathfrak{o}\beta_1 = \mathfrak{o};$$

mithin sind α_1, β_1 relative Primzahlen, und es gibt ganze Zahlen α_2, die der Kongruenz

$$\alpha_1\alpha_2 \equiv 1 \pmod{\beta_1}$$

genügen (§ 174, S. 533, § 178, XIII, S. 559 und S. 556).

Ist nun π das Produkt aller derjenigen in δ aufgehenden Primzahlen des Körpers Ω, die nicht in β_1 aufgehen (evtl. $\pi = 1$, wenn es keine solche Primzahl gibt), so sind β_1, π relative Primzahlen, und folglich (§ 180, II, S. 568) gibt es in $\mathfrak{o}$ Zahlen μ, die den simultanen Kongruenzen

$$\mu \equiv \alpha_2 \pmod{\beta_1}, \ \mu \equiv 1 \pmod{\pi}$$

genügen; hieraus folgt, daß μ relative Primzahl zu π und (wie α_2) zu β_1, also auch zu β ist, weil jede in $\beta = \delta\beta_1$ aufgehende Primzahl entweder in β_1 oder in δ, also in π aufgeht. Aus der ersteren dieser Folgerungen folgt ferner

$$\alpha_1\mu \equiv \alpha_1\alpha_2 \equiv 1 \pmod{\beta_1},$$

also gibt es in $\mathfrak{o}$ eine Zahl ν, die der Bedingung

$$\alpha_1\mu + \beta_1\nu = 1, \quad \alpha\mu + \beta\nu = \delta$$

genügt, woraus der Beweis von I, nämlich

$$N(\alpha\mu + \beta\nu) = N(\delta) = \frac{N(\beta)}{N(\beta_1)} \text{ abs.} < N(\beta)$$

folgt, weil β_1 keine Einheit, also $N(\beta_1) > 1$ ist (α nicht teilbar durch β).

II. Umkehrung: Der endliche Körper Ω, dessen Hauptordnung $\mathfrak{o}$, ist gewiß einklassig, wenn es für je zwei Zahlen α, β in $\mathfrak{o}$, deren letztere von Null verschieden ist, immer zwei Zahlen μ, ν in $\mathfrak{o}$ gibt, deren erstere relative Primzahl zu β ist, und die der Bedingung

$$N(\alpha\mu + \beta\nu) \text{ abs.} < N(\beta)$$

genügen.

Bei dem Beweise wollen wir, wenn α, β, α', β' Zahlen in $\mathfrak{o}$ sind, durch das Zeichen

$$(\alpha, \beta) \sim (\alpha', \beta')$$

andeuten, daß der Komplex aller gemeinsamen Teiler von α, β identisch mit dem aller gemeinsamen Teiler von α', β' ist. Sind nun α, β gegeben, und μ, ν so gewählt, daß sie den beiden Bedingungen genügen, und setzen wir

$$\gamma = \alpha\mu + \beta\nu,$$

so folgt daraus

$$(\alpha, \beta) \sim (\beta, \gamma);$$

denn offenbar ist jeder gemeinsame Teiler von α, β auch ein Teiler von γ, also gemeinsamer Teiler von β, γ; und aus $\alpha\mu = \gamma - \beta\nu$ folgt, daß jeder gemeinsame Teiler von β, γ auch ein Teiler von $\alpha\mu$ und, weil er als Teiler von β relative Primzahl zu μ ist, auch Teiler von α, also gemeinsamer Teiler von α, β ist, wie behauptet war. Aus jedem Paare α, β, wo β von Null verschieden, kann man daher eine Zahl γ in $\mathfrak{o}$ bilden, die den Bedingungen

$$(\alpha, \beta) \sim (\beta, \gamma) \quad \text{und} \quad N(\gamma) \text{ abs.} < N(\beta)$$

genügt.

Der Fall $\gamma = 0$ tritt offenbar nur dann ein, wenn jeder Teiler von β, also auch β selbst in α aufgeht (und umgekehrt, wenn α durch β teilbar ist, so kann man μ, ν wie in I so wählen, daß $\gamma = 0$ wird); in diesem Fall besitzen also α, β einen größten gemeinsamen Teiler β.

Ist aber γ von Null verschieden, so kann man wieder eine Zahl δ in $\mathfrak{o}$ bilden, die den Bedingungen

$$(\gamma, \delta) \sim (\beta, \gamma) \sim (\alpha, \beta) \quad \text{und} \quad N(\delta) < N(\gamma) < N(\beta)$$

genügt, woraus offenbar auch $(\gamma, \delta) \sim (\alpha, \beta)$ folgt. Fährt man, wenn δ nicht Null ist, so fort, so erhält man eine Reihe von Zahlen $\beta, \gamma, \delta, \varepsilon, \cdots$ in $\mathfrak{o}$, deren Normen absolut immer kleiner werden; es muß daher in dieser Reihe nach einer endlichen Anzahl von Schritten auch die Zahl Null auftauchen, und wenn τ in ihr die letzte von Null verschiedene Zahl ist, so ergibt sich:

$$(\alpha, \beta) \sim (\tau, 0),$$

woraus wie oben folgt, daß je zwei Zahlen α, β in $\mathfrak{o}$, deren letzte nicht verschwindet, einen größten gemeinsamen Teiler τ in $\mathfrak{o}$ besitzen, was auch durch

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}\tau$$

ausgedrückt werden kann; mithin ist (§ 178, XII, S. 559) jedes Ideal des Körpers Ω ein Hauptideal, d. h. Ω ist einklassig, w. z. b. w.

Erläuterungen zur vorstehenden Abhandlung.

Das hier gegebene Kriterium ist erst in neuester Zeit — im Rahmen allgemeinerer Untersuchungen — wiedergefunden worden: H. Hasse, Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen. J. f. M. 159 (1928), S. 3—12. Die Zitate beziehen sich auf die 4. Auflage von Dirichlet-Dedekind; der Satz selbst liegt aber viel weiter zurück, wie eine nicht druckfertige, sehr alte Ausarbeitung zeigt.

Noether.

XXXIX.

Konstruktion von Quaternionkörpern.

Der in dem Quaternionkörper Ω enthaltene biquadratische Körper sei H; man kann dann

$$\Omega = H(\omega), \quad \omega^2 = \mu$$

setzen, wo μ eine ganze Zahl in H bedeutet. Jede Zahl in Ω ist von der Form $x + y\omega$, wo x, y in H enthalten; soll das Quadrat $(x+y\omega)^2 = (x^2 + \mu y^2) + 2xy\omega$ in H enthalten sein, so muß $xy = 0$ sein, also $x = 0$, falls $x + y\omega$ nicht in H enthalten (also nicht $y = 0$) ist.

Bezeichnet man die Quaterniongruppe Q des Körpers Ω mit $1, \alpha, \beta, \gamma, \varepsilon, \varepsilon\alpha, \varepsilon\beta, \varepsilon\gamma$, wo

$$\varepsilon^2 = 1,$$
$$\varepsilon = \alpha^2 = \beta^2 = \gamma^2 = \alpha^{-2} = \beta^{-2} = \gamma^{-2},$$
$$\beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma,$$
$$\gamma\beta = \alpha^{-1} = \varepsilon\alpha, \quad \alpha\gamma = \beta^{-1} = \varepsilon\beta, \quad \beta\alpha = \gamma^{-1} = \varepsilon\gamma,$$

so liegt $(\omega\alpha)^2 = \mu\alpha$ in H, und da $\omega\alpha$ in Ω, aber nicht in H enthalten ist, so kann man

$$\omega\alpha = u\omega$$

und entsprechend

$$\omega\beta = v\omega,$$
$$\omega\gamma = w\omega$$

setzen, wo u, v, w Zahlen in H sind. Sodann ist

$$\omega\varepsilon = -\omega, \quad \mu\varepsilon = \mu,$$

also

$$\begin{aligned} \omega\alpha^2 &= \omega\varepsilon &&= -\omega &&= \omega u\,(u\alpha), \\ \omega\beta\alpha &= \omega\varepsilon\gamma &&= -\omega w &&= \omega u\,(v\alpha), \\ \omega\gamma\alpha &= \omega\beta &&= \omega v &&= \omega u\,(w\alpha), \end{aligned}$$

und entsprechend ergibt sich

$$\begin{aligned} \omega w &= \omega v\,(u\beta), & -\omega v &= \omega w\,(u\gamma), \\ -\omega &= \omega v\,(v\beta), & \omega u &= \omega w\,(v\gamma), \\ -\omega u &= \omega v\,(w\beta), & -\omega &= \omega w\,(w\gamma), \end{aligned}$$

folglich

$$(1) \quad \begin{cases} u\alpha = -u^{-1}, & u\beta = wv^{-1}, & u\gamma = -vw^{-1}, \\ v\alpha = -wu^{-1}, & v\beta = -v^{-1}, & v\gamma = uw^{-1}, \\ w\alpha = vu^{-1}, & w\beta = -uv^{-1}, & w\gamma = -w^{-1}, \end{cases}$$
$$\mu\alpha = \mu u^2, \qquad \mu\beta = \mu v^2, \qquad \mu\gamma = \mu w^2.$$

Ist H insbesondere einklassig, so kann man μ als eine durch kein Primzahlquadrat in H teilbare ganze Zahl in H annehmen. Dann sind auch $\mu\alpha, \mu\beta, \mu\gamma$ durch kein Primzahlquadrat teilbar, und somit müssen u, v, w Einheiten sein. Ist daher π eine in μ aufgehende Primzahl in H, so müssen auch $\pi\alpha, \pi\beta, \pi\gamma$ in μ aufgehen; bedeutet p die durch π teilbare natürliche Primzahl, so muß daher, wenn p durch kein Primzahlquadrat in H teilbar ist, also p nicht in der Grundzahl von H aufgeht, die Zahl μ durch das Produkt p aller verschiedenen in p aufgehenden Primzahlen π teilbar sein. Die Zahl μ ist also das Produkt aus einer natürlichen Zahl m, einer Einheit und möglicherweise noch einer oder mehreren voneinander verschiedenen in der Grundzahl aufgehenden Primzahlen in H; dabei ist m ein Produkt von lauter voneinander und von den Primteilern der Grundzahl verschiedenen natürlichen Primzahlen.

Beispielsweise sei H der einklassige Körper $R(\sqrt{2}, \sqrt{3}, \sqrt{6})$, wo R den Körper der rationalen Zahlen bedeutet; μ sei wiederum eine durch kein Primzahlquadrat in H teilbare ganze Zahl in H. Die Grundzahl (48^2) von H setzt sich aus den Primfaktoren 2 und 3 zusammen. Dabei ist 3 das Quadrat der Primzahl $\sqrt{3}$ in H, und 2 ist bis auf eine Einheit als Faktor die vierte Potenz der Primzahl

$$1 + \eta = 1 + \frac{1+\sqrt{3}}{\sqrt{2}} = \frac{1+\sqrt{2}+\sqrt{3}}{\sqrt{2}}$$

in H. Die Fundamentaleinheiten in H sind ferner

$$a = 1 + \sqrt{2}, \quad \eta = \frac{1+\sqrt{3}}{\sqrt{2}} = \sqrt{b} = \sqrt{2+\sqrt{3}},$$
$$\tau = \sqrt{2} + \sqrt{3} = \sqrt{c} = \sqrt{5+2\sqrt{6}}.$$

Also kann man setzen

$$\mu = \pm m a^{e_1} \eta^{e_2} \tau^{e_3} (1+\eta)^{e_4} (\sqrt{3})^{e_5},$$

wo m eine durch kein Primzahlquadrat teilbare natürliche Zahl und relative Primzahl zu 6 ist und jede der Zahlen e_1, e_2, e_3, e_4, e_5 gleich 0 oder 1 ist.

Man kann jetzt setzen

$$(\sqrt{2}, \sqrt{3}, \sqrt{6}, \omega)\ \alpha = (\ \sqrt{2}, -\sqrt{3}, -\sqrt{6}, u\omega),$$
$$(\sqrt{2}, \sqrt{3}, \sqrt{6}, \omega)\ \beta = (-\sqrt{2}, \sqrt{3}, -\sqrt{6}, v\omega),\quad \omega\varepsilon = -\omega,\ \mu\varepsilon = \mu.$$
$$(\sqrt{2}, \sqrt{3}, \sqrt{6}, \omega)\ \gamma = (-\sqrt{2}, -\sqrt{3}, \sqrt{6}, w\omega),$$

Dann ist

$$\begin{aligned} \alpha\alpha &= \alpha, & \alpha\beta &= -\alpha^{-1}, & \alpha\gamma &= -\alpha^{-1}, \\ \eta\alpha &= -\eta^{-1}, & \eta\beta &= -\eta, & \eta\gamma &= \eta^{-1}, \\ \tau\alpha &= -\tau^{-1}, & \tau\beta &= \tau^{-1}, & \tau\gamma &= -\tau, \end{aligned}$$

$$(1+\eta)\alpha = -\eta^{-1}(1-\eta),\ (1+\eta)\beta = 1-\eta,\ (1+\eta)\gamma = \eta^{-1}(1+\eta),$$

also, da man leicht

$$\frac{1-\eta}{1+\eta} = -\tau^{-1}$$

bestätigt,

$$(1+\eta)\alpha = (1+\eta)\eta^{-1}\tau^{-1},\quad (1+\eta)\beta = -(1+\eta)\tau^{-1},$$
$$(1+\eta)\gamma = (1+\eta)\eta^{-1},$$

endlich

$$(\sqrt{3})\alpha = -\sqrt{3},\quad (\sqrt{3})\beta = \sqrt{3},\quad (\sqrt{3})\gamma = -\sqrt{3}.$$

Also ist

$$\mu\alpha = \pm m a^{e_1} (-\eta^{-1})^{e_2} (-\tau^{-1})^{e_3} (1+\eta)^{e_4} \eta^{-e_4} \tau^{-e_4} (-\sqrt{3})^{e_5}$$
$$= \pm m a^{e_1} (-1)^{e_2+e_3+e_5} \eta^{-e_2-e_4} \tau^{-e_3-e_4} (1+\eta)^{e_4} (\sqrt{3})^{e_5},$$

$$\frac{\mu\alpha}{\mu} = (-1)^{e_2+e_3+e_5} \eta^{-2e_2-e_4} \tau^{-2e_3-e_4} = u^2,$$

also

$$e_4 = 0,\quad e_2 + e_3 + e_5 \equiv 0 \pmod 2,\quad u = (\pm)'\ \eta^{-e_2} \tau^{-e_3},$$
$$\mu = \pm m a^{e_1} \eta^{e_2} \tau^{e_3} (\sqrt{3})^{e_5}.$$

Hieraus ergibt sich weiter

$$\mu\beta = \pm m\ (-a^{-1})^{e_1}\ (-\eta)^{e_2}\ \tau^{-e_3}\ (\sqrt{3})^{e_5},$$
$$\frac{\mu\beta}{\mu} = (-1)^{e_1+e_2} a^{-2e_1} \tau^{-2e_3} = v^2,$$

also

$$e_1 + e_2 \equiv 0 \pmod 2,\quad e_1 = e_2,\quad v = (\pm)''\ a^{-e_1} \tau^{-e_3},$$
$$\mu = \pm m a^{e_1} \eta^{e_1} \tau^{e_3} (\sqrt{3})^{e_5}$$

und mit Rücksicht auf das Obige auch

$$u = (\pm)'\ \eta^{-e_1} \tau^{-e_3},$$
$$e_1 + e_3 + e_5 \equiv 0 \pmod 2.$$

Unter Benutzung von (1) erhält man weiter

$$u\alpha = (\pm)' (-\eta^{-1})^{-e_1} (-\tau^{-1})^{-e_3} = (\pm)' (-1)^{e_1+e_3} \eta^{e_1} \tau^{e_3}$$
$$= -u^{-1} = -(\pm)'\ \eta^{e_1} \tau^{e_3},$$

also

$$(-1)^{e_1+e_3} = -1,\quad e_1 + e_3 \equiv 1 \pmod 2;$$

also ist

$$e_5 = 1,$$
$$\mu = \pm m a^{e_1} \eta^{e_1} \tau^{e_3} \sqrt{3}$$

und entweder $e_1 = 0$, $e_3 = 1$ oder $e_1 = 1$, $e_3 = 0$. In ähnlicher Weise ergibt sich

$$v\beta = (\pm)''\ (-a^{-1})^{-e_1} \tau^{e_3} = (\pm)''\ (-1)^{e_1} a^{e_1} \tau^{e_3}$$
$$= -v^{-1} = -(\pm)''\ a^{e_1} \tau^{e_3},$$

also

$$(-1)^{e_1} = -1,\quad e_1 = 1,\quad e_3 = 0,$$
$$\mu = \pm m a \eta \sqrt{3}. \tag{2}$$

Mein erstes Beispiel (1886) war

$$\mu = (1+\sqrt{2})(\sqrt{2}+\sqrt{3})\sqrt{2}\sqrt{3} = a\tau\sqrt{2}\sqrt{3}.$$

Diese Zahl hat nicht die Gestalt (2); das erklärt sich daraus, daß μ oben als durch kein Primzahlquadrat teilbar vorausgesetzt wurde. In der Tat unterscheidet sich μ von der unter (2) fallenden Zahl $a\eta\sqrt{3}$ nur durch den Faktor

$$\frac{\tau\sqrt{2}}{\eta} = \frac{2(\sqrt{2}+\sqrt{3})}{1+\sqrt{3}},$$

der das Quadrat der Zahl $1 - \dfrac{1-\sqrt{3}}{\sqrt{2}}$ in H ist.

Ist umgekehrt μ von der Gestalt (2), wo m eine beliebige durch kein Primzahlquadrat teilbare und zu 6 teilerfremde natürliche Zahl ist, und ist $\omega^2 = \mu$, so erzeugt ω über dem Körper H einen Quaternionkörper. Das erkennt man folgendermaßen:

Man bezeichne mit α, β, γ drei Permutationen des Körpers $\Omega = H(\omega)$, welche die auf den biquadratischen Körper $R(\sqrt{2}, \sqrt{3})$ bezüglichen Eigenschaften

$$(3)\qquad \begin{cases} (\sqrt{2}, \sqrt{3}, \sqrt{6})\,\alpha = (\ \sqrt{2}, -\sqrt{3}, -\sqrt{6}), \\ (\sqrt{2}, \sqrt{3}, \sqrt{6})\,\beta = (-\sqrt{2}, \ \sqrt{3}, -\sqrt{6}), \\ (\sqrt{2}, \sqrt{3}, \sqrt{6})\,\gamma = (-\sqrt{2}, -\sqrt{3}, \ \sqrt{6}) \end{cases}$$

besitzen [solcher Permutationen α, β, γ gibt es je eine oder je zwei, je nachdem der noch unbekannte Grad von Ω gleich 4 oder 8 ist, da zu jeder Permutation des biquadratischen Körpers $R(\sqrt{2}, \sqrt{3})$ genau eine bzw. zwei Permutationen von Ω als Multipla gehören]; die identische Permutation von Ω sei 1. Nun ist

$$\omega^2\alpha = \pm m(1+\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}}(-\sqrt{3}) = \omega^2\left(\frac{1-\sqrt{3}}{\sqrt{2}}\right)^2,$$

$$\omega^2\beta = \pm m(1-\sqrt{2})\frac{1+\sqrt{3}}{-\sqrt{2}}\ \sqrt{3}\ = \omega^2(1-\sqrt{2})^2,$$

$$\omega^2\gamma = \pm m(1-\sqrt{2})\frac{1-\sqrt{3}}{-\sqrt{2}}(-\sqrt{3}) = \omega^2(1-\sqrt{2})^2\left(\frac{1-\sqrt{3}}{\sqrt{2}}\right)^2,$$

mithin

$$(4)\qquad \begin{cases} \omega\alpha = \omega\dfrac{1-\sqrt{3}}{\sqrt{2}}\cdot e_1, \\ \omega\beta = \omega(1-\sqrt{2})\cdot e_2, \\ \omega\gamma = \omega(1-\sqrt{2})\dfrac{1-\sqrt{3}}{\sqrt{2}}\cdot e_3 \end{cases} \qquad (e_1^2 = e_2^2 = e_3^2 = 1).$$

Hieraus folgt weiter

$$(5)\qquad \begin{cases} \omega\alpha^2 = \omega\dfrac{1-\sqrt{3}}{\sqrt{2}}e_1\cdot\dfrac{1+\sqrt{3}}{\sqrt{2}}e_1 = -\omega, \\ \omega\beta^2 = \omega(1-\sqrt{2})\,e_2\cdot(1+\sqrt{2})\,e_2 = -\omega, \\ \omega\gamma^2 = \omega(1-\sqrt{2})\dfrac{1-\sqrt{3}}{\sqrt{2}}e_3\cdot(1+\sqrt{2})\dfrac{1+\sqrt{3}}{-\sqrt{2}}e_3 = -\omega, \end{cases}$$

also

$$(6)\qquad (\sqrt{2}, \sqrt{3}, \omega)\,\alpha^2 = (\sqrt{2}, \sqrt{3}, \omega)\,\beta^2 = (\sqrt{2}, \sqrt{3}, \omega)\,\gamma^2 = (\sqrt{2}, \sqrt{3}, -\omega).$$

Man kann also setzen

$$(7)\qquad \alpha^2 = \beta^2 = \gamma^2 = \varepsilon.$$

Aus (5) oder (6) geht hervor, daß ω nicht in $R(\sqrt{2}, \sqrt{3})$ enthalten ist, weil sonst zufolge $(\sqrt{2}, \sqrt{3})\,\alpha^2 = (\sqrt{2}, \sqrt{3})$ auch $\omega\alpha^2$ gleich ω sein müßte; mithin ist $R(\sqrt{2}, \sqrt{3}, \omega)$ vom Grade 8, und da derselbe durch fünf verschiedene Permutationen 1, α, β, γ, ε in sich selbst übergeht, so muß dasselbe auch für seine übrigen drei Permutationen gelten; mithin ist er ein Normalkörper. Aus (5) und (4) folgt weiter

$$\omega\alpha^3 = -\omega\alpha = -\omega\frac{1-\sqrt{3}}{\sqrt{2}}e_1,$$

$$\omega\beta^3 = -\omega\beta = -\omega(1-\sqrt{2})\,e_2,$$

$$\omega\gamma^3 = -\omega\gamma = -\omega(1-\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}}e_3;$$

vergleicht man mit (4) und bedenkt, daß α^3, β^3, γ^3 auf den Körper $R(\sqrt{2}, \sqrt{3})$ genau so wirken wie α, β, γ in (3), so dürfen wir offenbar $e_1 = e_2 = e_3 = -1$ annehmen, wodurch

$$\omega\alpha = -\omega\frac{1-\sqrt{3}}{\sqrt{2}},\ \omega\beta = -\omega(1-\sqrt{2}),\ \omega\gamma = -\omega(1-\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}},$$

$$\omega\alpha^3 = \omega\frac{1-\sqrt{3}}{\sqrt{2}},\ \omega\beta^3 = \omega(1-\sqrt{2}),\ \omega\gamma^3 = \omega(1-\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}}$$

wird. Zufolge (7) ist ferner

$$\alpha^3 = \varepsilon\alpha = \alpha\varepsilon = \alpha_1,\quad \beta^3 = \varepsilon\beta = \beta\varepsilon = \beta_1,\quad \gamma^3 = \varepsilon\gamma = \gamma\varepsilon = \gamma_1,$$

$$(\sqrt{2}, \sqrt{3}, \omega)\,\alpha_1 = (\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon\alpha = (\sqrt{2}, \sqrt{3}, -\omega)\,\alpha = (\ \sqrt{2}, -\sqrt{3}, -\omega\alpha),$$
$$(\sqrt{2}, \sqrt{3}, \omega)\,\beta_1 = (\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon\beta = (\sqrt{2}, \sqrt{3}, -\omega)\,\beta = (-\sqrt{2}, \ \sqrt{3}, -\omega\beta),$$
$$(\sqrt{2}, \sqrt{3}, \omega)\,\gamma_1 = (\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon\gamma = (\sqrt{2}, \sqrt{3}, -\omega)\,\gamma = (-\sqrt{2}, -\sqrt{3}, -\omega\gamma),$$

und da

$$(\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon^2 = (\sqrt{2}, \sqrt{3}, -\omega)\,\varepsilon = (\sqrt{2}, \sqrt{3}, \omega),$$

so ist

$$\varepsilon^2 = 1 = \alpha^4 = \beta^4 = \gamma^4 = \alpha_1^4 = \beta_1^4 = \gamma_1^4;$$
$$\alpha_1^2 = \beta_1^2 = \gamma_1^2 = \varepsilon;$$
$$\alpha_1^3 = \alpha,\ \beta_1^3 = \beta,\ \gamma_1^3 = \gamma.$$

Ferner ist

$$\omega\beta\gamma = [-\omega(1-\sqrt{2})]\gamma = \omega(1-\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}}\cdot(1+\sqrt{2})$$

$$= -\omega\frac{1-\sqrt{3}}{\sqrt{2}} = \omega\alpha, (\sqrt{2},\sqrt{3})\beta\gamma = (-\sqrt{2},\sqrt{3})\gamma = (\sqrt{2},-\sqrt{3})$$

$$= (\sqrt{2},\sqrt{3})\alpha;$$

$$\omega\gamma\alpha = \left[-\omega(1-\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}}\right]\alpha = \omega\frac{1-\sqrt{3}}{\sqrt{2}}\cdot(1-\sqrt{2})\frac{1+\sqrt{3}}{\sqrt{2}}$$

$$= -\omega(1-\sqrt{2}) = \omega\beta, (\sqrt{2},\sqrt{3})\gamma\alpha = (-\sqrt{2},-\sqrt{3})\alpha$$

$$= (-\sqrt{2},\sqrt{3}) = (\sqrt{2},\sqrt{3})\beta;$$

$$\omega\alpha\beta = \left(-\omega\frac{1-\sqrt{3}}{\sqrt{2}}\right)\beta = \omega(1-\sqrt{2})\cdot\frac{1-\sqrt{3}}{-\sqrt{2}} = \omega\gamma,$$

$$(\sqrt{2},\sqrt{3})\alpha\beta = (\sqrt{2},-\sqrt{3})\beta = (-\sqrt{2},-\sqrt{3}) = (\sqrt{2},\sqrt{3})\gamma.$$

Daraus ergeben sich die drei ersten der sechs folgenden Gleichungen:

$$\beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma,$$
$$\gamma\beta = \alpha_1, \quad \alpha\gamma = \beta_1, \quad \beta\alpha = \gamma_1,$$

aus denen die übrigen und das Schema der Komposition folgen.

Notwendige und hinreichende Bedingung bei allgemeinem biquadratischem Unterkörper.

Über dem Körper $H = R(\sqrt{a},\sqrt{b})$, wo a und b relative Primzahlen, voneinander und von 1 verschieden und durch kein Primzahlquadrat teilbar sind, sei ein Quaternionkörper $\Omega = H(\omega)$ errichtet. Sind α, β, γ, ε Permutationen dieses Körpers mit den Eigenschaften

$$\varepsilon^2 = 1,$$
$$\alpha^2 = \beta^2 = \gamma^2 = \varepsilon,$$
$$\beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma,$$

so liegen die Zahlen

$$\omega(\omega\alpha) = u, \quad \omega(\omega\beta) = v, \quad \omega(\omega\gamma) = w$$

in H*), und es ist

$$\omega\varepsilon = -\omega,$$
$$\omega(\omega\alpha) = u = -u\alpha, \quad (\omega\beta)(\omega\gamma) = u\beta = -u\gamma;$$
$$\omega(\omega\beta) = v = -v\beta, \quad (\omega\gamma)(\omega\alpha) = v\gamma = -v\alpha;$$
$$\omega(\omega\gamma) = w = -w\gamma, \quad (\omega\alpha)(\omega\beta) = w\alpha = -w\beta.$$

*) [Vgl. den Anfang.]

