THEORIE DER ABEL'SCHEN ZAHLKÖRPER

VON

H. WEBER
in MARBURG.

I. ABEL'SCHE KÖRPER UND KREISKÖRPER.

In der Folge beabsichtige ich eine Reihe von Untersuchungen über Abel'sche Zahlkörper zu veröffentlichen, deren letztes Ziel es ist, alle diese Körper vollständig zu bestimmen und darzustellen. Den Satz, welcher dies ermöglicht, hat KRONECKER zuerst in einer Mitteilung in den Monatsberichten der Berliner Akademie vom 20ten Juni 1853, welche auch in SERRET's *Cours d'algèbre supérieure* abgedruckt ist, ausgesprochen, den Satz nämlich, dass die Wurzeln aller Abel'scher Gleichungen im Gebiete der rationalen Zahlen sich aus Einheitswurzeln rational zusammensetzen lassen, dass also mit andern Worten alle Abel'schen Körper zugleich Kreiskörper sind. Nach dieser ersten Mitteilung KRONECKER's machten aber damals die Gleichungen, deren Grad eine Potenz von 2 ist, noch Schwierigkeiten. In späteren Mitteilungen (Monatsberichte der Berliner Akademie vom 14 Apr. 1856, 16 Apr. 1877, 7 Dec. 1882) ist KRONECKER wiederholt auf den Gegenstand zurückgekommen, ohne über den Beweis des Satzes wesentlich mehr als die Andeutung zu geben, dass die KUMMER'sche Zerlegung gewisser in der Kreisteilung vorkommender complexer Zahlen in ihre idealen Primfactoren dabei gebraucht wird. Eben dies ergiebt sich auch aus einer Bemerkung von KUMMER im Eingang der Abhandlung: *Theorie der idealen Primfactoren etc.* (Abhandlungen der Berliner Akademie 1856). Dieser schöne und merkwürdige *Kronecker'sche Satz* gehört ohne Zweifel zu den zukunftsreichsten der Algebra,

da er auf die Wege weist, auf welchen allein ein tieferer Einblick in das Wesen der algebraischen Zahlgrössen zu hoffen ist. Der Satz aber, obwohl vor mehr als dreissig Jahren entdeckt, ist noch lange nicht in dem Maasse wie er es verdient, gekannt und verstanden, und ich glaube daher der Sache zu dienen, wenn es mir gelingt, durch die Mitteilung eines alle Fälle umfassenden Beweises das Verständniss desselben zu erleichtern und zu fördern. Das Hilfsmittel, dessen ich mich bei diesem Beweise bediene ist die von DEDEKIND entwickelte Theorie der algebraischen Zahlen, deren Terminologie und Hauptsätze ich als bekannt voraussetze. Der Leser findet dieselben in einfacher und klarer Darstellung vorgetragen im XI. Supplement zu der dritten Auflage der DIRICHLET'schen Vorlesungen über Zahlentheorie. Die in der vorliegenden Arbeit mit *D.* bezeichneten Citate beziehen sich auf dieses Werk. Auch in mündlichem und schriftlichem Verkehr habe ich mit meinem Freunde DEDEKIND vielfach über den Gegenstand dieser Untersuchungen verhandelt, und verdanke ihm nützlichen Rath und Anregung, besonders in Beziehung auf die elegante Formulierung des Problems in der ersten Abhandlung.

Der besseren Übersicht wegen habe ich die Untersuchung in drei getrennte Abhandlungen geteilt, deren jede so viel als möglich ein für sich abgeschlossenes Ganze bildet.

Die erste dieser Abhandlungen behandelt die allgemeine Theorie der Abel'schen Zahlkörper und insbesondere die Kreiskörper und ihre Darstellung. Es wird darin der meines Wissens früher noch nicht vollständig erbrachte Beweis geführt, dass durch die directe Verallgemeinerung der GAUSS'schen Perioden *alle* Kreiskörper, und jeder nur einmal, dargestellt werden. KRONECKER berührt diesen Gegenstand in den Monatsberichten der Berliner Akademie vom 14ten Apr. 1856; jedoch bezieht sich die dortige Mitteilung nur auf die regulären Kreiskörper.

Diejenigen Abel'schen Körper, deren Grad eine Potenz von 2 ist, bieten eine eigentümliche Schwierigkeit, und erfordern (wenigstens bis jetzt noch) die Zuziehung eines fremdartigen Hilfsmittels. Es war daher notwendig, in einer zweiten Abhandlung eine Untersuchung durchzuführen über die Anzahl der Idealclassen und die Einheiten in den Kreiskörpern, deren Ordnung eine Potenz von 2 ist.

Die dritte Abhandlung endlich soll den vollständigen Beweis des KRONECKER'schen Satzes liefern.

§ 1. *Allgemeines über algebraische Zahlkörper und Körperpermutationen.*

Unter einem algebraischen Zahlkörper n^{ten} Grades verstehen wir den Inbegriff $R(x)$ aller rationalen Functionen (mit rationalen Coefficienten) von x, wenn x eine Wurzel einer irreducibeln Gleichung n^{ten} Grades

$$f(x) = 0 \tag{1}$$

ist, deren Coefficienten rationale Zahlen sind.

1. Jede Zahl eines solchen Körpers ist wieder die Wurzel einer Gleichung n^{ten} Grades, welche entweder irreducibel oder eine ganze Potenz einer irreducibeln Gleichung ist. Es giebt unendlich viele Zahlen im Körper $R(x)$, welche irreducibeln Gleichungen n^{ten} Grades genügen, und wenn y eine solche ist, so ist der Körper $R(y)$ mit dem Körper $R(x)$ identisch, (weil alsdann sowohl y rational durch x als auch x rational durch y ausdrückbar ist). Solche Zahlen y können *primitive* Zahlen des Körpers $R(x)$ genannt werden, weil sie nicht zugleich in einem zweiten Körper von gleichem oder niedrigerem Grad enthalten sind.

2. Sind die Zahlen eines Körpers $R(y)$ sämmtlich in dem Körper $R(x)$ enthalten, so heisst $R(y)$ ein Teiler von $R(x)$; y ist eine Zahl in $R(x)$ welche einer irreducibeln Gleichung vom Grade des Körpers $R(y)$ genügt; und darnach ergiebt sich aus (1) dass der Grad von $R(y)$ ein Teiler des Grades von $R(x)$ ist.

3. Unter dem Product zweier Körper $R(x_1)$, $R(x_2)$ versteht man den Inbegriff $R(x_1, x_2)$ aller rationalen Functionen von x_1 und x_2; dies Product hat (nach n° 2) sowohl $R(x_1)$ als $R(x_2)$ zum Teiler. Es ergiebt sich hieraus sofort die Definition des Productes von mehreren Factoren.

4. Sind $x_1, x_2, \ldots, x_n$ die n Wurzeln der Gleichung (1) so heissen die Körper $R(x_1), R(x_2), \ldots, R(x_n)$ (die auch alle oder teilweise identisch sein können) *conjugierte Körper.* Der Übergang von einem Körper zu einem seiner conjugierten heisst eine *Permutation,* das Ersetzen der Zahlen des einen Körpers durch die entsprechenden des andern eine *Substitution.* Das Product aller mit einander conjugierten Körper heisst die *Norm* eines jeden dieser Körper. Bezeichnen wir mit z eine rationale

Function von $x_1, x_2, \ldots, x_n$, welche bei allen Vertauschungen dieser Grössen $\Pi(n)$ verschiedene Werte annimmt, so ist $R(z)$ die Norm von $R(x_1)$ (deren Grad niedriger sein kann als $\Pi(n)$). Ein Körper, der mit allen seinen conjugierten identisch ist, und der mithin seine eigene Norm ist, heisst ein *Normalkörper* oder ein *Galois'scher Körper*. Jede Norm ist ein solcher Normalkörper, und der Normalkörper kann auch dadurch charakterisiert werden, dass er mit seiner Norm gleichen Grad hat. (*D.* § 163.)

5. Die Permutationen von $R(z)$ bilden unter sich eine *Gruppe,* deren Grad gleich dem Grade von R ist. Denn die conjugierten Werte $z, z', z'', \ldots$ sind alle in $R(z)$ enthalten und werden also in bestimmter Weise unter einander vertauscht, wenn z durch eine Substitution S' durch z' ersetzt wird. Ersetzt man hierauf mittelst einer zweiten Substitution S'' z durch z'', so geht dadurch z' in z''' über, und die Substitution, durch welche z direct in z''' übergeht ist also aus den beiden Substitutionen $S'S''$ *zusammengesetzt;* hierbei darf im Allgemeinen die Reihenfolge nicht vertauscht werden. *Diese Substitutionsgruppe heisst die Gruppe,* nicht nur des Körpers $R(z)$, sondern eines jeden der Körper $R(x_1), R(x_2), \ldots$. Jede Zahl des Körpers $R(x_1)$ kann durch die Substitutionen dieser Gruppe in jede der mit ihr conjugierten Zahlen übergeführt werden. Denn nehmen wir an, dass dies für irgend eine solche Zahl x nicht der Fall sei, so würde eine gewisse Gruppe der conjugierten Werte von x nur unter sich vertauscht. Diese würden also schon für sich die Wurzeln einer Gleichung mit rationalen Coëfficienten sein, entgegen dem Satze n° 1.

6. Da die Zahlen $x_1, x_2, \ldots, x_n$ alle dem Körper $R(z)$ angehören, so werden sie durch jede der Substitutionen S in gewisser Weise unter einander vertauscht. Es entsteht so eine gewisse Gruppe von Substitutionen der Grössen $x_1, x_2, \ldots, x_n$, welche keine andere ist als die Galois'sche Gruppe der Gleichung (1), da jede rationale Function dieser Grössen, welche einen rationalen Wert hat durch die Permutationen des Körpers $R(z)$ ungeändert bleibt und umgekehrt.

7. Aus diesen Begriffsbestimmungen ergiebt sich, dass die Norm eines Divisors eines Körpers ein Divisor der Norm ist, und dass die Norm eines Productes zweier oder mehrerer Körper gleich dem Producte der Normen ist. Also ist auch das Product zweier oder mehrerer Normalkörper selbst ein Normalkörper.

§ 2. *Abel'sche Körper.*

Wir nennen einen algebraischen Zahlkörper einen *Abel'schen,* wenn seine Substitutionsgruppe eine Abel'sche Gruppe ist, d. h. wenn ihre Substitutionen alle unter einander vertauschbar sind. Daraus folgt:

1. *Jeder Abel'sche Körper ist ein Normalkörper.* Es sei nämlich $R(x)$ ein solcher Körper vom Grade n und x irgend eine primitive Zahl des Körpers, deren conjugierte Werte $x_1, x_2, \ldots, x_n$ sind. In der Gruppe des Körpers existiert gewiss wenigstens eine Substitution S_k, durch welche x_1 in einen beliebigen der conjugierten Werte, x_k, übergeht. (§ 1, n° 5.) Ist dann S irgend eine Substitution, durch welche x_1 in x_k übergeht, so bleibt durch die Substitution

$$S_h^{-1} S_k S^{-1} S_h \tag{1}$$

das Element x_h ungeändert; wegen der vorausgesetzten Vertauschbarkeit ist aber die Substitution (1) $= S_k S^{-1}$, und diese Substitution lässt daher alle $x_1, x_2, \ldots, x_n$ ungeändert. Sie ist also die identische Substitution und folglich ist

$$S = S_k. \tag{2}$$

Demnach ist der Grad der Norm von $R(x)$ gleich dem Grade dieses Körpers und daher $R(x)$ *ein Normalkörper.*[1] Man kann also die Substitutionen S_k in eindeutiger Weise durch das Symbol (x_1, x_k) bezeichnen, wobei noch das eine Glied der Bezeichnung, x_1, beliebig genommen werden kann, wenn das zweite passend bestimmt wird. Man kann etwa setzen

$$S_a = (x_1, x_{a_1}) = (x_b, x_{a_b})$$

und erhält

$$S_a S_b = (x_1, x_{b_{a_1}}), \qquad S_b S_a = (x_1, x_{a_{b_1}}) \tag{3}$$

also

$$x_{b_{a_1}} = x_{a_{b_1}}. \tag{4}$$

[1] Vgl. über diesen Satz KRONECKER, Berliner Monatsberichte, 16 Apr. 1877.

2. Eine einfache Folgerung dieser Definition, ist es, dass alle Teiler Abel'scher Körper selbst Abel'sche Körper sind.

3. Ein Abel'scher Körper heisst *regulär* wenn die Gruppe seiner Substitutionen durch Wiederholung einer einzigen unter ihnen erschöpft werden kann. In diesem Fall lassen sich die conjugierten Werte einer Zahl des Körpers derart in einen einzigen Cyklus $x_0, x_1, x_2, \ldots, x_{n-1}$ ordnen, dass dieselben durch die Substitutionen der Gruppe cyklisch vertauscht werden. Dieser Fall *muss* eintreten, wenn n eine Primzahl ist.

4. Unter dem Grad einer Abel'schen Gruppe versteht man die Anzahl der Elemente, welche sie enthält. Der Grad eines einzelnen Elementes ist der Exponent der niedrigsten Potenz dieses Elementes, welche gleich dem Hauptelement (gleich »1», in unserem Falle gleich der identischen Substitution) wird. Ist p irgend eine im Grade der Gruppe aufgehende Primzahl, so existieren in der Gruppe Elemente vom Grade p.[1]

5. Wenn in der Gruppe G unseres Körpers $R(x)$ irgend eine andere Gruppe G_1 vom Grade n_1 als Teiler enthalten ist, so giebt es in $R(x)$ Zahlen, welche durch die Substitutionen von G_1 ungeändert bleiben, dagegen durch jede andere Substitution von G sich ändern. Eine solche Zahl ist z. B. bei passender Bestimmung der rationalen Zahl t

$$y = (t - x_1)(t - x_2) \ldots (t - x_{n_1})$$

wenn $x_1, x_2, \ldots, x_{n_1}$ die Werte sind, in welche x durch die Substitutionen G_1 übergeht. Von einer solchen Zahl sagt man, sie *gehöre zu* der Gruppe G_1. Aus ihr entspringt ein Körper $R(y)$ vom Grade $n:n_1$, ein Teiler von $R(x)$, der ebenfalls als zur Gruppe G_1 *gehörig* bezeichnet sein soll. Wenn umgekehrt y eine Zahl in $R(x)$ ist, so bilden diejenigen Substitutionen in G, durch welche y ungeändert bleibt, eine Gruppe G_1, welche ein Teiler von G ist, und der Körper $R(y)$ *gehört* zur Gruppe G_1.

---

[1] Die Hauptsätze über Abel'sche Gruppen findet man in des Verfassers Arbeit *Über die Darstellung von Primzahlen durch quadratische Formen*, Mathematische Annalen, Bd. 20, S. 301 (1882), ferner: Schering, *Die Fundamentalclassen der zusammensetzbaren arithmetischen Formen*, Abhandlungen der Gesellschaft der Wissenschaften zu Göttingen, Bd. 14 (1868); Kronecker, Monatsberichte der Berliner Akademie 1 Dec. 1870; Frobenius *und* Stickelberger, *Gruppen von vertauschbaren Elementen*, Journal für Mathematik, Bd. 86, 1878.

Jeder Teiler $R(y)$ von $R(x)$ gehört also zu einem bestimmten Teiler G_1 von G und umgekehrt.

Gehört y_1 zu G_1, y_2 zu G_2, und ist G_2 in G_1 enthalten, so ist der Körper $R(y_1)$ in $R(y_2)$ enthalten. Sind $R(y_1)$, $R(y_2)$ zwei Divisoren von $R(x)$, welche zu den Gruppen G_1, G_2 gehören, so gehört das Product $R(y_1, y_2)$ zu dem grössten gemeinschaftlichen Teiler von G_1 und G_2 und der grösste gemeinschaftliche Teiler von $R(y_1)$, $R(y_2)$, d. h. der Inbegriff aller in beiden Körpern zugleich enthaltenen Zahlen, zum kleinsten gemeinschaftlichen Vielfachen der beiden Gruppen G_1, G_2.

6. Ein Abel'scher Körper wird *zerlegbar* genannt, wenn er (im Sinne von § 1, n° 3) das Product zweier anderer Abel'scher Körper ist. Im entgegengesetzten Fall heisst er einfach. Daraus ergiebt sich unmittelbar, dass ein zerlegbarer Abel'scher Körper in eine *endliche* Anzahl einfacher zerlegt werden kann.

Hierbei sei zur Vermeidung von Irrtümern bemerkt, dass die Zerlegbarkeit keineswegs aus dem Vorhandensein eines Teilers folgt, und dass die Zerlegung in einfache Körper nicht nur auf *eine* Art geschehen kann.

7. Ein Abel'scher Körper ist stets zerlegbar, wenn in seinem Grad zwei verschiedene Primzahlen p, q aufgehen. Bezeichnen nämlich S_1, S_2 zwei Substitutionen der Gruppe G von den Graden p, q, deren es nach n° 4 immer giebt, und y_1, y_2 zwei Zahlen des Körpers, die zu den aus den Potenzen von S_1, S_2 gebildeten Gruppen p^{ten} und q^{ten} Grades gehören, so sind $R(y_1)$, $R(y_2)$ zwei Teiler von $R(x)$ von den Graden $n:p$; $n:q$. Der aus beiden zusammengesetzte Körper $R(y_1, y_2)$ ist gleichfalls ein Teiler von $R(x)$; sein Grad ist aber sowohl durch $n:p$ als durch $n:q$ teilbar und muss also $= n$ sein. Hiernach ist $R(y_1, y_2)$ mit $R(x)$ identisch. Darnach lassen sich alle Abel'schen Körper aus solchen zusammensetzen, deren Grad eine Primzahlpotenz ist.

8. Ein nicht regulärer Abel'scher Körper, dessen Grad eine Primzahlpotenz p^π ist, ist zerlegbar. Sei nämlich S eine Substitution in G vom Grade p, und S_1 eine zweite, welche nicht unter den Potenzen von S enthalten ist. Dass bei irregulären Gruppen solche vorhanden sind, ist leicht einzusehen. Die Zahlen y, y_1 mögen zu den durch die Potenzen dieser beiden Substitutionen gebildeten Gruppen gehören. Dann ist y_1 nicht im Körper $R(y)$ vom Grade $n:p$ enthalten, da es ja sonst durch die Substitu-

tion S ungeändert bleiben müsste. Der Grad des Körpers $R(y, y_1)$ ist dann durch $n:p$ teilbar, kann aber nicht $= n:p$ sein, weil sonst $R(y, y_1)$ mit $R(y)$ identisch wäre; andererseits ist dieser Grad ein Teiler von n und muss mithin $= n$ sein. Es ist also wieder $R(y, y_1)$ mit $R(x)$ identisch. *Es lassen sich also alle Abel'schen Körper aus regulären Abel'schen Körpern zusammensetzen, deren Grad eine Primzahlpotenz ist.*

Ein regulärer Körper, dessen Grad eine Primzahlpotenz ist, ist dagegen unzerlegbar, weil jeder Teiler eines solchen Körpers jeden anderen Teiler von gleichem oder niedrigerem Grade wieder als Teiler enthält.

§ 3. *Abel'sche Gruppen und Gruppencharaktere.*

Für die spätere Anwendung sollen zunächst einige der Hauptsätze über Abel'sche Gruppen zusammengestellt werden, die im Wesentlichen bekannt sind. Die Beweise findet man in der oben citierten Abhandlung des Verfassers.

