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

$$(7) \qquad (n, \alpha)^m \equiv 1, \ (n, \alpha) \equiv (n+1, \alpha) \ (\text{mod. } p^n)$$

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

$$(8) \qquad (n, \alpha) \equiv (1, \alpha)^{p^{n-1}} \ (\text{mod. } p^n)$$

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

$$(9) \qquad x_n^{p-1} \equiv 1 \ (\text{mod. } p^n),$$

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

$$(10) \qquad \alpha^{p-1} = M_0$$

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

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

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

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

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

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.