Bezeichnet man $\omega(\omega\alpha)(\omega\beta)(\omega\gamma)$ mit h, so ist

$$\omega(\omega\alpha)(\omega\beta)(\omega\gamma) = u(u\beta) = v(v\gamma) = w(w\alpha) = h,$$
$$\omega^3 = \frac{uvw}{h}.$$

Man kann annehmen, es sei

$$(\sqrt{a},\sqrt{b},\sqrt{a}\sqrt{b})\alpha = (\sqrt{a},-\sqrt{b},-\sqrt{a}\sqrt{b}),$$
$$(\sqrt{a},\sqrt{b},\sqrt{a}\sqrt{b})\beta = (-\sqrt{a},\sqrt{b},-\sqrt{a}\sqrt{b}),$$
$$(\sqrt{a},\sqrt{b},\sqrt{a}\sqrt{b})\gamma = (-\sqrt{a},-\sqrt{b},\sqrt{a}\sqrt{b}).$$

Man setze nun

$$u = q + x\sqrt{a} + y\sqrt{b} + z\sqrt{a}\sqrt{b}$$

mit rationalen q, x, y, z. Dann ist

$$u\alpha = q + x\sqrt{a} - y\sqrt{b} - z\sqrt{a}\sqrt{b},$$

und wegen $u = -u\alpha$ muß

$$u = (y + z\sqrt{a})\sqrt{b}, \quad u\beta = (y - z\sqrt{a})\sqrt{b}$$

sein. In entsprechender Weise ergibt sich

$$v = (y_1 + z_1\sqrt{b})\sqrt{a}, \quad v\gamma = -(y_1 - z_1\sqrt{b})\sqrt{a},$$
$$w = y_2\sqrt{a} + z_2\sqrt{b}, \quad w\alpha = y_2\sqrt{a} - z_2\sqrt{b}$$

mit rationalen y_1, z_1, y_2, z_2, also

$$h = b(y^2 - az^2) = -a(y_1^2 - bz_1^2) = ay_2^2 - bz_2^2.$$

Man kann voraussetzen, daß y, z, y_1, z_1, y_2, z_2 ganze rationale Zahlen sind, da man sonst ω nur mit einer passenden natürlichen Zahl zu multiplizieren braucht. Wegen der über a und b getroffenen Voraussetzungen kann man also setzen

$$y = ar, \quad y_1 = bs, \quad y_2 = bt, \quad z_2 = ap$$

mit ganzen rationalen r, s, t, p. Es folgt

$$\frac{h}{ab} = ar^2 - z^2 = z_1^2 - bs^2 = bt^2 - ap^2$$ *).

*) [Die Bedingung ist auch hinreichend; vgl. die Erläuterung.]

Erläuterungen zur vorstehenden Abhandlung.

Die Arbeit findet sich im Nachlaß in nicht ganz druckfertiger Gestalt. In der wohl ziemlich gleichzeitigen Arbeit „Über Gruppen, deren sämtliche Teiler Normalteiler sind“ (XXVII) ist das Hauptergebnis vorweggenommen, da der dortige Ausdruck

$$\omega^2 = r(2+\sqrt{2})(3+\sqrt{6}) \qquad (r \neq 0 \text{ beliebig rational})$$

sich nur durch einen in $R(\sqrt{2}, \sqrt{3})$ quadratischen Faktor von der Normalform (2) unterscheidet. (Vgl. die Rechnung auf S. 379. Durch einen solchen Faktor unterscheidet sich auch das obige r von dem dortigen m.)

Das Ergebnis, daß jeder Quaternionkörper über $R(\sqrt{2}, \sqrt{3})$ durch die Quadratwurzel eines Ausdrucks (2) erzeugt wird, scheint erst aus späterer Zeit zu stammen. Aber daß die Quadratwurzeln aus den Zahlen (2) Beispiele von Quaternionkörpern ergeben, findet sich schon auf einem von Dedekind mit dem Datum des 15. Februar 1886 versehenen Blatt bewiesen *) (vgl. XXVII, S. 91). Jene Tatsache ergibt sich als Sonderfall einer von Dedekind am vorhergehenden Tage gefundenen, zunächst als notwendig erkannten Bedingung, die sich auf die Unterkörper vierten Grades beliebiger Quaternionkörper bezieht und in einigen diophantischen Gleichungen besteht. Diese Bemerkungen tragen das Datum des 14. Februar 1886 und sind hier am Schluß unter Hinzufügung überleitender Worte wiedergegeben. Die diophantischen Gleichungen sind übrigens auch hinreichend; das ergibt sich unschwer, indem man in den Bezeichnungen von S. 383

$$\omega^2 = \frac{u\,v\,w}{h}$$

setzt und die Isomorphismen des durch ω erzeugten Oberkörpers untersucht.

Die in der Erläuterung zu XXVII erwähnte Arbeit von Mertens über denselben Gegenstand geht von der Gleichung und nicht vom Körper aus und beschränkt sich auf die Aufstellung einer notwendigen Bedingung.

W. Weber.

*) Die dortige Herleitung ist fast wörtlich, nur mit den erforderlichen Verallgemeinerungen, in diese Arbeit aufgenommen worden, da der betreffende Teil im späteren Manuskript nur angedeutet war.

XL.

Zur Theorie der Ideale (Göttingen 1894). Anwendung auf die Kreiskörper.

Lemma 1. Ist m eine natürliche Zahl, und α eine primitive Wurzel der Gleichung

$$\alpha^m = 1,$$

so ist

$$\alpha - 1 = 0,$$

wenn $m = 1$,

$$(\alpha-1)^{\varphi(m)} = \varepsilon p,$$

wenn m durch eine und nur eine Primzahl p teilbar ist, und ε eine Einheit bedeutet; $\alpha - 1 = \varepsilon$, wenn m durch mindestens zwei verschiedene Primzahlen teilbar ist.

Beweis. Der erste Fall ist evident. Durchläuft $\alpha' = \alpha^r$ im zweiten Falle alle $\varphi(m)$ primitiven m-ten Einheitswurzeln, und nimmt man $rr' \equiv 1 \pmod{m}$, so sind

$$\frac{\alpha'-1}{\alpha-1} = \frac{\alpha^r-1}{\alpha-1} \quad \text{und} \quad \frac{\alpha-1}{\alpha'-1} = \frac{\alpha'^{r'}-1}{\alpha'-1}$$

ganz, also Einheiten, und da

$$\prod(x-\alpha') = \frac{x^m-1}{x^{\frac{m}{p}}-1}, \quad \text{also} \quad \prod(1-\alpha') = p,$$

so folgt das zweite Resultat. Ist endlich $m = pqn$ durch zwei verschiedene Primzahlen p, q teilbar, so ist $\alpha - 1$ gemeinsamer Teiler von $\alpha^{qn} - 1$ und $\alpha^{pn} - 1$, also (nach dem zweiten Fall) gemeinsamer Teiler von p und q, also eine Einheit, w. z. b. w.

Lemma 2. Es sei $\mathfrak{p}$ ein Primideal eines endlichen Körpers Ω, und p die durch $\mathfrak{p}$ teilbare natürliche Primzahl, $N(\mathfrak{p}) = p^f$, wo f der Grad von $\mathfrak{p}$. Ist nun α eine in Ω enthaltene primitive m-te Einheitswurzel, und setzt man $m = m'p'$, wo p' die höchste in m aufgehende Potenz von p ist, so gehört α zum Exponent m' (mod. $\mathfrak{p}$).

Beweis. Ist ω relative Primzahl zu $\mathfrak{p}$ in Ω, so ist

$$\omega^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}},$$

und der Exponent, zu welchem ω gehört (mod. $\mathfrak{p}$), ist die kleinste natürliche Zahl e, welche der Bedingung $\omega^e \equiv 1$ (mod. $\mathfrak{p}$) genügt; dann ist e ein Divisor von $N(\mathfrak{p})-1$, also gewiß unteilbar durch p. Wendet man dies auf den Fall $\omega = \alpha$ an, so folgt aus $\alpha^m = \alpha^{m'p'} = 1 \equiv 1$ (mod. $\mathfrak{p}$), daß e Divisor von $m'p'$, also auch von m' ist. Setzt man nun $m' = ee'$, so ist α^e eine primitive $(e'p')$-te Einheitswurzel, und da $\alpha^e - 1 \equiv 0$ (mod. $\mathfrak{p}$), also keine Einheit ist, so sind (nach Lemma 1) nur zwei Fälle möglich: Entweder ist $e'p' = 1$, also $e' = 1$, $e = m' = m$. Oder $e'p'$ ist durch eine und nur eine Primzahl q teilbar; dann ist $\alpha^e - 1$ (nach Lemma 1) Divisor von q, und da $\alpha^e - 1$, also auch q durch $\mathfrak{p}$ teilbar ist, so muß $q = p$ sein; also ist $e'p'$ Potenz von p, und da e' als Divisor von m' nicht durch p teilbar ist, so muß auch in diesem Falle $e' = 1$, $e = m'$ sein. Also ist in beiden Fällen $e = m'$, w. z. b. w.

Zusatz. Da e Divisor von $N(\mathfrak{p})-1 = p^f - 1$ ist, so folgt $p^f \equiv 1$ (mod. m').

Lemma 3. Es sei wieder α eine primitive m-te Einheitswurzel, und $\Omega = R(\alpha) = K_m$ der durch α erzeugte Körper. Als bekannt wird nur Folgendes vorausgesetzt. Die sämtlichen $\varphi(m)$ primitiven m-ten Einheitswurzeln $\alpha' = \alpha^r$, wo r alle nach m inkongruenten relativen Primzahlen zu m durchläuft, sind die sämtlichen Wurzeln einer Gleichung vom Grade $\varphi(m)$ mit rationalen Koeffizienten (ihre Irreduzibilität soll erst bewiesen, nicht vorausgesetzt werden). Jedenfalls folgt hieraus, daß alle n mit α konjugierten Zahlen unter diesen Zahlen α' zu suchen sind; durch jede der n entsprechenden Permutationen φ' geht α in eine dieser n Zahlen $\alpha\varphi' = \alpha' = \alpha^{r'}$ über, und da $\Omega' = \Omega\varphi' = R(\alpha') = R(\alpha^{r'})$ offenbar ein Divisor von Ω und folglich (!) auch $= \Omega$ ist, so ist Ω ein Normalkörper. Sind φ', φ'' zwei solche Permutationen von Ω, und zwar $\alpha\varphi' = \alpha^{r'}$, $\alpha\varphi'' = \alpha^{r''}$, so folgt $(\alpha\varphi')\varphi'' = (\alpha^{r'})\varphi'' = (\alpha\varphi'')^{r'} = (\alpha^{r''})^{r'} = \alpha^{r'r''}$, ebenso $(\alpha\varphi'')\varphi' = \alpha^{r''r'}$, mithin $\varphi'\varphi'' = \varphi''\varphi'$, d. h. Ω ist ein Abelscher Körper, und die Gruppe Φ aller n Permutationen φ ist eine Abelsche Gruppe. Man kann eine Permutation φ, durch welche α in $\alpha\varphi = \alpha^r$ übergeht, kurz als Permutation r bezeichnen, wo r ein beliebiger Repräsentant der ganzen Zahlenklasse r (mod. m) ist, und die Zusammensetzung der Permutationen φ in der Gruppe Φ entspricht der Multiplikation dieser Zahlenklassen; die identische Permutation entspricht der Zahlenklasse 1 (mod. m). Diese Gruppe Φ ist dann ein Teiler der aus allen $\varphi(m)$ Klassen bestehenden Gruppe, also ihr Grad n ein Divisor von $\varphi(m)$.

Satz: Es ist $n = \varphi(m)$; d. h. die Gleichung, deren Wurzeln die $\varphi(m)$ primitiven m-ten Einheitswurzeln sind, ist irreduzibel; Φ ist die Gruppe aller $\varphi(m)$ Zahlenklassen r (mod. m), deren Elemente r relative Primzahlen zu m sind.

Beweis. Ist p eine natürliche Primzahl, die nicht in m aufgeht, und $\mathfrak{p}$ irgendein in p aufgehendes Primideal des Körpers Ω, so gibt es [zur Theorie der Ideale] in der Gruppe Φ mindestens eine Permutation ψ_0 von der Art, daß jede ganze Zahl ω in Ω der Kongruenz

$$\omega^p \equiv \omega\psi_0 \pmod{\mathfrak{p}}$$

genügt. Wendet man dies auf $\omega = \alpha$ an und setzt

$$\alpha\psi_0 = \alpha^{p_0},$$

wo p_0 relative Primzahl zu m, durch welche ψ_0 vollständig definiert ist, so folgt

$$\alpha^p \equiv \alpha^{p_0} \pmod{\mathfrak{p}}.$$

Wendet man hierauf das obige Lemma 2 an, so ist $p' = 1$, $m' = m$ zu setzen, also gehört α (mod. $\mathfrak{p}$) zum Exponent m, mithin ist $p_0 \equiv p$ (mod. m), und folglich $\alpha\psi_0 = \alpha^{p_0} = \alpha^p$. Es ist daher α^p konjugiert mit α. Ist nun r eine beliebige relative Primzahl zu m, so kann man immer $r \equiv p_1 p_2 p_3 \cdots$ (mod. m) setzen, wo $p_1, p_2, p_3 \cdots$ natürliche Primzahlen bedeuten; nun gibt es, wie eben gezeigt, immer Permutationen $\varphi_1, \varphi_2, \varphi_3, \cdots$ in der Gruppe Φ, für welche $\alpha\varphi_1 = \alpha^{p_1}$, $\alpha\varphi_2 = \alpha^{p_2}$, $\alpha\varphi_3 = \alpha^{p_3} \cdots$, also auch $\alpha\varphi_1\varphi_2\varphi_3 \cdots = \alpha^{p_1 p_2 p_3 \cdots} = \alpha^r$ wird; mithin ist jede Potenz α^r, d. h. jede primitive m-te Einheitswurzel α' konjugiert mit α, w. z. b. w. (Ähnlichkeit mit meinem Beweise in Crelles Journal Bd. 54).

Erläuterungen zur vorstehenden Abhandlung.

Der hier gegebene Irreduzibilitätsbeweis der Kreisteilungsgleichung beruht auf den beiden Tatsachen:

1. Eine primitive m-te Einheitswurzel bleibt primitiv modulo jedem nicht in m aufgehenden Primideal $\mathfrak{p}$ des Körpers K dieser Einheitswurzeln.

2. Es gibt eine Substitution ψ_0 der Zerlegungsgruppe von $\mathfrak{p}$, für die $\omega\,\psi_0 \equiv \omega^p (\mathfrak{p})$ für jedes ganze ω aus K.

Die vermöge 2. gegebene Zuordnung zwischen Galoisgruppe und Klassengruppe — aus der die Irreduzibilität unmittelbar folgt — ist die Zuordnung im Sinn des allgemeinen Artinschen Reziprozitätsgesetzes, aber in stark abgeschwächter und daher elementarer Form. Denn die Zuordnung geschieht nur zu allen Primzahlen enthaltenden Klassen, also zu einem Erzeugendensystem der Klassengruppe, was zur Festlegung des ganzen Isomorphismus hier ausreicht. Die Frage, ob dieses Erzeugendensystem die Klassengruppe erschöpft, also der Satz von der arithmetischen Progression, bleibt unberührt.

Daß auch die Irreduzibilität der Valenzgleichung in der Theorie der komplexen Multiplikation sich entsprechend beweisen läßt, hat Dedekind an anderer Stelle ohne Beweis-Ausführung bemerkt. Es handelt sich wohl wesentlich um den in Weber, Algebra, Bd. 3, § 122 (2. Auflage) übergegangenen Beweis für die Irreduzibilität der Klassengleichung.

Noether.

XLI.

Gruppencharaktere von Zahlklassen in endlichen Körpern.

Ist $\mathfrak{o}$ das System aller ganzen Zahlen ω des endlichen Körpers Ω, und $\mathfrak{m}$ ein Ideal in $\mathfrak{o}$, so bestehen alle diejenigen Zahlen μ in $\mathfrak{o}$, welche relative Primzahlen zu $\mathfrak{m}$ sind, aus $\varphi(\mathfrak{m})$ Klassen $\mathfrak{m} + \mu$, welche eine Abelsche Gruppe bilden: multipliziert man jede Zahl einer solchen Klasse $\mathfrak{m} + \mu_1$ mit jeder Zahl einer solchen Klasse $\mathfrak{m} + \mu_2$, so gehören alle diese Produkte wieder einer einzigen solchen Klasse $\mathfrak{m} + \mu_1\mu_2$ an (was man durch $\mathfrak{m} + \mu_1\mu_2 = (\mathfrak{m} + \mu_1)(\mathfrak{m} + \mu_2)$ bezeichnen könnte). Zunächst einige Hülfssätze *).

Satz 1. Ist ν relative Primzahl zum Ideal $\mathfrak{n}$, so gibt es Zahlen μ, welche relative Primzahlen zum Ideal $\mathfrak{m}$ sind und zugleich die Kongruenz

$$\mu \equiv \nu \pmod{\mathfrak{n}} \tag{1}$$

erfüllen, d. h. in der Klasse $\mathfrak{n} + \nu$ enthalten sind; das System aller dieser Zahlen μ besteht aus $\varphi(\mathfrak{p})$ Klassen $\mathfrak{n}\mathfrak{p} + \mu$, wo $\mathfrak{p}$ das Produkt aller derjenigen in $\mathfrak{m}$ aufgehenden verschiedenen Primideale bedeutet, welche nicht in $\mathfrak{n}$ aufgehen (falls gar kein solches Primideal vorhanden ist, ist $\mathfrak{p} = \mathfrak{o}$ zu setzen).

Beweis. Alle Zahlen π, die relative Primzahlen zu $\mathfrak{p}$ sind, bestehen aus $\varphi(\mathfrak{p})$ Klassen $\mathfrak{p} + \pi$. Soll eine Zahl μ, die der Kongruenz (1) genügt, relative Primzahl zu $\mathfrak{m}$ werden, so ist erforderlich, daß sie auch einer dieser Klassen $\mathfrak{p} + \pi$ angehört, also einer der $\varphi(\mathfrak{p})$ entsprechenden Kongruenzen

$$\mu \equiv \pi \pmod{\mathfrak{p}} \tag{2}$$

genügt; und dies ist auch hinreichend, weil μ zufolge (1) durch kein Primideal teilbar ist, welches sowohl in $\mathfrak{m}$ als in $\mathfrak{n}$ aufgeht. Da

*) Besser gleich von Anfang an: Sind $\mathfrak{m}, \mathfrak{n}$ Ideale, ω eine Zahl in $\mathfrak{o}$, so soll mit $(\mathfrak{m}; \mathfrak{n} + \omega)$ das System aller derjenigen in der Klasse $\mathfrak{n} + \omega$ enthaltenen Zahlen bezeichnet werden, welche relative Primzahlen zu $\mathfrak{m}$ sind. — Bedingung der Existenz: $\mathfrak{m} + \mathfrak{n} + \mathfrak{o}\,\omega = \mathfrak{o}$, d. h. ω relative Primzahl zu $\mathfrak{m} + \mathfrak{n}$.

ferner $\mathfrak{n}$, $\mathfrak{p}$ relative Primideale sind, so liefert die Kongruenz (1) in Verbindung mit je einer der $\varphi(\mathfrak{p})$ Kongruenzen (2) je eine Zahlklasse $\mathfrak{n}\mathfrak{p}+\mu$, und diese $\varphi(\mathfrak{p})$ Klassen sind verschieden voneinander; w. z. b. w.

Zusatz 1. Bedeutet $\mathfrak{m}'$ das kleinste gemeinsame Vielfache der Ideale $\mathfrak{m}$, $\mathfrak{n}$, so ist $\mathfrak{m}'$ auch teilbar durch $\mathfrak{n}\mathfrak{p}$, also auch das kleinste gemeinsame Vielfache von $\mathfrak{m}$, $\mathfrak{n}\mathfrak{p}$; jede Klasse $\mathfrak{n}\mathfrak{p}+\mu$ besteht aus $(\mathfrak{n}\mathfrak{p}, \mathfrak{m}')$ Klassen $\mathfrak{m}'+\mu$, und folglich ist

$$(3) \qquad (\mathfrak{n}\mathfrak{p}, \mathfrak{m}')\,\varphi(\mathfrak{p}) = \frac{N(\mathfrak{m}')\,\varphi(\mathfrak{p})}{N(\mathfrak{n}\mathfrak{p})} = \frac{N(\mathfrak{m}')}{N(\mathfrak{n})}\cdot\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})}$$

die Anzahl der sämtlichen verschiedenen Klassen $\mathfrak{m}'+\mu$, aus welchen das System der Zahlen μ besteht.

Zusatz 2. Ist $\mathfrak{n}$ ein Teiler von $\mathfrak{m}$, also $\mathfrak{m}'=\mathfrak{m}$, und bedeutet $\mathfrak{q}$ das Produkt aller verschiedenen in $\mathfrak{n}$ aufgehenden, also $\mathfrak{p}\,\mathfrak{q}$ das Produkt aller verschiedenen in $\mathfrak{m}$ aufgehenden Primideale, so ist

$$\varphi(\mathfrak{m}) = N(\mathfrak{m})\frac{\varphi(\mathfrak{p}\,\mathfrak{q})}{N(\mathfrak{p}\,\mathfrak{q})} = N(\mathfrak{m})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})}\cdot\frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})},$$

$$\varphi(\mathfrak{n}) = N(\mathfrak{n})\frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})},$$

und folglich ist

$$(4) \qquad \frac{N(\mathfrak{m})}{N(\mathfrak{n})}\cdot\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})} = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})}$$

die Anzahl aller Klassen $\mathfrak{m}+\mu$, aus denen das System der Zahlen μ besteht. [Läßt man ν in (1) die $\varphi(\mathfrak{n})$ verschiedenen Zahlklassen $\mathfrak{n}+\nu$ durchlaufen, welche aus relativen Primzahlen zu $\mathfrak{n}$ bestehen, so erhält man die sämtlichen $\varphi(\mathfrak{m}) = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})}\varphi(\mathfrak{n})$ Zahlklassen $\mathfrak{m}+\mu$, welche aus relativen Primzahlen zu $\mathfrak{m}$ bestehen.]

Definition 1. Ist das Ideal $\mathfrak{n}$ ein Divisor des Ideals $\mathfrak{m}$, so soll mit $\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right)$ das System aller derjenigen Zahlen ν bezeichnet werden, welche der Kongruenz

$$(5) \qquad \nu \equiv 1 \pmod{\mathfrak{n}}$$

genügen und zugleich relative Primzahlen zu $\mathfrak{m}$ sind; dasselbe besteht aus $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})}$ Klassen $\mathfrak{m}+\nu$, die mit

$$(6) \qquad \mathfrak{m}+\nu_1, \mathfrak{m}+\nu_2 \ldots \mathfrak{m}+\nu_n$$

bezeichnet werden mögen, wenn zur Abkürzung

$$(7) \qquad \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})} = n$$

gesetzt wird. — Das System $\left(\frac{\mathfrak{m}}{0}\right)$ besteht aus allen relativen Primzahlen μ zu $\mathfrak{m}$, nämlich aus $\varphi(\mathfrak{m})$ Klassen $\mathfrak{m}+\mu$; das System $\left(\frac{\mathfrak{m}}{\mathfrak{m}}\right)$ besteht aus der einzigen Klasse $\mathfrak{m}+1$.

Satz 2. Die n Klassen $\mathfrak{m}+\nu$ des Systems $\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right)$ bilden eine Abelsche Gruppe; sind μ, μ' zwei nach $\mathfrak{n}$ kongruente relative Primzahlen zu $\mathfrak{m}$, d. h. also Zahlen in $\left\langle\frac{\mathfrak{m}}{0}\right\rangle$, so ist

$$(8) \qquad \mu' \equiv \mu\,\nu \pmod{\mathfrak{m}}$$

und umgekehrt.

Beweis. Denn sind ν, ν' Zahlen in $\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right)$, also $\nu \equiv \nu' \equiv 1 \pmod{\mathfrak{n}}$, so ist auch $\nu\,\nu' \equiv 1 \pmod{\mathfrak{n}}$, und da ν, ν' relative Primzahlen zu $\mathfrak{m}$, d. h. in $\left(\frac{\mathfrak{m}}{0}\right)$ enthalten sind, so ist auch $\nu\,\nu'$ in $\left(\frac{\mathfrak{m}}{0}\right)$, also auch in $\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right)$ enthalten. Sind ferner μ, μ' Zahlen in $\left\langle\frac{\mathfrak{m}}{0}\right\rangle$, so gibt es stets eine und nur eine Klasse $\mathfrak{m}+\nu$ in $\left\langle\frac{\mathfrak{m}}{0}\right\rangle$, welche der Kongruenz (8) und folglich auch der Kongruenz $\mu' \equiv \mu\,\nu \pmod{\mathfrak{n}}$ genügt; ist nun $\mu' \equiv \mu \pmod{\mathfrak{n}}$, so folgt, weil μ', μ auch in $\left(\frac{\mathfrak{n}}{0}\right)$ enthalten sind, $1 \equiv \nu \pmod{\mathfrak{n}}$, d. h. ν ist in $\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right)$ enthalten. Umgekehrt: genügen drei Zahlen ν, μ, μ' in $\left\langle\frac{\mathfrak{m}}{0}\right\rangle$ der Kongruenz (8), und ist ν in $\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right)$ enthalten, genügt also der Kongruenz (5), so folgt $\mu' \equiv \mu \pmod{\mathfrak{n}}$. W. z. b. w.