1. Es sei G eine Abel'sche Gruppe vom Grade n, und S seien ihre Elemente. Diese Elemente lassen sich durch eine *Basis* darstellen, in der Weise

$$S = S_1^{s_1} S_2^{s_2} \dots S_\nu^{s_\nu}, \tag{1}$$

so dass man jedes Element S von G ein und nur einmal erhält, wenn $s_1 \pmod{n_1}$, $s_2 \pmod{n_2}$, ..., $s_\nu \pmod{n_\nu}$ je ein vollständiges Restsystem durchläuft. Es ist alsdann

$$n = n_1 n_2 \dots n_\nu. \tag{2}$$

2. Wählt man die Grössen $\omega_1, \omega_2, \dots, \omega_\nu$ unter den Wurzeln der Gleichungen

$$\omega_1^{n_1} = 1, \qquad \omega_2^{n_2} = 1, \quad \dots, \quad \omega_\nu^{n_\nu} = 1$$

beliebig aus, und setzt (nach (1))

$$\chi(S) = \omega_1^{s_1} \omega_2^{s_2} \dots \omega_\nu^{s_\nu}, \tag{3}$$

so erhält man die n *Charaktere* der Gruppe G. Für irgend zwei Elemente S, S' von G ist dann stets

$$\chi(S)\chi(S') = \chi(SS'). \tag{4}$$

Wenn umgekehrt eine Function $\chi(S)$ der Bedingung (4) genügt, so ist sie unter den n Charakteren enthalten.

Die Charaktere bilden unter sich eine Abel'sche Gruppe vom Grade n, wenn man unter $\chi\chi'(S)$ den Charakter

$$(\omega_1\omega_1')^{s_1}(\omega_2\omega_2')^{s_2}\ldots(\omega_\nu\omega_\nu')^{s_\nu}$$

versteht.

3. Auf Grund dieses Satzes lassen sich die Divisoren der Gruppe G genauer charakterisieren. Es sei

$$g = S,\ S',\ S'',\ \ldots$$

eine in G enthaltene Gruppe (ein Divisor von G). Ist G durch die Elemente g nicht erschöpft, so wähle man ein in g nicht enthaltenes Element S_1 und bilde die Reihe der Elemente

$$g_1 = S_1S,\ S_1S',\ S_1S'',\ \ldots$$

welche lauter von einander und von g verschiedene Elemente enthält. Ist G noch nicht erschöpft, so wähle man S_2 so dass es weder in g noch in g_1 enthalten ist, und bilden die dritte Reihe

$$g_2 = S_2S,\ S_2S',\ S_2S'',\ \ldots$$

und fahre so fort, bis die Gruppe G erschöpft ist. Diese Reihen g, g_1, g_2, ... bilden unter sich eine Abel'sche Gruppe H, wenn wir die Composition derselben in dem Sinne erklären, dass g_1g_2 die Reihe

$$g_1g_2 = S_1S_2S,\ S_1S_2S',\ S_1S_2S'',\ \ldots$$

bedeute.

Wir betrachten die Charaktere $\xi(g)$ dieser Gruppe H und setzen, wenn S_i, S_i', S_i'', ... in g_i enthalten sind

$$\xi(g_i) = \xi(S_i) = \xi(S_i') = \xi(S_i'') = \ldots.$$

Hierdurch ist eine Reihe von Functionen $\xi(S)$ bestimmt, welche der Bedingung

$$\xi(S)\xi(S') = \xi(SS')$$

genügen, und die daher unter den Charakteren $\chi(S)$ enthalten sind. *Für die Elemente S, S', S'', ..., die in der Gruppe g vorkommen, und nur für diese,*

haben alle diese Functionen den Wert $+1$. Daraus folgt der Satz: Alle Elemente einer Abel'schen Gruppe G, für welche ein oder mehrere Charaktere den Wert $+1$ haben, bilden einen Divisor von G, und umgekehrt erhält man *alle Divisoren* von G, wenn man alle diejenigen Elemente sucht, welche einem einzelnen oder einer beliebigen Anzahl von Charakteren den Wert $+1$ erteilen.

Der Inbegriff derjenigen Charaktere $\xi(S)$, welche für die sämmtlichen Elemente der Gruppe g den Wert $+1$ haben, bildet unter sich eine Abel'sche Gruppe deren Grad $= n:n_1$ ist, wenn n_1 den Grad von g bedeutet, und die Gruppe G ist durch diese vollständig bestimmt. Wir sagen, die Gruppe g *gehöre* zu dieser Gruppe von Charakteren (oder umgekehrt diese Charakterengruppe zur Gruppe g).

§ 4. *Die Kreiskörper.*

Unter einem Kreiskörper versteht man jeden aus rationalen Zahlen und Einheitswurzeln zusammengesetzten Zahlkörper. Ist r eine primitive m^{te} Einheitswurzel, so soll der Körper $R(r)$, welcher aus *sämmtlichen* rationalen Functionen von r besteht, der *vollständige Kreiskörper der Ordnung* m heissen, und mit Ω_m bezeichnet werden.

Da man beliebig viele Einheitswurzeln immer als Potenzen einer und derselben Einheitswurzel darstellen kann, so folgt, dass *jeder* Kreiskörper ein *Divisor eines vollständigen Kreiskörpers ist. Man erhält daher jeden Kreiskörper und jeden nur einmal, wenn man alle diejenigen Divisoren eines vollständigen Kreiskörpers* m^{ter} *Ordnung aufsucht, die nicht zugleich in Kreiskörpern niedrigerer Ordnung enthalten sind.*

Da r die Wurzel einer irreducibeln Gleichung vom Grade $\varphi(m)$ ist, so ist $\varphi(m)$ auch der Grad des Körpers Ω_m. Die Gruppe des Körpers besteht aus sämmtlichen Substitutionen

$$(r,\ r^n)$$

wenn n die sämmtlichen relativen Primzahlen zu m (mod m) durchläuft; diese Gruppe, die wir mit N bezeichnen wollen, kann dargestellt werden durch die sämmtlichen nach dem Modul m reducierten zu m teilerfremden

Zahlen. Diese Gruppe ist eine Abel'sche, und folglich ist *jeder Kreiskörper ein Abel'scher Körper.*

Um die sämmtlichen Divisoren eines vollständigen Kreiskörpers zu ermitteln, hat man nach § 2, n° 5 die sämmtlichen Teiler der Gruppe N aufzusuchen, d. h. die sämmtlichen nach dem Modul m genommenen Zahlsysteme

$$(\mathfrak{K}) \qquad k_0,\ k_1,\ k_2,\ \ldots$$

die sich bei der Multiplication unter einander reproducieren. Zu jeder solchen Gruppe gehört ein Teiler von Ω_m und umgekehrt, zu jedem Teiler von Ω_m eine solche Gruppe.

1. Ist m_1 ein Teiler von m, so ist auch der vollständige Kreiskörper Ω_{m_1} ein Teiler von Ω_m. Die Gruppe, zu welcher dieser Teiler gehört besteht aus allen denjenigen Zahlen k, welche der Bedingung genügen

$$k \equiv 1 \pmod{m_1}.$$

Sind m_1, m_2 zwei Divisoren von m, deren grösster gemeinschaftlicher Teiler d ist, so gehört (nach § 2, n° 5) der grösste gemeinschaftliche Teiler von Ω_{m_1}, Ω_{m_2} zu der Gruppe

$$k \equiv 1 \pmod{d}$$

und ist also der vollständige Kreiskörper Ω_d.

2. Nun sollen unter den Divisoren von Ω_m diejenigen aufgesucht werden, welche nicht zugleich in vollständigen Kreiskörpern niedrigerer Ordnung enthalten sind. Nach n° 1 sind also solche und nur solche Divisoren von Ω_m auszuscheiden, die zugleich Divisoren von Ω_{m_1} sind, wenn m_1 in m enthalten ist.

Auszuscheiden sind also alle diejenigen Divisoren von Ω_m und nur diese, welche zugleich Divisoren von einem der Körper $\Omega_{\frac{m}{q}}$ sind, wenn q irgend eine der in m aufgehenden Primzahlen bedeutet. Das heisst, man hat von den Divisoren $\mathfrak{K}$ der Gruppe N diejenigen auszuscheiden, welche eine der Gruppen

$$(\mathfrak{K}_q) \qquad k \equiv 1 \left(\mathrm{mod}\,\frac{m}{q}\right)$$

als Teiler enthalten. Die übrig bleibenden Gruppen $\mathfrak{R}$, und nur diese liefern *primitive Divisoren* von Ω_m, und man erhält also auf diese Weise *alle Kreiskörper und jeden nur einmal.*

§ 5. *Darstellung der Kreiskörper durch die Perioden.*

Um die primitiven Divisoren Ω von Ω_m auf die einfachste Weise darzustellen, hat man eine möglichst einfache Function von r zu suchen, welche zu der Gruppe $\mathfrak{R}$ von Ω gehört. Dass diesen Zweck die Perioden (im GAUSS'schen Sinne)

$$\eta = \sum^{k} r^{k}$$

erfüllen, wird dann bewiesen sein, wenn gezeigt werden kann, dass unter den conjugierten Werten $\eta_1, \eta_2, \eta_3, \ldots$ dieser Perioden nicht zwei einander gleiche vorkommen. Um dies zu beweisen, ist es nötig, auf die Charaktere der Gruppe N etwas genauer einzugehen.

1. Es sei

$$m = 2^{\lambda} q_1^{\varkappa_1} q_2^{\varkappa_2} \ldots \tag{1}$$

$\lambda = 0$ oder $\geqq 2$, $q_1, q_2, \ldots$ die von einander verschiedenen in m aufgehenden ungeraden Primzahlen. Man setze

$$a = b = 1 \text{ für } \lambda = 0; \qquad a = 2, \qquad b = \frac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2} \text{ für } \lambda \geqq 2 \tag{2}$$

$$c_1 = \varphi(q_1^{\varkappa_1}) = q_1^{\varkappa_1 - 1}(q_1 - 1), \qquad c_2 = \varphi(q_2^{\varkappa_2}), \ldots$$

und verstehe unter $g_1, g_2, \ldots$ primitive Wurzeln von $q_1^2, q_2^2, \ldots$ Dann lässt sich für jede zu m teilerfremde Zahl n ein System von *Indices* $\alpha, \beta, \gamma_1, \gamma_2, \ldots$ nach den Moduln $a, b, c_1, c_2, \ldots$ aus den Congruenzen bestimmen

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}; \qquad n \equiv g_1^{\gamma_1} \pmod{q_1^{\varkappa_1}}, \qquad n \equiv g_2^{\gamma_2} \pmod{q_2^{\varkappa_2}}, \ldots \tag{3}$$

Versteht man dann unter $\varepsilon, \theta, \omega_1, \omega_2, \ldots$ *primitive* Wurzeln der Gleichungen

$$\varepsilon^a = 1, \qquad \theta^b = 1, \qquad \omega_1^{c_1} = 1, \qquad \omega_2^{c_2} = 1, \ldots \tag{4}$$

und bezeichnet mit α', β', γ_1', γ_2', ... die Indices einer Zahl n', so erhält man die Charaktere der Gruppe N in der Form

$$\chi_{n'}(n) = \varepsilon^{\alpha'\alpha}\theta^{\beta'\beta}\omega_1^{\gamma_1'\gamma_1}\omega_2^{\gamma_2'\gamma_2}\ldots \tag{5}$$

2. Die Charakterengruppe, zu welcher eine der in n° 2, § 4 ausgeschlossenen Gruppen $\mathfrak{K}_{q_1}$ gehört, erhält man falls q_1 nur einmal in m aufgeht indem man $\omega_1^{\gamma_1'} = 1$ setzt, und wenn q_1 mehrmals in m aufgeht, indem man γ_1' durch q_1 teilbar annimmt. Um die Charakterengruppe zu welcher $\mathfrak{K}_2$ gehört, zu bilden, hat man, falls $\lambda = 2$ ist, α', falls $\lambda > 2$ ist β' durch 2 teilbar anzunehmen. Die auf diese Weise definierten Charakterengruppen sollen mit $\mathfrak{C}_{q_1}$, $\mathfrak{C}_{q_2}$, ..., $\mathfrak{C}_2$ bezeichnet werden.

3. Ist nun $\mathfrak{K}$ ein Divisor der Gruppe N, h_1 eine Zahl in N, die nicht in $\mathfrak{K}$ enthalten ist, h_2 eine Zahl in N, die weder in $\mathfrak{K}$ noch in $h_1\mathfrak{K}$ vorkommt, u. s. f., so zerfällt N in die Reihen

$$\begin{aligned}
(\mathfrak{K}) \quad & k_0, \quad k_1, \quad k_2, \ldots \\
(h_1\mathfrak{K}) \quad & h_1k_0, \quad h_1k_1, \quad h_1k_2, \ldots \\
(h_2\mathfrak{K}) \quad & h_2k_0, \quad h_2k_1, \quad h_2k_2, \ldots \\
& \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot
\end{aligned}$$

Diese Reihen bilden im Sinne von § 3, n° 2, eine Gruppe H. Wir bezeichnen mit $\xi(n)$ diejenigen unter den Charakteren $\chi(n)$, zu welchen die Gruppe $\mathfrak{K}$ gehört und mit $\mathfrak{C}$ die Gruppe derselben. Da hiernach

$$\xi(k_0) = \xi(k_1) = \xi(k_2) = \ldots = 1 \tag{6}$$

ist, so erhält man für die Charaktere der Gruppe H die Ausdrücke $\xi(h_0)$, $\xi(h_1)$, $\xi(h_2)$, ...

Hieraus ergiebt sich, wenn wir

$$\eta_h = \sum^{k} r^{hk} \tag{7}$$

setzen,

$$\sum^{h} \xi(h)\eta_h = \sum^{n} \xi(n) r^n. \tag{8}$$

4. Es sollen nun die Bedingungen gesucht werden, unter welchen mehrere der η_h einander gleich sind. Ist

$$\eta_1 = \eta_h = \eta_{h'} = \ldots$$

so bilden diese in dem Sinne eine Gruppe, dass auch

$$\eta_1 = \eta_{hh'}$$

ist, und diese Gruppe ist ein Divisor von H, den wir mit H' bezeichnen. Die Perioden η_h zerfallen in Reihen von gleich vielen unter einander gleichen.

Die Gruppe H' ist wieder dadurch charakterisiert, dass sie aus allen denjenigen $h\mathfrak{R}$ besteht, für welche eine gewisse Gruppe unter den Charakteren ξ, die wir mit ξ' bezeichnen wollen, den Wert $+1$ hat. Die übrigen unter den Charakteren ξ, welche also für einige Elemente der Gruppe H' von 1 verschieden sind, bezeichnen wir mit ξ''. *Solche Charaktere ξ'' existieren immer, wenn H' mehr als ein Element enthält, wenn also wirklich mehrere der Perioden η einander gleich sind.*

5. Ist nun h' irgend eine zu m teilerfremde Zahl, so lässt sich die Summe (8) so schreiben:

$$\sum_{n}^{n}\xi(n)r^n = \sum\xi(h'n)r^{h'n} = \xi(h')\sum\xi(n)r^{h'n} = \xi(h')\sum\xi(h)\eta_{h'h}.$$

Wir nehmen nun an, es sei $\eta_1 = \eta_{h'}$, und folglich auch

$$\eta_h = \eta_{hh'}$$

dann folgt aus der letzten Gleichung wegen (8)

$$\sum_{n}^{n}\xi(n)r^n = \xi(h')\sum_{n}^{n}\xi(n)r^n.$$

Findet sich nun der Charakter ξ unter den ξ'', so kann man h' so wählen, dass $\xi(h')$ von 1 verschieden ist, und daraus folgt:

$$\sum\xi''(n)r^n = 0. \tag{9}$$

Diese Bedingung lässt sich nun in folgender Weise umformen. Bezeichnen wir mit $r_0, r_1, r_2, \ldots$ primitive Einheitswurzeln der Ordnung 2^λ, $q_1^{\varkappa_1}, q_2^{\varkappa_2}, \ldots$ so kann man jede primitive m^{te} Einheitswurzel in der Form annehmen

$$r = r_0 r_1 r_2 \ldots \tag{10}$$

Ist dann (nach (5))

$$\xi''(n) = \varepsilon^{\alpha''\alpha}\theta^{\beta''\beta}\omega_1^{\gamma_1''\gamma_1}\omega_2^{\gamma_2''\gamma_2}\ldots, \tag{11}$$

so zerfällt die linke Seite von (9) in Factoren:

$$\sum^{\alpha,\beta}\varepsilon^{\alpha''\alpha}\theta^{\beta''\beta}\eta_0^{(-1)^{\alpha}5^{\beta}}\sum^{\gamma_1}\omega_1^{\gamma_1''\gamma_1}\eta_1^{g_1\gamma_1}\sum^{\gamma_2}\omega_2^{\gamma_2''\gamma_2}\eta_2^{g_2\gamma_2}\ldots = 0, \tag{12}$$

woraus folgt, dass wenigstens einer dieser Factoren verschwinden muss.

6. Wir wollen nun, um die Kette der Schlüsse nicht zu unterbrechen die folgenden, im nächsten § zu beweisenden Sätze voraussetzen.

a) Die Summe

$$\sum^{\gamma_1}\omega_1^{\gamma_1''\gamma_1}\eta_1^{g_1\gamma_1}$$

kann nicht verschwinden, wenn $\varkappa_1 = 1$, also q_1 ein einfacher Factor von m ist; ist $\varkappa_1 > 1$ so verschwindet dieser Ausdruck dann und nur dann, wenn

$$\gamma_1'' \equiv 0 \pmod{q_1}.$$

b) Die Summe

$$\sum^{\alpha,\beta}\varepsilon^{\alpha''\alpha}\theta^{\beta''\beta}\eta_0^{(-1)^{\alpha}5^{\beta}}$$

verschwindet, wenn $\lambda = 2$ ist, dann und nur dann, wenn

$$\alpha'' \equiv 0 \pmod 2$$

und wenn $\lambda \gtreqless 3$, dann und nur dann, wenn

$$\beta'' \equiv 0 \pmod 2.$$

7. Hieraus schliessen wir zunächst, dass die Gleichung (9), (12) auch dann noch befriedigt sein muss, wenn ξ'' durch einen der Charaktere ξ' ersetzt wird. Denn setzen wir

$$\xi'(n) = \varepsilon^{\alpha'\alpha}\theta^{\beta'\beta}\omega_1^{\gamma_1'\gamma_1}\omega_2^{\gamma_2'\gamma_2}\ldots$$

und nehmen an es sei, falls m durch eine höhere als die erste Potenz von q_1, q_2, ... teilbar ist, γ_1', γ_2', ... nicht durch q_1, q_2, ... teilbar, ebenso falls m durch 4 aber nicht durch 8 teilbar ist, α', und falls m durch 8 teilbar ist β' ungerade, wie es nach n° 6 sein muss, wenn $\sum\xi'(n)\vartheta^n$ von Null verschieden ist, so kann man in dem zusammengesetzten Charakter

$$\xi'^s\xi''(n) = \varepsilon^{(\alpha' s+\alpha'')\alpha}\theta^{(\beta' s+\beta'')\beta}\omega_1^{(\gamma_1' s+\gamma_1'')\gamma_1}\omega_2^{(\gamma_2' s+\gamma_2'')\gamma_2}\ldots,$$

der offenbar zu den Charakteren ξ'' gehört, die ganze Zahl s so bestimmen, dass $\gamma_1' s + \gamma_1''$ nicht durch q_1, $\gamma_2' s + \gamma_2''$ nicht durch q_2, u. s. f. und, eventuell, $\alpha' s + \alpha''$ oder $\beta' s + \beta''$ nicht durch 2 teilbar wird. Dadurch aber kommt man zu einem Widerspruch mit der Gleichung (9).