Satz 3. Sind $\mathfrak{a}$, $\mathfrak{b}$ Faktoren des Ideals $\mathfrak{m}$, so ist die Gruppe

$$\left.\begin{array}{l}\left(\frac{\mathfrak{m}}{\mathfrak{a}-\mathfrak{b}}\right) \text{ der größte gem. Divisor} \\ \left(\frac{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}\right) \text{ das kleinste gem. Multiplum}\end{array}\right\} \text{ der Gruppen } \left\langle\frac{\mathfrak{m}}{\mathfrak{a}}\right\rangle, \left\langle\frac{\mathfrak{m}}{\mathfrak{b}}\right\rangle.$$

Beweis. Das Erstere leicht; denn wenn $\mathfrak{m}+\mu$ eine beiden Gruppen $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$ gemeinsame Klasse ist, so ist $\mu \equiv 1 \pmod{\mathfrak{a}}$ und $\mu \equiv 1 \pmod{\mathfrak{b}}$, also auch $\mu \equiv 1 \pmod{\mathfrak{a}-\mathfrak{b}}$, d. h. die Klasse $\mathfrak{m}+\mu$ ist in $\binom{\mathfrak{m}}{\mathfrak{a}-\mathfrak{b}}$ enthalten; und umgekehrt, wenn letzteres der Fall, so ist $\mu \equiv 1 \pmod{\mathfrak{a}-\mathfrak{b}}$, also auch $\mu \equiv 1 \pmod{\mathfrak{a}}$ und $\mu \equiv 1 \pmod{\mathfrak{b}}$, d. h. die Klasse $\mathfrak{m}+\mu$ ist beiden Gruppen $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$ gemeinsam, w. z. b. w. — Das Letztere liegt etwas tiefer. Ist M das kl. gem. Multiplum von $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$, so sind alle Klassen $\mathfrak{m}+\alpha$ von $\binom{\mathfrak{m}}{\mathfrak{a}}$ und alle Klassen $\mathfrak{m}+\beta$ von $\binom{\mathfrak{m}}{\mathfrak{b}}$, also auch alle Klassen $\mathfrak{m}+\alpha\beta$ in M enthalten, und das System dieser Klassen $\mathfrak{m}+\alpha\beta$, welches eine Gruppe bildet $(\alpha_1\beta_1 \cdot \alpha_2\beta_2 \equiv (\alpha_1\alpha_2)\,(\beta_1\beta_2))$, ist identisch mit M. Da nun $\alpha \equiv 1 \pmod{\mathfrak{a}}$ und $\beta \equiv 1 \pmod{\mathfrak{b}}$, so ist auch $\alpha \equiv \beta \equiv \alpha\beta \equiv 1 \pmod{\mathfrak{a}+\mathfrak{b}}$, und folglich sind alle Klassen $\mathfrak{m}+\alpha\beta$ von M in $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ enthalten. Umgekehrt, wenn $\mathfrak{m}+\mu$ eine Klasse in $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$, also $\mu \equiv 1 \pmod{\mathfrak{a}+\mathfrak{b}}$ und relative Primzahl zu $\mathfrak{m}$ ist, so kann man zunächst eine Zahl α_0 bestimmen, welche gleichzeitig den Kongruenzen $\alpha_0 \equiv 1 \pmod{\mathfrak{a}}$, $\alpha_0 \equiv \mu \pmod{\mathfrak{b}}$ genügt [D. § 171, III, alle diese Zahlen α_0 bilden eine Klasse $(\mathfrak{a}-\mathfrak{b})+\alpha_0$], und zwar wird α_0 relative Primzahl zu $\mathfrak{a}$ und $\mathfrak{b}$, also auch zu $\mathfrak{a}-\mathfrak{b}$; nach Satz 1 gibt es daher auch Zahlen α, welche relative Primzahlen zu $\mathfrak{m}$ sind und der Kongruenz $\alpha \equiv \alpha_0 \pmod{\mathfrak{a}-\mathfrak{b}}$, also auch den Kongruenzen $\alpha \equiv 1 \pmod{\mathfrak{a}}$, $\alpha \equiv \mu \pmod{\mathfrak{b}}$ genügen (nach Zusatz 2 gibt es $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a}-\mathfrak{b})}$ verschiedene solche Klassen $\mathfrak{m}+\alpha$). Da α relative Primzahl zu $\mathfrak{m}$ (α enthalten in $\binom{\mathfrak{m}}{\mathfrak{a}}$), so kann man β so bestimmen, daß $\alpha\beta \equiv \mu \pmod{\mathfrak{m}}$ wird; weil μ relative Primzahl zu $\mathfrak{m}$, so gilt dasselbe auch von β; da ferner $\alpha \equiv \mu \pmod{\mathfrak{b}}$, so ist $\mu\beta \equiv \mu \pmod{\mathfrak{b}}$, und da μ relative Primzahl zu $\mathfrak{m}$, also auch zu $\mathfrak{b}$, so folgt $\beta \equiv 1 \pmod{\mathfrak{b}}$, d. h. β ist enthalten in $\binom{\mathfrak{m}}{\mathfrak{b}}$. Also ist jede in $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ enthaltene Klasse $\mathfrak{m}+\mu$ von der Form $\mathfrak{m}+\alpha\beta$, wo $\mathfrak{m}+\alpha$ in $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\mathfrak{m}+\beta$ in $\binom{\mathfrak{m}}{\mathfrak{b}}$ enthalten, d. h. jede Klasse $\mathfrak{m}+\mu$ von $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ ist in M enthalten. Also $M = \binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$, w. z. b. w.

Bemerkung. Der zweite Teil des zweiten Satzes kann auch so bewiesen werden. Nach einem allgemeinen Satze über Abelsche Gruppen A, B, deren gr. gem. Div. D, kl. gem. Multiplum M, ist $ab = \partial m$, wo a, b, ∂, m die Grade (Anzahlen der Elemente) von A, B, D, M bedeuten (D. § 149, S. 396 — 397). Setzt man $A = \binom{\mathfrak{m}}{\mathfrak{a}}$, $B = \binom{\mathfrak{m}}{\mathfrak{b}}$, so ist nach dem ersten Teile

$$D = \binom{\mathfrak{m}}{\mathfrak{a}-\mathfrak{b}}, \text{ also } a = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a})}, \quad b = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{b})}, \; \partial = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a}-\mathfrak{b})},$$

also

$$m = \frac{\varphi(\mathfrak{m})\,\varphi(\mathfrak{a}-\mathfrak{b})}{\varphi(\mathfrak{a})\,\varphi(\mathfrak{b})} = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a}+\mathfrak{b})}$$

[weil allgemein $\varphi(\mathfrak{a})\,\varphi(\mathfrak{b}) = \varphi(\mathfrak{a}-\mathfrak{b})\,\varphi(\mathfrak{a}+\mathfrak{b})$ ist, leicht zu zeigen*)]. Da nun im ersten Teile des Beweises des zweiten Satzes schon gezeigt ist, daß M in $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ enthalten, so muß, weil M denselben Grad $m = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a}+\mathfrak{b})}$ besitzt wie $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$, notwendig $M = \binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ sein, w. z. b. w.

Definition 2. Ist die Klassengruppe H ein Divisor von $\binom{\mathfrak{m}}{\mathfrak{o}}$, so betrachte man alle diejenigen Faktoren $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ... von $\mathfrak{m}$, deren zugehörige Klassengruppen $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$, $\binom{\mathfrak{m}}{\mathfrak{c}}$ ... Divisoren von H sind

*) $\mathfrak{p}$ das Produkt aller verschiedenen Primideale, die in $\mathfrak{a}$, nicht in $\mathfrak{b}$,
$\mathfrak{q}$ „ „ „ „ „ „ nicht in $\mathfrak{a}$, aber in $\mathfrak{b}$,
$\mathfrak{r}$ „ „ „ „ „ „ in $\mathfrak{a}$ und in $\mathfrak{b}$
aufgehen; so ist

$$\varphi(\mathfrak{a}) = N(\mathfrak{a})\frac{\varphi(\mathfrak{p}\mathfrak{r})}{N(\mathfrak{p}\mathfrak{r})} = N(\mathfrak{a})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})}\cdot\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})},$$

$$\varphi(\mathfrak{b}) = N(\mathfrak{b})\frac{\varphi(\mathfrak{q}\mathfrak{r})}{N(\mathfrak{q}\mathfrak{r})} = N(\mathfrak{b})\frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})}\cdot\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})},$$

$$\varphi(\mathfrak{a}-\mathfrak{b}) = N(\mathfrak{a}-\mathfrak{b})\frac{\varphi(\mathfrak{p}\mathfrak{q}\mathfrak{r})}{N(\mathfrak{p}\mathfrak{q}\mathfrak{r})} = N(\mathfrak{a}-\mathfrak{b})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})}\cdot\frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})}\cdot\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})},$$

$$\varphi(\mathfrak{a}+\mathfrak{b}) = N(\mathfrak{a}+\mathfrak{b})\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})},$$

und da $\mathfrak{a}\mathfrak{b} = (\mathfrak{a}-\mathfrak{b})(\mathfrak{a}+\mathfrak{b})$, also auch $N(\mathfrak{a})\,N(\mathfrak{b}) = N(\mathfrak{a}-\mathfrak{b})\,N(\mathfrak{a}+\mathfrak{b})$, so folgt auch $\varphi(\mathfrak{a})\,\varphi(\mathfrak{b}) = \varphi(\mathfrak{a}-\mathfrak{b})\,\varphi(\mathfrak{a}+\mathfrak{b})$, w. z. b. w.

(jedenfalls ist $\binom{\mathfrak{m}}{\mathfrak{m}} = \mathfrak{m} + 1$ in der Gruppe H enthalten). Nach dem eben bewiesenen Satze befindet sich unter diesen Idealen $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ auch deren größter gemeinsamer Divisor $\mathfrak{n} = \mathfrak{a} + \mathfrak{b} + \mathfrak{c} \ldots$, und offenbar sind $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ die sämtlichen Ideale, welche Multipla von $\mathfrak{n}$ und zugleich Divisoren von $\mathfrak{m}$ sind. Dieses Ideal $\mathfrak{n}$ soll der Exponent der Gruppe H heißen. Die charakteristische Eigenschaft desselben besteht hierin:

1. Ist ν relative Primzahl zu $\mathfrak{m}$ und $\equiv 1 \pmod{\mathfrak{n}}$, so ist die Klasse $\mathfrak{m} + \nu$ in H enthalten (d. h. $\binom{\mathfrak{m}}{\mathfrak{n}}$ Divisor von H).

2. Ist $\mathfrak{n}'$ Faktor von $\mathfrak{m}$, aber nicht teilbar durch $\mathfrak{n}$, so gibt es eine Zahl ν', welche der Kongruenz $\nu' \equiv 1 \pmod{\mathfrak{n}'}$ genügt und relative Primzahl zu $\mathfrak{m}$ ist und der Art, daß die Klasse $\mathfrak{m} + \nu'$ nicht in H enthalten ist (d. h. $\binom{\mathfrak{m}}{\mathfrak{n}'}$ nicht Divisor von H).

Oder: $\binom{\mathfrak{m}}{\mathfrak{n}'}$ ist Divisor von H oder nicht, je nachdem $\mathfrak{n}'$ teilbar ist durch $\mathfrak{n}$ oder nicht.

Definition 3. Eine Funktion ψ, welche für jede in $\mathfrak{o}$ enthaltene Zahl ω einen bestimmten endlichen Wert $\psi(\omega)$ besitzt, soll eine Klassenfunktion für das Ideal $\mathfrak{m}$ oder auch periodisch nach $\mathfrak{m}$ heißen, wenn je zwei nach $\mathfrak{m}$ kongruente Zahlen α, β einen und denselben Wert $\psi(\alpha) = \psi(\beta)$ erzeugen, d. h. wenn für jede in $\mathfrak{o}$ enthaltene Zahl ω und jede in $\mathfrak{m}$ enthaltene Zahl μ stets

$$\psi(\omega) = \psi(\omega + \mu) \qquad [\text{Bezeichnung: } \psi(\mathfrak{m} + \omega) = \psi(\omega)]$$

ist; das Ideal $\mathfrak{m}$ heißt eine Periode von ψ.

Offenbar ist jedes Vielfache einer Periode von ψ ebenfalls eine Periode von ψ.

Bemerkung. Man könnte bei dem Begriffe einer Periode $\mathfrak{m}$ von ψ größerer Allgemeinheit wegen davon absehen, daß $\mathfrak{m}$ ein Ideal in $\mathfrak{o}$ sein soll, und lediglich annehmen, daß $\mathfrak{m}$ irgend ein Modul sein soll, mit der einzigen Beschränkung, daß $(\mathfrak{o}, \mathfrak{m}) > 0$, also ψ nur eine endliche Anzahl verschiedener Werte haben soll. Dies würde aber keine wirkliche Erweiterung des obigen Begriffs geben; denn zufolge der letzten Bemerkung würde auch der Modul $\mathfrak{o} - \mathfrak{m}$ als Multiplum von $\mathfrak{m}$, und ebenso das kleinste durch den Modul $\mathfrak{m}$ oder $\mathfrak{o} - \mathfrak{m}$ teilbare Ideal, welches immer $= \frac{\mathfrak{o} - \mathfrak{m}}{\mathfrak{o}}$ ist, ebenfalls eine Periode von ψ sein. Dagegen würde eine Erweiterung des Begriffs dadurch eintreten (?) *), daß die Funktion ψ nicht auf alle Zahlen von $\mathfrak{o}$, sondern nur auf alle Zahlen irgend einer Ordnung wirkt. —

Satz 4. Sind die Ideale $\mathfrak{a}, \mathfrak{b}$ Perioden der Funktion ψ, so ist auch ihr größter gemeinsamer Teiler $\mathfrak{a} + \mathfrak{b}$ eine Periode von ψ.

Beweis. Denn wenn ω, α, β beliebige Zahlen in $\mathfrak{o}, \mathfrak{a}, \mathfrak{b}$ bedeuten, so ist nach der Annahme $\psi(\omega) = \psi(\omega + \alpha)$ und $\psi(\omega) = \psi(\omega + \beta)$; ersetzt man in der letzten Gleichung ω durch $\omega + \alpha$, so folgt $\psi(\omega) = \psi(\omega + \alpha) = \psi(\omega + \alpha + \beta)$, also $\psi(\omega) = \psi(\omega + \delta)$, wo $\delta = \alpha + \beta$ jede Zahl des Ideals $\mathfrak{a} + \mathfrak{b}$ bedeutet, w. z. b. w. —

Hieraus geht hervor, daß der gr. gem. Teiler $\mathfrak{m}$ aller Perioden von ψ ebenfalls eine Periode von ψ ist, und daß folglich alle Perioden von ψ die sämtlichen Vielfachen von $\mathfrak{m}$ sind, welches Ideal die kleinste Periode von ψ heißen soll, weil sie von allen Perioden die kleinste Norm besitzt. (Besser Hauptperiode!)

Definition 4. Eine (nach $\mathfrak{m}$ periodische) Funktion ψ aller in $\mathfrak{o}$ enthaltenen Zahlen soll ein Charakter heißen, wenn für je zwei solche Zahlen ω, ω' das Gesetz

$$\psi(\omega\,\omega') = \psi(\omega)\,\psi(\omega')$$

gilt, und ψ nicht für alle ω verschwindet. —

Satz 5. Ist der Charakter ψ periodisch, und ist $\mathfrak{m}$ seine kleinste Periode, so ist $\psi(\omega)$ dann und nur dann von Null verschieden, und zwar

$$\psi(\omega)^{\varphi(\mathfrak{m})} = 1,$$

wenn ω relative Primzahl zu $\mathfrak{m}$ ist.

Beweis. Da $\omega \cdot 1 = \omega$, also $\psi(\omega)\,\psi(1) = \psi(\omega)$ ist und $\psi(\omega)$ nicht für alle ω verschwindet, so ist

$$\psi(1) = 1.$$

Ist ω relative Primzahl zu $\mathfrak{m}$, also $\omega^{\varphi(\mathfrak{m})} \equiv 1 \pmod{\mathfrak{m}}$, so folgt

$$\psi\{\omega^{\varphi(\mathfrak{m})}\} = \psi(\omega)^{\varphi(\mathfrak{m})} = \psi(1) = 1.$$

Ist aber ω nicht relative Primzahl zu $\mathfrak{m}$, so ist das kleinste gemeinsame Vielfache $\mathfrak{o}\,\omega - \mathfrak{m}$ von $\mathfrak{o}\,\omega$ und $\mathfrak{m}$ von der Form $\omega\,\mathfrak{m}'$, wo das Ideal $\mathfrak{m}'$ ein echter Teiler von $\mathfrak{m}$ ($\mathfrak{m} = \mathfrak{m}'(\mathfrak{o}\,\omega + \mathfrak{m})$) und folglich keine Periode von ψ ist; es gibt daher zwei nach $\mathfrak{m}'$ kon-

*) [Das Fragezeichen ist später zugefügt.]

gruente Zahlen α, β, welche verschiedene Werte $\psi(\alpha)$, $\psi(\beta)$ erzeugen; da nun $\omega(\alpha-\beta)$ teilbar durch $\omega\mathfrak{m}'$, also auch durch $\mathfrak{m}$ ist, so folgt

$$\omega\alpha \equiv \omega\beta \pmod{\mathfrak{m}}; \quad \psi(\omega\alpha) = \psi(\omega\beta), \quad \psi(\omega)\psi(\alpha) = \psi(\omega)\psi(\beta),$$

mithin

$$\psi(\omega) = 0,$$

w. z. b. w.

Definition 5. Die Anzahl der verschiedenen Charaktere ψ von kleinster Periode $\mathfrak{m}$ soll mit $\varphi'(\mathfrak{m})$ bezeichnet werden. [Besser $\varphi_1(\mathfrak{m})$!]

Zu ihrer Bestimmung dient folgende Betrachtung. Ist ψ ein solcher Charakter, so kann er zugleich aufgefaßt werden als einer der $\varphi(\mathfrak{m})$ Charaktere der Abelschen Gruppe, welche von den $\varphi(\mathfrak{m})$ Klassen $\mathfrak{m}+\varrho$ gebildet wird, die den sämtlichen nach $\mathfrak{m}$ inkongruenten relativen Primzahlen ϱ zu $\mathfrak{m}$ entsprechen; in dem Sinne $\psi(\mathfrak{m}+\varrho) = \psi(\mu+\varrho) = \psi(\varrho)$, $\psi(\mathfrak{m}+\varrho)\psi(\mathfrak{m}+\varrho') = \psi(\mathfrak{m}+\varrho\varrho')$. Umgekehrt, ist ψ ein Charakter dieser Abelschen Gruppe von Klassen $\mathfrak{m}+\varrho$, und setzt man $\psi(\omega) = \psi(\mathfrak{m}+\omega)$ oder $= 0$, je nachdem ω relative Primzahl zu $\mathfrak{m}$ ist oder nicht, so ist $\psi(\omega)$ offenbar eine Funktion von der Periode $\mathfrak{m}$, weil immer $\psi(\omega) = \psi(\omega+\mu)$, und zwar ein Charakter, weil offenbar $\psi(\omega\omega') = \psi(\omega)\psi(\omega')$. Die kleinste Periode $\mathfrak{n}$ dieses Charakters ψ ist notwendig ein Divisor von $\mathfrak{m}$; da nun ein Charakter $\psi(\omega)$ von der kleinsten Periode $\mathfrak{n}$ stets und nur dann verschwindet (nach Satz 5), wenn ω relative Primzahl zu $\mathfrak{n}$ ist, und da andererseits $\psi(\omega)$ nach Definition stets und nur dann verschwindet, wenn ω relative Primzahl zu $\mathfrak{m}$ ist, so deckt sich das System $\binom{\mathfrak{n}}{0}$ aller relativen Primzahlen zu $\mathfrak{n}$ mit dem System $\binom{\mathfrak{m}}{0}$ aller relativen Primzahlen zu $\mathfrak{m}$; setzt man daher $\mathfrak{m} = \mathfrak{p}\mathfrak{m}'$, wo $\mathfrak{p}$ das Produkt aller verschiedenen in $\mathfrak{m}$ aufgehenden Primideale bedeutet (oder $\mathfrak{o}$, falls $\mathfrak{m} = \mathfrak{o}$ ist), so muß $\mathfrak{n} = \mathfrak{p}\mathfrak{n}'$ sein, wo $\mathfrak{n}'$ ein Divisor von $\mathfrak{m}'$. Umgekehrt: ist ψ ein Charakter von kleinster Periode $\mathfrak{n} = \mathfrak{p}\mathfrak{n}'$, wo $\mathfrak{n}'$ irgend ein Divisor von $\mathfrak{m}'$, so ist $\psi(\omega)$ auch ein Charakter von der Periode $\mathfrak{m}$, welcher stets und nur dann von Null verschieden ist, wenn ω relative Primzahl zu $\mathfrak{m}$ ist, und ihm entspricht ein vollständig bestimmter Abelscher Klassencharakter $\psi(\mathfrak{m}+\varrho)$. Mithin verteilen sich die sämtlichen $\varphi(\mathfrak{m})$ Charaktere $\psi(\mathfrak{m}+\varrho)$ in ebenso viele Systeme, als es Divisoren $\mathfrak{n}'$ von $\mathfrak{m}'$ gibt, und da dasjenige System, welches zu $\mathfrak{n}'$ gehört, aus $\varphi'(\mathfrak{p}\mathfrak{n}')$

Individuen besteht, so ergibt sich, daß die über alle $\mathfrak{n}'$ ausgedehnte Summe

$$\sum\varphi'(\mathfrak{p}\mathfrak{n}') = \varphi(\mathfrak{m}) = N(\mathfrak{m})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})} = N(\mathfrak{m}')\varphi(\mathfrak{p}),$$

also

$$\sum\frac{\varphi'(\mathfrak{p}\mathfrak{n}')}{\varphi(\mathfrak{p})} = N(\mathfrak{m}')$$

ist. Da dieser Satz für jedes Ideal $\mathfrak{m}'$ gilt, welches nur durch solche Primideale teilbar ist, die in $\mathfrak{p}$ aufgehen, so folgt, wenn man $\mathfrak{m}'$ durch jeden Divisor von $\mathfrak{m}'$ ersetzt, nach bekannten Sätzen

$$\varphi'(\mathfrak{m}) = \varphi(\mathfrak{p})\varphi(\mathfrak{m}') = \varphi(\mathfrak{p})\varphi\left(\frac{\mathfrak{m}}{\mathfrak{p}}\right). \quad \text{Satz 6.}$$

Satz 7. Sind $\mathfrak{m}_1$, $\mathfrak{m}_2$ relative Primideale, so ist

$$\varphi'(\mathfrak{m}_1\mathfrak{m}_2) = \varphi'(\mathfrak{m}_1)\varphi'(\mathfrak{m}_2).$$

Beweis. Denn bedeuten $\mathfrak{p}_1$, $\mathfrak{p}_2$ die Produkte aller verschiedenen, bzw. in $\mathfrak{m}_1$, $\mathfrak{m}_2$ aufgehenden Primideale, so ist $\mathfrak{p}_1\mathfrak{p}_2$ das Produkt aller verschiedenen in $\mathfrak{m}_1\mathfrak{m}_2$ aufgehenden Primideale, also

$$\varphi'(\mathfrak{m}_1\mathfrak{m}_2) = \varphi(\mathfrak{p}_1\mathfrak{p}_2)\varphi\left(\frac{\mathfrak{m}_1\mathfrak{m}_2}{\mathfrak{p}_1\mathfrak{p}_2}\right) = \varphi(\mathfrak{p}_1)\varphi\left(\frac{\mathfrak{m}_1}{\mathfrak{p}_1}\right)\cdot\varphi(\mathfrak{p}_2)\varphi\left(\frac{\mathfrak{m}_2}{\mathfrak{p}_2}\right) = \varphi'(\mathfrak{m}_1)\varphi'(\mathfrak{m}_2),$$

w. z. b. w.

Definition 6. Es bedeute $\Phi'(\mathfrak{m})$ die Anzahl aller verschiedenen Charaktere von der Periode $\mathfrak{m}$, also

$$\Phi'(\mathfrak{m}) = \sum\varphi'(\mathfrak{n}),$$

wo $\mathfrak{n}$ alle Faktoren von $\mathfrak{m}$ durchläuft (weil jeder Charakter von der Periode $\mathfrak{m}$ einen der Faktoren $\mathfrak{n}$ zur kleinsten Periode hat, und umgekehrt).

Satz 8. Sind $\mathfrak{m}_1$, $\mathfrak{m}_2$ relative Primideale, so ist

$$\Phi'(\mathfrak{m}_1\mathfrak{m}_2) = \Phi'(\mathfrak{m}_1)\Phi'(\mathfrak{m}_2).$$

Beweis. Denn jeder Divisor von $\mathfrak{m}_1\mathfrak{m}_2$ läßt sich stets und nur auf eine Weise in die Form $\mathfrak{n}_1\mathfrak{n}_2$ setzen, wo $\mathfrak{n}_1$, $\mathfrak{n}_2$ Faktoren von $\mathfrak{m}_1$, $\mathfrak{m}_2$, und umgekehrt, also

$$\begin{aligned}\Phi'(\mathfrak{m}_1\mathfrak{m}_2) &= \sum\varphi'(\mathfrak{n}_1\mathfrak{n}_2) = \sum\varphi'(\mathfrak{n}_1)\varphi'(\mathfrak{n}_2)\\ &= \sum\varphi'(\mathfrak{n}_1)\sum\varphi'(\mathfrak{n}_2) = \Phi'(\mathfrak{m}_1)\Phi'(\mathfrak{m}_2),\end{aligned}$$

w. z. b. w.

Satz 9. Ist $\mathfrak{m}$ teilbar durch das Primideal $\mathfrak{p}$ und kein anderes, also $= \mathfrak{p}^n$, wo $n \geqq 1$, so ist

$$\Phi'(\mathfrak{m}) = 1 + \varphi(\mathfrak{p}^n) = 1 + \varphi(\mathfrak{m}).$$

Beweis. Denn es ist (nach Satz 6)

$$\begin{aligned}\Phi'(\mathfrak{m}) &= \varphi'(\mathfrak{o}) + \varphi'(\mathfrak{p}) + \varphi'(\mathfrak{p}^2) + \cdots + \varphi'(\mathfrak{p}^n)\\ &= 1 + \varphi(\mathfrak{p}) + \varphi(\mathfrak{p})\varphi(\mathfrak{p}) + \varphi(\mathfrak{p})\varphi(\mathfrak{p}^2) + \cdots + \varphi(\mathfrak{p})\varphi(\mathfrak{p}^{n-1})\\ &= 1 + \varphi(\mathfrak{p})\{\varphi(\mathfrak{o}) + \varphi(\mathfrak{p}) + \cdots + \varphi(\mathfrak{p}^{n-1})\} = 1 + \varphi(\mathfrak{p})N(\mathfrak{p}^{n-1})\\ &= 1 + \varphi(\mathfrak{p}^n).\end{aligned}$$

Satz 10. Ist $\mathfrak{m} = \mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}\ldots$, wo $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}\ldots$ (wirkliche) Potenzen von lauter verschiedenen Primidealen (nicht $= \mathfrak{o}$), so ist

$$\Phi'(\mathfrak{m}) = (1 + \varphi(\mathfrak{a}))(1 + \varphi(\mathfrak{b}))(1 + \varphi(\mathfrak{c}))\ldots$$

Beweis unmittelbar aus (8) und (9).

Gehen wir näher ein auf die Verteilung der $\varphi(\mathfrak{m})$ Charaktere ψ der aus den Klassen $\mathfrak{m} + \varrho$ bestehenden Abelschen Gruppe auf die Faktoren $\mathfrak{n} = \mathfrak{p}\mathfrak{n}'$ von $\mathfrak{m} = \mathfrak{p}\mathfrak{m}'$, wo $\mathfrak{p}$, $\mathfrak{m}'$, $\mathfrak{n}'$ die obige Bedeutung haben. Es sei ψ ein solcher Charakter, und (ψ) die Gruppe aller derjenigen Klassen $\mathfrak{m} + \varrho$, welche der Bedingung

$$\psi(\mathfrak{m} + \varrho) = \psi(\varrho) = 1$$

genügen (aus $\psi(\varrho) = 1$, $\psi(\varrho') = 1$ folgt auch $\psi(\varrho\,\varrho') = 1$). Sind nun $\mathfrak{m} + \alpha$, $\mathfrak{m} + \beta$ irgend zwei Klassen der Gruppe $\binom{\mathfrak{m}}{\mathfrak{o}}$, welche denselben Charakter $\psi(\mathfrak{m} + \alpha) = \psi(\mathfrak{m} + \beta)$ besitzen, so kann man stets eine und nur eine Klasse $\mathfrak{m} + \varrho$ so bestimmen, daß $\alpha\varrho \equiv \beta \pmod{\mathfrak{m}}$, also $(\mathfrak{m} + \alpha)(\mathfrak{m} + \varrho) = \mathfrak{m} + \beta$, also $\psi(\mathfrak{m} + \alpha)\psi(\mathfrak{m} + \varrho) = \psi(\mathfrak{m} + \beta) = \psi(\mathfrak{m} + \alpha)$, also $\psi(\mathfrak{m} + \varrho) = 1$ wird; mithin ist $\beta \equiv \alpha\varrho$, wo $\mathfrak{m} + \varrho$ der Gruppe (ψ) angehört; und umgekehrt, durchläuft $\mathfrak{m} + \varrho$ alle Klassen der Gruppe (ψ), während α eine feste Klasse, so ist $\psi(\mathfrak{m} + \alpha\varrho) = \psi(\mathfrak{m} + \alpha)$. Die Gruppe $\binom{\mathfrak{m}}{\mathfrak{o}}$ besteht aus einer Anzahl von Komplexen von der Form $(\psi)(\mathfrak{m} + \alpha)$; alle und nur die Klassen, welche einem und demselben solchen Komplex angehören, erzeugen einen und denselben Wert des Charakters ψ; die Anzahl der verschiedenen Komplexe $(\psi)(\mathfrak{m} + \alpha)$, aus denen $\binom{\mathfrak{m}}{\mathfrak{o}}$ besteht, ist auch die Anzahl der verschiedenen Werte des Charakters ψ. (Dies ist eine allgemeine Eigenschaft der Charaktere Abelscher Gruppen.) (ψ) heiße die Gruppe des Charakters ψ.

Nun sei $\mathfrak{a}$ der Exponent der Gruppe (ψ) (Definition 2), so soll $\mathfrak{a}$ auch der Exponent des Charakters ψ heißen. Wir betrachten

das System $\binom{\mathfrak{a}}{\mathfrak{o}}$ aller relativen Primzahlen σ zu $\mathfrak{a}$, welches aus $\varphi(\mathfrak{a})$ Klassen $\mathfrak{a} + \sigma$ besteht. Das System aller der Zahlen, welche eine bestimmte solche Klasse $\mathfrak{a} + \sigma$ mit dem System $\binom{\mathfrak{m}}{\mathfrak{o}}$ gemein hat, besteht [nach (4) in Zusatz 2] aus $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a})}$ Klassen $\mathfrak{m} + \mu$. Ein solches System, welches der Klasse $\mathfrak{a} + 1$ entspricht, ist die Gruppe $\binom{\mathfrak{m}}{\mathfrak{a}}$, welche ein Divisor der Gruppe (ψ) ist. Und wenn $\mathfrak{m} + \mu$ eine der $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a})}$ Klassen von $\binom{\mathfrak{m}}{\mathfrak{o}}$ ist, welche in $\mathfrak{a} + \sigma$ enthalten sind, so ist der Komplex $\binom{\mathfrak{m}}{\mathfrak{a}}(\mathfrak{m} + \mu)$ das System aller dieser Klassen, welche folglich auch in dem Komplex $(\psi)(\mathfrak{m} + \mu)$ enthalten sind; mithin hat der Charakter ψ für alle diese, der Klasse $\mathfrak{a} + \sigma$ entsprechenden Klassen $\mathfrak{m} + \mu$ einen und denselben Wert. Definiert man nun eine Klassenfunktion $\psi'(\mathfrak{a} + \sigma)$ so, daß $\psi'(\mathfrak{a} + \sigma) = \psi(\mathfrak{m} + \mu)$ wird, so ist ψ' für jede Klasse $\mathfrak{a} + \sigma$ eindeutig bestimmt, und zwar ist ψ' ein Charakter der Abelschen Gruppe $\binom{\mathfrak{a}}{\mathfrak{o}}$, welche aus diesen $\varphi(\mathfrak{a})$ Klassen $\mathfrak{a} + \sigma$ besteht. Denn wenn $\mathfrak{a} + \sigma_1$, $\mathfrak{a} + \sigma_2$ irgend zwei Klassen in $\binom{\mathfrak{a}}{\mathfrak{o}}$ bedeuten, und wenn $\mathfrak{m} + \mu_1$, $\mathfrak{m} + \mu_2$ irgend zwei bzw. in ihnen enthaltene Klassen von $\binom{\mathfrak{m}}{\mathfrak{o}}$ bedeuten, so ist das Produkt der letzteren $(\mathfrak{m} + \mu_1)(\mathfrak{m} + \mu_2) = \mathfrak{m} + \mu_1\mu_2$ in dem Produkte $(\mathfrak{a} + \sigma_1)(\mathfrak{a} + \sigma_2) = \mathfrak{a} + \sigma_1\sigma_2$ enthalten; da nun $\psi'(\mathfrak{a} + \sigma_1) = \psi(\mathfrak{m} + \mu_1)$, und $\psi'(\mathfrak{a} + \sigma_2) = \psi(\mathfrak{m} + \mu_2)$ ist, so folgt $\psi'(\mathfrak{a} + \sigma_1)\psi'(\mathfrak{a} + \sigma_2) = \psi(\mathfrak{m} + \mu_1)\psi(\mathfrak{m} + \mu_2) = \psi(\mathfrak{m} + \mu_1\mu_2) = \psi'(\mathfrak{a} + \sigma_1\sigma_2)$, w. z. b. w. Und zwar ist $\mathfrak{a}$ selbst der Exponent dieses Charakters ψ' oder der Gruppe (ψ'). Denn wenn $\mathfrak{b}$ ein echter Faktor von $\mathfrak{a}$ ist, so ist $\binom{\mathfrak{m}}{\mathfrak{b}}$ nicht in der Gruppe (ψ) enthalten (Definition 2), es gibt folglich eine in $\mathfrak{b} + 1$ enthaltene Klasse $\mathfrak{m} + \lambda$, welche nicht in (ψ) enthalten ist, woraus folgt, daß $\psi'(\mathfrak{a} + \lambda) = \psi(\mathfrak{m} + \lambda)$ nicht $= 1$ ist; mithin ist die in $\mathfrak{b} + 1 = \mathfrak{b} + \lambda$, also auch in $\binom{\mathfrak{a}}{\mathfrak{b}}$ enthaltene Klasse $\mathfrak{a} + \lambda$ nicht in der Gruppe (ψ') enthalten, w. z. b. w. [während $\binom{\mathfrak{a}}{\mathfrak{a}} = \mathfrak{a} + 1$ in (ψ') enthalten ist].

Also: jeder Charakter ψ der Abelschen Gruppe $\binom{\mathfrak{m}}{0}$, dessen Exponent der Faktor $\mathfrak{a}$ von $\mathfrak{m}$ ist, erzeugt in der angegebenen Weise $(\psi(\mathfrak{m}+\mu) = \psi'(\mathfrak{a}+\mu))$ einen bestimmten Charakter ψ' der Abelschen Gruppe $\binom{\mathfrak{a}}{0}$, dessen Exponent $\mathfrak{a}$ ist.

Umgekehrt: Ist $\mathfrak{a}$ Faktor des Ideals $\mathfrak{m}$ und ψ' ein Charakter der Abelschen Gruppe $\binom{\mathfrak{a}}{0}$, dessen Exponent $\mathfrak{a}$, so wird ψ' in der angegebenen Weise $(\psi(\mathfrak{m}+\mu) = \psi'(\mathfrak{a}+\mu))$ durch einen und nur einen Charakter ψ der Abelschen Gruppe $\binom{\mathfrak{m}}{0}$ erzeugt; und dann ist gewiß $\mathfrak{a}$ auch der Exponent von ψ (allgemeiner: ψ und ψ' haben einen und denselben Exponenten).

Erläuterungen zur vorstehenden Abhandlung.

Es handelt sich um die „Sparsamkeit", von der Dedekind in dem im Nachlaß publizierten Brief an Frobenius vom 8. Juli 1896 spricht. Und zwar werden die „natürlichen" Charaktere — jetzt gewöhnlich als eigentliche bezeichnet — allgemeiner als im Brief für einen (endlichen) algebraischen Zahlkörper erklärt. Zugleich gelangt Dedekind zum Begriff des Führers, insbesondere des Führers eines Charakters — in Anlehnung an den Fall des Kreiskörpers als Exponent bezeichnet —; zwar bei Zugrundelegung einer Zahlklasseneinteilung, aber mit Überlegungen, die genau so im allgemeinen Fall der Klassenkörpertheorie gelten.

Die Anwendung dieser Begriffe auf die Zerlegung der Zetafunktion eines beliebigen Kreiskörpers in eigentliche L-Reihen — unter Benutzung der bekannten Primidealzerlegung — ist in dem erwähnten Brief auseinandergesetzt; der Führer-Diskriminantensatz für den Kreiskörper wird in XLII gebracht.

Über seine Publikationsabsichten, anläßlich eines Beitrags für die Festschrift zur Braunschweiger Naturforscherversammlung, schreibt Dedekind an Frobenius (13. April 1897): . . . ich beschloß, meine langjährigen Arbeiten über die allgemeinsten Kreiskörper (lediglich auf Grund des „Skelettes" vom 8. Juni 1882 behandelt, dazu gehören die „natürlichen" Charaktere und die „Sparsamkeit", wovon ich Ihnen im vorigen Jahre geschrieben habe) zum Gegenstande zu wählen; allein diese Sache ist so umfassend, und meine Krankheit machte mir einen solchen Querstrich, daß ich daran verzweifle, es rechtzeitig fertig zu machen. . . . (18. April 1897): . . . Ihren Rat, für meinen Beitrag zur Festschrift doch mein zweites Thema (allgemeinste Kreiskörper-Ideale) zu wählen, werde ich schwerlich befolgen können; eine Trennung in zwei Teile, deren zweiter dann an einem ganz andern Orte (etwa in Crelle?) erscheinen müßte, wäre doch sehr unangenehm. . . .

Inwieweit diese nicht publizierten Arbeiten — zu denen auch XL, XLII und die Ausarbeitung von XVI aus Bd. I gehören — auf die Entwicklung der Klassenkörpertheorie von Einfluß gewesen sind, läßt sich nicht mehr feststellen, da der Briefwechsel Dedekind-Weber aus diesen Jahren anscheinend nicht mehr existiert.

Noether.

XLII.

Grundideale von Kreiskörpern.

Es sei m eine natürliche Zahl, die im folgenden stets beibehalten wird. Ist a ein Divisor von m, so soll mit

$$\varepsilon a$$

der Inbegriff aller ganzen rationalen Zahlen bezeichnet werden, welche relative Primzahlen zu m (also auch zu a) und $\equiv 1 \pmod{a}$ sind. Dieser Inbegriff besteht aus

$$\frac{\varphi(m)}{\varphi(a)}$$

Klassen (mod. m), und diese Klassen bilden eine Gruppe, welche selbst mit εa bezeichnet werden soll.

Hiernach ist $\varepsilon 1$ der Inbegriff aller relativen Primzahlen zu m, welcher aus $\varphi(m)$ Klassen besteht. Ebenso ist εm die Hauptklasse.

$$(\varepsilon m, \varepsilon a) = \frac{\varphi(m)}{\varphi(a)}; \quad (\varepsilon a, \varepsilon 1) = \varphi(a).$$

Sind a, b Divisoren von m, c ihr kleinstes gemeinsames Vielfaches, d ihr größter gemeinsamer Teiler, also $ab = cd$, so ist

$$\left.\begin{array}{l} \varepsilon d \text{ das kleinste gemeinsame Vielfache} \\ \varepsilon c \text{ der größte gemeinsame Teiler} \end{array}\right\} \text{der Gruppen } \varepsilon a, \varepsilon b,$$

$$\varepsilon d = \varepsilon a \cdot \varepsilon b,$$
$$\varepsilon c = \varepsilon a \,|\, \varepsilon b,$$

wo $|$ das Zeichen für den größten gemeinsamen Teiler von Gruppen ist. Ist H irgendeine in $\varepsilon 1$ als Teiler enthaltene Gruppe, so ist das kleinste gemeinsame Vielfache aller in H enthaltenen Gruppen von der Form εa selbst eine solche Gruppe εd, wo d der größte gemeinsame Teiler aller a. Diese Zahl d heißt der Exponent der Gruppe H. Also: Ist a teilbar durch d, so ist εa in H enthalten; ist a nicht teilbar durch d, so ist εa nicht in H enthalten.

Es sei θ eine primitive Wurzel der Gleichung $\theta^m = 1$; $K(m) = R(\theta)$ sei der durch θ erzeugte vollständige Kreiskörper vom Grade $\varphi(m)$; dieser gehört zur Gruppe $\varepsilon m \equiv 1 \pmod{m}$.

Es sei $\mathfrak{Q}$ ein Divisor von $K(m)$, zur Gruppe H gehörig und vom Grade $n = (H, \varepsilon 1)$. Durchläuft h alle in H enthaltenen $\frac{\varphi(m)}{n}$ Klassen, so ist

$$f(x) = \Pi(x - \theta^h)$$

die in $\mathfrak{Q}$ irreduzibele Funktion von x, welche für $x = \theta$ verschwindet, und das Grundideal von $K(m)$ in bezug auf $\mathfrak{Q}$ ist ($\sim$ bedeutet: assoziiert mit)

$$\sim f'(\theta) = \Pi(\theta - \theta^h) \sim \Pi(1 - \theta^{h-1}), \quad \text{mit Ausschluß von } h \equiv 1 \pmod{m}.$$

Jeder Faktor $(1 - \theta^{h-1})$ ist nur dann keine Einheit, sondern Faktor einer in m aufgehenden natürlichen Primzahl p, wenn der kleinste Nenner des Bruches $\frac{h-1}{m}$ eine Potenz von p ist; und zwar ist gleichzeitig (Modul-Bezeichnung)

$$\left[1, \frac{h-1}{m}\right] = \left[\frac{1}{p^s}\right] \text{ mit } 1 - \theta^{h-1} \sim p^{\frac{1}{\varphi(p^s)}}; \quad s > 0.$$

Nun sei m' der größte durch p nicht teilbare Divisor von

$$m = m' p^k; \quad k > 0.$$

Damit eine Zahl h der vorstehenden Bedingung genüge, ist erforderlich

$$h \equiv 1 \left(\text{mod.} \frac{m}{p^s} = m' p^{k-s}\right), \quad h - 1 = u \cdot m' p^{k-s},$$

wo, wenn $s > 0$ ist, u nicht teilbar durch p; d. h. h muß eine Zahl der Gruppe $\varepsilon \frac{m}{p^s}$ sein, also ein Element des größten gemeinsamen Teilers

$$Q_s = H \,|\, \varepsilon \frac{m}{p^s}$$

der Gruppen H und $\varepsilon \frac{m}{p^s}$; es sei

$$q_s = (\varepsilon m, Q_s)$$

der Grad von Q_s. Es darf aber h nicht $\equiv 1 \left(\text{mod.} \frac{m}{p^{s-1}} = \frac{m}{p^s} \cdot p\right)$, also nicht in $\varepsilon \frac{m}{p^{s-1}}$ enthalten, also keine der q_{s-1} Zahlen in Q_{s-1} sein. Mithin ist $q_s - q_{s-1}$ die Anzahl der obigen h, und folglich ist der betreffende Faktor von $f'(\theta)$, welcher nur Faktoren von p enthält,

$$\sim p^{\frac{q_1 - q_0}{\varphi(p)} + \frac{q_2 - q_1}{\varphi(p^2)} + \frac{q_3 - q_2}{\varphi(p^3)} + \cdots + \frac{q_k - q_{k-1}}{\varphi(p^k)}}.$$

Offenbar ist

$$Q_0 = \varepsilon m, \quad q_0 = 1.$$

Der Grad der Gruppe $\varepsilon \frac{m}{p^s}$ ist

$$\frac{\varphi(m)}{\varphi\left(\frac{m}{p^s}\right)} = \frac{\varphi(m')\varphi(p^k)}{\varphi(m')\varphi(p^{k-s})} = \frac{\varphi(p^k)}{\varphi(p^{k-s})} = p^s \text{ oder} = \varphi(p^k) = p^k - p^{k-1},$$

je nachdem $s < k$ oder $s = k$.

Also ist q_s Divisor von p^s, wenn $s < k$, und q_k Divisor von $\varphi(p^k)$. Außerdem ist Q_s Divisor von Q_{s+1}, also auch q_s Divisor von q_{s+1}. Ferner ist

$$\left(Q_s, \ \varepsilon \frac{m}{p^s}\right) = \left(H, \ \varepsilon \frac{m}{p^s}\right) = \left(H, H\varepsilon \frac{m}{p^s}\right),$$

$$q_s \left(H, H\varepsilon \frac{m}{p^s}\right) = (\varepsilon m, Q_s)\left(Q_s, \ \varepsilon \frac{m}{p^s}\right) = \left(\varepsilon m, \ \varepsilon \frac{m}{p^s}\right) = \frac{\varphi(p^k)}{\varphi(p^{k-s})},$$

$$\frac{q_1}{p} = \frac{1}{\left(H, \varepsilon \frac{m}{p}\right)}, \ \frac{q_2}{p^2} = \frac{1}{\left(H, \varepsilon \frac{m}{p^2}\right)}, \ \cdots, \ \frac{q_{k-1}}{p^{k-1}} = \frac{1}{\left(H, \varepsilon \frac{m}{p^{k-1}}\right)},$$

$$\frac{q_k}{\varphi(p^k)} = \frac{1}{\left(H, \varepsilon \frac{m}{p^k}\right)}, \ \frac{q_0}{1} = \frac{1}{(H, \varepsilon m)} = 1.$$

Ist $\mathfrak{Q}$ der Körper $R = K(1)$ der rationalen Zahlen, so ist $H = \varepsilon 1$ die Gesamtgruppe, mithin $Q_s = \varepsilon \frac{m}{p^s}$, und

$$q_s = \frac{\varphi(p^k)}{\varphi(p^{k-s})},$$

$$q_k - q_{k-1} = \varphi(p^k) - p^{k-1} = (p-2)p^{k-1} = \frac{p-2}{p-1}\varphi(p^k),$$

$$q_{k-1} - q_{k-2} = p^{k-1} - p^{k-2} = \varphi(p^{k-1}), \ q_{k-2} - q_{k-3} = \varphi(p^{k-2});$$
$$\cdots q_1 - q_0 = p - 1 = \varphi(p),$$

und folglich wird

$$p^{k-1+\frac{p-2}{p-1}} = p^{k-\frac{1}{p-1}}$$

der betreffende Faktor des absoluten (d. h. nach R genommenen) Grundideals von $K(m)$.

Wenn Ω und H wieder die allgemeine Bedeutung haben, so ist daher

$$p^{k-\frac{1}{p-1}-\frac{q_1-q_0}{\varphi(p)}-\frac{q_2-q_1}{\varphi(p^2)}-\cdots-\frac{q_k-q_{k-1}}{\varphi(p^k)}}$$
$$= p^{k-\frac{q_1}{p}-\frac{q_2}{p^2}-\cdots-\frac{q_{k-1}}{p^{k-1}}-\frac{q_k}{\varphi(p^k)}}$$
$$= p^{\Sigma\left(1-\frac{1}{\left(H,\,\varepsilon\frac{m}{p^s}\right)}\right)} = p^{\Sigma\left(1-\frac{1}{\left(\Omega,\,K\left(\frac{m}{p^s}\right)\right)}\right)}$$

der betreffende Faktor des Grundideals des Körpers Ω nach R.

Da alle $\varepsilon\frac{m}{p^s}$ Teiler der Gruppe $\varepsilon\frac{m}{p^k} = \varepsilon m'$ sind, so ist Q_s auch der gr. g. T. von H, $\varepsilon\frac{m}{p^s}$ und $\varepsilon m'$, also auch Q_s der gr. g. T. von Q_k und $\varepsilon\frac{m}{p^s}$.

Ist ψ ein Charakter der Abelschen Gruppe $\varepsilon 1$, so soll ψ_0 die Gruppe aller derjenigen Elemente r von $\varepsilon 1$ bedeuten, für welche $\psi(r) = 1$ ist, und unter dem Exponenten von ψ soll der Exponent der Gruppe ψ_0 verstanden sein.

Ist H irgendein Teiler von $\varepsilon 1$ und (wie oben) Ω der zugehörige Körper vom Grade $n = (H, \varepsilon 1)$, so ist n die Anzahl aller derjenigen Charaktere ψ, deren Gruppen ψ_0 Vielfache von H sind.

Es soll das Produkt der Exponenten dieser n Charaktere ψ oder vielmehr die höchste in demselben aufgehende Potenz von p ermittelt werden.

Es sei ψ einer dieser n Charaktere und sein Exponent $= m'' p^{k-s}$, wo m'' nicht teilbar durch p, also Divisor von m', und $0 \leqq s < k$.

Dann ist $\varepsilon m'' p^{k-s}$ Teiler von ψ_0, also auch $\varepsilon m' p^{k-s} = \varepsilon\frac{m}{p^s}$ Teiler von ψ_0; also ist auch $H\varepsilon\frac{m}{p^s}$ Teiler von ψ_0.

Umgekehrt aber, wenn $H\varepsilon\frac{m}{p^s}$ Teiler von ψ_0, so ist der Exponent von ψ_0 ein Divisor von $\frac{m}{p^s}$, und die höchste in ihm aufgehende Potenz von p ist Divisor von p^{k-s}.

Nun ist $\left(H\varepsilon\frac{m}{p^s}, \varepsilon 1\right)$ die Anzahl aller dieser ψ, also ebenso $\left(H\varepsilon\frac{m}{p^{s+1}}, \varepsilon 1\right)$ die Anzahl aller ψ, deren Exponent höchstens durch p^{k-s-1} teilbar ist, also $\left(H\varepsilon\frac{m}{p^s}, \varepsilon 1\right) - \left(H\varepsilon\frac{m}{p^{s+1}}, \varepsilon 1\right)$ die Anzahl derjenigen ψ, deren Exponent die Potenz p^{k-s} genau enthält.

Nun ist

$$(H, \varepsilon 1) = \left(H, H\varepsilon\frac{m}{p^s}\right)\left(H\varepsilon\frac{m}{p^s}, \varepsilon 1\right) = n;$$

und

$$q_s\left(H, H\varepsilon\frac{m}{p^s}\right) = \frac{\varphi(p^k)}{\varphi(p^{k-s})},$$

folglich

$$\frac{\varphi(p^k)}{\varphi(p^{k-s})}\left(H\varepsilon\frac{m}{p^s}, \varepsilon 1\right) = n q_s,\ \left(H\varepsilon\frac{m}{p^s}, \varepsilon 1\right) = n q_s \frac{\varphi(p^{k-s})}{\varphi(p^k)}$$
$$= \frac{n q_s}{p^s} \text{ oder } = \frac{n q_k}{\varphi(p^k)},$$

je nachdem

$$s < k \quad \text{oder} \quad s = k.$$

Also ist

1	$\frac{n q_{k-1}}{p^{k-1}} - \frac{n q_k}{\varphi(p^k)}$	Anzahl der ψ, in deren Exponent der Faktor p,
2	$\frac{n q_{k-2}}{p^{k-2}} - \frac{n q_{k-1}}{p^{k-1}}$	" " " " " " " " p^2.
$k-1$	$\frac{n q_1}{p} - \frac{n q_2}{p^2}$	" " " " " " " " p^{k-1}.
k	$n - \frac{n q_1}{p}$	" " " " " " " " p^k.

Also

$$p^{kn-\frac{nq_1}{p}-\frac{nq_2}{p^2}-\cdots-\frac{nq_{k-1}}{p^{k-1}}-\frac{nq_k}{\varphi(p^k)}} = \left(p^{k-\frac{q_1}{p}-\frac{q_2}{p^2}-\cdots-\frac{q_{k-1}}{p^{k-1}}-\frac{q_k}{\varphi(p^k)}}\right)^n.$$

Mithin ist dies Produkt aller Exponenten der n Charaktere ψ des Körpers Ω zugleich die n^{te} Potenz des Grundideals von Ω, d. h. $= \pm$ Grundzahl von Ω, w. z. b. w. (Norm des Grundideals.)

Erläuterungen. 1. Ist die Gruppe H von Elementen h irgendein Teiler der Gruppe $\varepsilon 1$, so ist

$$(H, \varepsilon 1)$$

die Anzahl aller derjenigen Charaktere ψ der Gruppe $\varepsilon 1$, welche Multipla des identischen (oder Haupt-) Charakters der Gruppe H sind, welche also für alle Elemente h der Gruppe H der Bedingung

$$\psi(h) = 1$$

genügen; oder mit anderen Worten: $(H, \varepsilon 1)$ ist die Anzahl aller derjenigen Charaktere ψ, deren Gruppen ψ_0 Vielfache von H sind, also der Bedingung

$$(\psi_0, H) = 1$$

genügen.

2. Ist a (wie auf S. 401) irgendein Divisor von m, und εa wieder die Gruppe von $\frac{\varphi(m)}{\varphi(a)}$ Klassen (mod. m), deren Zahlen relative Primzahlen zu m und zugleich $\equiv 1 \pmod{a}$ sind, so ist die Aussage

$$(H, \varepsilon a) = 1 \quad \text{(also } \varepsilon a \text{ Teiler von } H)$$

gleichbedeutend damit, daß der Exponent d der Gruppe H ein Divisor von a ist.

3. Speziell bedeutet also die Aussage

$$(\psi_0, \varepsilon a) = 1,$$

daß der Exponent des Charakters ψ (d. h. der Exponent der Gruppe ψ_0) Divisor von a ist.

4. Das System der beiden gleichzeitigen Aussagen

$$(\psi_0, H) = 1, \quad (\psi_0, \varepsilon a) = 1$$

ist gleichbedeutend mit der einen Aussage

$$(\psi_0, H \varepsilon a) = 1;$$

diese letztere bedeutet also, daß erstens ψ ein Multiplum des Hauptcharakters der Gruppe H [also $\psi(h) = 1$ für alle h], und daß zweitens der Exponent von ψ ein Divisor von a ist; zufolge 1. (wenn dort H durch $H \varepsilon a$ ersetzt wird) ist

$$(H \varepsilon a, \varepsilon 1) \quad \text{die Anzahl} = f(a)$$

aller dieser Charaktere.

5. Bedeutet daher, wenn a irgendein Divisor von m, und H eine feste Gruppe ist,

$$f'(a)$$

die Anzahl aller derjenigen Charaktere ψ der Gruppe $\varepsilon 1$, welche

Multipla des Hauptcharakters von H sind, und deren Exponent $= a$ ist, so ist die über alle Divisoren d von a erstreckte Summe

$$\sum f'(d) = (H \varepsilon a, \varepsilon 1) = f(a)$$

und folglich umgekehrt

$$f'(a) = \sum \eta\left(\frac{a}{d}\right)(H \varepsilon d, \varepsilon 1) = \sum \eta\left(\frac{a}{d}\right) f(d),$$ d alle Divisoren von a,

wo η die Funktion von Mertens-Cantor bedeutet.