8. Nach n° 2 und n° 6 kann man dem hiermit Bewiesenen den folgenden Ausdruck geben. *Wenn unter den zur Gruppe $\mathfrak{K}$ gehörigen Perioden η_h mehrere gleiche vorkommen, so muss jeder der Charaktere ξ, der Gruppe $\mathfrak{C}$ in einer der Gruppen $\mathfrak{C}_{q_1}$, $\mathfrak{C}_{q_2}$, ..., $\mathfrak{C}_2$ enthalten sein,* (wobei nur diejenigen Primzahlen q_1, q_2, ... in Betracht kommen, welche *mehrfache* Factoren von m sind und $\mathfrak{C}_2$ nur falls m durch 4 teilbar ist).

9. Daraus kann nun weiter gefolgert werden, dass unter den Gruppen $\mathfrak{C}_{q_1}$, $\mathfrak{C}_{q_2}$, ..., $\mathfrak{C}_2$ mindestens eine durch die Gruppe $\mathfrak{C}$ teilbar ist, *und dass folglich $\mathfrak{K}$ durch eine der Gruppen $\mathfrak{K}_{q_1}$, $\mathfrak{K}_{q_2}$, ..., $\mathfrak{K}_2$ teilbar ist.* Es ist nämlich, wenn χ ein beliebiger der Charaktere von N ist, χ^{q_1} in $\mathfrak{C}_{q_1}$, χ^{q_2} in $\mathfrak{C}_{q_2}$, ..., χ^2 in $\mathfrak{C}_2$ enthalten. Nehmen wir nun an, es sei keine der Gruppen $\mathfrak{C}_{q_1}$, $\mathfrak{C}_{q_2}$, ..., $\mathfrak{C}_2$ durch $\mathfrak{C}$ teilbar, so kann man die Charaktere ξ_0, ξ_1, ξ_2, ... in $\mathfrak{C}$ so wählen, dass ξ_0 nicht in $\mathfrak{C}_2$, ξ_1 nicht in $\mathfrak{C}_{q_1}$, ξ_2 nicht in $\mathfrak{C}_{q_2}$, ... enthalten ist; dann wäre aber der zusammengesetzte Charakter

$$\xi_0^{q_1 q_2 \cdots} \xi_1^{2 q_2 \cdots} \xi_2^{2 q_1 \cdots} \cdots$$

zwar in $\mathfrak{C}$, aber weder in $\mathfrak{C}_{q_1}$ noch in $\mathfrak{C}_{q_2}$... noch in $\mathfrak{C}_2$ enthalten, entgegen dem in n° 8 Bewiesenen.

10. Hieraus folgt nun, dass, wenn man die in § 4, n° 2 characterisierten Gruppen ausgeschieden hat, unter den conjugierten Perioden niemals mehrere gleiche vorkommen, und dass man also *sämmtliche Kreiskörper* rational durch diese Perioden darstellen kann. Man kann dieselben sogar in einem gewissen Sinne *linear* durch die Perioden ausdrücken. Denn setzt man allgemein, auch wenn a nicht relativ prim zu m ist

$$\eta_a = \sum^{k} \vartheta^{ak}$$

so erhält man, wenn k, k' von einander unabhängig die Gruppe $\mathfrak{K}$ durchlaufen, für beliebige a, b:

$$\eta_a \eta_b = \sum^{k,k'} \vartheta^{ak+bk'} = \sum^{k,k'} \vartheta^{(ak+b)k'} = \sum \eta_{ak+b}.$$

§ 6. *Beweis des Lemma n° 6.*

Zur Vervollständigung bleibt uns noch übrig die in n° 6 angeführten Hilfssätze zu beweisen.

1. Ist zunächst p eine *ungerade* Primzahl, r eine primitive Einheitswurzel der Ordnung p^π, ω eine solche der Ordnung $\varphi(p^\pi)$, g eine primitive Wurzel von p^2, und für jede durch p nicht teilbare Zahl n

$$g^\gamma \equiv n \pmod{p^\pi} \tag{1}$$

so setzen wir, indem wir n ein vollständiges System modulo p^π in congruenter durch p nicht teilbarer Zahlen durchlaufen lassen,

$$(\omega^h, r) = \sum^{n} \omega^{h\gamma} r^n \tag{2}$$

$$(\omega^h, r^{n'}) = \omega^{-h\gamma'} \sum^{n} \omega^{h\gamma} r^n = \omega^{-h\gamma'} (\omega^h, r), \tag{3}$$

und wenn man mit $r^{n'}$ multipliciert und die Summe nimmt:

$$(\omega^{-h}, r)(\omega^h, r) = \sum^{n, n'} \omega^{h\gamma} r^{n'(n+1)}. \tag{4}$$

a) Ist $\pi = 1$, so ist die nach n' genommene Summe

$$\sum^{n'} r^{n'(n+1)} = -1, \qquad n < p-1$$

$$= p-1, \qquad n = p-1,$$

und da

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

also für

$$n = p-1, \qquad \gamma = \frac{p-1}{2},$$

so folgt

$$(\omega^h, r)(\omega^{-h}, r) = (-1)^h p. \tag{5}$$

Es kann also in diesem Fall (ω^h, r) nicht verschwinden.

b) Ist $\pi > 1$, so ist

$$\sum^{n'} r^{n'(n+1)}$$

immer dann $= 0$, wenn $n + 1$ nicht durch $p^{\pi-1}$ teilbar ist, und es ist

für $n + 1 = p^{\pi}$, $\sum^{n'} r^{n'(n+1)} = p^{\pi-1}(p - 1)$, $\gamma = \frac{1}{2}\varphi(p^{\pi})$

für $n + 1 = \lambda p^{\pi-1}$, $\sum^{n'} r^{n'(n+1)} = -p^{\pi-1}$, $\gamma = \frac{1}{2}\varphi(p^{\pi}) + \nu\varphi(p^{\pi-1})$,

worin λ und ν gleichzeitig ein vollständiges Restsystem modulo p durchlaufen (mit Ausschluss von 0).

Hiernach wird also

$$(\omega^h, r)(\omega^{-h}, r) = (-1)^h p^{\pi} - (-1)^h p^{\pi-1} \sum_{0,p-1}^{\nu} \omega^{h\nu\varphi(p^{\pi-1})},$$

also wenn h nicht durch p teilbar ist

$$(\omega^h, r)(\omega^{-h}, r) = (-1)^h p^{\pi}. \tag{6}$$

Ist aber h durch p teilbar, so folgt aus (3)

$$(\omega^h, r^{1+\lambda p^{\pi-1}}) = (\omega^h, r), \qquad (\lambda = 0, 1, \ldots, p-1)$$

und wenn man die Summe über alle λ bildet,

$$(\omega^h, r) = 0, \qquad h \equiv 0 \pmod{p}, \tag{7}$$

womit n° 6 a) des vorigen § bewiesen ist.

2. Es seien jetzt r, θ primitive Einheitswurzeln der Ordnung 2^{λ}, $2^{\lambda-2}$, und für jedes ungerade n

$$(-1)^{\alpha} 5^{\beta} \equiv n \pmod{2^{\lambda}}, \tag{8}$$

worin α, β wie in § 5, (1) nach den Moduln a, b genommen sind. Setzen wir nun

$$[(-1)^h, \theta^k, r] = \sum^{n} (-1)^{h\alpha} \theta^{k\beta} r^n, \tag{9}$$

dann ergiebt sich zunächst direct:

a) Ist $\lambda = 2$, so verschwindet $[(-1)^h, \theta^k, r]$ dann und nur dann wenn $h \equiv 0 \pmod 2$.

b) Ist $\lambda \geqq 3$, so folgt wie oben

$$[(-1)^h, \theta^k, r^{n'}] = (-1)^{-h\alpha'} \theta^{-k\beta'} [(-1)^h, \theta^k, r], \tag{10}$$

also:

$$[(-1)^h,\ \theta^k,\ r][(-1)^{-h},\ \theta^{-k},\ r] = \sum^{n,n'}(-1)^{h\alpha}\theta^{k\beta}r^{n'(1+n)}.$$

Die nach n' genommene Summe ist nun

$$\sum^{n'} r^{n'(n+1)} = 0, \text{ wenn } n+1 \text{ nicht durch } 2^{\lambda-1} \text{ teilbar ist,}$$

$$= 2^{\lambda-1} \quad \text{für} \quad n+1 = 2^{\lambda}, \quad \alpha = 1, \quad \beta = 0$$

$$= -2^{\lambda-1} \quad \text{für} \quad n+1 = 2^{\lambda-1}, \quad \alpha = 1, \quad \beta = 2^{\lambda-3},$$

woraus sich, falls k ungerade ist,

$$(11) \qquad [(-1)^h,\ \theta^k,\ r][(-1)^{-h},\ \theta^{-k},\ r] = (-1)^h 2^{\lambda}, \qquad k \equiv 1 \pmod 2$$

ergiebt.

Setzt man aber in (10)

$$n' = 1 + 2^{\lambda-1},$$

also

$$r^{n'} = -r, \qquad \alpha' = 0, \qquad \beta' = 2^{\lambda-3},$$

so folgt

$$[(-1)^h,\ \theta^k,\ -r] = (-1)^k[(-1)^h,\ \theta^k,\ r],$$

woraus unmittelbar hervorgeht, dass im Falle eines geraden k

$$(12) \qquad [(-1)^h,\ \theta^k,\ r] = 0, \qquad k \equiv 0 \pmod 2,$$

womit also auch n° 6 b) des vorigen § bewiesen ist.

§ 7. *Die Ideale der vollständigen Kreiskörper.*

Die Primideale oder idealen Primfactoren in den vollständigen Kreiskörpern beliebiger Ordnung hat KUMMER aufgestellt in der Abhandlung: *Theorie der idealen Primfactoren der complexen Zahlen, welche aus Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist.* (Abh. der Berliner Akademie, 1856.) Das Resultat findet man in anderer Form bei *D.* § 179 und zwar vollständig abgeleitet für den Fall, dass die Ordnung eine Primzahl ist; man gelangt aber auf wesentlich dem-

selben Weg auch zu den allgemeinen Resultaten, von welchen hier, soviel in der Folge gebraucht wird, zusammengestellt werden soll.

1. Die Potenzen von r: $1, r, r^2, \ldots, r^{\varphi(m)-1}$ bilden im Körper Ω_m eine Basis von $\mathfrak{o}$, d. h. es lässt sich jede *ganze* Zahl des Körpers Ω_m als ganze rationale Function, höchstens vom Grade $\varphi(m) - 1$ mit *ganzen* rationalen Zahlcoëfficienten darstellen.

2. Ein beliebiges Ideal $\mathfrak{a}$ oder eine Zahl α des Körpers Ω_m geht durch die Substitution (r, r^n) in ein *conjugiertes* Ideal oder eine conjugierte Zahl über, welche wir mit $\mathfrak{a}_n$, α_n bezeichnen, worin n relativ prim zu m ist. Die zu einem Primideal conjugierten Ideale sind ebenfalls Primideale und wenn eine ganze rationale Zahl durch irgend ein Ideal teilbar ist, so ist sie auch durch die sämmtlichen conjugierten Ideale teilbar.

Ist $\mathfrak{p}$ ein in der rationalen Primzahl p aufgehendes Primideal und

$$N(\mathfrak{p}) = p^f$$

so heisst $\mathfrak{p}$ ein *Primideal f^{ten} Grades.*

3. Ist p' die höchste in m aufgehende Potenz von p, $m = p'm'$, und gehört p zum Exponenten $f \pmod{m'}$, so ist $\varphi(m') = ef$, und $\mathfrak{o}p$ ist die $\varphi(p')^{te}$ Potenz eines Products von e von einander verschiedenen Primidealen f^{ten} Grades.

4. Ist ins Besondere $p' = 1$, also p in m nicht enthalten, und gehört p zum Exponenten $f \pmod{m}$ so zerfällt p in e verschiedene Primideale f^{ten} Grades. Unter den conjugierten Idealen $\mathfrak{p}_n$ sind

$$\mathfrak{p}_n, \mathfrak{p}_{np}, \mathfrak{p}_{np^2}, \ldots, \mathfrak{p}_{np^{f-1}}$$

und *nur* diese mit einander identisch, woraus hervorgeht dass die e in p aufgehenden Primideale conjugiert sind.

5. Die Primideale $\mathfrak{p}$ sind dann und nur dann vom ersten Grade, wenn

$$p \equiv 1 \pmod{m}.$$

In diesem Falle ist jede ganze Zahl des Körpers Ω_m mit einer *ganzen rationalen* Zahl nach $\mathfrak{p}$ congruent, und wenn r mit a congruent ist, so muss a zum Exponenten m nach dem Modul p gehören.[1] Ist daher g eine primitive Wurzel von p, so können wir setzen

[1] Ist nämlich $r \equiv a \pmod{\mathfrak{p}}$, so folgt $a^m \equiv 1 \pmod{p}$ und diese Congruenz kann für

$$r \equiv g^{-\frac{p-1}{m}} \pmod{\mathfrak{p}_1}, \tag{1}$$

woraus folgt:

$$r^n \equiv g^{-\frac{p-1}{m}} \pmod{\mathfrak{p}_n} \tag{2}$$

oder, wenn n' aus der Congruenz

$$nn' \equiv 1 \pmod{m} \tag{3}$$

bestimmt wird

$$r \equiv g^{-n'\frac{p-1}{m}} \pmod{\mathfrak{p}_n} \tag{4}$$

wodurch die conjugierten Ideale $\mathfrak{p}_n$ vollständig charakterisiert sind.

6. Ist $m = q^k$ eine Primzahlpotenz, so ist q associiert mit $(1-r)^{\varphi(m)}$ und $\mathfrak{o}(1-r)$ ein Primideal, also $\mathfrak{o}q$ die $\varphi(m)^{\text{te}}$ Potenz eines Primideals ersten Grades, und zwar eines *Hauptideals*.

7. Es sei m_1 ein Teiler von m,

$$m = m_1 m_2,$$

und folglich Ω_{m_1} ein Teiler von Ω_m. Es sei ferner p eine Primzahl $\equiv 1 \pmod{m_1}$ und teilerfremd zu m. Diese Primzahl zerfällt im Körper Ω_{m_1} in $\varphi(m_1)$ von einander verschiedene Primideale, die wir mit $\mathfrak{P}_{n_1}$ bezeichnen, wobei n_1 ein vollständiges System zu m_1 teilerfremder Zahlen durchläuft; setzen wir $r^{m_2} = r_1$, so geht $\mathfrak{P}_{n_1}$ aus $\mathfrak{P}_1$ hervor durch die Substitution $(r_1, r_1^{n_1})$. Die Ideale $\mathfrak{o}\mathfrak{P}_{n_1}$ sind nun Ideale im Körper Ω_m, welche der Bedingung genügen

$$\mathfrak{o}\Pi\mathfrak{P}_{n_1} = \mathfrak{o}p,$$

und die daher keine anderen idealen Primfactoren enthalten können als die Primfactoren $\mathfrak{p}_n$ von p in Ω_m und die zusammen alle $\mathfrak{p}_n$ und jeden nur einmal enthalten. Wenn $\mathfrak{p}_1$ in $\mathfrak{o}\mathfrak{P}_1$ aufgeht, so geht $\mathfrak{p}_n$ in $\mathfrak{o}\mathfrak{P}_n$ auf; da aber $\mathfrak{P}_n$ ungeändert bleibt, wenn sich der Index um Vielfache von m_1 ändert, so folgt die Zerlegung

$$\mathfrak{o}\mathfrak{P}_1 = \overset{s}{\Pi}\mathfrak{p}_{1+sm_1}, \qquad \mathfrak{o}\mathfrak{P}_{n_1} = \overset{s}{\Pi}\mathfrak{p}_{n_1+sm_1},$$

---

keine niedrigere Potenz von a stattfinden, weil $m = \overset{s}{\underset{1, m-1}{\Pi}}(1 - r^s)$, also keiner von den Factoren $(1 - r^s)$ durch $\mathfrak{p}$ teilbar sein kann.

worin sich die Producte nach s nur soweit zu erstrecken haben, als sie von einander verschiedene Ideale $\mathfrak{p}_n$ liefern.

8. Ist m eine Potenz einer *ungeraden Primzahl* q, und ist $m_1 > 1$ der *grösste gemeinschaftliche* Teiler von $p - 1$ und m, so ist

$$p^{m_2} \equiv 1 \pmod{m}$$

und m_2 ist die niedrigste Potenz von p welche dieser Bedingung genügt, so dass in der Reihe

$$1, p, p^2, \ldots, p^{m_2-1}$$

sämmtliche Zahlen von der Form $1 + sm_1$, $s = 0, 1, \ldots, m_2 - 1$, und, nach dem Modul m reduciert, jede nur einmal, enthalten sind. Es zerfällt also nach n° 4 p im Körper Ω_{m_1} und im Körper Ω_m in gleichviel Idealfactoren und es ist daher

$$\mathfrak{o}\mathfrak{P}_1 = \mathfrak{p}_1, \qquad \mathfrak{o}\mathfrak{P}_{n_1} = \mathfrak{p}_{n_1}.$$

Ist $q = 2$, so gilt dasselbe nur unter der Voraussetzung dass $m_1 \gtreqless 4$ ist; für $m_1 = 2$ würde der Körper Ω_{m_1} mit dem der rationalen Zahlen zusammenfallen.[1]

§ 8. *Das Kummer'sche Theorem.*

Es sei jetzt p wie oben eine Primzahl $\equiv 1 \pmod{m}$, r eine m^{te}, r_1 eine p^{te} Einheitswurzel, und g eine primitive Congruenzwurzel von p, welche als Basis eines Systems von Indices genommen wird. Setzen wir in den Ausdrücken (2), § 6, r_1 an Stelle von r und r an Stelle von ω^h, so gehen dieselben über in

$$(1) \qquad (r, r_1) = (r, \eta) = \sum_{\nu}^{\nu} r^{\operatorname{ind}_\nu} r_1^\nu,$$

ein Ausdruck, der nur von den m Perioden

$$(2) \qquad \eta_\nu = r_1^\nu + r_1^{\nu g^m} + \ldots + r_1^{\nu g^{p-1-m}}$$

[1] Diese Sätze sind ganz specielle Fälle einer allgemeinen Untersuchung von DEDEKIND über die Ideale in den Divisoren eines Normalkörpers, deren baldige Veröffentlichung sehr dankenswert wäre. Vgl. auch DEDEKIND: *Sur la théorie des nombres entiers algébriques,* § 27 (Bulletin des sciences mathématiques 1877); Comptes rendus der Pariser Akademie vom 24ten Mai 1880.

abhängig ist. Ersetzt man in demselben r_1 durch r_1^ν, so folgt:

$$(r,\ \eta_\nu) = r^{-\mathrm{ind}\,\nu}(r,\ \eta), \tag{3}$$

woraus hervorgeht, dass

$$(r,\ \eta)^m, \qquad (r^n,\ \eta)(r,\ \eta)^{m-n}, \qquad (r^a,\ \eta)^{a'}(r^b,\ \eta)^{b'}\ldots \tag{4}$$

ganze Zahlen des Körpers Ω_m sind, wenn a, a', b, b', ... ganze positive der Bedingung $aa' + bb' + \ldots \equiv 0 \pmod m$ genügende Zahlen bedeuten.

Aus der Formel (5), § 6

$$(r^n,\ \eta)(r^{-n},\ \eta) = \pm p \tag{5}$$

folgt, dass in den Zahlen $(r^n,\ \eta)^m$ keine anderen Primideale aufgehen als solche, die auch in p enthalten sind, und es ist eine schöne und wichtige Entdeckung von KUMMER,[1] dass die Zerlegung dieser Zahlen in ihre Primfactoren vollständig durchgeführt werden kann. Da diese Zerlegung für unsere Aufgabe von der grössten Bedeutung ist, so soll dieselbe hier reproduciert werden.