6. Das Produkt der Exponenten aller Charaktere ψ, welche Multipla des Hauptcharakters der Gruppe sind, und deren Anzahl zufolge 1. $= (H, \varepsilon 1)$ ist, ist daher das über alle Divisoren a von m ausgedehnte Produkt

$$\Pi a^{f'(a)}.$$

7. Setzt man

$$n = (H, \varepsilon 1),$$

so ist

$$n = (H, H \varepsilon a)(H \varepsilon a, \varepsilon 1); \quad (H \varepsilon a, \varepsilon 1) = \frac{n}{(H, H \varepsilon a)};$$

ferner ist

$$(H, H \varepsilon a) = (H, \varepsilon a) = (H \mid \varepsilon a, \varepsilon a),$$

wo $A \mid B$ allgemein den größten gemeinsamen Teiler der Gruppen A, B bedeutet; immer ist $(A, B) = (A, AB) = (A \mid B, B)$. Ferner ist

$$(\varepsilon m, \varepsilon a) = \frac{\varphi(m)}{\varphi(a)} = (\varepsilon m, H \mid \varepsilon a)(H \mid \varepsilon a, \varepsilon a);$$

bezeichnet man daher

$$(\varepsilon m, H \mid \varepsilon a) = t(a),$$

welches der Grad des größten gemeinsamen Teilers $H \mid \varepsilon a$ der beiden Gruppen H und εa ist, so wird

$$(H \mid \varepsilon a, \varepsilon a) = \frac{\varphi(m)}{\varphi(a)} \cdot \frac{1}{t(a)}; \quad (H \varepsilon a, \varepsilon 1) = \frac{n}{\varphi(m)} \cdot \varphi(a) t(a) = f(a).$$

Außerdem ist

$$\varphi(m) = (\varepsilon m, \varepsilon 1) = (\varepsilon m, H)(H, \varepsilon 1) = (\varepsilon m, H) n; \quad \frac{\varphi(m)}{n} = (\varepsilon m, H).$$

8. Es werden nur noch solche Charaktere ψ der Gruppe $\varepsilon 1$ betrachtet, welche Multipla des Hauptcharakters der Gruppe H sind, also der Bedingung $(\psi_0, H) = 1$ genügen und deren Anzahl $= n = (H, \varepsilon 1)$ ist.

Ist nun p eine in m aufgehende natürliche Primzahl und

$$m = m' p^k, \quad k > 0, \quad m' \text{ nicht teilbar durch } p,$$

so ist

$$\left(H \varepsilon \frac{m}{p^s}, \varepsilon 1\right), \quad \text{wo } 0 \leqq s \leqq k,$$

die Anzahl derjenigen Charaktere ψ, deren Exponenten Divisoren von

$$\frac{m}{p^s} = m' p^{k-s}$$

sind. Also

$(H \varepsilon m', \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von m'	$= f(m')$
$(H \varepsilon m' p, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p$	$= f(m' p)$
$(H \varepsilon m' p^2, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^2$	$= f(m' p^2)$
. . . . .	. . . . .
$(H \varepsilon m' p^{k-1}, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^{k-1}$	$= f(m' p^{k-1})$
$n = (H \varepsilon m' p^k, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^k = m$	$= f(m' p^k) = f(m)$

$= (H \varepsilon m, \varepsilon 1)$

$= (H, \varepsilon 1)$.

Also ist

$(H \varepsilon m' p, \varepsilon 1) - (H \varepsilon m', \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p, nicht den Faktor p^2 enthalten,

$(H \varepsilon m' p^2, \varepsilon 1) - (H \varepsilon m' p, \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p^2, nicht den Faktor p^3 enthalten,

. . . . . .

$(H \varepsilon m' p^k, \varepsilon 1) - (H \varepsilon m' p^{k-1}, \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p^k, nicht den Faktor p^{k+1} enthalten.

Mithin ist der Exponent der höchsten im Produkte der Exponenten aller n Charaktere ψ aufgehenden Potenz von p

$$= \{(H \varepsilon m' p, \varepsilon 1) - (H \varepsilon m', \varepsilon 1)\} + 2\{(H \varepsilon m' p^2, \varepsilon 1) - (H \varepsilon m' p, \varepsilon 1)\} + \cdots + k\{(H \varepsilon m' p^k, \varepsilon 1) - (H \varepsilon m' p^{k-1}, \varepsilon 1)\}$$

$$= k(H, \varepsilon 1) - \{(H \varepsilon m', \varepsilon 1) + (H \varepsilon m' p, \varepsilon 1) + \cdots + (H \varepsilon m' p^{k-1}, \varepsilon 1)\}$$

$$= kn - \sum_{s=0}^{s=k-1} f(m' p^s).$$

Es ist aber

$$(H, \varepsilon 1) = (H, H \varepsilon m' p^s)(H \varepsilon m' p^s, \varepsilon 1) = (H, \varepsilon m' p^s) f(m' p^s),$$

also wird der Potenzexponent von p

$$= n\left\{k - \sum_{s=0}^{s=k-1} \frac{1}{(H, \varepsilon m' p^s)}\right\}.$$

Es ist aber

$$(H, \varepsilon m' p^s) = (H \mid \varepsilon m' p^s, \varepsilon m' p^s),$$

also

$$(\varepsilon m, H \mid \varepsilon m' p^s)(H, \varepsilon m' p^s) = (\varepsilon m, \varepsilon m' p^s) = \frac{\varphi(m)}{\varphi(m' p^s)} = \frac{\varphi(p^k)}{\varphi(p^s)},$$

also

$$\frac{1}{(H, \varepsilon m' p^s)} = \frac{(\varepsilon m, H \mid \varepsilon m' p^s)}{p^{k-s}}, \quad \text{wenn } s > 0,$$

und

$$\frac{1}{(H, \varepsilon m')} = \frac{(\varepsilon m, H \mid \varepsilon m')}{\varphi(p^k)}.$$

Also wird der obige Potenzexponent von p

$$= n\left\{k - \frac{(\varepsilon m, H \mid \varepsilon m')}{\varphi(p^k)} - \sum_{s=1}^{s=k-1} \frac{(\varepsilon m, H \mid \varepsilon m' p^s)}{p^{k-s}}\right\}.$$

Erläuterungen zur vorstehenden Abhandlung.

Es handelt sich um eine Anwendung der in XLI entwickelten allgemeinen Begriffe.

Der hier für den Kreiskörper gegebene Führer-Diskriminantensatz — Darstellung der Diskriminante als Produkt der Führer (Exponenten bei Dedekind) der Charaktere der zugehörigen Klassengruppe — ist im allgemeinen Fall der relativ-Abelschen Körper auf zwei verschiedene Arten erbracht: mit transzendenten Methoden (Heckesche L-Reihen mit Größencharakteren) und arithmetisch unter Benutzung des Umkehrsatzes der Klassenkörpertheorie (vgl. den Bericht von Hasse, I, II; Jahresber. d. d. Math.-Ver. **35** und Ergänzungsbd. VI).

Das Analogon für Galoissche, nicht Abelsche Körper hat neuerdings E. Artin aufgestellt (Journ. f. Math. **164** (1931)).

Noether.

XLIII.

Untersuchung der Gruppe X.

(Einige Sätze aus der Untersuchung der Beziehungen zwischen den Idealen in verschiedenen Körpern. Schreiben an G. Frobenius vom 8. Juni 1882.)

Es sei χ eine nicht identische Permutation der Gruppe X (also $g > 1$), und $\mathfrak{p}^r$ die höchste in allen Differenzen $\omega\chi - \omega$ aufgehende Potenz von $\mathfrak{p}$, also

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}^r},$$

aber nicht identisch

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}^{r+1}}, \quad r \geqq 1.$$

Dann sei $\mathfrak{o}_1$ das System aller derjenigen Zahlen ω_1 in $\mathfrak{o}$, welche die Kongruenz

$$\omega_1\chi \equiv \omega_1 \pmod{\mathfrak{p}^{r+1}}$$

erfüllen. Zunächst leuchtet ein, daß $\mathfrak{o}_1$ ein Modul ist, weil aus $\alpha\chi \equiv \alpha$, $\beta\chi \equiv \beta \pmod{\mathfrak{p}^{r+1}}$ auch $(\alpha-\beta)\chi = \alpha\chi - \beta\chi \equiv \alpha - \beta \pmod{\mathfrak{p}^{r+1}}$ folgt, und zwar ist $\mathfrak{o}_1$ ein echtes Vielfaches von $\mathfrak{o}$, weil $\mathfrak{o}$ nicht teilbar durch $\mathfrak{o}_1$ ist. Da ferner $\mathfrak{p}\chi = \mathfrak{p}$, also auch $\mathfrak{p}^{r+1}\chi = \mathfrak{p}^{r+1}$ ist, so genügt jede in $\mathfrak{p}^{r+1}$ enthaltene Zahl π_{r+1}, weil $\pi_{r+1}\chi = \pi'_{r+1}$ ebenfalls in $\mathfrak{p}^{r+1}$ enthalten ist, der Kongruenz $\pi_{r+1}\chi \equiv \pi_{r+1} \pmod{\mathfrak{p}^{r+1}}$, weil $\pi'_{r+1} \equiv \pi_{r+1} \equiv 0 \pmod{\mathfrak{p}^{r+1}}$ ist; mithin ist $\mathfrak{p}^{r+1}$ teilbar durch $\mathfrak{o}_1$, und folglich enthält $\mathfrak{o}_1$ auch n voneinander unabhängige Zahlen; $\mathfrak{o}_1$ ist ein endlicher n-gliedriger Modul, dessen Basis zugleich eine Basis des Körpers Ω ist. Da $\mathfrak{o} < \mathfrak{o}_1 < \mathfrak{p}^{r+1}$, so ist

$$(\mathfrak{o}, \mathfrak{p}^{r+1}) = p^{(r+1)f} = (\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{p}^{r+1}),$$

also

$$(\mathfrak{o}, \mathfrak{o}_1) = p^h, \quad 0 < h \leqq (r+1)f.$$

Sodann leuchtet ein, daß $\mathfrak{o}_1$ eine Ordnung ist; denn für jede ganze rationale, d. h. in $\mathfrak{z}$ enthaltene Zahl z ist $z\chi = z$, also ist $\mathfrak{z} > \mathfrak{o}_1$,

und da aus $\alpha\chi \equiv \alpha$, $\beta\chi \equiv \beta \pmod{\mathfrak{p}^{r+1}}$ auch $(\alpha\beta)\chi = \alpha\chi \cdot \beta\chi \equiv \alpha\beta \pmod{\mathfrak{p}^{r+1}}$ folgt, so ist auch $\mathfrak{o}_1^2 > \mathfrak{o}_1$, w. z. b. w. (D., S. 505). Da $\mathfrak{p}^{r+1} > \mathfrak{o}_1$, so ist der Führer

$$\frac{\mathfrak{o}_1}{\mathfrak{o}} = \mathfrak{p}^k, \quad 0 < k \leqq r+1, \quad (\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{p}^k) = (\mathfrak{o}, \mathfrak{p}^k) = p^{kf},$$
$$0 < h \leqq kf$$

oder vielmehr $0 < h < kf$, weil $\mathfrak{o}_1$ notwendig ein echter Teiler von $\mathfrak{p}^k$ ist.

Nun sei ϱ eine bestimmte durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl, so ist $\mathfrak{o}\varrho + \mathfrak{p}^2 = \mathfrak{p}$, also $\mathfrak{o}\varrho^r + \mathfrak{p}^{2r} = \mathfrak{o}\varrho^r + \mathfrak{p}^{r+1} = \mathfrak{p}^r$; da nun alle $\omega\chi - \omega$ in $\mathfrak{p}^r$ enthalten sind, so kann man setzen

$$\omega\chi \equiv \omega + \varrho^r d\omega \pmod{\mathfrak{p}^{2r}},$$

wo $d\omega$ eine zu ω gehörige Zahl ist, die mod. $\mathfrak{p}^r$ bestimmt ist. Für alle in $\mathfrak{o}_1$ enthaltenen Zahlen ω_1, und nur für diese, ist

$$d\omega_1 \equiv 0 \pmod{\mathfrak{p}}.$$

Nun folgen aus $(\alpha \pm \beta)\chi = \alpha\chi \pm \beta\chi$ und $(\alpha\beta)\chi = (\alpha\chi)(\beta\chi)$, und aus

$$\alpha\chi \equiv \alpha + \varrho^r d\alpha, \quad \beta\chi \equiv \beta + \varrho^r d\beta \pmod{\mathfrak{p}^{2r}}$$

die Gesetze (Differentialrechnung)

$$d(\alpha \pm \beta) \equiv d\alpha \pm d\beta, \quad d(\alpha\beta) \equiv \beta d\alpha + \alpha d\beta \pmod{\mathfrak{p}^r}$$

und hieraus weiter

$$d(\omega^m) \equiv m\omega^{m-1} d\omega \pmod{\mathfrak{p}^r}.$$

Da hieraus $d(\varrho^2) \equiv 2\varrho d\varrho \pmod{\mathfrak{p}^r}$, also $d(\varrho^2) \equiv 0 \pmod{\mathfrak{p}}$ folgt, so ist ϱ^2 in $\mathfrak{o}_1$ enthalten; da ferner $\mathfrak{p}^2 = \mathfrak{o}\varrho^2 + \mathfrak{p}^{r+1}$, also jede in $\mathfrak{p}^2$ enthaltene Zahl

$$\pi_2 = \omega\varrho^2 + \pi_{r+1}$$

gesetzt werden kann, wo ω in $\mathfrak{o}$, π_{r+1} in $\mathfrak{p}^{r+1}$ enthalten ist, so folgt $d\pi_2 \equiv \omega d(\varrho^2) + \varrho^2 d\omega + d\pi_{r+1} \pmod{\mathfrak{p}^r}$, also $d\pi_2 \equiv 0 \pmod{\mathfrak{p}}$, folglich $\mathfrak{p}^2 > \mathfrak{o}_1$, also $k = 1$ oder $= 2$.

[Dieser Satz über die Substitutionen der höheren Verzweigungsgruppen — der, nach der Überschrift zu schließen, vor der Publikation in den Göttinger Nachrichten zu liegen scheint — wurde in der Literatur nie in dieser Fassung ausgesprochen. E. N.]

XLIV.

Ideale in Normalkörpern.

Ist χ irgend eine Permutation des Normalkörpers Ω, ω irgend eine Zahl in Ω, so setze man

$$\omega\chi = \omega + d\omega, \quad \omega\chi^s = \omega + \frac{s}{1}d\omega + \frac{s(s-1)}{1\cdot 2}d^2\omega + \cdots = (1+d)^s\omega,$$

$$d^s\omega = \omega(\chi - 1)^s \text{ symbolisch;}$$

aus $(\alpha \pm \beta)\chi = \alpha\chi \pm \beta\chi$ und $(\alpha\beta)\chi = (\alpha\chi)(\beta\chi)$ folgt

$$d(\alpha \pm \beta) = d\alpha \pm d\beta, \quad d(\alpha\beta) = \beta d\alpha + \alpha d\beta + d\alpha d\beta.$$

Alle Zahlen ω, welche der Bedingung $d\omega = 0$ genügen, bilden den zu der Gruppe $1, \chi, \chi^2, \chi^3 \cdots$ gehörigen Körper, welcher $= \Omega$ ist, falls χ die identische Permutation von Ω ist.

Von jetzt ab bedeute ω jede ganze Zahl des Körpers Ω, also jede Zahl in $\mathfrak{o}$, so ist $d\omega$ ebenfalls in $\mathfrak{o}$ enthalten, und zufolge $d(\alpha - \beta) = d\alpha - d\beta$ bilden alle diese Zahlen $d\omega$ einen durch $\mathfrak{o}$ teilbaren Modul, der mit $d\mathfrak{o}$ bezeichnet werden kann. Ist χ die identische Permutation, so ist $d\mathfrak{o} = 0$. Ist h der kleinste positive Exponent, für welchen $\chi^h = 1$, so ist $n = hk$ der Grad von Ω (Bezeichnung wie im Schreiben an G. Frobenius von 1882. 6. 8.), k der Grad des Körpers aller derjenigen Zahlen ω, deren $d\omega = 0$. Ist

$$\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k]$$

das System aller ganzen Zahlen dieses Körpers, und

$$\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n],$$

so folgt, weil gleichzeitig

$$\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

und

$$d\omega = x_1 d\omega_1 + x_2 d\omega_2 + \cdots + x_n d\omega_n$$

ist,

$$d\mathfrak{o} = [d\omega_1, d\omega_2, \cdots, d\omega_n].$$

Da nun

$$\varepsilon_r = a_{1,r}\omega_1 + a_{2,r}\omega_2 + \cdots + a_{n,r}\omega_n,$$

also

$$0 = a_{1,r}d\omega_1 + a_{2,r}d\omega_2 + \cdots + a_{n,r}d\omega_n$$

und die aus den ganzen rationalen Zahlen $a_{i,r}$ gebildeten Determinanten k^{ten} Grades nicht alle verschwinden, so sind von den n Zahlen $d\omega_1$, $d\omega_2, \cdots, d\omega_n$ höchstens $n - k = (h-1)k$ voneinander unabhängig. Umgekehrt: findet zwischen diesen Zahlen $d\omega_i$ eine Relation $\sum x_i d\omega_i = 0$ statt, mit ganzen rationalen Koeffizienten x_i, so ist $d\sum x_i\omega_i = 0$, also $\sum x_i\omega_i$ in $\mathfrak{e}$ enthalten, also

$$\sum x_i\omega_i = \sum y_i\varepsilon_i, \quad x_r = \sum y_i a_{r,i}.$$

Als Basis des Körpers Ω kann man

$$\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \quad \omega_{k+1}, \cdots, \omega_n$$

wählen, wo $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k$ eine Basis des zu der Gruppe χ gehörigen Körpers Ω' bilden,

$$\omega = h_1\varepsilon_1 + h_2\varepsilon_2 + \cdots + h_k\varepsilon_k + h_{k+1}\omega_{k+1} + \cdots + h_n\omega_n,$$
$$d\omega = h_{k+1}d\omega_{k+1} + \cdots + h_n d\omega_n,$$
$$d\omega_{k+1}, \cdots, d\omega_n \text{ Basis der Schar } d\Omega.$$

Denn wäre

$$h_{k+1}d\omega_{k+1} + \cdots + h_n d\omega_n = 0,$$

so ist

$$h_{k+1}\omega_{k+1} + \cdots + h_n\omega_n$$

in Ω' enthalten, also

$$= h_1\varepsilon_1 + \cdots + h_k\varepsilon_k,$$

woraus folgt, daß alle $h = 0$ sind.

[Diese formale Differentiation war offenbar zur Untersuchung der Differente gedacht, wie weitere angefangene Rechnungen zeigen, wo dieselben Betrachtungen modulo p auftreten; darauf weist auch die Überschrift hin. E. N.]

XLV.

Aus Briefen an Frobenius*).

8. Juni 1882**).

... Die Ihnen bekannte Existenz einer Substitution F (bei mir Permutation ψ_0), für welche $\omega^p \equiv F\omega \pmod{\mathfrak{p}}$, bildet auch bei mir die eigentliche Basis; Sie schreiben zwar: „Ich irre wohl nicht, wenn ich annehme, dass der durch diesen Satz angedeutete Weg einer von denen ist, die auch Sie früher einmal eingeschlagen, dann aber wohl schliesslich verlassen und durch einen bessern ersetzt haben.“ Aber ich glaube kaum, dass es einen besseren Weg giebt. Mit Hülfe der Theorie der höheren Congruenzen und mit viel Geduld und Zeit ist es mir nach und nach gelungen, die Schwierigkeiten zu überwinden und die Gesetze möglichst einfach zu gestalten. In diesen ist auch, wie Sie vermuthen, der Satz enthalten, für den Sie einen Beweis wünschen, und den Sie so aussprechen:

Ist eine rationale Primzahl $\mathfrak{o}'p = \mathfrak{p}'_1\mathfrak{p}'_2 \cdots \mathfrak{p}'_{e'}$, wo $\mathfrak{p}'_1, \mathfrak{p}'_2 \cdots \mathfrak{p}'_{e'}$ verschiedene Primideale in $\mathfrak{o}'$ von den Graden $f'_1, f'_2, \cdots f'_{e'}$ sind, so giebt es in der Gruppe Φ des Körpers Ω' eine Substitution ψ_0, die aus e' Cyklen von $f'_1, f'_2, \cdots f'_{e'}$ Elementen besteht.

In der That, wenn alle $a_r = 1$, mithin alle $g_r = g$ sind, so ist X gemeinschaftlicher Theiler aller $\varphi_r \Phi' \varphi_r^{-1}$ und überhaupt aller mit Φ' conjugirten Gruppen $\varphi\Phi'\varphi^{-1}$; da diese aber, wenn wirklich Φ die

*) [Diese Briefe wurden durch Herrn Landau freundlichst zur Verfügung gestellt. Die Briefe von Frobenius an Dedekind waren im Nachlaß nicht zu finden; es fehlten im Nachlaß die Briefe aus den Jahren 1880—1900. E. N.]

**) [Im wesentlichen wiedergegeben bei Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Sitzungsber. d. Preuß. Akademie d. Wissensch. 1896. E. N.]

Gruppe von Ω', d. h. Ω die Norm von Ω' ist, keinen gemeinsamen Theiler haben, so muß $X = 1$, $g = 1$ sein, d. h. p ist durch kein Primidealquadrat in Ω theilbar. Dann ist

$$\Psi'_r = 1 + \psi_r^{f'_r} + \psi_r^{2f'_r} + \cdots + \psi_r^{(f_r-1)f'_r},$$

wo $\psi_r = \varphi_r^{-1}\psi_0\varphi_r$,

$$\Phi'\varphi_r^{-1}\Psi' = \Phi'\varphi_r^{-1} + \Phi'\varphi_r^{-1}\psi_0 + \Phi'\varphi_r^{-1}\psi_0^2 + \cdots + \Phi'\varphi_r^{-1}\psi_0^{f'_r-1};$$

ersetzt man in der Zerlegung

$$\Phi = \Phi'\varphi_1^{-1}\Psi' + \cdots + \Phi'\varphi_{e'}^{-1}\Psi'$$

jeden einzelnen Complex $\Phi'\varphi_r^{-1}\Psi'$ durch das vorstehende System der f'_r Complexe, so wird Φ überhaupt in

$$n' = f'_1 + f'_2 + \cdots + f'_{e'}$$

Complexe $\Phi'\varphi$ zerlegt, deren jedem bekanntlich eine Permutation von Ω' (eine Wurzel der irreductibeln Gleichung vom Grade n') entspricht; die Permutation ψ_0 verwandelt dieselben in die Complexe $\Phi'\varphi\psi_0$, bringt also eine Permutation dieser n' Complexe (Elemente) $\Phi'\varphi$ hervor, bei welcher die in $\Phi'\varphi_r^{-1}\Psi'$ enthaltenen f'_r Complexe (Elemente, Wurzeln) cyklisch in einander übergehen.

14. Juni 1882*).

... Auf den hiermit wieder zurückerfolgenden Blättern (13—15) haben Sie die Existenz einer Permutation ψ_0 (oder Substitution F) sehr kurz bewiesen. Bei mir ergiebt sich dieselbe z. B. aus der leicht zu beweisenden Existenz einer ganzen Zahl Θ, welche (mod. $\mathfrak{p}$) einer irreductibelen Congruenz f^{ten} Grades mit rationalen Coefficienten genügt, und welche man zugleich (für unseren Zweck) so wählen kann, dass sie nicht durch $\mathfrak{p}$, wohl aber durch jedes andere in p aufgehende Primideal theilbar ist; wenn nun $f(t) = \Pi(t - \Theta|\varphi)$, so ist $f(\Theta) = 0$, mithin $f(\Theta^p) \equiv 0 \pmod{\mathfrak{p}}$, folglich $\Theta^p \equiv \Theta|\psi_0 \pmod{\mathfrak{p}}$; wäre ferner $\mathfrak{p}|\psi_0^{-1}$ verschieden von $\mathfrak{p}$, so wäre $\Theta \equiv 0 \pmod{\mathfrak{p}|\psi_0^{-1}}$, also $\Theta|\psi_0 \equiv 0 \pmod{\mathfrak{p}}$, also $\Theta^p \equiv 0 \pmod{\mathfrak{p}}$, also auch $\Theta \equiv 0 \pmod{\mathfrak{p}}$, contra hyp. Also $\mathfrak{p}|\psi_0^{-1} = \mathfrak{p}$; $\mathfrak{p}|\psi_0 = \mathfrak{p}$. Nun ist (zufolge Def. von Θ)

*) [Im wesentlichen wiedergegeben bei Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. E. N.]

jede ganze Zahl $\omega \equiv F(\Theta) \pmod{\mathfrak{p}}$, wo $F(t)$ eine ganze Function mit ganzen rationalen Coefficienten; mithin $\omega|\psi_0 \equiv F(\Theta)|\psi_0 = F(\Theta|\psi_0) \equiv F(\Theta^p) \equiv F(\Theta)^p \equiv \omega^p \pmod{\mathfrak{p}|\psi_0 = \mathfrak{p}}$.

5. Februar 1883*).

... Ihr thätiges Interesse an der Zahlentheorie ist mir sehr erfreulich, und die grosse Abkürzung der Untersuchung über die Discriminante, die Sie und Hr. Stickelberger aufgefunden haben, gefällt mir besonders deshalb, weil die mir immer unliebsame Zuziehung der Theorie der höheren Congruenzen (mit Variabeln) wieder aufgehoben wird. Ihr rationales $R(\omega)$ ist mir freilich lange bekannt gewesen, aber ich habe nie daran gedacht, es auf so glückliche Weise zu verwenden. Immerhin lege ich aus besonderen, persönlichen Gründen einigen Werth auf den Satz, dass es immer eine reguläre Ordnung giebt, deren Führer durch ein gegebenes Primideal nicht theilbar ist; hierin besteht für mich der letzte Rest und wirkliche Kern ehemaliger Vermuthungen, die zu klären ich lange Zeit gebraucht habe. Zwar weiss ich nicht mehr, ob ich jemals geglaubt habe, jedes System $\mathfrak{o}$ aller in einem Körper Ω enthaltenen ganzen Zahlen sei eine reguläre Ordnung (welcher Fall für die ersten Kummer'schen Untersuchungen so sehr günstig gewesen ist), aber lange Zeit habe ich es für äusserst wahrscheinlich gehalten und kaum bezweifelt, dass es immer reguläre Ordnungen $\mathfrak{n}$ gebe, für welche $(\mathfrak{o}, \mathfrak{n})$ durch eine gegebene rationale Primzahl nicht theilbar ist; meine alten Papiere enthalten viele Beweisversuche, die natürlich immer im Sande verlaufen, bis endlich die bessere Erkenntniss kam; und dann hat es wieder lange gedauert, bis ich (etwa vor zwei Jahren, wie ich glaube) das oben genannte Residuum sicher stellen konnte.

Ihr Kriterium darüber, ob ein Ideal $\mathfrak{k}$ Führer einer Ordnung sein kann, scheint mir mit dem meinigen auch äusserlich fast identisch zu werden, sobald man die Elementartheiler Ihrer Determinante als invariante Theiler der Classenanzahl $(\mathfrak{b}, \mathfrak{a})$ für beliebige Moduln $\mathfrak{a}$, $\mathfrak{b}$ auffasst, die ganz unabhängig von Determinanten definirt werden können und von denen der erste der kleinste Multiplicator

*) [Einige Einzelheiten aus diesem Briefe sind in § 170 der vierten Auflage der Zahlentheorie übernommen; der in dem Briefe gegebene volle Überblick über die Fragen der Modultheorie ist nirgends publiziert. Für den Schluß des Briefes vgl. XXIX. E. N.]

ist, der $\mathfrak{b}$ in ein Multiplum von $\mathfrak{a}$ verwandelt. Sie haben, wie Sie schreiben, aus Ihrer Form noch keinen Nutzen ziehen können für die Beantwortung der Frage nach den Ordnungen, die ein solches Ideal zum Führer haben; dasselbe gilt auch für meine Form. Diese Aufgabe will besonders angegriffen sein. Es leuchtet ein, dass das kleinste gemeinschaftliche Vielfache beliebig vieler Ordnungen $\mathfrak{n}_1, \mathfrak{n}_2 \cdots$ immer wieder eine Ordnung $\mathfrak{n}$ ist, deren Führer $\mathfrak{k}$ zugleich das kleinste gemeinschaftliche Vielfache von den Führern $\mathfrak{k}_1, \mathfrak{k}_2 \cdots$ jener Ordnungen ist; und dieser Satz lässt sich wenigstens dahin umkehren, dass jede Ordnung $\mathfrak{n}$ das kleinste gemeinschaftliche Vielfache solcher Ordnungen $\mathfrak{n}_1, \mathfrak{n}_2 \cdots$ ist, für welche $(\mathfrak{o}, \mathfrak{n}_1)$, $(\mathfrak{o}, \mathfrak{n}_2) \cdots$ die verschiedenen in $(\mathfrak{o}, \mathfrak{n})$ aufgehenden höchsten Primzahlpotenzen sind; dadurch wird die Untersuchung auf die Betrachtung solcher Ordnungsführer $\mathfrak{k}$ zurückgeführt, deren Normen Primzahlpotenzen sind. Die nähere Untersuchung, die mehr lästig, als principiell schwierig ist, ergiebt eine große Reichhaltigkeit; die Grundlage bildet der einfachste Fall, wo $\mathfrak{k}$ ein Primideal $\mathfrak{p}$ vom Grade f ist: die Anzahl der verschiedenen Ordnungen $\mathfrak{n}$, welche $\mathfrak{p}$ zum Führer haben, ist um eins kleiner, als die Anzahl der Divisoren m von f; jedem echten Divisor m entspricht eine Ordnung $\mathfrak{n}$, welche aus den sämmtlichen Wurzeln v der Congruenz

$$v^{p^m} \equiv v \pmod{\mathfrak{p}}$$

besteht; $(\mathfrak{n}, \mathfrak{p}) = p^m$; $N(\mathfrak{p}) = p^f$.

Diese Untersuchung bildet ein Capitel der allgemeinen Theorie der n-gliedrigen Moduln in einem Körper n^{ten} Grades, welche in meiner Gauss-Festschrift (1877), wie ich dort ausdrücklich bemerkt habe, keineswegs vollständig behandelt ist; aber ihre wichtigsten Grundlagen sind doch in dieser Schrift enthalten. Es kommt hierbei auf den Unterschied zwischen umkehrbaren und nicht umkehrbaren Moduln an; ich nenne einen Modul $\mathfrak{a}$ umkehrbar (auch im allgemeinsten Sinn des Worts Modul), wenn ein Modul $\mathfrak{b}$ existirt, für welchen $\mathfrak{a}\mathfrak{b} = \mathfrak{a}^0$, d. h. gleich der Ordnung von $\mathfrak{a}$ wird; alle solche Moduln $\mathfrak{b}$ liefern ein und dasselbe Product $\mathfrak{b}\mathfrak{a}^0$, das ich mit $\mathfrak{a}^{-1}$ bezeichne, und dessen Ordnung immer $= \mathfrak{a}^0$ ist; jedes Product von umkehrbaren Moduln ist wieder ein umkehrbarer Modul, und seine Ordnung ist das Product aus den Ordnungen der Factoren. Unter den n-gliedrigen Moduln eines Körpers Ω vom Grade n sind die einfachsten die Moduln, deren Ordnung $= \mathfrak{o}$; sie sind alle umkehrbar und identisch

mit den Ideal-Quotienten; die Regeln ihrer Multiplication und Division stimmen genau mit denjenigen für rationale Brüche überein; die Definition der Norm ist selbstverständlich. Ähnliches (mit Modification) gilt für die Moduln einer jeden regulären, allgemeiner jeder solchen Ordnung $\mathfrak{n}$, deren Complement $\mathfrak{n}'$ umkehrbar ist (weil für jeden solchen Modul $\mathfrak{a}$ immer $\mathfrak{a}\mathfrak{a}' = \mathfrak{n}'$ ist). Aber sobald $n > 2$ ist, haben durchaus nicht mehr alle Ordnungen diese Eigenschaft. Ist nun $\mathfrak{m}$ ein beliebiger Modul, $\mathfrak{n}$ seine Ordnung, so ist $\mathfrak{m}\mathfrak{o}$ immer ein Modul der Ordnung $\mathfrak{o}$, also ein Ideal-Quotient, und der Führer von $\mathfrak{m}$, d. h. der Quotient $\frac{\mathfrak{m}}{\mathfrak{o}}$ ist $= \mathfrak{f}\mathfrak{m}$, wo $\mathfrak{f}$ der Führer von $\mathfrak{n}$; $N(\mathfrak{m})$ wird definirt als $N(\mathfrak{m}\mathfrak{o})$. Umgekehrt, ist $\mathfrak{a}$ ein Modul der Ordnung $\mathfrak{o}$, so folgt aus der Festschrift (1877) die wichtige Existenz mindestens eines umkehrbaren Moduls $\mathfrak{m}$ jeder Ordnung $\mathfrak{n}$, für welchen $\mathfrak{m}\mathfrak{o} = \mathfrak{a}$ wird; und die sämmtlichen Moduln $\mathfrak{m}$, derselben Ordnung $\mathfrak{n}$, welche derselben Forderung $\mathfrak{m}_1\mathfrak{o} = \mathfrak{a}$ genügen, sind die sämmtlichen Producte $\mathfrak{m}\mathfrak{e}$, wo $\mathfrak{e}$ alle diejenigen Moduln der Ordnung $\mathfrak{n}$ durchläuft, für welche $\mathfrak{e}\mathfrak{o} = \mathfrak{o}$ wird. Der Reichthum an solchen Moduln $\mathfrak{e}$ ist sehr gross; sie sind natürlich lauter ganze Moduln, d. h. Vielfache von $\mathfrak{o}$, und zugleich Theiler des Führers $\mathfrak{f}$, da $\frac{\mathfrak{e}}{\mathfrak{o}} = \frac{\mathfrak{n}}{\mathfrak{o}} = \mathfrak{f}$ ist.

Hierin bestehen, wenn ich mich recht erinnere, die hauptsächlichsten Gedanken der genannten Theorie, die ich übrigens noch niemals vollständig ausgearbeitet habe; doch hoffe ich, Ihnen nichts Unrichtiges geschrieben zu haben. Wichtig ist diese Theorie, und namentlich scheint sie unerlässlich für die Aufstellung der allgemeinsten Gesetze, welche die bisher bekannten, sogenannten Reciprocitätssätze in sich schliessen. Bei cubischen Körpern Ω z. B. kommt die Primideal-Zerlegung derjenigen rationalen Primzahlen p, von denen die Grundzahl $D = \Delta(\Omega)$ quadratischer Rest ist (die übrigen p machen keine Schwierigkeit), auf die Betrachtung der ursprünglichen quadratischen Formen $(a, \frac{1}{2}b, c)$ zurück, deren Discriminante $b^2 - 4ac = D$ ist; die Anzahl der Classen dieser Formen oder der entsprechenden Modul-Classen ist immer durch 3 theilbar, und ein gewisses Drittel dieser Classen bildet eine Gruppe; je nachdem p durch eine Form dieser Gruppe darstellbar ist oder nicht, ist $\mathfrak{o}p$ in Ω ein Product von drei Primidealen ersten Grades oder ein Primideal dritten Grades. Für negative D hängt dies mit der complexen Multiplication der

elliptischen Functionen zusammen, was auch Kronecker vollständig erkannt zu haben scheint. Ich habe diesen Satz, der ohne jeden Zweifel ganz allgemein, auch für positive D gilt, vor 11 Jahren durch Induction gefunden (Schlömilch's Zeitschrift, Jahrgang 18; 1873. Literaturzeitung S. 22 und S. 43, wo der durch die Schuld des Herrn Schlömilch ausgelassene Zusatz steht), gestehe aber gern, dass ich ihn noch nicht für alle Fälle bewiesen habe; doch hoffe ich dies noch zu erreichen. Er gilt sogar, wenn D eine positive Quadratzahl, mithin Ω ein Normalkörper ist, der aus der Kreistheilung entspringt. Ich glaube gewiss, man wird dereinst ganz allgemeine Gesetze finden, welche gestatten, die Primideale eines Körpers unmittelbar abzuleiten aus seiner Discriminante und seinen übrigen Invarianten (die auch Ideale verwandter Körper sein können); doch mögen wir wohl noch recht weit von diesem Ziele entfernt sein! In den letzten Jahren habe ich mich sehr wenig mit diesen Fragen beschäftigt, zu denen ich aber grosse Lust habe zurückzukehren, weil sie mir von allen die interessantesten zu sein scheinen. . . .

8. Februar 1895*).

. . . Auf Ihre Arbeit über die Gruppen bin ich sehr gespannt, da die Einfachheit Ihrer Methoden, unter Anderem Ihr Beweis, dass in einer Gruppe, deren Grad durch die Primzahl p theilbar ist, es immer ein Element p^{ter} Ordnung giebt, mich sehr erfreut hat; ich war in den ersten Jahren meiner Gruppen-Studien (1855—1858) auf einem viel umständlicheren Wege dahin gekommen. Auch später habe ich gewisse Gruppen-Fragen immer nur so weit verfolgt, wie es Veranlassungen von anderer Seite her mit sich brachten; sollte es also der Zufall wollen, dass ich mich mit dem Gegenstande Ihrer Arbeit schon jemals beschäftigt hätte, so würde ich doch gewiss weit hinter Ihnen zurückgeblieben sein. Um auf gut Glück zu rathen, frage ich: drängen sich in Ihre Untersuchung auch übercomplexe Grössen ein mit nicht commutativer Multiplication? Doch will ich Sie keineswegs mit der Bitte um eine Antwort bemühen, die

*) [Die jetzt folgenden Briefstellen geben einen wesentlichen Beitrag zur Geschichte der Theorie der hyperkomplexen Größen und der Gruppendeterminante. Auf die Rolle, die Dedekind in dieser Theorie gespielt hat, weist Frobenius an verschiedenen Stellen hin, in den Einleitungen zu den Arbeiten über Gruppencharaktere, über die Primfaktoren der Gruppendeterminante und über die Darstellung der endlichen Gruppen. E. N.]

ich am besten durch Ihre Abhandlung erhalten werde. Ihre äusserst scharfsinnige Untersuchung über die Elementartheiler der Determinanten habe ich mit grossem Interesse studirt; ich leugne nicht, dass ich bei dem Beweise in §. 1 die unbestimmte Empfindung habe, als könnte er auch wohl ohne die Gleichung (6) auf S. 4 gelingen, aber ich bin ganz ausser Stande, etwas Anderes an die Stelle zu setzen. . . .

12. Februar 1895.

. . . Keine Entschuldigung habe ich für meine gewagte Bemerkung bezüglich Ihrer Abhandlung über die Elementartheiler — die unbestimmte Empfindung entspringt aus einer in diesem Falle wohl sehr thörichten Abneigung gegen Potenzen-Folgen — um so mehr muss ich um Nachsicht wegen deren Äusserung bitten. Auch meine Frage wegen der Benutzung übercomplexer Grössen in der Gruppen-Theorie war sehr dreist; sie ging hervor aus einer Beobachtung, die ich im Februar 1886 gemacht, dann aber nicht weiter verfolgt habe, obwohl sie mir merkwürdig genug erschien; vielleicht darf ich mir einmal erlauben, sie Ihnen vorzulegen, auf die Gefahr hin, dass sie vor Ihrer Kritik gänzlich dahin schwindet, möglicherweise auch gar nicht einmal neu ist. . . .

25. März 1896.

. . . Da ich einmal von Gruppen spreche, so möchte ich noch eine andere Betrachtung erwähnen, auf die ich im Februar 1886 gekommen bin. Zu jeder Gruppe n^{ten} Grades G bilde ich eine Form n^{ten} Grades H mit n Variabelen, die ich die Determinante von G nenne: sind $1, 2 \cdots n$ die in irgend einer Ordnung aufgeschriebenen Elemente von G, so lasse ich jedem Elemente r der Gruppe G eine Variabele x_r entsprechen, und bilde die Determinante

$$H = \begin{vmatrix} x_{11'}, & x_{21'} \cdots x_{n1'} \\ x_{12'}, & x_{22'} \cdots x_{n2'} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ x_{1n'}, & x_{2n'} \cdots x_{nn'} \end{vmatrix},$$

wo r' das zu r reciproke Element von G bedeutet. Ist G eine Abel'sche Gruppe, und sind ψ', $\psi'' \cdots \psi^{(n)}$ die ihr entsprechenden Charaktere (Einheitswurzeln), so ist die Determinante H eine zerlegbare Form, nämlich das Product der n linearen Factoren

$$\sum^{r} \psi^{(s)}(r)\, x_r = \psi^{(s)}(1)\, x_1 + \cdots + \psi^{(s)}(n)\, x_n,$$

die den n Werthen von s entsprechen (ein Satz, welcher in dieser Allgemeinheit, wie ich glaube, noch nicht ausgesprochen ist). Wenn aber G keine Abel'sche Gruppe ist, so besitzt ihre Determinante H, soweit ich es untersucht habe, ausser linearen Factoren (wie z. B. immer $x_1 + x_2 + \cdots + x_n$) auch Factoren höheren Grades, die im gewöhnlichen Sinne unzerlegbar sind; aber diese werden wieder zerlegbar in lineare Factoren, wenn man ausser den gewöhnlichen Zahlen als Coefficienten auch übercomplexe Zahlen (mit nicht commutativer Multiplication) gestattet, die den Gesetzen der Gruppe G entsprechen. Bei der obigen Quaternion-Gruppe Q z. B. treten auf diese Weise bei der erzwungenen Zerlegung ihrer Determinante in lineare Factoren (deren vier gewöhnliche Coefficienten haben) in der That Hamilton's Quaternion-Zahlen auf. Man darf überhaupt wohl vermuthen, dass die Eigenschaften einer Gruppe G hinsichtlich ihrer Theiler sich in der Zerlegung ihrer Determinante H wiederspiegeln werden; ausser einer Spur, die auf einen Zusammenhang zwischen der Anzahl der gewöhnlichen linearen Factoren von H und denjenigen Normaltheilern A von G hindeutet, welche die Eigenschaft $Ars = Asr$ besitzen, habe ich aber noch gar Nichts gefunden, und es ist überhaupt wohl möglich, dass bei der ganzen Sache vorläufig wenig herauskommen wird. . . .

3. April 1896.

. . . Erwähnen möchte ich noch Folgendes*). Man sieht leicht, dass Q durch 24 Transformationen, bei welchen sich nur die sechs Buchstaben α, α^{-1}, β, β^{-1}, γ, γ^{-1} mit einander vertauschen, isomorph in sich selbst übergeht; die Gruppe T dieser Transformationen ist also eine Untergruppe von der Gruppe V_6 aller 720 Versetzungen von 6 Elementen, und zwar habe ich gefunden, dass diese Gruppe T isomorph ist mit der Gruppe V_4 aller 24 Versetzungen von 4 Elementen a, b, c, d. Bezeichnet man nämlich allgemein mit (a, d) die Vertauschung (Transposition) von nur zwei verschiedenen Elementen a, d, so wird die Gruppe T erzeugt durch die drei Elemente zweiten Grades

$$(\alpha, \alpha^{-1})\,(\beta, \gamma)\,(\beta^{-1}, \gamma^{-1}) \equiv (a, d),$$
$$(\beta, \beta^{-1})\,(\gamma, \alpha)\,(\gamma^{-1}, \alpha^{-1}) \equiv (b, d),$$
$$(\gamma, \gamma^{-1})\,(\alpha, \beta)\,(\alpha^{-1}, \beta^{-1}) \equiv (c, d),$$

*) [Es war hier und im vorangehenden Brief ein Überblick über die Arbeit XXVII über Gruppen, deren sämtliche Teiler normal sind, vorangegangen; Q bedeutet die Quaternionengruppe. E. N.]

wo das Zeichen $\equiv$ das isomorphische Entsprechen bedeuten soll. Dass die Gruppe V_6 eine solche transitive Untergruppe $T \equiv V_4$ (vom Index 30) besitzt, wird wohl schon lange bekannt sein; jedenfalls soll dies von meinem Aufsatz über die Hamilton'schen Gruppen ausgeschlossen werden.

Ebenso wenig werde ich dort von der allgemeinen Bedeutung der Commutatoren $\psi^{-1}\varphi^{-1}\psi\varphi$ sprechen, auf welche ich vor vielen Jahren bei der Aufgabe gekommen bin, aus irgend einem Normal-Körper alle darin enthaltenen Abel'schen Körper auszuscheiden. Man findet leicht (— was, wie ich aus Ihrem Briefe schliesse, auch Ihnen gewiss bekannt ist —) den Satz: „Die erforderliche und hinreichende Bedingung dafür, dass A ein invarianter Theiler der Gruppe G, und zugleich G/A eine Abel'sche Gruppe ist ($Ars = Asr$), besteht darin, dass alle Commutatoren von je zwei Elementen r, s der Gruppe G in der Gruppe A enthalten sind; die kleinste solche Gruppe A (diejenige nämlich, welche durch alle Commutatoren erzeugt wird) ist der gemeinsame Theiler von allen A.“ Ich erwähne dies auch nur, um nochmals auf die von Ihnen günstig aufgenommene Determinante H irgend einer Gruppe G zurückzukommen, welche ich vor 10 Jahren an einigen sehr speciellen Beispielen (V_3 vom Grade 6, Q vom Grade 8) und einigen allgemeineren (complexe Multiplication) untersucht habe. Auf Ihre Anfrage wegen des einen Punctes gestehe ich, dass ich nichts Bestimmtes weiss, aber ich vermuthe allerdings, dass die Anzahl der linearen Factoren der Determinante H der Index der eben genannten kleinsten Gruppe A, also der Grad der Abel'schen Gruppe G/A ist, und dass diese Factoren in gewisser Weise den Charakteren dieser letzteren Gruppe entsprechen. Es würde mich sehr freuen, wenn Sie sich in diese Dinge versenken wollten, weil ich deutlich fühle, dass ich hier Nichts zu Stande bringen werde. Dass Ihre Determinante der Charakteristiken-Gruppe in den Thetafunctionen wesentlich mit meinem H übereinstimmt (besser umgekehrt), scheint mir nach Einblick in Ihre Abhandlung (Crelle 96, S. 100) ganz unzweifelhaft, und Ihnen gebührt daher auch die volle Priorität für diese Gruppen-Determinanten *). Was den Fall der Abel'schen

*) [Frobenius erwähnt in der Arbeit über die Primfaktoren der Gruppendeterminante, daß er vom Additionstheorem aus, und nicht durch die Gruppe der Relationen, auf die Determinante der Charakteristiken gekommen sei. E. N.]

Gruppen betrifft, so habe ich wohl in den Wiener Sitzungs-Berichten einige darauf bezügliche Aufsätze (von Gegenbauer?) gesehen; doch glaube ich nicht, dass der Satz in seiner Allgemeinheit dort ausgesprochen ist. . . .

6. April 1896.

. . . Für den Fall, dass Sie sich noch näher mit den Gruppen-Determinanten beschäftigen wollen, erlaube ich mir hiermit, Ihnen wenigstens zwei von den Beispielen zu senden, die ich im Februar 1886 ausgerechnet habe; doch übergehe ich die übercomplexe Zerlegung der nicht linearen Factoren.

Beispiel 1.

Gruppe V_3 der sechs Versetzungen von drei Buchstaben a, b, c.

Bezeichnung und Composition der Substitutionen:

	a	b	c
1	a	b	c
2	b	c	a
3	c	a	b
4	a	c	b
5	c	b	a
6	b	a	c

	1^{-1}	2^{-1}	3^{-1}	4^{-1}	5^{-1}	6^{-1}
1	1	3	2	4	5	6
2	2	1	3	5	6	4
3	3	2	1	6	4	5
4	4	5	6	1	3	2
5	5	6	4	2	1	3
6	6	4	5	3	2	1

Setzt man $1 + \varrho + \varrho^2 = 0$

und
$$u = x_1 + x_2 + x_3, \qquad v = x_4 + x_5 + x_6,$$
$$u_1 = x_1 + \varrho x_2 + \varrho^2 x_3, \qquad v_1 = x_4 + \varrho x_5 + \varrho^2 x_6,$$
$$u_2 = x_1 + \varrho^2 x_2 + \varrho x_3, \qquad v_2 = x_4 + \varrho^2 x_5 + \varrho x_6,$$

so wird die Gruppen-Determinante

$$\begin{vmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_5 & x_6 & x_4 \\ x_3 & x_2 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_3 & x_2 \\ x_5 & x_6 & x_4 & x_2 & x_1 & x_3 \\ x_6 & x_4 & x_5 & x_3 & x_2 & x_1 \end{vmatrix} = (u+v)(u-v)(u_1 u_2 - v_1 v_2)^2$$

am kürzesten wohl durch Multiplication mit der Determinante

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \varrho & \varrho^2 & 1 & \varrho & \varrho^2 \\ 1 & \varrho^2 & \varrho & 1 & \varrho^2 & \varrho \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \varrho & \varrho^2 & -1 & -\varrho & -\varrho^2 \\ 1 & \varrho^2 & \varrho & -1 & -\varrho^2 & -\varrho \end{vmatrix} = 6^3 = 216.$$

Die Gruppe $1 + 2 + 3$ der Commutatoren hat den Index zwei, gleich der Anzahl der linearen Factoren.

Beispiel 2.

Bezeichnet man die Elemente $1, \varepsilon, \alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \gamma^{-1}$ der Quaternion-Gruppe Q mit 1, 2, 3, 4, 5, 6, 7, 8, so ist die entsprechende Gruppen-Determinante

$$\begin{vmatrix} x_1 & x_2 & x_4 & x_3 & x_6 & x_5 & x_8 & x_7 \\ x_2 & x_1 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_3 & x_4 & x_1 & x_2 & x_8 & x_7 & x_5 & x_6 \\ x_4 & x_3 & x_2 & x_1 & x_7 & x_8 & x_6 & x_5 \\ x_5 & x_6 & x_7 & x_8 & x_1 & x_2 & x_4 & x_3 \\ x_6 & x_5 & x_8 & x_7 & x_2 & x_1 & x_3 & x_4 \\ x_7 & x_8 & x_6 & x_5 & x_3 & x_4 & x_1 & x_2 \\ x_8 & x_7 & x_5 & x_6 & x_4 & x_3 & x_2 & x_1 \end{vmatrix}$$

$$= \begin{vmatrix} u_1 & u_2 & u_3 & u_4 \\ u_2 & u_1 & u_4 & u_3 \\ u_3 & u_4 & u_1 & u_2 \\ u_4 & u_3 & u_2 & u_1 \end{vmatrix} \times \begin{vmatrix} v_1 & -v_2 & -v_3 & -v_4 \\ v_2 & v_1 & -v_4 & v_3 \\ v_3 & v_4 & v_1 & -v_2 \\ v_4 & -v_3 & v_2 & v_1 \end{vmatrix}$$

$$= \begin{cases} (u_1 + u_2 + u_3 + u_4)\,(u_1 + u_2 - u_3 - u_4)\,(u_1 - u_2 + \\ \quad + u_3 - u_4)\,(u_1 - u_2 - u_3 + u_4) \\ \quad \times (v_1^2 + v_2^2 + v_3^2 + v_4^2)^2, \end{cases}$$

wo

$$\begin{Bmatrix} u_1 \\ v_1 \end{Bmatrix} = x_1 \pm x_2, \quad \begin{Bmatrix} u_2 \\ v_2 \end{Bmatrix} = x_3 \pm x_4, \quad \begin{Bmatrix} u_3 \\ v_3 \end{Bmatrix} = x_5 \pm x_6, \quad \begin{Bmatrix} u_4 \\ v_4 \end{Bmatrix} = x_7 \pm x_8.$$

Die Anzahl vier der linearen Factoren ist zugleich der Index der Commutator-Gruppe $[2] = 1 + 2$. Die Quadratsumme $v_1^2 + v_2^2$

$+ v_3^2 + v_4^2$ hat mich damals sehr erfreut und dazu veranlasst, auch andere Gruppen-Determinanten in lineare Factoren mit übercomplexen Coefficienten zu zerlegen; dies gelingt zwar, aber herausgekommen ist dabei Nichts!

Mit dem Wunsche, dass diese immerhin merkwürdigen Erscheinungen Sie zu einer tieferen Ergründung reizen mögen, verbleibe ich ...

27. April 1896.

... Aber so viel sehe ich zu meiner unaussprechlichen Freude auch jetzt schon, dass Sie in raschem Siegeslaufe wahrhaft bewunderungswürdige Erfolge errungen haben, und wenn ich heute auch ausser Stande bin, über die Sache selbst zu schreiben, so will ich doch nicht länger zögern, Ihnen meine herzlichsten Glückwünsche zu diesen Erfolgen zu senden, denen ich eine sehr hohe Bedeutung für die Gruppen-Theorie zuschreibe. Meine Bewunderung ist um so grösser, je aufrichtiger ich mir eingestehen muss, dass ich nimmermehr zu solchen Erfolgen hätte gelangen können, weil meiner gar zu einseitigen Bildung das erforderliche Rüstzeug fehlt, das Sie wie kein Anderer beherrschen. Ich würde daher auch Bedenken tragen, die beiliegenden Bogen Ihrer Einsicht zu unterbreiten, aber da Sie mich in einem Ihrer Briefe zur Mittheilung fernerer Beispiele von Gruppen-Determinanten aufgefordert haben, so sende ich Ihnen hierbei ein altes Beispiel 3. und ein daraus durch Verallgemeinerung kürzlich entstandenes Beispiel 4. auf die Gefahr hin, dass Sie über meine ungeübte Handhabung der Technik lächeln werden. Von der schon mehrmals erwähnten Zerlegung in hypercomplexe lineare Factoren, die, wie schwach sie mir augenblicklich auch erscheint, doch vielleicht den Keim von etwas Brauchbarem enthalten kann, werde ich mir ein anderes Mal zu schreiben erlauben, wenn mein Denken sich gebessert hat. ...

Gruppen-Determinanten.

Beispiel 3 (vom 17. Februar 1886).