Multipliciert man die Gleichung (3) mit $r^{(s+1)\,\mathrm{ind}\,\nu} r_1^\nu$ und nimmt die Summe über alle positiven ν, die kleiner als p sind, so folgt wegen (1)

$$(r^s,\ \eta)(r,\ \eta) = \sum_{1,\,p-1}^{\nu,\,\nu'} r^{(s+1)\,\mathrm{ind}\,\nu + \mathrm{ind}\,\nu'} r_1^{\nu(\nu'+1)}; \tag{6}$$

für $\nu' = p - 1$ verschwindet die nach ν genommene Summe, falls, wie vorausgesetzt sein soll, r eine *primitive* m^{te} Einheitswurzel und $s + 1$ durch m nicht teilbar ist. Wir können daher die linke Seite von (6) nach (3) so schreiben:

$$\sum_{1,\,p-2}^{\nu'} r^{\mathrm{ind}\,\nu'}(r^{s+1},\ \eta_{\nu'+1}) = (r^{s+1},\ \eta) \sum_{1,\,p-2}^{\nu} r^{\mathrm{ind}\,\nu - (s+1)\,\mathrm{ind}\,(\nu+1)},$$

und erhalten also:

$$\frac{(r^s,\ \eta)(r,\ \eta)}{(r^{1+s},\ \eta)} = \sum_{1,\,p-2}^{\nu} r^{\mathrm{ind}\,\nu - (s+1)\,\mathrm{ind}\,(\nu+1)} = \psi_s(r), \tag{7}$$

so dass $\psi_s(r)$ *eine ganze Zahl in* Ω_m ist.

[1] In der oben citirten Abhandlung. Vgl. auch BACHMANN, *die Lehre von d. Kreisteilung,* XIX. Vorlesung.

Wenden wir (7) an auf $s = 1, 2, \ldots, m-2$, so folgt:

$$(r, \eta)(r, \eta) = (r^2, \eta)\psi_1(r),$$
$$(r, \eta)(r^2, \eta) = (r^3, \eta)\psi_2(r),$$
$$(r, \eta)(r^{m-2}, \eta) = (r^{m-1}, \eta)\psi_{m-2}(r),$$

und durch Multiplication

$$(r, \eta)^{m-1} = (r^{-1}, \eta)\psi_1(r)\psi_2(r)\ldots\psi_{m-2}(r),$$

woraus endlich noch mittels (5) folgt:

$$(8) \qquad (r, \eta)^m = \pm p\psi_1(r)\psi_2(r)\ldots\psi_{m-2}(r).$$

Der in (7) enthaltene Ausdruck von ψ_s muss nun noch umgeformt werden. Setzt man

$$(9) \qquad \operatorname{ind}\nu - \operatorname{ind}(1+\nu) \equiv \nu' \pmod{p-1}$$

so durchläuft ν' gleichzeitig mit ν, wenn auch in anderer Ordnung, die Zahlen $1, 2, \ldots, p-2$, da von den Werten der linken Seite von (9) nicht zwei unter einander und keine der Null congruent sind nach dem Modul $p-1$. Es ist dann ferner

$$g^{\nu'} \equiv \nu g^{-\operatorname{ind}(1+\nu)} \pmod{p}$$

oder

$$(1+\nu)g^{\nu'} \equiv \nu \pmod{p}, \qquad (1+\nu)(1-g^{\nu'}) \equiv 1 \pmod{p},$$

also

$$\operatorname{ind}(1+\nu) \equiv -\operatorname{ind}(1-g^{\nu'}) \pmod{p-1},$$

und hiernach lässt sich (7), wenn man wieder ν an Stelle von ν' setzt, so darstellen:

$$(10) \qquad \psi_s(r) = \sum_{1,p-2}^{\nu} r^{\nu + s\operatorname{ind}(1-g^{\nu})}.$$

Ist nun $\mathfrak{p}_n$ eines der in p aufgehenden Primideale und also (nach n° 5 (4) § 7)

$$(11) \qquad r \equiv g^{-n'\frac{p-1}{m}} \pmod{\mathfrak{p}_n}, \qquad nn' \equiv 1 \pmod{m}$$

so folgt aus (10), wenn wir mit

$$(11)\qquad \begin{array}{l} \sigma \text{ den kleinsten positiven Rest von } -sn'\dfrac{p-1}{m} \\ \tau \quad \text{» \quad » \quad » \quad » \quad » \quad } n'\dfrac{p-1}{m} \end{array} \quad [\mathrm{mod}\,(p-1)]$$

bezeichnen, so dass σ, so lange $s+1<m$ ist, niemals $=\tau$ sein kann,

$$(12)\qquad \psi_s \equiv \sum_{0,\,p-2}^{\nu} g^{-\nu\tau}(1-g^{\nu})^{\sigma} \pmod{\mathfrak{p}_n},$$

wobei das dem $\nu=0$ entsprechende Glied als verschwindend beigefügt werden kann. Entwickelt man diese Formel nach dem binomischen Satze, so ergiebt sich

$$(13)\qquad \psi_s \equiv \sum_{0,\,p-2}^{\nu}\sum_{0,\,\sigma}^{\nu'} (-1)^{\nu'}\frac{\Pi(\sigma)}{\Pi(\nu')\,\Pi(\sigma-\nu')}g^{\nu(\nu'-\tau)} \pmod{\mathfrak{p}_n}.$$

Nun ist die nach ν genommene Summe nach dem Modul p mit 0 congruent, wenn ν' nicht $=\tau$ ist, und mit -1 für $\nu'=\tau$, und daraus folgt:

$$(14)\qquad \begin{array}{ll} \psi_s \equiv 0 \pmod{\mathfrak{p}_n}, & \sigma<\tau \\ \psi_s \equiv (-1)^{\tau+1}\dfrac{\Pi(\sigma)}{\Pi(\tau)\,\Pi(\sigma-\tau)} \pmod{\mathfrak{p}_n}, & \sigma>\tau, \end{array}$$

im letzteren Fall also ψ_s *nicht* durch $\mathfrak{p}_n$ teilbar. Ist $n+n_1\equiv 0 \pmod m$, so ist $\sigma+\sigma_1\equiv\tau+\tau_1\equiv 0\ [\mathrm{mod}\,(p-1)]$ also $(\sigma-\tau)+(\sigma_1-\tau_1)=0$, so dass also ψ_s von zweien Idealen $\mathfrak{p}_n$, $\mathfrak{p}_{-n}$ immer *durch eines* und *nur durch eines* teilbar ist.

Da ferner aus (7) mittels (5) hervorgeht

$$(15)\qquad \psi_s(r)\psi_s(r^{-1}) = p,$$

so folgt, dass $\psi_s(r)$ nicht durch das Quadrat eines Primideals teilbar ist.

Hiernach findet sich leicht die Zerlegung von

$$(r,\ \eta)^m = \pm p\psi_1(r)\psi_2(r)\ldots\psi_{m-2}(r),$$

indem man abzählt, wie oft ein Primideal $\mathfrak{p}_n$ in dem Product auf der rechten Seite vorkommt.

Verstehen wir unter t, t' die *kleinsten positiven Reste* von n, n' nach dem Modul m, so ist

$$\tau = t^{\frac{p-1}{m}}$$

und die kleinsten positiven Reste von $-n'$, $-2n'$, $\ldots$, $-(m-2)n'$ nach dem Modul m sind

$$1, \quad 2, \quad t'-1, \quad t'+1, \quad \ldots, \quad m-1.$$

Unter diesen sind $t'-1$, welche kleiner als t' sind, und ebenso oft kommt also $\mathfrak{p}_t$ in $\psi_1\psi_2\ldots\psi_{m-2}$ vor. Dazu kommt noch einmal der Factor $\mathfrak{p}_t$ in p, und daher:

$$\mathfrak{o}(r, \eta)^m = \prod^{t} \mathfrak{p}_t^{t'}, \tag{16}$$

worin t' die *kleinste positive* Zahl ist, welche der Bedingung

$$tt' \equiv 1 \pmod{m} \tag{17}$$

genügt, wodurch die gesuchte Zerlegung gefunden ist. Wir bemerken zu derselben nur noch, dass man über die Einheitswurzel r oder über g so verfügen kann, dass unter den conjugierten Factoren von p jeder beliebige an die Stelle von $\mathfrak{p}_1$ tritt, wie aus § 7, n° 5 sofort hervorgeht.

Der hierdurch bewiesene Satz ist namentlich deshalb von Wichtigkeit, weil er ganz allgemein ausser der Primzahl p selbst gewisse Combinationen der conjugierten Primideale $\mathfrak{p}_n$ kennen lehrt, welche *Hauptideale* sind.

§ 9. *Von den Einheiten im Körper Ω_m.*

Wir schliessen diese Betrachtungen mit dem Beweis zweier Sätze über die Einheiten in den vollständigen Kreiskörpern, welche ebenfalls, wenigstens für den Fall dass die Ordnung des Körpers eine Primzahl ist, von KUMMER bewiesen sind.[1]

---

[1] Vgl. KUMMER: *Bestimmung der Anzahl nicht aequivalenter Classen für die aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben. Zwei besondere Untersuchungen über die Classenanzahl und über die Einheiten der aus λ^{ten}*

1. Ist $\mathfrak{E}(r)$ eine ganze Zahl des Körpers Ω_m, welche der Bedingung genügt

$$\mathfrak{E}(r)\mathfrak{E}(r^{-1}) = 1, \tag{1}$$

so ist notwendig

$$\mathfrak{E}(r) = \pm r^{\nu} \tag{2}$$

worin ν ein ganzzahliger Exponent ist. In Folge der Formel (1) ist nämlich $\mathfrak{E}(r)$ eine *reducierte Einheit* des Körpers Ω_m und mithin eine Einheitswurzel (vgl. *D.*, § 177, S. 566). Ist also $\mathfrak{E}(r) = \pm \rho$, so muss der aus ρ entspringende vollständige Kreiskörper ein Teiler von Ω_m sein, und folglich muss ρ eine Potenz von r sein. (§ 4, n° 1.)

2. Ist $m = q^k$ eine Primzahlpotenz, so ist jede Einheit $\mathfrak{E}(r)$ des Körpers Ω_m in der Form darstellbar

$$\mathfrak{E}(r) = r^{\nu} e(r) \tag{3}$$

worin $e(r)$ eine *reelle* Einheit, d. h. eine Einheit ist, welche der Bedingung

$$e(r) = e(r^{-1}) \tag{4}$$

genügt, und folglich nur von den zweigliedrigen Perioden

$$r + r^{-1}$$

abhängt. Um dies zu beweisen, wenden wir den Satz n° 1 auf den Quotienten $\mathfrak{E}(r):\mathfrak{E}(r^{-1})$ an, wodurch sich ergiebt:

$$\mathfrak{E}(r) = \pm r^{\nu}\mathfrak{E}(r^{-1}). \tag{5}$$

a) Ist zunächst q ungerade, so kann ν gerade angenommen werden, da man ν eventuell durch $\nu + m$ ersetzen kann, und es lässt sich zeigen, dass in (5) das untere Zeichen unzulässig ist; denn nach § 7, n° 6 ist $\mathfrak{v}(1 - r)$ ein in q aufgehendes Primideal, und aus (5) folgt

$$\mathfrak{E}(r) \equiv \mathfrak{E}(1) \equiv \pm \mathfrak{E}(1) \pmod{\mathfrak{v}(1 - r)},$$

Wurzeln der Einheit gebildeten complexen Zahlen, beide in Crelle's Journal, Bd. 40. *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers*, Journal de Liouville, T. XVI.

woraus für das untere Zeichen folgen würde

$$\mathfrak{E}(r) \equiv 0 \pmod{\mathfrak{o}(1-r)}.$$

Es könnte also $\mathfrak{E}(r)$ keine Einheit sein; also hat

$$\varepsilon(r) = r^{-\frac{1}{2}\nu}\mathfrak{E}(r) \tag{6}$$

die in (4) verlangte Eigenschaft.

b) Ist $q = 2$, so ist $r^{\frac{1}{2}m} = -1$, und man kann daher (5) in der Form schreiben

$$\mathfrak{E}(r) = r^{\nu}\mathfrak{E}(r^{-1}). \tag{7}$$

Es ist jetzt zu zeigen, dass ν gerade sein muss. Wäre ν ungerade, so würde aus (7) durch Vertauschung von r mit $-r$ folgen

$$\frac{\mathfrak{E}(r)}{\mathfrak{E}(-r)} = -\frac{\mathfrak{E}(r^{-1})}{\mathfrak{E}(-r^{-1})} = \varepsilon(r) = -\varepsilon(r^{-1}).$$

Die Einheit $\varepsilon(r)$ würde sich also als lineare und homogene Function von

$$(r - r^{-1}),\ (r^2 - r^{-2}),\ \ldots,\ \left(r^{\frac{1}{2}m} - r^{-\frac{1}{2}m}\right)$$

mit ganzzahligen Coefficienten darstellen lassen. (§ 7, n° 1.) Es wäre also

$$\varepsilon(r) \equiv \varepsilon(1) \equiv 0 \pmod{\mathfrak{o}(1-r)}$$

was dem Begriff der Einheit widerspricht. Setzt man daher

$$r^{-\frac{1}{2}\nu}\mathfrak{E}(r) = \varepsilon(r) \tag{8}$$

so genügt diese Zahl der in (4) gestellten Forderung.

Ist m eine zusammengesetzte Zahl, so findet der in n° 2 ausgesprochene Satz nicht mehr statt.

3. Ist m wieder eine Potenz von 2, so findet sich unter den mit r conjugierten Zahlen auch $-r$. Eine Zahl, die durch die Substitution $(r, -r)$ ungeändert bleibt, gehört dem Körper $\Omega_{\frac{m}{2}}$ an, während eine Zahl, welche durch diese Substitution ihr Zeichen ändert, durch Multiplication mit r in eine Zahl des Körpers $\Omega_{\frac{m}{2}}$ verwandelt wird. Es lässt sich

nun auf dem in b) eingeschlagenen Wege beweisen, dass bei einer reellen Einheit dieser letztere Fall nicht eintreten kann, dass also eine Einheit $\mathfrak{E}(r)$ des Körpers Ω_m nicht gleichzeitig die beiden Bedingungen

$$\mathfrak{E}(r) = \mathfrak{E}(r^{-1}), \qquad \mathfrak{E}(r) = -\mathfrak{E}(-r)$$

erfüllen kann; denn es würde eine solche Function linear und homogen mit ganzzahligen Coëfficienten darstellbar sein durch

$$(r + r^{-1}),\ (r^3 + r^{-3}),\ (r^5 + r^{-5}),\ \ldots$$

und folglich wäre

$$\mathfrak{E}(r) \equiv \mathfrak{E}(1) \equiv \mathfrak{E}(-1) \equiv 0 \pmod{\mathfrak{v}(1 - r)}$$

was bei einer Einheit nicht möglich ist.

II. ÜBER DIE ANZAHL DER IDEALCLASSEN UND DIE EINHEITEN IN DEN KREISKÖRPERN, DEREN ORDNUNG EINE POTENZ VON 2 IST.

In den grundlegenden Arbeiten über die idealen Primfactoren der complexen Zahlen hat KUMMER die Anzahl der Idealclassen in den Kreiskörpern von Primzahlordnung bestimmt.

In der vorliegenden Arbeit soll nach denselben Principien eine Untersuchung über die Anzahl der Idealclassen durchgeführt werden für den einfachsten Fall, in welchem die Ordnung eine zusammengesetzte Zahl ist, nämlich eine Potenz von 2, welche für die spätere Anwendung auf die Theorie der Abel'schen Körper notwendig ist, wohl aber auch einiges selbständige Interesse beanspruchen kann. Die vorhergehende Abhandlung *über Abel'sche Körper und Kreiskörper* soll mit I citiert werden.

§ 1. *Erster Ausdruck für die Anzahl der Idealclassen.*

Es sei λ eine positive ganze Zahl, grösser als 2, und wir setzen

$$(1) \qquad m = 2^\lambda, \qquad \nu = 2^{\lambda-2}, \qquad \mu = 2^{\lambda-3}, \qquad \varphi(m) = 2^{\lambda-1}.$$

Es sei r eine primitive m^{te} Einheitswurzel, also eine Wurzel der irreducibeln Gleichung

$$(2) \qquad x^{2^{\lambda-1}} + 1 = 0$$

und Ω_m oder Ω_λ oder kurz Ω der vollständige Kreiskörper der Ordnung m.

Bezeichnen wir mit $\mathfrak{a}$ die sämmtlichen Ideale des Körpers Ω, mit $N(\mathfrak{a})$ ihre Normen, so hängt die Bestimmung der Anzahl h der Idealclassen des Körpers Ω ab von der Bestimmung des Grenzwertes

$$(3) \qquad \lim_{s=1}(s-1)\sum \frac{1}{N(\mathfrak{a})^s} = gh,$$

worin g ein Zahlenfactor ist, dessen Definition und Bestimmung weiter unten zur Sprache kommen wird.

Die in (3) vorkommende Summe lässt sich zunächst in ein unendliches Product umwandeln, welches auf alle Primideale $\mathfrak{p}$ des Körpers Ω erstreckt ist[1]

$$(4) \qquad \sum \frac{1}{N(\mathfrak{a})^s} = \prod \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

Nun ist (vgl. I, § 7, n° 4, n° 6) unter den Idealen $\mathfrak{p}$ zunächst enthalten das Hauptideal $\mathfrak{o}(1-r)$, dessen Norm $= 2$ ist. Wenn ferner p eine Primzahl ist, welche $(\mathrm{mod}\, m)$ zum Exponenten 2^k gehört $(k \lesseqgtr \lambda - 2)$, so zerfällt $\mathfrak{o}p$ in $2^{\lambda-k-1}$ verschiedene Primideale vom Grade 2^k, deren Norm also $= p^{2^k}$ ist. Demnach wird

$$(5) \qquad \sum \frac{1}{N(\mathfrak{a})^s} = \frac{1}{1-2^{-s}} \prod \frac{1}{(1-p^{-s2^k})^{2^{\lambda-k-1}}},$$

worin das Product $\prod$ sich auf alle *ungeraden* Primzahlen p erstreckt.

[1] Vgl. *D.*, S. 578 f.

Wir betrachten nun die Gruppe N der nach dem Modul m genommenen *ungeraden Zahlen* n, deren Grad $2^{\lambda-1}$ ist, und ihre Charaktere $\chi(n)$. Ist n eine zum Exponenten 2^k gehörige Zahl, so bilden die Potenzen von n einen Divisor von N vom Grade 2^k, und unter den Charakteren χ giebt es (I, § 3, n° 3) genau $2^{\lambda-k-1}$ welche der Bedingnng

$$\chi(n) = 1$$

genügen. Die sämmtlichen Charaktere χ zerfallen also in 2^k Reihen, deren jede nur solche χ enthält, für welche $\chi(n)$ einen und denselben Wert hat, während dieser Wert für die verschiedenen Reihen verschieden ist. Da überdies alle $\chi(n)$ (wegen $n^{2^k} \equiv 1 \pmod m$) $2^{k\text{te}}$ Einheitswurzeln sind, so folgt:

Unter den $2^{\lambda-1}$ *Werten* $\chi(n)$ *kommt jede* $2^{k\text{te}}$ *Einheitswurzel und jede genau* $2^{\lambda-k-1}$ *mal vor.* Dies Resultat können wir auch, wenn x eine beliebige Variable bedeutet, so schreiben:

$$(6) \qquad (1 - x^{2^k})^{2^{\lambda-k-1}} = \prod^{\chi}[1 - \chi(n)x],$$

worin das Product sich auf alle Charaktere χ erstreckt, und n eine beliebige zum Exponenten 2^k gehörige Zahl bedeutet. Setzen wir $x = p^{-s}$ und $n = p$, so nimmt hiernach die Formel (5) die Gestalt an:

$$(7) \qquad \sum \frac{1}{N(\mathfrak{a})^s} = \frac{1}{1 - 2^{-s}} \prod^{p} \prod^{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Entwickelt man, ähnlich wie in (5) die einzelnen Factoren auf der rechten Seite von (7) nach Potenzen von p^{-s} und vereinigt dieselben dann durch Multiplication, so folgt wie dort

$$(8) \qquad \sum \frac{1}{N(\mathfrak{a})^s} = \frac{1}{1 - 2^{-s}} \prod^{\chi} \sum^{n} \frac{\chi(n)}{n^s},$$

worin jetzt die Summen rechts auf alle ungeraden Zahlen n und das Product auf alle Charactere χ zu erstrecken ist.