Verallgemeinerung von Beispiel 1. — Es sei $\mathfrak{A}$ eine Abel'sche Gruppe von m Elementen

$$\alpha = 1, 2, 3 \cdots m,$$

und es seien

$$\psi = \psi_1, \psi_2, \psi_3 \cdots \psi_m$$

die Charaktere von $\mathfrak{A}$ (Dirichlet, Aufl. 3, S. 581; Aufl. 4, S. 612); dieselben bilden eine (mit $\mathfrak{A}$ isomorphe) Gruppe in der Weise, dass je zwei solche ψ', ψ'' einen Charakter $\psi'\psi''$ erzeugen, welcher durch $\psi'\psi''(\alpha) = \psi'(\alpha)\psi''(\alpha)$ für alle α definirt ist; $\psi^{-1}(\alpha) = \psi(\alpha^{-1})$; $\psi\psi^{-1} = \psi^0$ ist der Haupt-Charakter, $\psi^0(\alpha) = 1$ für alle α und alle ψ. Die aus den m^2 Einheits-Wurzeln $\psi(\alpha)$ gebildete Determinante

$$\Psi = \begin{vmatrix} \psi_1(1) & \cdots & \psi_1(m) \\ \cdot & \cdots & \cdot \\ \psi_m(1) & \cdots & \psi_m(m) \end{vmatrix} = \pm\Psi' = \pm \begin{vmatrix} \psi_1^{-1}(1) & \cdots & \psi_1^{-1}(m) \\ \cdot & \cdots & \cdot \\ \psi_m^{-1}(1) & \cdots & \psi_m^{-1}(m) \end{vmatrix}$$

ist von Null verschieden; $\Psi\Psi' = m^m$. —

Nun bilde ich aus $\mathfrak{A}$ durch Hinzufügung eines Elementes zweiter Ordnung β, welches sich mit den α nach dem Gesetze

$$\beta\alpha = \alpha^{-1}\beta$$

verbindet, das System

$$\mathfrak{G} = \mathfrak{A} + \mathfrak{A}\beta,$$

welches, wie man leicht sieht (vergl. das folgende Beispiel 4), eine Gruppe ist (im Beispiel 1. war $m = 3$). Es soll die Determinante D dieser Gruppe $\mathfrak{G}$ gebildet werden, also eine Function von $2m$ Variabelen x_α, y_α, die resp. den Elementen α, $\alpha\beta$ entsprechen, nämlich

$$D = \left|\begin{array}{ccc|ccc} x_{11^{-1}} & \cdots & x_{m1^{-1}} & y_{11} & \cdots & y_{m1} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ x_{1m^{-1}} & \cdots & x_{mm^{-1}} & y_{1m} & \cdots & y_{mm} \\ \hline y_{11} & \cdots & y_{m1} & x_{11^{-1}} & \cdots & x_{m1^{-1}} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ y_{1m} & \cdots & y_{mm} & x_{1m^{-1}} & \cdots & x_{mm^{-1}} \end{array}\right|$$

Um sie umzuformen, multiplicire ich sie zeilenweise mit

$$\Psi\Psi' = \left|\begin{array}{ccc|ccc} \psi_1(1) & \cdots & \psi_1(m) & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \psi_m(1) & \cdots & \psi_m(m) & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & \psi_1^{-1}(1) & \cdots & \psi_1^{-1}(m) \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & \psi_m^{-1}(1) & \cdots & \psi_m^{-1}(m) \end{array}\right|$$

und zwar (wie immer im Folgenden) in der Weise, dass die Spalte des Productes durch die Zeile des Multiplicands D, die Zeile des

Productes durch die Zeile des Multiplicators $\Psi\Psi'$ bestimmt wird; führt man noch die Bezeichnungen

$$u_\mu = \sum^{\alpha} x_\alpha \psi_\mu(\alpha), \qquad v_\mu = \sum^{\alpha} y_\alpha \psi_\mu(\alpha),$$
$$u'_\mu = \sum^{\alpha} x_\alpha \psi_\mu^{-1}(\alpha), \qquad v'_\mu = \sum^{\alpha} y_\alpha \psi_\mu^{-1}(\alpha)$$

ein, so wird das Product

$$D\Psi\Psi' = \left|\begin{array}{cc|cc} u_1\psi_1(1) & \cdots & v_1\psi_1^{-1}(1) & \cdots \\ \cdot & \cdots & \cdot & \cdots \\ u_m\psi_m(1) & \cdots & v_m\psi_m^{-1}(1) & \cdots \\ \hline v'_1\psi_1(1) & \cdots & u'_1\psi_1^{-1}(1) & \cdots \\ \cdot & \cdots & \cdot & \cdots \\ v'_m\psi_m(1) & \cdots & u'_m\psi_m^{-1}(1) & \cdots \end{array}\right.$$
$$\left.\begin{array}{cc} v_1\psi_1^{-1}(m) & \cdots \\ \cdot & \cdots \\ v_m\psi_m^{-1}(m) & \cdots \\ \hline u'_1\psi_1^{-1}(m) & \cdots \\ \cdot & \cdots \\ u'_m\psi_m^{-1}(m) & \cdots \end{array}\right|.$$

Diese Determinante ist aber zugleich das Product aus Multiplicand

$$\Psi\Psi' = \left|\begin{array}{ccc|ccc} \psi_1(1) & \cdots & \psi_m(1) & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \psi_1(m) & \cdots & \psi_m(m) & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & \psi_1^{-1}(1) & \cdots & \psi_m^{-1}(1) \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & \psi_1^{-1}(m) & \cdots & \psi_m^{-1}(m) \end{array}\right|$$

und Multiplicator

$$\prod^{\mu}(u_\mu u'_\mu - v_\mu v'_\mu) = \left|\begin{array}{ccc|ccc} u_1 & \cdots & 0 & v_1 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & u_m & 0 & \cdots & v_m \\ \hline v'_1 & \cdots & 0 & u'_1 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & v'_m & 0 & \cdots & u'_m \end{array}\right|.$$

Mithin ist unsere Gruppen-Determinante

$$D = \prod^{\mu}(u_\mu u'_\mu - v_\mu v'_\mu) = \prod^{\mu} \begin{vmatrix} u_\mu, & v_\mu \\ v'_\mu, & u'_\mu \end{vmatrix}$$

zunächst ein Product von m Factoren zweiten Grades. Bedeutet nun a die Anzahl der zweiseitigen (ambigen) Elemente $\alpha = \alpha^{-1}$ der Gruppe $\mathfrak{A}$, so ist $m = aa'$, wo a' die Anzahl aller verschiedenen

Quadrate α^2 bedeutet. Zugleich ist a die Anzahl aller zweiseitigen Charaktere $\psi = \psi^{-1}$; dies folgt unmittelbar aus der oben erwähnten Isomorphie der Gruppe $\mathfrak{A}$ mit der ihrer Charaktere, oder auch aus der Betrachtung der Gruppe $\mathfrak{A}'$ der a' Quadrate α^2, weil ihr Index $(\mathfrak{A}', \mathfrak{A}) = a$ nach einem allgemeinen Satz zugleich die Anzahl derjenigen Charaktere ψ von $\mathfrak{A}$ sein muß, welche den Haupt- (oder jeden anderen bestimmten) Charakter der Untergruppe $\mathfrak{A}'$ in sich schliessen, also die Eigenschaft $\psi(\alpha^2) = 1$, d. h. $\psi = \psi^{-1}$ haben. Für jeden zweiseitigen Charakter ψ_μ wird $u'_\mu = u_\mu$, $v'_\mu = v_\mu$, also $u_\mu u'_\mu - v_\mu v'_\mu = (u_\mu + v_\mu)(u_\mu - v_\mu)$, woraus $2a$ verschiedene lineare Factoren von D entspringen. Die übrigen $m - a$ Charaktere zerfallen in $\frac{1}{2}(m - a)$ Paare ψ_μ und $\psi_{\mu'} = \psi_\mu^{-1}$, und da $u_{\mu'} = u'_\mu$, $v_{\mu'} = v'_\mu$, $u'_{\mu'} = u_\mu$, $v'_{\mu'} = v_\mu$, so entspricht jedem Paar das Quadrat $(u_\mu u'_\mu - v_\mu v'_\mu)^2$ einer quadratischen Function, welche (im gewöhnlichen Sinne) unzerlegbar ist. Die Commutatoren von je zwei Elementen der Gruppe $\mathfrak{G}$ sind, wie man leicht findet, die a' Quadrate α^2; die von ihnen gebildete Gruppe $\mathfrak{A}'$ hat in $\mathfrak{G}$ den Index $(\mathfrak{A}', \mathfrak{G}) = (\mathfrak{A}', \mathfrak{A})(\mathfrak{A}, \mathfrak{G}) = 2a$, welcher mit der Anzahl der linearen Factoren von D übereinstimmt. —

Gruppen-Determinanten.

Beispiel 4 (vom 18. April 1896).

Verallgemeinerung von Beispiel 3. — Zu der Abel'schen Gruppe $\mathfrak{A}$ von m Elementen α (und m Charakteren ψ) lasse ich eine beliebige Gruppe $\mathfrak{B}$ von n Elementen β hinzutreten, welche sich mit jenen nach dem Gesetze

(1) $$\beta\alpha = \alpha^{\beta'}\beta$$

verbinden, unter der Annahme, dass die den n Elementen β entsprechenden n Exponenten β' relative Primzahlen zu m sind und dem Gesetze

(2) $$(\beta_1\beta_2)' \equiv \beta'_1\beta'_2 \pmod{m}$$

genügen. Ich nehme ferner an, dass $\mathfrak{A}$ und $\mathfrak{B}$ nur das Haupt-Element $\alpha^0 = \beta^0$ gemeinsam haben; dann bildet der aus mn verschiedenen Elementen $\alpha\beta$ bestehende Complex

(3) $$\mathfrak{G} = \mathfrak{A}\mathfrak{B}$$

eine Gruppe. Dies ergiebt sich am deutlichsten, wenn man die Gruppen $\mathfrak{A}, \mathfrak{B}$ zunächst ganz getrennt betrachtet und jeder Combination

eines Elementes α von $\mathfrak{A}$ mit einem Elemente β von $\mathfrak{B}$ ein etwa mit (α, β) zu bezeichnendes Element eines neuen Systems $\mathfrak{G}$ entsprechen läßt, mit der Bedingung, daß diese mn Elemente (α, β) alle von einander verschieden sein sollen (der Einfachheit wegen); die Composition dieser Elemente definire man durch

(4) $$(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1\alpha_2^{\beta'_1}, \beta_1\beta_2),$$

so ist $\mathfrak{G}$ wirklich eine Gruppe. Denn erstens gehorcht diese Composition (4) zufolge (2) dem associativen Gesetz; zweitens ist

(5) $$(\alpha^0, \beta^0)(\alpha, \beta) = (\alpha, \beta)(\alpha^0, \beta^0) = (\alpha, \beta),$$

weil $(\beta^0)' \equiv 1 \pmod{m}$; definirt man ferner die n Zahlen β'' durch

(6) $$\beta'\beta'' \equiv 1 \pmod{m},$$

woraus auch

(7) $$(\beta_1\beta_2)'' \equiv \beta''_1\beta''_2 \pmod{m}$$

folgt, so ist drittens

(8) $$(\alpha, \beta)(\alpha^{-\beta''}, \beta^{-1}) = (\alpha^{-\beta''}, \beta^{-1})(\alpha, \beta) = (\alpha^0, \beta^0).$$

Hiermit ist die Gruppen-Eigenschaft von $\mathfrak{G}$ bekanntlich erwiesen, und man kann

(9) $$(\alpha, \beta)^0 = (\alpha^0, \beta^0), \qquad (\alpha, \beta)^{-1} = (\alpha^{-\beta''}, \beta^{-1})$$

setzen. Zufolge (4) ist nun

(10) $$(\alpha, \beta) = (\alpha, \beta^0)(\alpha^0, \beta),$$

(11) $$(\alpha_1, \beta^0)(\alpha_2, \beta^0) = (\alpha_1\alpha_2, \beta^0),$$

(12) $$(\alpha^0, \beta_1)(\alpha^0, \beta_2) = (\alpha^0, \beta_1\beta_2).$$

Es giebt also in $\mathfrak{G}$ eine mit $\mathfrak{A}$ isomorphe Abel'sche Gruppe von m Elementen (α, β^0), und eine mit $\mathfrak{B}$ isomorphe Gruppe von n Elementen (α^0, β), und zufolge (10) ist $\mathfrak{G}$ das Product aus diesen beiden Gruppen, welche nur das Haupt-Element (α^0, β^0) gemeinsam haben; hieraus folgt die Berechtigung, in $\mathfrak{G}$ jedes Element (α, β^0) kurz durch α, jedes Element (α^0, β) kurz durch β zu bezeichnen, woraus dann $\alpha^0 = \beta^0$ und $(\alpha, \beta) = \alpha\beta$, $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$ folgt. Die Composition (4) lautet

$$\alpha_1\beta_1\alpha_2\beta_2 = \alpha_1\alpha_2^{\beta'_1}\beta_1\beta_2,$$

worin (1) enthalten ist. (In diesem Winter habe ich mich mit viel allgemeineren Zusammensetzungen von zwei Gruppen $\mathfrak{A}, \mathfrak{B}$ zu einer Product-Gruppe $\mathfrak{A}\mathfrak{B}$ beschäftigt). —

Bezeichnet man nun der Einfachheit halber die dem Elemente $\alpha\beta$ entsprechende Variabele der Gruppen-Determinante D selbst mit $\alpha\beta$ (statt mit $x_{\alpha\beta}$), und ordnet die letztere in n^2 Felder von je m^2 Elementen, so wird

$$D = \begin{vmatrix} \cdots(\alpha\beta_1)(\alpha_1\ \beta_1)^{-1}\cdots & \cdots & \cdots(\alpha\beta_n)(\alpha_1\ \beta_1)^{-1}\cdots \\ \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ \cdots(\alpha\beta_1)(\alpha_m\ \beta_1)^{-1}\cdots & \cdots & \cdots(\alpha\beta_n)(\alpha_m\ \beta_1)^{-1}\cdots \\ \hline \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ \hline \cdots(\alpha\beta_1)(\alpha_1\ \beta_n)^{-1}\cdots & \cdots & \cdots(\alpha\beta_n)(\alpha_1\ \beta_n)^{-1}\cdots \\ \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ \cdots(\alpha\beta_1)(\alpha_m\ \beta_n)^{-1}\cdots & \cdots & \cdots(\alpha\beta_n)(\alpha_m\ \beta_n)^{-1}\cdots \end{vmatrix},$$

wo α in jeder Zeile jedes Feldes alle m Elemente $\alpha_1, \alpha_2 \cdots \alpha_m$ von $\mathfrak{A}$ in derselben Ordnung durchläuft. Nun bilde ich aus jedem Charakter ψ von $\mathfrak{A}$ und jedem Element β von $\mathfrak{B}$ die lineare Function von m Variabelen

$$(\beta,\ \psi) = \sum_{\alpha}^{\alpha}(\alpha\beta)\psi(\alpha);$$

die Charakter-Potenzen $\psi^{\beta''}$ sind ebenfalls Charaktere ψ, und man erhält

$$\sum_{\alpha}^{\alpha}(\alpha\beta)(\alpha_\mu\beta_\nu)^{-1}\psi^{\beta''}(\alpha) = \sum_{\alpha}^{\alpha}(\alpha\beta\beta_\nu^{-1}\alpha_\mu^{-1})\psi^{\beta''}(\alpha)$$

$$= \sum_{\alpha}^{\alpha}(\alpha\alpha_\mu^{-\beta'\beta''_\nu}\beta\beta_\nu^{-1})\psi^{\beta''}(\alpha) = \sum_{\alpha}^{\alpha}(\alpha\beta\beta_\nu^{-1})\psi^{\beta''}(\alpha\alpha_\mu^{\beta'\beta''_\nu})$$

$$= (\beta\beta_\nu^{-1},\ \psi^{\beta''})\psi^{\beta''_\nu}(\alpha_\mu).$$

Multiplicirt man daher (wie im Beispiel 3) den Multiplicand D mit dem Multiplicator

$$\pm\mathfrak{P}^n = \begin{vmatrix} \cdots\psi_1^{\beta''_1}(\alpha)\cdots & 0\ \cdot\ 0 & 0\ \cdots\ 0 \\ \cdots\cdots & \cdots & \cdots\cdots \\ \cdots\psi_m^{\beta''_1}(\alpha)\cdots & 0\ \cdot\ 0 & 0\ \cdots\ 0 \\ \hline 0\ \cdots\ 0 & & 0\ \cdots\ 0 \\ \hline 0\ \cdots\ 0 & 0\ \cdot\ 0 & \cdots\psi_1^{\beta''_n}(\alpha)\cdots \\ \cdots\cdots & \cdots & \cdots\cdots \\ 0\ \cdots\ 0 & 0\ \cdot\ 0 & \cdots\psi_m^{\beta''_n}(\alpha)\cdots \end{vmatrix},$$

so erhält man

$$\pm D\mathfrak{P}^n = \begin{vmatrix} \cdots(\beta_1\beta_1^{-1},\ \psi_1^{\beta''_1})\psi_1^{\beta''_1}(\alpha)\cdots & \cdots & \cdots(\beta_1\beta_n^{-1},\ \psi_1^{\beta''_1})\psi_1^{\beta''_n}(\alpha)\cdots \\ \cdots\cdots & \cdots & \cdots\cdots \\ \cdots(\beta_1\beta_1^{-1},\ \psi_m^{\beta''})\psi_m^{\beta''_1}(\alpha)\cdots & \cdots & \cdots(\beta_1\beta_n^{-1},\ \psi_m^{\beta''_1})\psi_m^{\beta''_n}(\alpha)\cdots \\ \hline \cdots\cdots & \cdots & \cdots\cdots \\ \hline \cdots(\beta_n\beta_1^{-1},\ \psi_1^{\beta''_n})\psi_1^{\beta''_1}(\alpha)\cdots & \cdots & \cdots(\beta_n\beta_n^{-1},\ \psi_1^{\beta''_n})\psi_1^{\beta''_n}(\alpha)\cdots \\ \cdots\cdots & \cdots & \cdots\cdots \\ \cdots(\beta_n\beta_1^{-1},\ \psi_m^{\beta''_n})\psi_m^{\beta''_1}(\alpha)\cdots & \cdots & \cdots(\beta_n\beta_n^{-1},\ \psi_m^{\beta''_n})\psi_m^{\beta''_n}(\alpha)\cdots \end{vmatrix}.$$

Dies ist wieder das Product aus dem Multiplicand

$$\pm\mathfrak{P}^n = \begin{vmatrix} \psi_1^{\beta''_1}(\alpha_1)\cdots\psi_m^{\beta''_1}(\alpha_1) & 0\ \cdot\ 0 & 0\ \cdots\ 0 \\ \cdots\cdots & \cdots & \cdots\cdots \\ \psi_1^{\beta''_1}(\alpha_m)\cdots\psi_m^{\beta''_1}(\alpha_m) & 0\ \cdot\ 0 & 0\ \cdots\ 0 \\ \hline 0\ \cdots\ 0 & \cdots & 0\ \cdots\ 0 \\ \hline 0\ \cdots\ 0 & 0\ \cdot\ 0 & \psi_1^{\beta''_n}(\alpha_1)\cdots\psi_m^{\beta''_n}(\alpha_1) \\ \cdots\cdots & \cdots & \cdots\cdots \\ 0\ \cdots\ 0 & 0\ \cdot\ 0 & \psi_1^{\beta''_n}(\alpha_m)\cdots\psi_m^{\beta''_n}(\alpha_m) \end{vmatrix}$$

und dem Multiplicator

$$\begin{vmatrix} (\beta_1\beta_1^{-1},\ \psi_1^{\beta''_1})\cdots 0 & \cdots & (\beta_1\beta_n^{-1},\ \psi_1^{\beta''_1})\cdots 0 \\ \cdots\cdots & \cdots & \cdots\cdots \\ 0\ \cdots(\beta_1\beta_1^{-1},\ \psi_m^{\beta''_1}) & \cdots & 0\ \cdots(\beta_1\beta_n^{-1},\ \psi_m^{\beta''_1}) \\ \hline \cdots\cdots & \cdots & \cdots\cdots \\ \hline (\beta_n\beta_1^{-1},\ \psi_1^{\beta''_n})\cdots 0 & \cdots & (\beta_n\beta_n^{-1},\ \psi_1^{\beta''_n})\cdots 0 \\ \cdots\cdots & \cdots & \cdots\cdots \\ 0\ \cdots(\beta_n\beta_1^{-1},\ \psi_m^{\beta''_n}) & \cdots & 0\ \cdots(\beta_n\beta_n^{-1},\ \psi_m^{\beta''_n}) \end{vmatrix},$$

welcher folglich $= D$ ist. Mithin ergiebt sich, wenn

$$D_\psi = \begin{vmatrix} (\beta_1\beta_1^{-1},\ \psi^{\beta''_1})\cdots(\beta_1\beta_n^{-1},\ \psi^{\beta''_1}) \\ \cdots\cdots\cdots \\ (\beta_n\beta_1^{-1},\ \psi^{\beta''_n})\cdots(\beta_n\beta_n^{-1},\ \psi^{\beta''_n}) \end{vmatrix}$$

gesetzt wird, unsere Gruppen-Determinante

$$D = \prod_{\psi} D_\psi$$

als Product von m Factoren n^{ten} Grades. —

Jeder Commutator der Gruppe $\mathfrak{B}$, d. h. jedes Element von der Form

$$\gamma = \beta_1^{-1}\beta_2^{-1}\beta_1\beta_2$$

ist permutabel mit jedem Element α von $\mathfrak{A}$, weil

$$\gamma' \equiv \beta_1''\beta_2''\beta_1'\beta_2' \equiv 1 \pmod{m},$$

also $\gamma\alpha = \alpha^{\gamma'}\gamma = \alpha\gamma$. Die von allen diesen Commutatoren γ erzeugte Gruppe sei $\mathfrak{C}$. Unter den Commutatoren der Product-Gruppe $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$ sind zunächst die folgenden

$$\beta^{-1}\alpha^{-1}\beta\alpha = \alpha^{1-\beta''}$$

zu bemerken; bedeutet e den grössten gemeinsamen Theiler aller n Zahlen $1-\beta''$ oder $1-\beta'$ mit m (oder mit dem höchsten Element-Grade in $\mathfrak{A}$), so bilden diese Commutatoren die Gruppe $\mathfrak{A}'$ aller a' verschiedenen Potenzen α^e, und es ist $m = aa'$, wo $a = (\mathfrak{A}', \mathfrak{A})$ die Anzahl aller e-seitigen, d. h. derjenigen Elemente α bedeutet, welche der Bedingung $\alpha^e = \alpha^0$ genügen; da jedem Charakter χ der Gruppe $\mathfrak{A}'$, z. B. ihrem Hauptcharakter genau a Charaktere ψ der Gruppe $\mathfrak{A}$ entsprechen, welche Multipla von χ sind oder χ einschliessen, d. h. für alle Elemente von $\mathfrak{A}'$ mit χ übereinstimmen, so ist a auch die Anzahl aller e-seitigen Charaktere $\psi = \psi^{\beta'} = \psi^{\beta''}$ von $\mathfrak{A}$, was auch aus der Isomorphie von $\mathfrak{A}$ mit der Charakter-Gruppe folgen würde. Da ferner jeder beliebige Commutator der Gruppe $\mathfrak{G}$ von der Form

$$(\alpha_1\beta_1)^{-1}(\alpha_2\beta_2)^{-1}(\alpha_1\beta_1)(\alpha_2\beta_2)$$
$$= \alpha_1^{\beta_1''(\beta_2''-1)}\alpha_2^{\beta_2''(1-\beta_1'')}\cdot\beta_1^{-1}\beta_2^{-1}\beta_1\beta_2 = \alpha^e\gamma$$

ist, so erzeugen alle diese Commutatoren die Gruppe $\mathfrak{A}'\mathfrak{C}$, deren Index $(\mathfrak{A}'\mathfrak{C}, \mathfrak{A}\mathfrak{B}) = (\mathfrak{A}'\mathfrak{C}, \mathfrak{A}\mathfrak{C})(\mathfrak{A}\mathfrak{C}, \mathfrak{A}\mathfrak{B}) = a(\mathfrak{C}, \mathfrak{B})$ ist. Wenn nun ψ ein e-seitiger Charakter ist, so geht der ihm entsprechende Factor

$$D_\psi = \begin{vmatrix} (\beta_1\beta_1^{-1}, \psi)\cdots(\beta_n\beta_1^{-1}, \psi) \\ \cdots\cdots\cdots\cdots \\ (\beta_1\beta_n^{-1}, \psi)\cdots(\beta_n\beta_n^{-1}, \psi) \end{vmatrix},$$

von D aus der Determinante

$$\begin{vmatrix} y_{\beta_1\beta_1^{-1}}\cdots y_{\beta_n\beta_1^{-1}} \\ \cdots\cdots\cdots \\ y_{\beta_1\beta_n^{-1}}\cdots y_{\beta_n\beta_n^{-1}} \end{vmatrix}$$

der Gruppe $\mathfrak{B}$ offenbar durch die lineare Transformation $y_\beta = (\beta, \psi)$ hervor und enthält folglich dieselbe Anzahl linearer Factoren. Aber mehr kann man auf diese Weise wohl nicht schliessen.

8. Juli 1896*).

. . . Nochmals bitte ich sehr um Entschuldigung für meine Saumseligkeit, für die ich nur wenige gute, aber viele schlechte Gründe angeben könnte; zu den letzteren gehört meine tadelnswerthe Schwäche, mich oft von Nebenfragen, die für die Hauptsache einer Untersuchung ganz werthlos sind, so gefangen nehmen zu lassen, dass ich darüber das eigentliche Ziel aus den Augen verliere. Zu den guten Gründen darf ich wohl den rechnen, dass ich in Folge Ihrer Anregung meine Papiere vom Februar 1886 über Gruppen-Determinanten und deren hypercomplexe lineare Factoren wieder durchstöbert habe.

Auf Ihre Frage, wann ich den allgemeinen Satz über die Zerlegung der Abel'schen Gruppen-Determinanten in lineare Charakter-Factoren gefunden habe, geben diese Papiere (12 Folioseiten vom 2. bis 17. Februar datirt, mit Formeln und nur wenigen Worten)**) nur den Aufschluss, dass dies schon in früherer Zeit geschehen sein muss. Sie behandeln nämlich (mit einer einzigen Ausnahme) nur noch Beispiele von nicht Abel'schen Gruppen, unter denen das vom 17. Februar 1886, welches ich Ihnen im April d. J. mitgetheilt habe, eine Gruppe $\mathfrak{G}$ betrifft, in der die allgemeinste Abel'sche Gruppe $\mathfrak{A}$ als Theiler enthalten ist; hierin steckt natürlich auch der obige Satz A über die Abel'schen Gruppen $\mathfrak{A}$, und die ganze Behandlung der Determinante von $\mathfrak{G}$ ist offenbar derjenigen nachgebildet, welche zur Zerlegung der Determinante von $\mathfrak{A}$, also zu dem Satze A führt; aber dieser Satz A wird nirgends mehr erwähnt. Auf den Begriff der allgemeinen Gruppen-Determinante bin ich zuerst bei dem Studium der Discriminante eines beliebigen Normalkörpers Ω geführt, indem ich solche (sehr nützliche) Basen von Ω betrachtete, die aus den Conjugirten einer einzigen Zahl ω bestehen (bisweilen besitzt auch das System o aller ganzen Zahlen in Ω eine solche Basis, z. B. wenn ω eine m^{te} Einheits-Wurzel, und m durch kein Quadrat theil-

*) [Ein Auszug aus diesem Brief findet sich in der Einleitung der Arbeit über Gruppencharaktere von Frobenius. E. N.]

**) [Dem Inhalt nach vollständig in den hier veröffentlichten Briefen enthalten. E. N.]

bar ist, und dasselbe gilt dann auch von allen Divisoren von Ω, z. B. allen quadratischen Körpern von ungerader Grundzahl); dieses Studium fällt wahrscheinlich in die Zeit um 1880 oder noch früher, und damals werde ich wohl den Satz A gefunden haben; was mich aber veranlasst hat, im Februar 1886 auf die Gruppen-Determinanten zurückzukommen, weiss ich nicht mehr.