Setzt man dies in (3) ein, so kann der Grenzübergang ausgeführt werden; es ist nämlich

$$(9) \qquad \lim_{s=1} \frac{s-1}{1 - 2^{-s}} \sum \frac{1}{n^s} = 1,$$

$$(10) \qquad \lim_{s=1} \sum \frac{\chi(n)}{n^s} = \sum \frac{\chi(n)}{n},$$

wenn in (10) der Hauptcharakter ausgeschlossen wird und rechts die unendlichen Reihen nach der Grössenfolge der Zahlen n angeordnet sind. (*D.*, § 110, 117.) Demnach ergiebt sich aus (3), wenn in dem Product Π jetzt der *Hauptcharakter ausgeschlossen wird*

$$gh = \overset{\chi}{\Pi}\Sigma\frac{\chi(n)}{n}. \tag{11}$$

§ 2. *Fortsetzung.*

Nach I, § 5, n° 1 erhält man die Charaktere $\chi(n)$ folgender Maassen. Es seien α, β die Indices von n, also:

$$(-1)^{\alpha}5^{\beta} \equiv n \pmod{2^{\lambda}}, \qquad \alpha \pmod 2, \qquad \beta \pmod{2^{\lambda-2}} \tag{1}$$

und es sei $\varepsilon = \pm 1$, θ eine *beliebige* $2^{\lambda-2\,\text{te}}$ Einheitswurzel, so hat man in (11) des vorigen Paragraphs alle Ausdrücke von der Form zu setzen

$$\chi(n) = \varepsilon^{\alpha}\theta^{\beta} \tag{2}$$

mit alleiniger Ausnahme von $\varepsilon = +1$, $\theta = +1$.

Die in (11) auftretenden Summen zerfallen dann, je nach den Werten von θ, ε in verschiedene Classen. Setzen wir nämlich, wenn θ sämmtliche *primitive* $2^{\lambda-2\,\text{te}}$ Einheitswurzeln durchläuft

$$\begin{aligned} P_{\lambda} &= \overset{\theta}{\Pi}\Sigma\frac{\chi(n)}{n}, \qquad \varepsilon = +1, \\ Q_{\lambda} &= \overset{\theta}{\Pi}\Sigma\frac{\chi(n)}{n}, \qquad \varepsilon = -1, \end{aligned} \tag{3}$$

so erhält man, da die Indices für den Modul 2^{k} denen für den Modul 2^{λ}, falls $k < \lambda$ ist, nach den Modul 2^{k} congruent sind, die sämmtlichen in (11) vorkommenden Factoren, wenn man in P_{λ} 3, 4, ..., λ, und in Q_{λ} 2, 3, 4, ..., λ für λ setzt. Demnach wird

$$gh = Q_2 P_3 Q_3 P_4 Q_4 \ldots P_{\lambda} Q_{\lambda}. \tag{4}$$

Für Q_2 erhält man direct den Wert

$$Q_2 = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \frac{\pi}{4}. \tag{5}$$

und wir können daher bei der ferneren Berechnung von P_λ, Q_λ stets $\lambda \geqq 3$ voraussetzen.

Um die Summen P_λ, Q_λ zu bestimmen, setzen wir (*D.*, Seite 596)

$$\sum_t \chi(t) x^t = f(x), \tag{6}$$

worin t *alle ungeraden Zahlen die kleiner als* m sind, durchläuft, so dass, da

$$\chi(t + 2^{\lambda-1}) = -\chi(t)$$

$f(x)$ verschwindet, sobald für x eine nicht primitive m^{te} Einheitswurzel oder Null gesetzt wird. Dann ergiebt sich

$$\sum \frac{\chi(n)}{n} = \int_0^1 \frac{f(x)dx}{x(1-x^m)} = -\frac{1}{m} \sum_t f(r^t) \log(1 - r^{-t}), \tag{7}$$

worin die Logarithmen so zu nehmen sind, dass ihre imaginären Bestandteile in dem Intervall $\pm \frac{\pi}{2} i$ liegen.

Nun ist aber nach der in I, § 6, (9) eingeführten Bezeichnung

$$f(r) = \sum_t \varepsilon^\alpha \theta^\beta r^t = (\varepsilon, \theta, r), \tag{8}$$

worin α, β die Indices von t sind, und also (I, § 6, (10))

$$f(r^t) = \varepsilon^{-\alpha} \theta^{-\beta} f(r), \tag{9}$$

und folglich

$$\sum \frac{\chi(n)}{n} = -\frac{1}{m} (\varepsilon, \theta, r) \sum_t \varepsilon^{-\alpha} \theta^{-\beta} \log(1 - r^{-t}). \tag{10}$$

Diese Formel gilt auch noch für $\lambda = 2$ und giebt wie oben

$$Q_2 = \frac{\pi}{4}. \tag{11}$$

Ferner ergiebt sich aus (10) für $\lambda = 3$

$$Q_3 = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \frac{1}{11} - \ldots = \frac{\pi}{2\sqrt{2}} \tag{12}$$

$$P_3 = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \ldots = \frac{1}{2\sqrt{2}} \log \frac{\sqrt{2}+1}{\sqrt{2}-1} = \frac{1}{\sqrt{2}} \log(\sqrt{2}+1). \tag{13}$$

Ist $\lambda > 3$, so kommen die Factoren in den Producten P_λ, Q_λ stets paarweise vor, so dass zwei Factoren, welche den Werten θ, θ^{-1} in χ entsprechen, ein Paar bilden, und bei der Berechnung dieser Paare hat man die in I, § 6, (11) bewiesene Formel

$$(\varepsilon,\ \theta,\ r)(\varepsilon,\ \theta^{-1},\ r) = \varepsilon m \tag{14}$$

zu benutzen.

§ 3. *Bestimmung der Factoren* Q_λ.

Die Berechnung der P_λ und Q_λ, $(\lambda \gtreqless 4)$ gestaltet sich verschieden. Wir beginnen mit Q_λ, und setzen zur Vereinfachung

$$\varphi(\theta) = \frac{-m}{2\pi i}\sum^{t}(-1)^{\alpha}\theta^{-\beta}\log(1-r^{-t}), \tag{1}$$

so dass nach (3), (10), (14) § 2:

$$Q_\lambda = \frac{(2\pi)^{\mu}}{m^{3\cdot 2^{\lambda-4}}}\prod^{\theta}\varphi(\theta). \tag{2}$$

Um $\varphi(\theta)$ zu berechnen, bemerken wir, dass durch die Vertauschung von t mit $m-t$, der Index α in $\alpha+1$ übergeht, während β ungeändert bleibt, und daher erhält man für $\varphi(\theta)$ auch

$$\varphi(\theta) = \frac{m}{2\pi i}\sum^{t}(-1)^{\alpha}\theta^{-\beta}\log(1-r^{t}), \tag{3}$$

und durch Addition beider Ausdrücke

$$\varphi(\theta) = \frac{m}{4\pi i}\sum^{t}(-1)^{\alpha}\theta^{-\beta}\log(-r^{t}), \tag{4}$$

worin der nunmehr rein imaginäre Logarithmus in dem Intervall $\pm\pi i$ liegt. Wir können also setzen

$$\begin{aligned} -r^{t} &= e^{\pi i\left(\frac{2t}{m}-1\right)} \\ \log(-r^{t}) &= \pi i\left(\frac{2t}{m}-1\right), \end{aligned} \tag{5}$$

und t ist alsdann, wie oben, der *kleinste positive Rest* von

$$(-1)^{\alpha} 5^{\beta} \pmod{m}.$$

Dann wird, da $\Sigma(-1)^{\alpha}\theta^{-\beta}$ verschwindet:

$$\varphi(\theta) = \frac{1}{2}\sum^{t}(-1)^{\alpha}\theta^{-\beta}t. \tag{6}$$

Zwei Werte von t, welche demselben β, aber verschiedenen Werten von α entsprechen, ergänzen einander zu m, und da auch $\Sigma\theta^{\beta}$ verschwindet, so ist

$$\varphi(\theta) = \sum_{0,\nu-1}^{\beta}\theta^{-\beta}t, \tag{7}$$

wenn t den kleinsten positiven Rest von $5^{\beta} \pmod{m}$ bedeutet. Der Ausdruck (7) lässt sich aber noch weiter vereinfachen. Es ist nämlich

$$\varphi(\theta) = \sum_{0,\mu-1}^{\beta}\theta^{-\beta}t + \sum_{\mu,\nu-1}^{\beta}\theta^{-\beta}t. \tag{8}$$

Setzt man in der letzten Summe $\beta + \mu$ an Stelle von β und bezeichnen den *kleinsten positiven* Rest von $5^{\beta+\mu} \pmod{m}$ mit t_1, so folgt, da $\theta^{\mu} = -1$ ist:

$$\varphi(\theta) = \sum_{0,\mu-1}^{\beta}\theta^{-\beta}(t - t_1). \tag{9}$$

Es ist darin

$$t_1 - t \equiv 5^{\beta}(5^{\mu} - 1) \pmod{m}, \tag{10}$$

also $t_1 \equiv t$ nach dem Modul $2^{\lambda-1}$, aber nicht nach dem Modul 2^{λ}. Es ist daher

$$t = t_1 + \varepsilon_{\beta}2^{\lambda-1} \tag{11}$$

und $\varepsilon_{\beta} = \pm 1$, je nachdem $t \gtrless 2^{\lambda-1}$ ist, da sowohl t als t_1 positiv und kleiner als m sind.

Wir erhalten also nach (9)

$$\varphi(\theta^{-1}) = 2^{\lambda-1}(\varepsilon_0 + \varepsilon_1\theta + \ldots + \varepsilon_{\mu-1}\theta^{\mu-1}), \tag{12}$$

und

$$(13)\quad (1-\theta)\varphi(\theta^{-1}) = m\left(\frac{\varepsilon_0+\varepsilon_{\mu-1}}{2}+\frac{\varepsilon_1-\varepsilon_0}{2}\theta+\ldots+\frac{\varepsilon_{\mu-1}-\varepsilon_{\mu-2}}{2}\theta^{\mu-1}\right).$$

Der Ausdruck

$$(14)\qquad \psi(\theta) = \frac{\varepsilon_0+\varepsilon_{\mu-1}}{2}+\frac{\varepsilon_1-\varepsilon_0}{2}\theta+\ldots+\frac{\varepsilon_{\mu-1}-\varepsilon_{\mu-2}}{2}\theta^{\mu-1}$$

ist nun eine *ganze Zahl* des Körpers $\Omega_{\lambda-2}$, und es ist, wenn die Normen

$$(15)\qquad N_{\lambda-2}\psi(\theta) = a_\lambda, \qquad N_{\lambda-2}(1-\theta) = 2$$

sich auf diesen Körper beziehen, nach (2)

$$(16)\qquad Q_\lambda = \frac{\pi^\mu a_\lambda}{2\nu^{2^{\lambda-4}}}.$$

Es ist aber

$$(17)\qquad \psi(\theta) \equiv \varepsilon_{\mu-1} \equiv \pm 1 \ [\mathrm{mod}\,(1-\theta)],$$

folglich $\psi(\theta)$ nicht durch $(1-\theta)$ teilbar; also auch die Norm von $\psi(\theta)$ nicht teilbar durch 2, woraus folgt, dass a_λ *eine ungerade ganze Zahl* ist; diese Zahl lässt sich für die ersten Fälle verhältnissmässig leicht aus (14) und (15) berechnen; man findet so z. B.

$$a_4 = 1, \qquad a_5 = 1, \qquad a_6 = 17, \qquad a_7 = 21121.$$

§ 4. *Bestimmung der Factoren* P_λ.

Um P_λ zu finden, fassen wir in der Summe auf der rechten Seite von (10) § 2, je vier Glieder zusammen, welche einem Wertpaar β und $\beta+\mu$ entsprechen und erhalten, da $\theta^\mu = -1$ ist, und da in dem Product θ mit θ^{-1} vertauscht werden kann, nach § 2, (3), (10), (14)

$$(1)\qquad P_\lambda = \frac{1}{m^{2^{\lambda-4}}}\prod_{0,\mu-1}^{\theta}\sum^{\beta}\theta^\beta \log\frac{(1-r^n)(1-r^{-n})}{(1+r^n)(1+r^{-n})},$$

worin $n \equiv 5^\beta \pmod m$. (Es ist hier n für t geschrieben, um anzudeuten dass es auf ein Vielfaches von m nicht ankommt.)

Die unter dem Logarithmus auftretenden Quotienten $(1 - r^n):(1 + r^n)$ sind *Einheiten* des Körpers Ω_λ, die sich nach I, § 9, von einer Einheitswurzel abgesehen, durch die zweigliedrigen Perioden $r + r^{-1}$ ausdrücken lassen. In der That ist, wenn man

$$r = e^{\frac{2\pi i}{m}} \tag{2}$$

setzt:

$$\frac{1 - r^n}{1 + r^n} = r^{-\nu n}\frac{r^{(1-\nu)n} + r^{-(1-\nu)n}}{2 + r^n + r^{-n}} = r^{-\nu n}(-1)^{\frac{n-1}{2}} \operatorname{tg}\frac{n\pi}{m}, \tag{3}$$

und wir wollen nunmehr die folgende Bezeichnung einführen:
wird β aus einer der beiden Congruenzen

$$n \equiv \pm 5^\beta \pmod m \tag{4}$$

bestimmt, so sei

$$\tau_\beta = r^{\nu n}\frac{1 - r^n}{1 + r^n} = (-1)^{\frac{n-1}{2}} \operatorname{tg}\frac{n\pi}{m} = \operatorname{tg}\left(5^\beta \frac{\pi}{m}\right). \tag{5}$$

Die Functionen τ_β bilden ein System von ν *reellen* Einheiten des Körpers Ω_λ, welche durch die Substitution (r, r^{-1}) ungeändert bleiben, und durch die Substitution $(r, r^{n'})$ in $\tau_{\beta+\beta'}$ übergehen, wenn β' von n' so abhängt wie β von n. Ins besondere hat man noch die Relationen (da $5^\mu \equiv 1 + 2^{\lambda-1} \pmod m$)

$$\tau_\beta \tau_{\beta+\mu} = -1. \tag{6}$$

Setzen wir noch

$$\log \tau_\beta^2 = l_\beta, \qquad l_{\beta+\mu} = -l_\beta, \tag{7}$$

so ergiebt sich hiernach aus (1)

$$P_\lambda = m^{-2^{\lambda-4}} \prod_{0,\mu-1}^{\theta} \sum_{}^{\beta} \theta^\beta l_\beta. \tag{8}$$

Das Product der Summen auf der rechten Seite dieses Ausdrucks lässt sich in Form einer Determinante darstellen, welche θ nicht mehr enthält; am einfachsten gelangt man dazu wohl auf folgendem Wege. Man setze

$$x = \sum_{0,\mu-1}^{\beta} \theta^\beta l_\beta \tag{9}$$

und bilde durch Multiplication mit den Potenzen von θ die Gleichungen

$$(10)\qquad \begin{aligned} x &= \quad l_0 \quad + \theta l_1 + \ldots + \theta^{\mu-1} l_{\mu-1} \\ \theta x &= -l_{\mu-1} + \theta l_0 + \ldots + \theta^{\mu-1} l_{\mu-2} \\ &\cdots\cdots\cdots\cdots \\ \theta^{\mu-1} x &= -l_1 \quad - \theta l_2 - \ldots + \theta^{\mu-1} l_0, \end{aligned}$$

und hieraus durch Elimination der Potenzen von θ

$$(11)\qquad \begin{vmatrix} l_0 - x, & l_1 & , \ldots, & l_{\mu-1} \\ -l_{\mu-1} & , & l_0 - x, \ldots, & l_{\mu-2} \\ \cdots & \cdots & \cdots & \cdots \\ -l_1 & , & -l_2 & , \ldots, l_0 - x \end{vmatrix} = 0.$$

Es ist dies eine Gleichung μ^{ten} Grades in Bezug auf x, in welcher die höchste Potenz von x den Coëfficienten 1 hat, deren Wurzeln die μ Factoren des Productes (8) sind. Man erhält daher dies Product, wenn man in vorstehender Determinante $x = 0$ setzt. Ist also

$$(12)\qquad (-1)^{2^{\lambda-4}} \begin{vmatrix} l_0 & , & l_1, \ldots, & l_{\mu-1} \\ l_1 & , & l_2, \ldots, & -l_0 \\ l_2 & , & l_3, \ldots, & -l_1 \\ \cdots & \cdots & \cdots & \cdots \\ l_{\mu-1}, & & -l_0, \ldots, & -l_{\mu-2} \end{vmatrix} = \Delta(\tau_0, \tau_1, \ldots, \tau_{\mu-1}),$$

so ergiebt sich nach einer Umstellung der Reihen, dass das Product der verschiedenen Werte von x in (9), welches als Product paarweise conjugiert imaginärer Grössen wesentlich positiv ist, den Wert Δ erhält. Daraus folgt dann

$$(13)\qquad P_\lambda = m^{-2^{\lambda-4}} \Delta(\tau_0, \tau_1, \ldots, \tau_{\mu-1}).$$

§ 5. *Von den reellen Einheiten des Körpers Ω_λ.*

Wir nehmen jetzt wieder $\lambda \geqq 3$ an und betrachten die *reellen Einheiten* des Körpers Ω_λ d. h. die von den zweigliedrigen Perioden $r + r^{-1}$ abhängigen, also dem Körper

$$\Omega'_\lambda = R(r + r^{-1})$$

angehörigen, da durch diese, multipliciert mit den Potenzen von r nach I, § 9 überhaupt alle Einheiten in Ω_λ erschöpft sind. Es werde ferner, wenn $\mathcal{E}(r)$ eine reelle Einheit in Ω_λ ist, unter $l\mathcal{E}(r)$ der *Logarithmus* von $\mathcal{E}(r)^2$ oder der doppelte *reelle Teil des Logarithmus von* $\mathcal{E}(r)$ verstanden. Wir führen ferner die Bezeichnung ein, wenn r die Bedeutung (2) § 4 hat:

$$r^{\delta^\beta} = r_\beta \tag{1}$$

woraus folgt:

$$r_{\beta+\mu} = -r_\beta; \tag{2}$$

unter einer *primitiven Einheit* des Körpers Ω verstehen wir eine solche reelle Einheit $\mathcal{E}(r)$, welche der Bedingung genügt

$$\mathcal{E}(r)\mathcal{E}(-r) = \pm 1, \qquad l\mathcal{E}(r) + l\mathcal{E}(-r) = 0 \tag{3}$$

und die nicht $= \pm 1$ ist, die also jedenfalls *nicht dem Körper* $\Omega_{\lambda-1}$ *angehört.*

Ein System von μ solchen Einheiten

$$\mathcal{E}_0(r),\ \mathcal{E}_1(r),\ \ldots,\ \mathcal{E}_{\mu-1}(r) \tag{4}$$

heisst ein System von *einander unabhängiger primitiver Einheiten*, wenn für jede derselben die Bedingung (3) erfüllt ist, und wenn die Determinante

$$\Sigma \pm l\mathcal{E}_0(r_0)l\mathcal{E}_1(r_1)\ldots l\mathcal{E}_{\mu-1}(r_{\mu-1}) = L(\mathcal{E}_0,\ \mathcal{E}_1,\ \ldots,\ \mathcal{E}_{\mu-1}) \tag{5}$$

einen von *Null verschiedenen* Wert hat.

Die in § 4, (5) definierten Einheiten $\tau_\beta(r)$ genügen der Bedingung

$$\tau_\beta(r_{\beta'}) = \tau_{\beta+\beta'}(r) \tag{6}$$

und wegen § 4, (6):

$$\tau_\beta(r)\tau_\beta(-r) = -1, \qquad \tau_\beta\tau_{\beta+\mu} = -1. \tag{7}$$

Die Determinante $L(\tau_0, \tau_1, \ldots, \tau_{\mu-1})$ ist von dem Factor $(-1)^{2^{\lambda-4}}$ abgesehen, mit der Determinante (12) § 4 identisch und kann also, als ein Factor der Classenzahl, nicht verschwinden. Die Einheiten

$$\tau_0, \tau_1, \ldots, \tau_{\mu-1} \tag{8}$$

bilden daher ein System unabhängiger primitiver Einheiten, wodurch die Existenz solcher Systeme bewiesen ist. (Für $\lambda = 3$ ergiebt sich dies unmittelbar aus der Betrachtung von $\tau_0(r)$.)

Ist $\mathcal{E}(r)$ eine beliebige *primitive* Einheit in Ω_λ, so lassen sich, da die Determinante (5) von Null verschieden ist, die Zahlen $e_0, e_1, \ldots, e_{\mu-1}$, welche die Exponenten der Einheit $\mathcal{E}(r)$ heissen mögen, so bestimmen, dass für $s = 0, 1, \ldots, \mu - 1$ die Gleichungen bestehen

$$l\mathcal{E}(r_s) = e_0 l\mathcal{E}_0(r_s) + e_1 l\mathcal{E}_1(r_s) + \ldots + e_{\mu-1} l\mathcal{E}_{\mu-1}(r_s) \tag{9}$$

und wegen der Relationen (3) gelten diese Formeln auch noch wenn r_s durch $-r_s$ ersetzt wird, d. h. für die *sämmtlichen conjugierten* Werte r.

Die Exponenten eines Products aus mehreren primitiven Einheiten sind die Summen der entsprechenden Exponenten der einzelnen Factoren.

Es lässt sich nun, ganz so wie (D, Seite 564) in der allgemeinen Theorie der Einheiten, nachweisen, dass *die Zahlen* $e_0, e_1, \ldots, e_{\mu-1}$ *rationale Brüche sind, und dass es eine gewisse von* $\mathcal{E}(r)$ *unabhängige kleinste ganze Zahl* e *giebt, mit welcher die Zahlen* $e_0, e_1, \ldots, e_{\mu-1}$ *multipliciert werden müssen, damit die Producte ganze Zahlen werden.* Wir geben diesem Beweis hier folgende Gestalt.

1. Es giebt in Ω nur eine *endliche Anzahl* ganzer Zahlen ρ, welche die Eigenschaft haben, dass die absoluten Werte sämmtlicher mit ρ conjugierten Zahlen unter einer endlichen Grenze bleiben, denn ist

$$\rho = a_0 + a_1 r + \ldots + a_{\frac{1}{2}m-1} r^{\frac{1}{2}m-1}$$

worin die a *ganze rationale* Zahlen sind, so ergiebt sich, wenn das Zeichen Σ sich auf alle conjugierten Werte bezieht

$$\tfrac{1}{2} m a_0 = \Sigma\rho, \qquad \tfrac{1}{2} m a_1 = \Sigma\rho r^{-1}, \quad \ldots, \quad \tfrac{1}{2} m a_{\frac{1}{2}m-1} = \Sigma\rho r^{1-\frac{1}{2}m},$$

woraus die Richtigkeit der Behauptung unmittelbar erhellt.

2. Lassen wir auf der rechten Seite von (9) die $e_0, e_1, \ldots, e_{\mu-1}$ das Intervall von 0 bis 1 durchlaufen, so bleiben die absoluten Werte dieser Ausdrücke unter bestimmten endlichen Grenzen, also auch die absoluten Werte der dadurch bestimmten $\mathfrak{E}(r_s)$, woraus nach 1. hervorgeht, dass die Exponenten $e_0, e_1, \ldots, e_{\mu-1}$, so lange sie echte Brüche sind, nur eine *endliche Anzahl* von Werten anzunehmen fähig sind.

3. Wir bestimmen die Reihen der ganzen rationalen Zahlen m_i', m_i'', m_i''', ... so dass die Differenzen

$$e_i - m_i', \quad 2e_i - m_i'', \quad 3e_i - m_i''', \quad \ldots \qquad (i=0, 1, \ldots, \mu-1)$$

positive echte Brüche werden. Jedes der Zahlensysteme

$$(10) \qquad ke_0 - m_0^{(k)}, \quad ke_1 - m_1^{(k)}, \quad \ldots, \quad ke_{\mu-1} - m_{\mu-1}^{(k)}$$

bildet dann ein in (9) zulässiges Exponentensystem, und daraus ergiebt sich, dass für einen gewissen Wert $k = e$, der jedenfalls nicht grösser ist als die Anzahl der nach n° 2 zulässigen echt gebrochenen Exponentensysteme, die sämmtlichen Glieder der Reihe (10) verschwinden müssen. Damit aber ist der zu beweisende Satz nachgewiesen. Wir können demselben auch den folgenden Ausdruck geben. Ist

$$\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\mu-1}$$

ein System von einander unabhängiger primitiver Einheiten, so giebt es eine von dieser Basis allein abhängige kleinste ganze Zahl e der Art, dass für *jede* primitive Einheit $\mathfrak{E}$ sich die *ganzen Zahlen* $e_0, e_1, \ldots, e_{\mu-1}$ (die also jetzt eine etwas andere Bedeutung haben als oben) so bestimmen lassen, dass

$$(11) \qquad \mathfrak{E}^e = \pm \mathfrak{E}_0^{e_0} \mathfrak{E}_1^{e_1} \ldots \mathfrak{E}_{\mu-1}^{e_{\mu-1}}.$$

Die Exponenten der Einheit $\mathfrak{E}$ sind alsdann

$$\frac{e_0}{e}, \quad \frac{e_1}{e}, \quad \ldots, \quad \frac{e_{\mu-1}}{e}.$$

§ 6. *Die Einheiten* τ_β.

Wir legen jetzt als unabhängige primitive Einheiten das System $\tau_0, \tau_1, \ldots, \tau_{\mu-1}$ zu Grunde und beweisen zunächst folgenden Satz.

1. *Wenn das Product*

$$\tau_0^{e_0}\tau_1^{e_1}\ldots\tau_{\mu-1}^{e_{\mu-1}} \tag{1}$$

mit allen seinen conjugierten Werten gleiches Vorzeichen hat, so müssen die (ganzzahligen) Exponenten $e_0, e_1, \ldots, e_{\mu-1}$ *sämmtlich gerade sein.* Um diesen Satz zu beweisen formen wir den Ausdruck zunächst um.

Nach unserer Definition § 4, (5) war

$$\tau_\beta = \operatorname{tg}\left(5^\beta \frac{\pi}{m}\right) = \frac{1}{2}\frac{\sin\left(\frac{2\pi}{m}5^\beta\right)}{\left[\cos\left(\frac{\pi}{m}5^\beta\right)\right]^2} \tag{2}$$

und wir setzen daher

$$\sigma_\beta = \sin\left(\frac{2\pi}{m}5^\beta\right). \tag{3}$$

Es ist dann (§ 5, (6)) offenbar nur zu beweisen, dass die $e_0, e_1, \ldots, e_{\mu-1}$ gerade Zahlen sein müssen, wenn

$$\sigma_\beta^{e_0}\sigma_{\beta+1}^{e_1}\ldots\sigma_{\beta+\mu-1}^{e_{\mu-1}} = S_\beta \tag{4}$$

für alle Werte von β dasselbe Vorzeichen hat. Die Zahlen σ_β erfüllen nun folgende Relationen:

$$\sigma_{\beta+\mu} = -\sigma_\beta \tag{5}$$

$$\sigma_{\beta+\frac{1}{2}\mu} = -\cos\left(\frac{2\pi}{m}5^\beta\right) \tag{6}$$

(weil nämlich $5^{\frac{1}{2}\mu} \equiv 1 + 2^{\lambda-2} \left(\operatorname{mod}\frac{1}{2}m\right)$ aber nicht $(\operatorname{mod} m)$), und also

$$\sigma_\beta\sigma_{\beta+\frac{1}{2}\mu} = -\frac{1}{2}\sin\left(\frac{4\pi}{m}5^\beta\right) = -\frac{1}{2}\sigma'_\beta \tag{7}$$

wo σ' aus σ hervorgeht, indem λ durch $\lambda - 1$ ersetzt wird, so dass

$$\sigma'_{\beta+\frac{1}{2}\mu} = -\sigma'_\beta. \tag{8}$$

Die Richtigkeit unserer Behauptung ist nun ersichtlich, wenn $\lambda = 3$ ist; denn in diesem Fall ist

$$\sigma_0 = \sin\frac{\pi}{4} = \sqrt{\frac{1}{2}}, \qquad \sigma_1 = \sin\frac{5\pi}{4} = -\sqrt{\frac{1}{2}}.$$

Wir nehmen daher an die Richtigkeit derselben sei erwiesen wenn λ durch $\lambda - 1$ ersetzt wird und suchen sie daraus für λ selbst herzuleiten. Zu diesem Ende bilden wir zunächst nach (4), (7), (8) das Product

$$S_\beta S_{\beta+\frac{1}{2}\mu} = \left(-\frac{1}{2}\right)^\mu (-1)^{\frac{1}{2}\mu} \sigma_\beta'^{e_0+e_{\frac{1}{2}\mu}} \sigma_{\beta+1}'^{e_1+e_{\frac{1}{2}\mu+1}} \cdots \sigma_{\beta+\frac{1}{2}\mu-1}'^{e_{\frac{1}{2}\mu-1}+e_{\mu-1}},$$

woraus nach der gemachten Voraussetzung folgt:

$$e_0 \equiv e_{\frac{1}{2}\mu}, \qquad e_1 \equiv e_{\frac{1}{2}\mu+1}, \quad \ldots, \quad e_{\frac{1}{2}\mu-1} \equiv e_{\mu-1} \pmod 2,$$

wonach mittelst (7) aus (4) folgt, dass auch

$$\sigma_\beta'^{e_0} \sigma_{\beta+1}'^{e_1} \cdots \sigma_{\beta+\frac{1}{2}\mu-1}'^{e_{\frac{1}{2}\mu-1}} = S_\beta' \tag{9}$$

für alle Werte von β dasselbe Vorzeichen hat. Nach Voraussetzung aber folgt hieraus

$$e_0 \equiv e_1 \equiv \ldots \equiv e_{\frac{1}{2}\mu-1} \equiv 0 \pmod 2$$

und dies ist der zu beweisende Satz.

2. Hieraus ergiebt sich in Verbindung mit dem Satze des vorigen Paragraphen:

Es giebt eine *ungerade ganze rationale Zahl* e derart, dass, wenn $\mathfrak{E}(r)$ eine beliebige primitive Einheit in Ω_λ bedeutet, die ganzen Zahlen e_0, e_1, $\ldots$, $e_{\mu-1}$ so bestimmt werden können, dass

$$\mathfrak{E}(r)^e = \pm \tau_0^{e_0} \tau_1^{e_1} \cdots \tau_{\mu-1}^{e_{\mu-1}}. \tag{10}$$

Denn der Schlusssatz des vorigen Paragraphen beweist zunächst überhaupt die Existenz einer solchen Zahl e; wäre dieselbe aber gerade, während die Zahlen e_0, e_1, $\ldots$, $e_{\mu-1}$ nicht alle zumal gerade sind, so stände dies im Widerspruch mit dem Satz 1.

Als Corollar hieraus ergiebt sich noch der Satz:

A) *Eine primitive Einheit des Körpers Ω, die mit allen ihren Conjugierten einerlei Vorzeichen hat, ist, vom Vorzeichen $\pm$ abgesehen, ein Quadrat einer primitiven Einheit.*

§ 7. *Fundamentalsysteme primitiver Einheiten.*

Es sei jetzt

$$\mathcal{E}_0(r),\ \mathcal{E}_1(r),\ \ldots,\ \mathcal{E}_{\mu-1}(r) \tag{1}$$

irgend ein System von einander unabhängiger primitiver Einheiten; haben dann die Grössen $l_0, l_1, \ldots, l_{\mu-1}$ dieselbe Bedeutung wie in § 4, (7), nämlich

$$l_\beta = l\tau_\beta \tag{2}$$

und ist e die ungerade ganze Zahl, deren Existenz im vorigen Paragraphen bewiesen ist, so kann man die ganzen Zahlen $e_{i,\varkappa}$ so bestimmen, dass

$$\begin{aligned}
el\mathcal{E}_i(r_0) &= e_{i,0}l_0 + e_{i,1}l_1 + \ldots + e_{i,\mu-1}l_{\mu-1}\\
el\mathcal{E}_i(r_1) &= e_{i,0}l_1 + e_{i,1}l_2 + \ldots - e_{i,\mu-1}l_0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
el\mathcal{E}_i(r_{\mu-1}) &= e_{i,0}l_{\mu-1} - e_{i,1}l_0 - \ldots - e_{i,\mu-1}l_{\mu-2},
\end{aligned} \tag{3}$$

woraus sich für $\lambda > 3$ durch Benutzung der Bezeichnung § 4, (12) ergiebt

$$\begin{aligned}
&(-1)^{2\lambda-4}\sum\pm l\mathcal{E}_0(r_0)l\mathcal{E}_1(r_1)\ldots l\mathcal{E}_{\mu-1}(r_{\mu-1})\\
&= \frac{\sum\pm e_{0,0}e_{1,1}\ldots e_{\mu-1,\mu-1}}{e^\mu} A(\tau_0,\ \tau_1,\ \ldots,\ \tau_{\mu-1}).
\end{aligned} \tag{4}$$

Da nun die Zahl e und ebenso die Determinante A einen von dem System (1) unabhängigen Wert hat, so geht hieraus hervor, dass man dies System so wählen kann, dass die Determinante

$$(-1)^{2\lambda-4}\sum\pm l\mathcal{E}_0(r_0)l\mathcal{E}_1(r_1)\ldots l\mathcal{E}_{\mu-1}(r_{\mu-1}) \tag{5}$$

einen möglichst kleinen positiven Wert L_λ erhält und ein solches System soll ein *Fundamentalsystem primitiver Einheiten* heissen.

Ist das System (1) ein solches Fundamentalsystem, so lässt sich jede primitive Einheit $\mathcal{E}(r)$ in der Weise darstellen

$$\mathcal{E} = \mathcal{E}_0^{g_0}\mathcal{E}_1^{g_1}\ldots\mathcal{E}_{\mu-1}^{g_{\mu-1}}, \tag{6}$$

so dass die Exponenten $g_0, g_1, \ldots, g_{\mu-1}$ *ganze Zahlen* sind. Denn ist z. B. g_0 ein Bruch, so existiert auch eine Einheit $\mathcal{E}$, in welcher g_0 ein positiver *echter Bruch* ist, und das System

$$\mathcal{E}, \mathcal{E}_1, \ldots, \mathcal{E}_{\mu-1}$$

ist gleichfalls unabhängig; für die Determinante

$$(-1)^{2\lambda-4}\Sigma\pm l\mathcal{E}(r_0)l\mathcal{E}_1(r_1)\ldots l\mathcal{E}_{\mu-1}(r_{\mu-1})$$

ergiebt sich aber der Wert $g_0 L_\lambda$, welcher, gegen die Voraussetzung, kleiner als L_λ ist. Hiernach können wir also auch, wenn die $g_{i,\varkappa}$ ganze Zahlen sind, setzen

$$l\tau_\beta(r_{\beta'}) = l_{\beta+\beta'} = g_{0,\beta}l\mathcal{E}_0(r_{\beta'}) + g_{1,\beta}l\mathcal{E}_1(r_{\beta'}) + \ldots + g_{\mu-1,\beta}l\mathcal{E}_{\mu-1}(r_{\beta'}) \tag{7}$$

woraus nach (3) folgt:

$$\Sigma\pm g_{0,0}g_{1,1}\ldots g_{\mu-1,\mu-1}\Sigma\pm e_{0,0}e_{1,1}\ldots e_{\mu-1,\mu-1} = e^\mu \tag{8}$$

und mithin ist

$$\Sigma\pm g_{0,0}g_{1,1}\ldots g_{\mu-1,\mu-1} = b_\lambda \tag{9}$$

eine *positive ungerade ganze Zahl.* Die Berechnung dieser Zahl stösst auf die bekannten Schwierigkeiten, die in der Theorie der Einheiten immer auftreten. Nur für den Fall $\lambda = 3$ ergiebt sich leicht aus der Theorie der PELL'schen Gleichung dass die Einheit $\tau_0 = \sqrt{2} - 1$ selbst eine fundamentale Einheit ist, da überhaupt *alle* Einheiten des Körpers Ω_3 in der Form $\sqrt{i}^{n_0}(\sqrt{2}-1)^{n_1}$ mit ganzzahligen Exponenten n_0, n_1 darstellbar sind. Es ist daher

$$L_3 = 2\log(\sqrt{2}+1) \tag{10}$$

der Minimalwert von $l\mathcal{E}(r)$. Hiernach erhält man aus (4), (8) und (9)

$$A(\tau_0, \tau_1, \ldots, \tau_{\mu-1}) = b_\lambda L_\lambda$$

und aus (13) § 2 und (13) § 4

$$P_3 = \frac{L_3}{2\sqrt{2}}, \qquad P_\lambda = m^{-2^{\lambda-4}} b_\lambda L_\lambda. \tag{11}$$

§ 8. *Die fundamentalen Einheiten des Körpers* Ω_λ.

Es kommt jetzt darauf an, ein vollständiges System fundamentaler Einheiten in Ω_λ zu bestimmen, (*D.*, Seite 565 f.), d. h. ein System von $\nu - 1$ (auch nicht primitiven) Einheiten

$$\vartheta_1(r),\ \vartheta_2(r),\ \ldots,\ \vartheta_{\nu-1}(r), \tag{1}$$

welche reell vorausgesetzt werden können, von der Art dass in der Form

$$r^{n_0}\vartheta_1^{n_1}\vartheta_2^{n_2}\ldots\vartheta_{\nu-1}^{n_{\nu-1}} \tag{2}$$

mit ganzzahligen Exponenten $n_0, n_1, \ldots, n_{\nu-1}$ *alle* Einheiten des Körpers Ω_λ darstellbar sind. Von besonderer Wichtigkeit ist dabei der absolute Wert

$$L(\vartheta_1, \vartheta_2, \ldots, \vartheta_{\nu-1}) \tag{3}$$

der aus den $(\nu-1)^2$ Grössen

$$\log \vartheta_i(r_\beta)\vartheta_i(r_\beta^{-1}) = l\vartheta_i(r_\beta) \qquad \binom{\beta=0,1,\ldots,\nu-2}{i=1,2,\ldots,\nu-1} \tag{4}$$

gebildeten Determinante. (Die Bezeichnung L soll in dem gleichen Sinne auch gebraucht werden für irgend ein, auch nicht fundamentales, System von $\nu - 1$ unabhängigen Einheiten in Ω.)