Ich füge einige Bemerkungen über die Charaktere der Abel'schen Gruppen $\mathfrak{A}$ hinzu. Das älteste Beispiel ihrer Anwendung ist wohl in den Resolventen von Lagrange (für cyklische $\mathfrak{A}$) zu erkennen. Sodann ist das (von Jacobi verallgemeinerte) Symbol von Legendre zu nennen. Die von Gauss (Art. 131) benutzten Zeichen R, N sind weniger glücklich, als die bestimmte Einführung der Einheits-Wurzeln ± 1 durch Legendre, und so kommt es (Art. 230), dass er auch unter dem Charakter einer Formen-Classe oder eines Geschlechtes eine Relation, nicht eine Zahl versteht; die der Zusammensetzung der Geschlechter entsprechende Zusammensetzung der Charaktere tritt zwar deutlich hervor (Art. 246—248), aber nicht als Multiplication von Zahlen. Die Umwandlung der Gauss'schen Geschlechts-Charaktere in Zahlen hat Dirichlet (Recherches sur diverses applications etc. §. 3) durch Benutzung des Symbols von Legendre bewirkt. Ferner hat Dirichlet in der Abhandlung über die arithmetische Progression alle Charaktere ψ (— ohne diesen Namen zu gebrauchen —) der Abel'schen Gruppe $G^{(m)}$ benutzt, welche von den $\varphi(m)$ Classen relativer Primzahlen zu m gebildet wird, und ebenso alle Charaktere der Gruppe der Formen-Classen (in der Skizze über die Darstellung unendlich vieler Primzahlen durch eine quadratische Form). Nach allem diesen lag es nahe, den Begriff und Namen der Charaktere für jede Abel'sche Gruppe $\mathfrak{A}$ einzuführen, wie ich es in der dritten Auflage von Dirichlet's Zahlentheorie gethan habe. Ich habe dort (in der vierten Auflage S. 612) zur Begründung der Existenz der Charaktere auf §. 149, also auf die Darstellung der Elemente von $\mathfrak{A}$ als Producte von Potenzen von Fundamental-Elementen hingedeutet; doch ziehe ich principiell den folgenden Weg vor, der Nichts von dieser Darstellung voraussetzt. Ist $\mathfrak{A}$ ein Theiler von $\mathfrak{B}$, so ist in jedem Charakter χ von $\mathfrak{B}$ ein Charakter ψ von $\mathfrak{A}$ enthalten (der für alle Elemente von $\mathfrak{A}$ mit χ übereinstimmt); ich nenne ψ den auf $\mathfrak{A}$ bezüglichen Divisor von χ, umgekehrt χ ein Multiplum von ψ. Dann ergiebt sich ganz leicht durch Induction

der Satz: Ist ψ ein Charakter von $\mathfrak{A}$, so ist der Index $(\mathfrak{A}, \mathfrak{B})$ [— mit $(\mathfrak{A}, \mathfrak{B})$ bezeichne ich auch in der allgemeinen Gruppen-Theorie die Anzahl der verschiedenen Complexe $\mathfrak{A}\beta$, aus denen der Complex $\mathfrak{A}\mathfrak{B}$ besteht —] zugleich die genaue Anzahl der verschiedenen Charaktere χ von $\mathfrak{B}$, welche Multipla von ψ sind. Dies leuchtet ein für $(\mathfrak{A}, \mathfrak{B}) = 1$, also $\mathfrak{A} = \mathfrak{B}$, und wenn es für alle Fälle $(\mathfrak{A}, \mathfrak{B}) < m$ bewiesen ist, so gilt es auch für $(\mathfrak{A}, \mathfrak{B}) = m$; denn entweder giebt es eine von $\mathfrak{A}$ und $\mathfrak{B}$ verschiedene Gruppe $\mathfrak{C}$, die Theiler von $\mathfrak{B}$ und Vielfaches von $\mathfrak{A}$ ist, oder nicht; in beiden Fällen ergiebt sich der Schluss leicht, weil im ersten Fall $m = (\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}, \mathfrak{C})(\mathfrak{C}, \mathfrak{B})$, also $(\mathfrak{A}, \mathfrak{C})$ und $(\mathfrak{C}, \mathfrak{B}) < m$ ist, und weil im zweiten Falle $\mathfrak{B} = \mathfrak{A} + \mathfrak{A}\beta + \mathfrak{A}\beta^2 + \cdots$ ist. Hierin ist aber Alles über Existenz und Anzahl der Charaktere enthalten, und der Satz ist ausserdem sehr nützlich.

Die Art, wie Dirichlet (bei der arithmetischen Progression) darthut, dass seine Reihen L_2 der zweiten Art von Null verschiedene Grenzwerthe haben, weil diese als Factoren der Classen-Anzahl der quadratischen Formen auftreten, führte mich, da ich die quadratischen Körper als Kreiskörper kannte, zu der Bemerkung (Aufl. 3, S. 596 und Aufl. 4, S. 625), dass eine ähnliche Schlussart auch für die Reihen L_3 der dritten Art gilt; denn wenn man den aus den m^{ten} Einheits-Wurzeln gebildeten Kreiskörper K_m betrachtet, und Kummer's Satz über dessen Primideale anwendet, so ist das Product aller $\varphi(m)$ Dirichlet'schen Reihen L identisch mit der Summe $\sum N(\mathfrak{a})^{-s}$, wo $\mathfrak{a}$ alle relativen Primideale zu m durchläuft. Ich weiss nicht, ob Kummer selbst diese Anwendung ausgesprochen hat, glaube es aber kaum.

Da Sie bei Ihrer Frage nach der Auffindungs-Zeit des obigen Satzes A die Classen-Anzahl der Ideale in einem beliebigen Kreiskörper erwähnen, so möchte ich Ihnen (wie neulich auch Weber) noch von einer schönen Sparsamkeit schreiben*), auf die Gefahr hin, dass dieselbe Ihnen, wie mir, schon lange bekannt ist. Die Identität

$$(1) \qquad \sum^{\mathfrak{a}} N(\mathfrak{a})^{-s} = \prod^{\psi} \sum^{n} \psi(n) n^{-s}$$

gilt nämlich auch dann, wenn $\mathfrak{a}$ alle Ideale in K_m, und n alle natürlichen Zahlen durchläuft, falls jeder der $\varphi(m)$ Charaktere ψ der

*) [Vergl. XLI.]

Gruppe $G^{(m)}$ eine erweiterte Bedeutung erhält, so dass ψ für jede ganze rationale Zahl x einen bestimmten Werth $\psi(x)$ annimmt, der mit dem ursprünglichen $\psi(x)$ übereinstimmt, wenn x relative Primzahl zu m ist, und ausserdem die Gesetze $\psi(x+m) = \psi(x)$ und $\psi(xy) = \psi(x)\psi(y)$ erfüllt. Eine solche Erweiterung eines gegebenen Charakters ψ von $G^{(m)}$ lässt sich im Allgemeinen auf mehrere Arten herstellen (deren Anzahl eine Potenz von 2 ist); von diesen genügt aber nur eine einzige der obigen Ideal-Identität (1), und zwar ist sie dadurch vollkommen bestimmt, daß $\psi(x)$ für möglichst wenige Zahlen x verschwinden soll. Einen so erweiterten Charakter ψ nenne ich einen natürlichen Charakter von $G^{(m)}$. Die oben gerühmte Sparsamkeit besteht nun zunächst darin, dass, wenn a ein Divisor von m, alle $\varphi(a)$ natürlichen Charaktere von $G^{(a)}$ auch natürliche Charaktere von $G^{(m)}$ sind; bezeichnet man daher mit $\varphi'(m)$ die Anzahl aller primitiven, nämlich derjenigen natürlichen Charaktere von $G^{(m)}$, welche zu keiner Gruppe $G^{(a)}$ mit kleinerem a gehören, so ist

$$\sum \varphi'(a) = \varphi(m); \tag{2}$$

mithin ist $\varphi'(ab) = \varphi'(a)\varphi'(b)$, wenn a, b relative Primzahlen sind, und für eine Primzahl p ist $\varphi'(p) = p-2$ und $\varphi'(p^n) = (p-1)^2 p^{n-2}$, falls $n > 1$; ferner ist $\varphi'(2m) = 0$, wenn m ungerade (es ist ja auch $K_{2m} = K_m$). Am schönsten offenbart sich aber die Sparsamkeit dadurch, dass die Identität (1) im folgenden Sinne für jeden Kreiskörper Ω gilt. Hat man m so gewählt, dass Ω Divisor von K_m wird, und ist H die Gruppe der Zahlclassen h (mod. m), zu welcher Ω gehört, also H Theiler von $G^{(m)}$, so gilt die Identität (1), wenn $\mathfrak{a}$ alle Ideale in Ω, und ψ alle diejenigen natürlichen Charaktere von $G^{(m)}$ durchläuft, welche der Bedingung $\psi(h) = 1$ genügen (alle Multipla des Haupt-Charakters von H); dies ist gewissermassen der analytische Ausdruck für meinen allgemeinen Satz über die Primideale von Ω (C. R. der Pariser Akademie vom 24. Mai 1880). —

Zu einem gründlichen Studium Ihrer Abhandlung „Über vertauschbare Matrizen“ bin ich aus den oben erwähnten schlechten Gründen noch nicht gekommen; doch glaube ich versichern zu können, dass ich auch bei meinen nach 1887 gelegentlich wieder aufgenommenen Versuchen, die Zerlegung in lineare Factoren auf einfachere Weise abzuleiten, durchaus nicht auf Ihre Wege gekommen bin. Doch

muthet mich Manches darin ähnlich an, wie meine übercomplexen Factoren der Gruppen-Determinanten, auf die ich aber heute nicht mehr eingehen kann. Vielleicht komme ich morgen dazu, die Armada dieser seltsamen Schiffe in See stechen zu lassen; doch wird es wohl heissen: Frobenius afflavit et dissipavit! ...

13. Juli 1896.

... Zuerst erwähne ich, dass mein Beispiel vom 17. Februar 1886 vollständiger und hübscher in der Gestalt $AB = BC$ dargestellt wird, wo A, B, C nicht Determinanten, sondern folgende Systeme, Matrizen, Formen bedeuten:

$$\left\{\begin{array}{ccc|ccc} x_{11-1} & \cdots & x_{m\,1-1} & y_{11} & \cdots & y_{m\,1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{1\,m-1} & \cdots & x_{m\,m-1} & y_{1\,m} & \cdots & y_{m\,m} \\ \hline y_{11} & \cdots & y_{m\,1} & x_{11-1} & \cdots & x_{m\,1-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ y_{1\,m} & \cdots & y_{m\,m} & x_{1\,m-1} & \cdots & x_{m\,m-1} \end{array}\right\} = A,$$

$$\left\{\begin{array}{ccc|ccc} \psi_1(1), & 0 & \cdots & \psi_m(1), & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \psi_1(m), & 0 & \cdots & \psi_m(m), & 0 \\ \hline 0, & \psi_1^{-1}(1) & \cdots & 0, & \psi_m^{-1}(1) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & \psi_1^{-1}(m) & \cdots & 0, & \psi_m^{-1}(m) \end{array}\right\} = B,$$

$$\left\{\begin{array}{cc|ccc|cc} u_1, & v_1' & 0 & \cdots & 0 & 0, & 0 \\ v_1, & u_1' & 0 & \cdots & 0 & 0, & 0 \\ \hline 0, & 0 & \cdots & \cdots & \cdots & 0, & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & 0 & \cdots & \cdots & \cdots & 0, & 0 \\ \hline 0, & 0 & 0 & \cdots & 0 & u_m, & v_m' \\ 0, & 0 & 0 & \cdots & 0 & v_m, & u_m' \end{array}\right\} = C.$$

Hieraus folgt dann der Satz über die Zerlegung der Gruppen-Determinante D in die Factoren $u_\mu u_\mu' - v_\mu v_\mu'$. Doch das müssen Sie längst durchschaut haben. Im Folgenden beschäftige ich mich ausschliesslich mit dem ersten Beispiel (Fall $m = 3$) vom 2. und 3. Februar 1886; an diesem Beispiel habe ich damals auch zuerst die Zerlegung in hypercomplexe lineare Factoren ausgeführt, und

erst dieser Erfolg hat mich etwas später (jedenfalls vor dem 15. Februar) zu der Beschäftigung mit der Quaternion-Gruppe veranlasst; ich habe Ihnen, wie ich glaube, geschrieben, dass die Reihenfolge die umgekehrte gewesen ist; das war aber ein Irrthum. Nun also! Es war $1+\varrho+\varrho^2=0$ und

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_1 & x_2 & x_5 & x_6 & x_4 \\ x_2 & x_3 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_2 & x_3 \\ x_5 & x_6 & x_4 & x_3 & x_1 & x_2 \\ x_6 & x_4 & x_5 & x_2 & x_3 & x_1 \end{vmatrix} = (u+v)(u-v)(u_1u_2-v_1v_2)^2.$$

$u = x_1+x_2+x_3$, $u_1 = x_1+\varrho x_2+\varrho^2 x_3$, $u_2 = x_1+\varrho^2 x_2+\varrho x_3$,
$v = x_4+x_5+x_6$, $v_1 = x_4+\varrho x_5+\varrho^2 x_6$, $v_2 = x_4+\varrho^2 x_5+\varrho x_6$,

also

$$u_1u_2 = x_1^2+x_2^2+x_3^2-x_1x_2-x_1x_3-x_2x_3,$$
$$v_1v_2 = x_4^2+x_5^2+x_6^2-x_4x_5-x_4x_6-x_5x_6.$$

Nun sei

$$u_1u_2-v_1v_2 = \alpha\beta,$$
$$\alpha = \alpha_1x_1+\alpha_2x_2+\alpha_3x_3+\alpha_4x_4+\alpha_5x_5+\alpha_6x_6,$$
$$\beta = \beta_1x_1+\beta_2x_2+\beta_3x_3+\beta_4x_4+\beta_5x_5+\beta_6x_6.$$

Bei der Addition, Subtraction, Multiplication rechne ich mit den 12 Coefficienten α_r, β_r wie mit gewöhnlichen Zahlen und verzichte nur bei ihrer Multiplication mit einander auf das commutative Gesetz, während dasselbe bei ihrer Multiplication mit gewöhnlichen Zahlen und den Variabelen x_r bestehen bleiben soll. Ebenso wird durchweg das associative und distributive Gesetz angenommen. Die Forderung der Identität der Coefficienten (rs) von x_rx_s in $u_1u_2-v_1v_2$ und in $\alpha\beta$ ergiebt dann 21 Bedingungen; um mit ihnen etwas anfangen zu können, setze ich (wenn dadurch auch die Allgemeinheit beeinträchtigt wird)

(A) $$\alpha_1 = 1, \quad \beta_1 = 1,$$

wodurch die Forderung $(11) = \alpha_1\beta_1 = 1$ erfüllt ist. Dann folgt:

(B)
$$\begin{cases} (12) = \alpha_2+\beta_2 = -1, & \beta_2 = -1-\alpha_2, \\ (13) = \alpha_3+\beta_3 = -1, & \beta_3 = -1-\alpha_3, \\ (14) = \alpha_4+\beta_4 = 0, & \beta_4 = -\alpha_4, \\ (15) = \alpha_5+\beta_5 = 0, & \beta_5 = -\alpha_5, \\ (16) = \alpha_6+\beta_6 = 0, & \beta_6 = -\alpha_6, \end{cases}$$

sodann

(C)
$$\begin{cases} (22) = \alpha_2\beta_2 = 1, & \alpha_2^2 = -1-\alpha_2, \\ (33) = \alpha_3\beta_3 = 1, & \alpha_3^2 = -1-\alpha_3, \\ (23) = \alpha_2\beta_3+\alpha_3\beta_2 = -1, & \alpha_2\alpha_3+\alpha_3\alpha_2 = +1-\alpha_2-\alpha_3, \end{cases}$$

ferner

(D)
$$\begin{cases} (44) = \alpha_4\beta_4 = -1, & \alpha_4^2 = 1, \\ (55) = \alpha_5\beta_5 = -1, & \alpha_5^2 = 1, \\ (66) = \alpha_6\beta_6 = -1, & \alpha_6^2 = 1, \\ (45) = \alpha_4\beta_5+\alpha_5\beta_4 = 1, & \alpha_4\alpha_5+\alpha_5\alpha_4 = -1, \\ (46) = \alpha_4\beta_6+\alpha_6\beta_4 = 1, & \alpha_4\alpha_6+\alpha_6\alpha_4 = -1, \\ (56) = \alpha_5\beta_6+\alpha_6\beta_5 = 1, & \alpha_5\alpha_6+\alpha_6\alpha_5 = -1, \end{cases}$$

endlich

(E)
$$\begin{cases} (24) = \alpha_2\beta_4+\alpha_4\beta_2 = 0, & \alpha_2\alpha_4+\alpha_4\alpha_2 = -\alpha_4, \\ (34) = \alpha_3\beta_4+\alpha_4\beta_3 = 0, & \alpha_3\alpha_4+\alpha_4\alpha_3 = -\alpha_4, \\ (25) = \alpha_2\beta_5+\alpha_5\beta_2 = 0, & \alpha_2\alpha_5+\alpha_5\alpha_2 = -\alpha_5, \\ (35) = \alpha_3\beta_5+\alpha_5\beta_3 = 0, & \alpha_3\alpha_5+\alpha_5\alpha_3 = -\alpha_5, \\ (26) = \alpha_2\beta_6+\alpha_6\beta_2 = 0, & \alpha_2\alpha_6+\alpha_6\alpha_2 = -\alpha_6, \\ (36) = \alpha_3\beta_6+\alpha_6\beta_3 = 0, & \alpha_3\alpha_6+\alpha_6\alpha_3 = -\alpha_6. \end{cases}$$

Zunächst folgt aus (A) und (B) ein Hoffnungsstrahl! Es wird nämlich

(F) $$\alpha+\beta = 2x_1-x_2-x_3, \quad \text{mithin} \quad \beta\alpha = \alpha\beta,$$

d. h. die linearen Factoren der Gruppen-Determinante sind alle permutabel mit einander, wodurch ihre Brauchbarkeit erheblich gewinnt.

Bedenkt man nun, dass aus (C) auch

$$\alpha_2^3 = \alpha_3^3 = 1,$$

ferner aus (D) z. B.

$$(\alpha_4\alpha_5)^2 = -1-\alpha_4\alpha_5 = \alpha_5\alpha_4, \quad (\alpha_4\alpha_5)^3 = (\alpha_5\alpha_4)^3 = 1,$$

und aus (C) und (E) z. B.

$$\alpha_2\alpha_4 = \alpha_4\alpha_2^2, \quad \alpha_4\alpha_2 = \alpha_2^2\alpha_4, \quad (\alpha_2\alpha_4)^2 = (\alpha_4\alpha_2)^2 = 1$$

folgt, so wird man fast mit Gewalt zu der Bemerkung getrieben, dass die 15 Bedingungen (C), (D), (E) widerspruchsfrei erfüllt werden,

wenn man zum Beispiel annimmt, dass die sechs Zahlen α_r bei ihrer Multiplication die Gesetze unserer Gruppe

(G)

1	α_2	α_3	α_4	α_5	α_6
α_2	α_3	1	α_5	α_6	α_4
α_3	1	α_2	α_6	α_4	α_5
α_4	α_6	α_5	1	α_3	α_2
α_5	α_4	α_6	α_2	1	α_3
α_6	α_5	α_4	α_3	α_2	1

befriedigen, und dass ausserdem die beiden Summen

(H) $$\eta = 1 + \alpha_2 + \alpha_3, \quad \omega = \alpha_4 + \alpha_5 + \alpha_6$$

verschwinden; zugleich bilden dann die Zahlen β_r^{-1} eine isomorphe Gruppe.

Mit diesem Ergebniss habe ich mich damals (am 3. Februar 1886) durchaus begnügt, und ich bin, weil es mir sehr merkwürdig schien, gleich zu anderen Beispielen übergegangen, erst zu einer Gruppe zehnten Grades, dann aber zu der Quaternion-Gruppe (deren Existenz nahe lag, mir aber bis dahin wahrscheinlich unbekannt geblieben war), und hier wurde ich durch das Auftreten der Summe von vier Quadraten beglückt. Damals habe ich auch zuerst Beispiele von Normalkörpern mit Quaternion-Gruppe construirt, was mir erst nach mehreren vergeblichen Versuchen gelang, als ich erkannte, dass der darin enthaltene biquadratische Abel'sche Körper (Product von drei quadratischen Körpern) durchaus reell sein muss. Dass aber diese Quaternion-Gruppe eine so grosse Rolle in den nicht Abel'schen (Hamilton'schen) Gruppen spielt, die nur Normaltheiler besitzen, habe ich erst im vorigen Jahre gefunden (zu der Vollendung der Abhandlung bin ich aber noch immer nicht gekommen).

Ich kehre zu dem obigen Beispiele der Versetzungen von drei Buchstaben zurück. Offenbar ist die durch (G) in Verbindung mit $\eta = 0$, $\omega \neq 0$ bestimmte Lösung der Bedingungen (C), (D), (E) nur eine particuläre, wie man schon daraus erkennt, dass die letzteren symmetrisch sowohl in Bezug auf α_2, α_3, als auch in Bezug auf α_4, α_5, α_6 sind. Aber wahrscheinlich giebt es ausser diesen zwei Lösungen

noch unendlich viele andere Arten, die sämmtlichen Producte der Zahlen α_r linear durch die letzteren so darzustellen, dass die Bedingungen (C), (D), (E) erfüllt werden unter Wahrung des associativen und distributiven Gesetzes. Man kann nämlich zwar leicht beweisen, dass

$$\eta^2 = 0, \quad \omega^2 = 0, \quad \eta\omega + \omega\eta = 0$$

sein muss; dass aber η und ω selbst $= 0$ sein müssen, habe ich nicht herstellen können. Freilich dürfte man ja sagen: da u_1, u_2 nur von den Differenzen $x_2 - x_1$, $x_3 - x_1$, und ebenso v_1, v_2 nur von den Differenzen $x_5 - x_4$, $x_6 - x_4$ abhängen, so kann man von vornherein verlangen, dass auch α, β nur von diesen vier Differenzen abhängen, worin ja die Bedeutung der Bedingungen $\eta = 0$, $\omega = 0$ liegt. Da ferner diese Differenzen umgekehrt durch die vier unabhängigen Variabelen u_1, u_2, v_1, v_2 sich ausdrücken lassen, so kommt das Ganze schliesslich auf eine Zerlegung der bilinearen Form oder Determinante

in lineare Factoren $$u_1 u_2 - v_1 v_2 = \alpha\beta$$

$$\alpha = \varkappa_1 u_1 + \varkappa_2 u_2 + \lambda_1 v_1 + \lambda_2 v_2, \quad \beta = \mu_1 u_1 + \mu_2 u_2 + \nu_1 v_1 + \nu_2 v_2$$

hinaus, wo die Coefficienten $\varkappa$, λ, μ, ν zufolge der obigen Lösung sehr niedliche Theiler der Null werden!

Ich habe mich in der letzten Woche ziemlich viel mit den Bedingungen (C), (D), (E) beschäftigt, und wenn Sie es wünschen, so will ich Ihnen gern noch Alles aufschreiben, was ich dabei gefunden habe. Aber ich halte es für sehr wohl möglich, dass Sie nach der heutigen Probe auf die ganze Zerlegung in hypercomplexe Factoren gar keinen Werth legen; meine eigene Meinung darüber schwankt hin und her. ...

5. Dezember 1896*).

... Die Correctur**) habe ich sogleich mit dem besten Willen angegriffen, die Sache selbst dabei gründlich durchzunehmen, aber ich habe bald eingesehen, dass ich dazu viel mehr Zeit gebrauchen würde, als Ihnen erwünscht wäre; mein Anlauf hat daher nur bis etwa zur zehnten Seite ausgereicht, und dann habe ich mich begnügt, das

*) [In die Zwischenzeit fällt ein Besuch von Frobenius, auf den sich die Bemerkung über Anregung zur Darstellungstheorie (Einleitung zu der Arbeit über Darstellung endlicher Gruppen) zu beziehen scheint, da die Briefe nichts über Darstellung enthalten. E. N.]

**) [Es handelt sich um die Frobeniussche Arbeit über die Primfaktoren der Gruppendeterminante. E. N.]

Übrige nur durchzulesen, um den hauptsächlichen Inhalt in mich aufzunehmen. Derselbe erfüllt mich mit aufrichtiger Bewunderung; so schwierig die grosse Aufgabe war, so belohnend ist auch die Frucht Ihrer gewaltigen Arbeit geworden, die Ihrem Ruhmeskranze ein neues Blatt hinzufügt. Mir gefällt noch ganz besonders, dass nun auch Ihre Vorarbeiten in neuem Lichte erscheinen.

Alles Dies würde ich, wie ich Ihnen schon einmal gesagt habe, niemals zu Stande gebracht haben, aber desto mehr freue ich mich, Ihnen die erste Veranlassung zu dieser schönen Arbeit gegeben zu haben. . . .

13. April 1897.

. . . Ich bin daher auch noch nicht im Stande, Ihre Mittheilungen über die Gruppen mit der erforderlichen vollständigen Klarheit in mich aufzunehmen; aber eine große Freude haben Sie mir doch durch dieselben bereitet; denn soweit ich sie verstehe, bleibt mir kein Zweifel, dass Sie einen neuen grossen Schritt auf Ihrer Siegesbahn gethan haben, und wenn dabei mein Luftschloss der Scheinzahlen vernichtet wird, so bin ich gar nicht betrübt darüber, sondern erfreut, dass Sie den wirklichen Kern der Sache aufdecken; auch zweifle ich gar nicht, dass Sie die letzten Schwierigkeiten ebenso überwinden werden wie im vorigen Jahr*). . . .

*) [Gemeint ist die mehrfach erwähnte Zerlegung in hyperkomplexe Faktoren. Diese spielt eine wesentliche Rolle in der Theorie der nichtkommutativen Körper und deren Zerfällungskörper (vgl. Wedderburn, Transactions of the Am. Math. Soc., Bd. XXII, S. 129—135, 1921; die Wiedergabe bei Dickson: Algebras and their Arithmetics, S. 230 und weitergehende Untersuchungen von E. Noether und R. Brauer; zusammenfassende Darstellung bei v. d. Waerden, Moderne Algebra, Bd. II). Bei dem Dedekindschen Beispiel (Brief vom 13. Juli 1896) handelt es sich um den durch das „allgemeine Element“ α (der entsprechenden zweiseitigen Komponente des Gruppenrings) erzeugten Zerfällungskörper, und um die Zerlegung der Norm von α in diesem (kommutativen) Körper; daher die Vertauschbarkeit $\alpha\beta = \beta\alpha$ (Formel (F)).

Daß die Zerlegung bei Frobenius nicht auftritt, erklärt sich daraus, daß Frobenius von vornherein den Körper aller komplexen Zahlen, also einen algebraisch abgeschlossenen Körper, als Koeffizientenbereich nimmt; hier gibt es keine endlichen nichtkommutativen Erweiterungskörper. Die durch das allgemeine Element erzeugten Zerfällungskörper existieren zwar, aber ihre Heranziehung wird unnötig. Das gilt übrigens auch von dem Dedekindschen Beispiel (nicht von dem Beispiel des Quaternionenkörpers), wo es sich schon um einen vollen Matrizenring über dem Körper der rationalen Zahlen handelt; wie Dedekind bemerkt, treten ja Teiler der Null bei der hyperkomplexen Zerlegung der Gruppendeterminante auf. E. N.]