Ist $\lambda = 3$, so ist $\vartheta_1 = \tau_0$ und $L(\vartheta_1)$ mit L_3 identisch. Im allgemeinen Fall bezeichnen wir wie oben mit

$$\mathfrak{E}_0,\ \mathfrak{E}_1,\ \ldots,\ \mathfrak{E}_{\mu-1} \tag{5}$$

ein *Fundamentalsystem primitiver Einheiten* in Ω_λ und mit

$$\Delta_1,\ \Delta_2,\ \ldots,\ \Delta_{\mu-1} \tag{6}$$

ein vollständiges Fundamentalsystem des Körpers $\Omega_{\lambda-1}$.

Die $\nu - 1$ Einheiten

$$\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\mu-1}, \qquad \Delta_1, \Delta_2, \ldots, \Delta_{\mu-1} \tag{7}$$

bilden zusammen ein System unabhängiger Einheiten in Ω_λ, und die Determinante

$$L(\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\mu-1}, \Delta_1, \Delta_2, \ldots, \Delta_{\mu-1}) \tag{8}$$

ergiebt sich aus den Eigenschaften der Einheiten $\mathfrak{E}$ und Δ

$$l\mathfrak{E}_i(r) = -l\mathfrak{E}_i(-r); \quad l\Delta_i(r) = l\Delta_i(-r) \tag{9}$$

gleich

$$2^{\mu-1} L_\lambda L(\Delta_1, \Delta_2, \ldots, \Delta_{\mu-1}). \tag{10}$$

Es ist jetzt also noch der Zusammenhang zwischen dem System (7) und (1) zu ermitteln. Zu diesem Zweck setzen wir, indem wir unter $m_{i,i'}$, $M_{i,i'}$ rationale ganze oder gebrochene Zahlen verstehen

$$\begin{aligned} 2l\delta_i(r) = {} & m_{0,i} l\mathfrak{E}_0(r) + m_{1,i} l\mathfrak{E}_1(r) + \ldots + m_{\mu-1,i} l\mathfrak{E}_{\mu-1}(r) \\ & + M_{1,i} l\Delta_1(r) + M_{2,i} l\Delta_2(r) + \ldots + M_{\mu-1,i} l\Delta_{\mu-1}(r), \end{aligned} \tag{11}$$

und erhalten nach (9):

$$\begin{aligned} l\delta_i(r)\delta_i(-r) &= M_{1,i} l\Delta_1(r) + M_{2,i} l\Delta_2(r) + \ldots + M_{\mu-1,i} l\Delta_{\mu-1}(r) \\ l\delta_i(r)\delta_i(-r)^{-1} &= m_{0,i} l\mathfrak{E}_0(r) + m_{1,i} l\mathfrak{E}_1(r) + \ldots + m_{\mu-1,i} l\mathfrak{E}_{\mu-1}(r). \end{aligned} \tag{12}$$

Da nun $\delta_i(r)\delta_i(-r)$ eine Einheit des Körpers $\Omega_{\lambda-1}$, und $\Delta_1, \Delta_2, \ldots, \Delta_{\mu-1}$ ein Fundamentalsystem dieses Körpers, da ferner $\delta_i(r)\delta_i(-r)^{-1}$ eine *primitive* Einheit in Ω_λ ist, und $\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\mu-1}$ ein Fundamentalsystem primitiver Einheiten, so ergiebt sich aus diesen Formeln, dass die $M_{i,i'}$, $m_{i,i'}$ *ganze* Zahlen sind.

Bezeichnen wir mit M den absoluten Wert der Determinante der Zahlen $m_{i,i'}$, $M_{i,i'}$, so ergiebt sich aus (11) und (10)

$$L(\delta_1, \delta_2, \ldots, \delta_{\nu-1}) = M 2^{-\mu} L_\lambda L(\Delta_1, \Delta_2, \ldots, \Delta_{\mu-1}). \tag{13}$$

Es folgt nun aber ferner aus der Voraussetzung, dass $\delta_1, \delta_2, \ldots, \delta_{\nu-1}$

ein Fundamentalsystem von Einheiten des Körpers Ω_λ bilden, die Existenz von ganzen rationalen Zahlen $n_{i,i'}$, $N_{i,i'}$ die den Gleichungen genügen

$$(14)\quad \begin{aligned} l\mathfrak{E}_i(r) &= n_{1,i}l\delta_1(r) + n_{2,i}l\delta_2(r) + \ldots + n_{\nu-1,i}l\delta_{\nu-1}(r), && (i=0,1,\ldots,\mu-1)\\ l\Delta_x(r) &= N_{1,x}l\delta_1(r) + N_{2,x}l\delta_2(r) + \ldots + N_{\nu-1,x}l\delta_{\nu-1}(r), && (x=1,2,\ldots,\mu-1)\end{aligned}$$

und wenn wir den absoluten Wert der Determinante der $n_{i,i'}$, $N_{i,i'}$ mit N bezeichnen, so folgt aus (11) und (14)

$$(15)\qquad MN = 2^{\nu-1}$$

woraus folgt, dass sowohl M als N Potenzen von 2 sind.

Es lässt sich nachweisen, dass M teilbar ist durch 2^μ. Man kann nämlich ein System von $\nu - 1 = 2\mu - 1$ ganzen rationalen Zahlen $x_1, x_2, \ldots, x_{\nu-1}$ *ohne gemeinsamen Teiler* so bestimmen, dass sie den $\mu - 1$ Gleichungen

$$(16)\qquad \sum_{1,\nu-1}^{i} M_{s,i}x_i = 0 \qquad (s=1,2,\ldots,\mu-1)$$

genügen. Da alsdann das Product

$$\delta_1^{x_1}\delta_2^{x_2}\ldots\delta_{\nu-1}^{x_{\nu-1}}$$

in Folge von (11) eine *primitive Einheit* in Ω_λ ist, und da die $\mathfrak{E}_0, \mathfrak{E}_1, \ldots, \mathfrak{E}_{\mu-1}$ ein Fundamentalsystem primitiver Einheiten bildet, so ergiebt sich nach (11)

$$(17)\qquad \sum_{1,\nu-1}^{i} m_{s,i}x_i \equiv 0 \pmod 2, \qquad (s=0,1,\ldots,\mu-1)$$

woraus folgt, dass die Determinante M durch 2 teilbar ist.

Da die $x_1, x_2, \ldots, x_{\nu-1}$ nicht alle gerade sind, so nehmen wir etwa x_1 ungerade, und bestimmen nun ein zweites Grössensystem $x_2', x_3', \ldots, x_{\nu-1}'$ aus den Gleichungen

$$\sum_{2,\nu-1}^{i} M_{s,i}x_i' = 0 \qquad (s=1,2,\ldots,\mu-1)$$

woraus ebenso die Teilbarkeit von M durch 2^2 folgt, und so kann man fortfahren, so lange die Anzahl der Unbekannten x die Anzahl der Gleichungen noch übertrifft, d. h. bis

$$(18)\qquad \sum_{\mu,\nu-1}^{i} M_{s,i}x_i^{(\mu-1)} = 0 \qquad (s=1,2,\ldots,\mu-1)$$

woraus die Teilbarkeit von M durch 2^μ folgt. Wir können also nach (15) setzen

$$M = 2^{\mu+\sigma}, \qquad N = 2^{\mu-\sigma-1} \tag{19}$$

worin σ eine ganze nicht negative Zahl ist.

Es wird sich im folgenden Paragraphen als Corollar ergeben, dass σ den Wert 0 hat, dass also M nicht durch eine *höhere* als die μ^{te} Potenz von 2 teilbar ist. Um aber die Kette der Schlussfolgerungen die sich an diese Betrachtung weiter knüpft, und zu einem wichtigen Resultate führt, hier nicht unterbrechen zu müssen, soll dieser Satz einstweilen vorausgesetzt werden.

Nimmt man also in (18) wieder an, es sei $x_\mu^{(\mu-1)}$ ungerade, so bestimme man die Zahlen $x_i^{(\mu)}$ aus den Gleichungen

$$\sum_{\mu+1,\,\nu-1}^{i} M_{s,i}\, x_i^{(\mu)} = 0 \qquad (s = 2, 3, \ldots, \mu-1) \tag{20}$$

es muss dann notwendig

$$\sum_{\mu+1,\,\nu-1}^{i} M_{1,i}\, x_i^{(\mu)} \equiv 1 \pmod 2 \tag{21}$$

sein; denn nehmen wir das Gegenteil an, also diese Summe sei gerade, etwa $= 2\xi$, so folgt aus (11) dass

$$\delta_{\mu+1}^{x_{\mu+1}^{(\mu)}}\, \delta_{\mu+2}^{x_{\mu+2}^{(\mu)}} \ldots \delta_{\nu-1}^{x_{\nu-1}^{(\mu)}}\, \Delta_1^{-\xi}$$

eine primitive Einheit in Ω_λ ist, woraus wie oben

$$\sum_{\mu+1,\,\nu-1}^{i} m_{s,i}\, x_i^{(\mu)} \equiv 0 \pmod 2 \qquad (s = 0, 1, \ldots, \mu-1)$$

folgt; es würde also gegen die Voraussetzung M durch $2^{\mu+1}$ teilbar sein.

Multipliciert man also die Gleichungen (11) für $i = \mu + 1, \mu + 2, \ldots, \nu - 1$ der Reihe nach mit $x_i^{(\mu)}$ und bildet die Summe, so ergiebt sich (mit Benutzung von (14)) eine Gleichung von der Form

$$l\Delta_1(r) = \sum_{0,\,\mu-1}^{i} A_{i,1}\, l\mathfrak{E}_i(r) + 2 \sum_{0,\,\nu-1}^{i} a_{i,1}\, l\delta_i(r) \tag{22}$$

worin die $A_{i,1}$, $a_{i,1}$ ganze Zahlen sind. An Stelle von Δ_1 kann in dieser

Formel ebenso gut $\Delta_2, \Delta_3, \ldots, \Delta_{\mu-1}$ treten. Dies Ergebniss lässt sich in folgenden bemerkenswerten *Satz* zusammenfassen:

B. *Jede Einheit des Körpers $\Omega_{\lambda-1}$ lässt sich darstellen als das Product aus einer primitiven Einheit und dem Quadrat einer Einheit des Körpers Ω_λ.*

Es hat dieser Satz, abgesehen von einer später zu machenden Anwendung das theoretische Interesse, dass er lehrt, dass im Körper Ω_λ noch fundamentalere Einheiten (um nach KUMMER's Vorgang diesen Comparativ zu brauchen) existieren, als das System der $\mathfrak{E}$, Δ.[1]

Wir lassen aber für jetzt die Voraussetzung wieder fallen, dass $\sigma = 0$ sei, und erhalten also aus (13) und (19)

$$L(\delta_1, \delta_2, \ldots, \delta_{\nu-1}) = 2^\sigma L_\lambda L(\Delta_1, \Delta_2, \ldots, \Delta_{\mu-1}).$$

Dieselbe Betrachtung lässt sich nun in Bezug auf $L(\Delta_1, \Delta_2, \ldots, \Delta_{\mu-1})$ wiederholen, so dass man schliesslich erhält:

$$L(\delta_1, \delta_2, \ldots, \delta_{\nu-1}) = 2^{\Sigma\sigma} L_\lambda L_{\lambda-1} \ldots L_3 \tag{23}$$

worin $\Sigma\sigma$ eine aus nicht negativen ganzen Zahlen zusammengesetzte Summe ist.

§ 9. *Die Classenanzahl.*

Es bleibt uns nur übrig, die gefundenen Resultate in die Formel (4) § 2

$$gh = Q_2 Q_3 Q_4 \ldots Q_\lambda . P_3 P_4 \ldots P_\lambda \tag{1}$$

einzusetzen, und den Wert von g zu bestimmen. Es ist aber nach § 2, (11), (12), § 3, (16)

$$Q_2 = \frac{\pi}{4}, \qquad Q_3 = \frac{\pi}{2\sqrt{2}}, \qquad Q_\lambda = \frac{\pi^\mu a_\lambda}{2 . 2^{(\lambda-2)2^{\lambda-4}}},$$

[1] Als Beispiel diene für $\lambda = 4$ die Formel

$$\operatorname{tg}\frac{\pi}{8} = \frac{\operatorname{tg}\frac{\pi}{16}}{\operatorname{tg}\frac{5\pi}{16}}\left(\frac{\cos\frac{\pi}{16}}{\cos\frac{5\pi}{16}}\right)^2.$$

und daraus findet man (mit Benutzung von $2 \cdot 2 + 3 \cdot 2^2 + \ldots + (\lambda - 2)2^{\lambda-3} = 2^{\lambda-2}(\lambda - 3)$)

$$Q_2 Q_3 Q_4 \ldots Q_\lambda = \frac{\pi^\nu a_4 a_5 \ldots a_\lambda}{\sqrt{2}\, 2^\lambda\, 2^{(\lambda-3)2^{\lambda-3}}}. \tag{2}$$

Desgleichen nach § 7, (11)

$$P_3 = \frac{L_3}{2\sqrt{2}}, \qquad P_\lambda = \frac{b_\lambda L_\lambda}{2^{\lambda 2^{\lambda-4}}},$$

woraus

$$P_3 P_4 \ldots P_\lambda = \sqrt{2}\, \frac{L_3 L_4 \ldots L_\lambda b_4 b_5 \ldots b_\lambda}{2^{(\lambda-1)2^{\lambda-3}}}, \tag{3}$$

und folglich

$$gh = \nu^{-\nu} 2^{-\lambda} L_3 L_4 \ldots L_\lambda \pi^\nu a_4 b_4 a_5 b_5 \ldots a_\lambda b_\lambda. \tag{4}$$

Für g hat man nach *D.*, Seite 577, (34) und 574, (25)

$$g = \frac{E(2\pi)^\nu}{\sqrt{D}}, \tag{5}$$

worin D die Grundzahl des Körpers Ω_λ ist, und (nach *D.*, Seite 567, (19) da die Anzahl der in Ω_λ enthaltenen Einheitswurzeln $= 2^\lambda$ ist)

$$E = 2^{-\lambda} L(\delta_1, \delta_2, \ldots, \delta_{\nu-1}). \tag{6}$$

Die Grundzahl D unseres Körpers ist aber, wenn

$$f(t) = t^{2\nu} + 1$$

bedeutet

$$D = N f'(r) = (2\nu)^{2\nu}. \tag{7}$$

Setzt man endlich noch für $L(\delta_1, \delta_2, \ldots, \delta_{\nu-1})$ aus § 8, (23) den Wert ein, so folgt:

$$g = 2^{-\lambda} \nu^{-\nu} \pi^\nu 2^{\Sigma\sigma} L_3 L_4 \ldots L_\lambda \tag{8}$$

und folglich

$$h = 2^{-\Sigma\sigma} a_4 b_4 a_5 b_5 \ldots a_\lambda b_\lambda. \tag{9}$$

Da nun die $a_4, b_4, \ldots, a_\lambda, b_\lambda$ wie oben bewiesen *ungerade ganze Zahlen* sind, und die Classenanzahl h eine ganze Zahl ist, also $\Sigma\sigma$ nicht positiv sein kann, so lassen sich aus (9) die zwei Folgerungen ziehen:

Die aus nicht negativen Gliedern bestehende Summe $\Sigma\sigma$ *und mithin jeder ihrer Summanden verschwindet, wodurch die beim Beweise des Satzes* B *gemachte Voraussetzung gerechtfertigt ist.*

C. *Die Classenzahl in den vollständigen Kreiskörpern, deren Ordnung eine Potenz von* 2 *ist, ist eine ungerade Zahl.*

III. DER KRONECKER'SCHE SATZ.

In den beiden vorangegangenen Abhandlungen, die in der Folge mit I, II citiert werden sollen, sind die Hilfsmittel enthalten, um zum vollständigen Beweis des KRONECKER'schen Satzes zu gelangen, mit dem sich die gegenwärtige Abhandlung beschäftigen soll:

Alle Abel'schen Körper sind Kreiskörper.

Nach I, § 2, n° 7 und n° 8 ist dieser Satz nur für *reguläre* Abel'sche Körper, deren Grad eine *Primzahlpotenz*, nachzuweisen. Es folgt dann daraus, dass die in I, § 5 näher bestimmten Körper nicht nur sämmtliche Kreiskörper, sondern alle Abel'schen Körper überhaupt umfassen.

§ 1. *Die Lagrange'schen Resolventen.*

Es sei $\mathfrak{R}$ ein gegebener regulärer Abel'scher Körper und

$$m = q^k \tag{1}$$

worin q eine Primzahl ist, sein Grad. Falls $q = 2$ ist, wird $k \geqq 2$ vorausgesetzt.[1] Ist x eine beliebige Zahl in $\mathfrak{R}$, so können die mit x conjugierten Zahlen

$$x_0, x_1, \ldots, x_{m-1} \tag{2}$$

[1] Für $m = 2$ ist der zu beweisende Satz evident, da jede Quadratwurzel in bekannter Weise durch Einheitswurzeln darstellbar ist. (Vgl. GAUSS, *Disqu. Arithmeticæ*, Art. 356.)

in der Weise angeordnet werden, dass sie durch die Permutationen der Gruppe von $\mathfrak{R}$ cyklisch in einander übergehen, und dass also diese Gruppe durch die Wiederholungen von (x_0, x_1) erschöpft wird. (I, § 2, n° 3.)

Wir betrachten neben dem Körper $\mathfrak{R}$ den vollständigen Kreiskörper Ω_m und den aus beiden zusammengesetzten Körper

$$\Omega = \mathfrak{R}\Omega_m.$$

1. Ist nun r eine primitive m^{te} Einheitswurzel, so besteht Ω aus allen rationalen Functionen $F(x_0, r)$ von x_0 und r, und wenn eine solche Zahl die Eigenschaft hat, durch die Substitutionen (x_0, x_1) der Gruppe von $\mathfrak{R}$ ungeändert zu bleiben, so ist sie nothwendig eine Zahl in Ω_m; denn aus

$$F(x_0, r) = F(x_1, r) = \ldots = F(x_{m-1}, r)$$

folgt

$$mF(x_0, r) = F(x_0, r) + F(x_1, r) + \ldots + F(x_{m-1}, r)$$

also eine symmetrische Function der $x_0, x_1, \ldots, x_{m-1}$.

2. Unter den Zahlen des Körpers Ω befinden sich auch die sogenannten LAGRANGE'schen Resolventen

$$\psi_a = \psi_a(x_0) = x_0 + r^a x_1 + r^{2a} x_2 + \ldots + r^{(m-1)a} x_{m-1} \tag{3}$$

worin a jede beliebige ganze Zahl sein kann, so dass man m solcher Functionen erhält. Durch diese kann man die Zahlen $x_0, x_1, \ldots, x_{m-1}$ ausdrücken mit Hilfe der Formeln

$$mx_k = \sum_{0, m-1}^{a} r^{-ak} \psi_a(x_0), \tag{4}$$

so dass die Lösung unserer Aufgabe auf den Nachweis zurückgeführt ist, dass sämmtliche ψ_a den Kreiskörpern angehören.

3. Durch die Substitution (x_0, x_1) geht $\psi_a(x_0)$ in

$$\psi_a(x_1) = r^{-a} \psi_a(x_0) \tag{5}$$

über und daraus folgt nach n° 1, dass die Zahlen

$$\omega_a = \psi_a^m \tag{6}$$

dem Körper Ω_m angehören; ebenso ergiebt sich allgemeiner, dass

$$\psi_a^{a'} \psi_b^{b'} \ldots \tag{7}$$

in Ω_m enthalten ist, wenn die ganzen Zahlen a, a', b, b', ... der Bedingung

$$aa' + bb' + \ldots \equiv 0 \pmod{m} \tag{8}$$

genügen.

4. Wir bezeichnen, wie in den beiden vorhergehenden Abhandlungen, mit n irgend eine nach dem Modul m genommene zu m teilerfremde Zahl, und weisen zunächst nach, *dass von den $\varphi(m)$ Zahlen $\psi_n(x_0)$ keine verschwinden kann, wenn wir voraussetzen, dass x eine primitive Zahl des Körpers $\mathfrak{R}$ sei.*

Wenn nämlich von den Zahlen ψ_n eine verschwindet, so verschwinden sie wegen n° 3 (6) sämmtlich (da man in der Gleichung $\omega_n = 0$ die primitive Wurzel r durch jede andere r^n ersetzen kann); dann sind alle auf der rechten Seite von (4) vorkommenden Zahlen a durch q teilbar und es folgt

$$x_k = x_{k+\frac{m}{q}}$$

also x keine primitive Zahl in $\mathfrak{R}$. (I, § 1, n° 1.) Auch sind umgekehrt, wenn x keine primitive Zahl in $\mathfrak{R}$ ist, die Zahlen $\psi_n = 0$. *Wir nehmen also für die Folge stets an, dass ψ_n von 0 verschieden sei.*

5. Ist a eine beliebige Zahl, n durch q nicht teilbar, so kann man die ganze rationale Zahl k so bestimmen dass

$$a + nk \equiv 0 \pmod{m}$$

dann ist aber nach n° 3, (7)

$$\psi_a \psi_n^k$$

in Ω_m enthalten. Es genügt daher der Nachweis, dass die Functionen ψ_n (oder selbst nur eine von ihnen) in den Kreiskörpern enthalten sind. Für diese Zahlen ψ_a hat man überdies aus n° 3, (7) den Satz:

$$\tilde{\omega}_n = \psi_1^{-n} \psi_n \tag{9}$$

ist in Ω_n enthalten.

§ 2. *Zerlegung der Zahlen ω_n in ideale Primfactoren.*

1. Zur Erleichterung des Überblicks schicke ich einige allgemeine Bemerkungen über den Gebrauch der Ideal-factoren voraus. Ist A ein beliebiger algebraischer Zahlkörper und sind α, β irgend zwei von Null verschiedene ganze Zahlen in demselben, so giebt es *ein* und *nur ein* Paar relativer Primideale $\mathfrak{a}$, $\mathfrak{b}$ derart dass

$$\mathfrak{a}\alpha = \mathfrak{b}\beta. \tag{1}$$

Sind α', β' zwei andere ganze Zahlen in A, welche der Bedingung genügen dass

$$\frac{\alpha}{\beta} : \frac{\alpha'}{\beta'}$$

eine Einheit ist, also

$$\alpha\beta' = \varepsilon\alpha'\beta, \tag{2}$$

so ist auch

$$\mathfrak{a}\alpha' = \mathfrak{b}\beta', \tag{3}$$

und wenn umgekehrt die Gleichungen (1), (3) bestehen, so folgt auch (2), d. h. die gebrochenen Zahlen $\alpha:\beta$ und $\alpha':\beta'$ sind bis auf einen Einheits-factor identisch (vgl. *D.* § 175). Die beiden Ideale $\mathfrak{a}$, $\mathfrak{b}$ sind äquivalent. Ist daher η irgend eine ganze oder gebrochene Zahl in A, so sind durch dieselbe die beiden relativen Primideale $\mathfrak{a}$, $\mathfrak{b}$ derart völlig bestimmt, dass

$$\mathfrak{a}\eta = \mathfrak{b}, \tag{4}$$

und $\mathfrak{a}$ kann definiert werden als der Inbegriff aller derjenigen ganzen Zahlen α, für welche das Product $\alpha\eta = \beta$ eine ganze Zahl wird. Der Inbegriff der Zahlen β bildet das Ideal $\mathfrak{b}$. Ist alsdann auch $\mathfrak{a}\eta' = \mathfrak{b}$ so sind η und η' nur durch einen Einheitsfactor verschieden.

Die Gleichung (4) schreiben wir auch so

$$\mathfrak{o}\eta = \frac{\mathfrak{b}}{\mathfrak{a}}, \tag{5}$$

und sprechen in diesem Sinne von *gebrochenen* Idealen.[1] Zerlegt man $\mathfrak{a}$ und $\mathfrak{b}$ in Primideale so kommt keines derselben in beiden zugleich vor, und wenn eines von ihnen, $\mathfrak{p}$, s mal im Zähler oder $-s$ mal im Nenner von (5) vorkommt, so werden wir sagen, $\mathfrak{p}^s$ sei die höchste Potenz von $\mathfrak{p}$ welche in η aufgeht, wobei s auch negativ sein kann.

2. Wir untersuchen nun in diesem Sinne die Zerlegung der Zahlen ω_n in ihre idealen Primfactoren im Körper Ω_m, und beginnen mit dem in der Primzahl q selbst aufgehenden Primideal

$$\mathfrak{q} = \mathfrak{o}(1 - r),$$

für welches

$$\mathfrak{o}q = \mathfrak{q}^{\varphi(m)}$$

ist. (I, § 7, n° 6.)

Es sei $\mathfrak{q}^s$ die höchste in ω aufgehende Potenz von $\mathfrak{q}$ und folglich auch die höchste in ω_n aufgehende. Da nun nach § 1, n° 3

$$\overset{n}{\Pi}\phi_n$$

eine Zahl in Ω_m ist, und zwar eine solche, welche sich durch die Substitution (r, r^n) nicht ändert, d. h. also eine *rationale Zahl* so ist $\overset{n}{\Pi}\omega_n$ die m^{te} Potenz einer rationalen Zahl. Die höchste in dieser Zahl aufgehende Potenz von $\mathfrak{q}$ ist $\mathfrak{q}^{s\varphi(m)}$ also q^s die höchste in dieser rationalen Zahl aufgehende Potenz der Primzahl q. Daraus folgt *dass s durch m teilbar sein muss.*

2. Es sei p eine von q verschiedene Primzahl, $\mathfrak{p}$ ein in derselben enthaltenes Primideal und $\mathfrak{p}^s$ die höchste in ω aufgehende Potenz von $\mathfrak{p}$. Wenn durch die Substitution (r, r^n) $\mathfrak{p}$ in $\mathfrak{p}_n$ übergeht, so ist $\mathfrak{p}_n^s$ die höchste in ω_n aufgehende Potenz von $\mathfrak{p}_n$, und nach § 1, (9) ist

$$\omega_1^{-n}\omega_n = \tilde{\omega}_n^m$$

die m^{te} Potenz einer Zahl in Ω_m. Nun ist (nach I, § 7, n° 4) $\mathfrak{p}_p$ mit $\mathfrak{p}$ identisch.

---

[1] Eine allgemeine Definition von gebrochenen Idealen findet sich bei DEDEKIND, *Über die Discriminanten endlicher Körper*, Abhandlungen der Gesellschaft der Wissenschaften zu Göttingen, Bd. 29.

Es ist also $\mathfrak{p}^{-s(p-1)}$ die höchste in $\tilde{\omega}_p^m$ aufgehende Potenz von $\mathfrak{p}$, woraus folgt

$$s(p-1) \equiv 0 \pmod{m}. \tag{6}$$

Wenn also m_1 der grösste gemeinschaftliche Teiler von m und $(p-1)$ ist, und

$$m = m_1 m_2 \tag{7}$$

so ist s teilbar durch m_2, *und wenn* $m_1 = 1$ *ist, so ist* $s \equiv 0 \pmod{m}$.

3. Ist nun

$\mathfrak{p}_n^{s_n}$ die höchste Potenz von $\mathfrak{p}_n$, welche in ω_1 aufgeht, so ist

$\mathfrak{p}_{\nu n}^{s_n}$ die höchste Potenz von $\mathfrak{p}_{\nu n}$, welche in ω_ν aufgeht, also, wenn

$$\nu'\nu \equiv 1 \pmod{m}, \tag{8}$$

$\mathfrak{p}_n^{s_{\nu' n}}$ die höchste Potenz von $\mathfrak{p}_n$ welche in ω_ν aufgeht (worin der Index von s nach dem Modul m zu nehmen ist). Und da nach § 1, n° 5 $\omega_1^{-\nu}\omega_\nu$ eine m^{te} Potenz einer Zahl in Ω_m ist:

$$\nu s_n \equiv s_{n\nu'} \pmod{m}. \tag{9}$$

Setzen wir hierin $n = 1$, und (mit Rücksicht auf n° 2) $s_1 \equiv am_2 \pmod{m}$, und schreiben n an Stelle von ν', so folgt

$$s_n \equiv am_2 n', \qquad nn' \equiv 1 \pmod{m}, \tag{10}$$

wobei a und n' nach dem Modul m_1 reduciert werden können.

Wenn wir also von dem Ideal $\mathfrak{o}\omega_1$ das Product

$$\overset{n}{\Pi}\mathfrak{p}_n^{m_2 a n'},$$

über alle von *einander verschiedenen* in p aufgehenden Primideale erstreckt, absondern, so bleiben nur solche Potenzen von $\mathfrak{p}_n$, deren Exponent durch m teilbar ist. Wiederholen wir dies Betrachtung bei allen in $\mathfrak{o}\omega_1$ vorkommenden zu verschiedenen Primzahlen p gehörigen Primideale, deren Anzahl offenbar endlich ist, so ergiebt sich für $\mathfrak{o}\omega$ folgende Zerlegung:

$$\mathfrak{o}\omega = \mathfrak{a}^m \overset{p}{\Pi}\overset{n}{\Pi}\mathfrak{p}_n^{m_2 a n'}, \tag{11}$$

worin das erste Productzeichen sich auf alle Primzahlen p, deren Primteiler in $\mathfrak{o}\omega$ vorkommen, das zweite auf alle in denselben aufgehenden von einander verschiedene Primideale $\mathfrak{p}_n$ bezieht.

4. Wir betrachten nun neben dem Körper Ω_m den Körper Ω_{m_1} und setzen [1]

$$r^{m_2} = r_1. \tag{12}$$

Da $p \equiv 1 \pmod{m_1}$ ist, so zerfällt in diesem Körper $\mathfrak{o}p$ in $\varphi(m_1)$ verschiedene Primideale ersten Grades, die wir mit $\mathfrak{P}_{n_1}$ bezeichnen, worin n_1 ein vollständiges System incongruenter relativer Primzahlen zu m_1 durchläuft.

Wenn wir nun wie in I, § 8 mit

$$\eta_0, \eta_1, \ldots, \eta_{m_1-1} \tag{13}$$

die aus $(p-1):m_1$ Gliedern bestehenden *Perioden der p^{ten} Einheitswurzeln* bezeichnen, und

$$(r_1^\nu, \eta_0) = \eta_0 + r_1^\nu \eta_1 + r_1^{2\nu}\eta_2 + \ldots + r_1^{(m_1-1)\nu}\eta_{m_1-1} \tag{14}$$

setzen, so erhalten wir nach dem an der erwähnten Stelle bewiesenen *Kummer'schen Theorem:* (I, § 8 (16))

$$\mathfrak{o}_1(r_1, \eta_0)^{m_1} = \prod_{t_1}^{t_1} \mathfrak{P}_{t_1}^{t_1'}, \tag{15}$$

worin t_1 die Reihe der zu m teilerfremden Zahlen $< m_1$ durchläuft, und t_1' die kleinste positive der Congruenz

$$t_1 t_1' \equiv 1 \pmod{m_1} \tag{16}$$

genügende Zahl ist.

Zerlegen wir nun nach I, § 7, n° 7 die Ideale $\mathfrak{o}\mathfrak{P}_{n_1}$ im Körper Ω_m in ihre Primideale, und erheben die Formel (15) in die m_2^{te} Potenz, so folgt, wenn t' die kleinste positive der Congruenz

$$tt' \equiv 1 \pmod{m_1}$$

genügende Zahl bedeutet:

$$\mathfrak{o}(r_1, \eta_0)^m = \prod_t^t \mathfrak{p}_t^{m_2 t'} \tag{17}$$

[1] Ist $m_1 = 2$, so ist Ω_{m_1} der Körper der rationalen Zahlen und $r_1 = -1$.

worin sich das Product nur auf die *von einander verschiedenen* Primideale $\mathfrak{p}_t$ erstreckt.

Wenden wir dieselbe Betrachtung auf die sämmtlichen Producte auf der linken Seite von (11) an, so folgt:

$$\mathfrak{v}\omega = \mathfrak{a}^m \prod^{p} (r_1, \eta_0)^{am}, \tag{18}$$

oder durch Anwendung der Substitution (r, r^n):

$$\mathfrak{v}\omega_n = \mathfrak{a}_n^m \prod^{p} (r^{m_2 n}, \eta_0)^{am}. \tag{19}$$

5. Die hierin vorkommenden Grössen $(r^{m_2 n}, \eta_0)$ sind specielle Fälle der ψ_n (I, § 8, (4)), und genügen daher den Bedingungen § 1, n° 3, dass

$$(r^{m_2 n}, \eta_0)^{m_1},\ (r^{m_2}, \eta_0)^{-n}(r^{m_2 n}, \eta_0), \tag{20}$$

$$(r^{m_2 a}, \eta_0)^{a'}(r^{m_2 b}, \eta_0)^{b'} \ldots \qquad (aa' + bb' + \ldots \equiv 0 \pmod{m_1})$$

Zahlen des Körpers Ω_{m_1} und folglich auch des Körpers Ω_m sind. Ins Besondere ist

$$(r^{m_2}, \eta_0)(r^{-m_2}, \eta_0) = \pm p.$$

6. *Daraus ergiebt sich für die conjugierten Ideale* $\mathfrak{a}_n$ *dass*

a) $\mathfrak{a}_n^m$ und b) $\mathfrak{a}_1^{-n}\mathfrak{a}_n$

Hauptideale sind.

§ 3. *Untersuchung des Falles, wo* m *eine Potenz von 2 ist.*

Von jetzt an ist es notwendig, den Fall einer Potenz von 2 von dem eines ungeraden m zu trennen, und wir wenden uns zunächst dem ersteren zu.

1. Um zunächst den einfachsten Fall $m = 4$ zu erledigen bemerken wir, dass in diesem Fall nur Hauptideale existieren, und dass die einzigen Einheiten des Körpers Ω_4 die Zahlen ± 1, $\pm i$ sind. Wenn also α_1 eine Zahl des Körpers Ω_4, d. h. eine (ganze oder gebrochene) GAUSS'sche

complexe Zahl und α_3 die mit ihr conjugierte Zahl bedeutet, so folgt aus (19), § 2

$$\omega_1 = \varepsilon_1 \alpha_1^4 \overset{p}{\prod} (r^{m_2}, \eta_0)^{4a}$$
$$\omega_3 = \varepsilon_3 \alpha_3^4 \overset{p}{\prod} (r^{-m_2}, \eta_0)^{4a} \tag{1}$$

worin entweder $\varepsilon_1 = \varepsilon_3 = \pm 1$ oder $\varepsilon_1 = -\varepsilon_3 = \pm i$ und $r^{m_2} = -1$, oder $= \pm i$. Damit ist aber, durch Ausziehen der vierten Wurzel, für diesen Fall die Frage erledigt.

2. Ist $m \overline{\overline{>}} 8$, so machen wir Gebrauch von den in der II^ten^ Abhandlung bewiesenen Sätzen. Nach dem dort in § 9 bewiesenen Satze C ist die Anzahl h der Idealclassen eine ungerade Zahl, und da $\mathfrak{a}^h$ immer ein Hauptideal ist (*D.*, Seite 541), so folgt, wenn $\mathfrak{a}^m$ ein Hauptideal ist, dass auch $\mathfrak{a}$ selbst ein solches sein muss; denn es sind h, m relative Primzahlen, und wenn man daher x, y so bestimmt dass $hx + my = 1$ wird, so ist

$$\mathfrak{a}^{hx+my} = \mathfrak{a},$$

also $\mathfrak{a}$ ein Hauptideal. Bezeichnen wir also mit α eine Zahl in Ω_m, mit $\varepsilon(r)$ eine reelle Einheit, so folgt aus (19) des vorigen Paragraphen:

$$\omega = r^k \varepsilon(r) \alpha^m \overset{p}{\prod} (r^{m_2}, \eta_0)^{am}. \tag{2}$$

Bildet man hieraus $\omega_1 \omega_{-1}$, so folgt nach § 1, n° 3 und § 2, n° 5 dass

$$\varepsilon(r)^2 = e(r)^m \tag{3}$$

eine genaue m^{te} *Potenz* einer Einheit ist.

Zieht man also aus (2) die $\frac{1}{2} m^{te}$ Wurzel und bezeichnet mit ρ eine weiterhin noch genauer zu betrachtende Einheitswurzel der Ordnung m^2 so folgt aus (2) wegen (3)

$$\psi_1^2 = \rho^2 e(r) \alpha^2 \overset{p}{\prod} (r^{m_2}, \eta_0)^{2a}, \tag{4}$$

worin die Einheit $e(r)$ *reell* angenommen werden kann. Die reelle Einheit $e(r)$ genügt nun wieder in Folge von § 1, n° 3; § 2, n° 5 den Bedingungen

$$e(r^n) e(r)^{-n} = \pm \varepsilon^2, \tag{5}$$

d. h. gleich dem Quadrat einer Einheit in Ω_m, und das Vorzeichen in (5) kann so gewählt werden, dass ε eine *reelle* Einheit ist.

Wenden wir die Formel (5) auf $n = \pm 1 + \frac{1}{2}m$ an, so folgt:

$$(6) \qquad \begin{aligned} e(r)e(-r) &= \pm \delta(r)^2 \\ e(r):e(-r) &= \pm \mathfrak{E}(r)^2 \end{aligned}$$

worin $\delta(r)$, $\mathfrak{E}(r)$ reelle Einheiten sind; die Einheit $\delta(r)$ genügt der Bedingung

$$\delta(r) = \pm \delta(-r)$$

worin aber nach I, § 9, n° 7 nur das obere Zeichen möglich ist, und mithin ist $\delta(r)$ eine reelle Einheit des Körpers $\Omega_{\frac{1}{2}m}$. Die Einheit $\mathfrak{E}(r)$ genügt der Gleichung

$$\mathfrak{E}(r)\mathfrak{E}(-r) = \pm 1$$

und ist also eine *primitive* Einheit des Körpers Ω_m (II, § 5). Aus (6) ergiebt sich dann durch Multiplication und Wurzelziehen

$$(7) \qquad e(r) = \mathfrak{E}(r)\delta(r)$$

(wo das positive Zeichen genommen werden kann, da $\mathfrak{E}$, δ nur bis aufs Vorzeichen definiert sind). Da wir nun nach II, § 8 B die Einheit $\delta(r)$ als Product einer *primitiven Einheit* mit dem Quadrat einer Einheit darstellen können, so können wir, indem wir die Wurzel dieses Quadrats mit α vereinigen, annehmen, *dass die in* (4) *vorkommende Einheit* $e(r)$ *selbst eine primitive Einheit sei.*

Wir leiten nun aus (4), indem wir r durch r^n ersetzen und die Wurzel ausziehen, für ψ_n den Ausdruck her

$$(8) \qquad \psi_n = \rho_n \sqrt{e(r^n)}\alpha_n \overset{p}{\Pi}(r^{m_2 n}, \eta_0)^a,$$

wobei bezüglich der Quadratwurzel nur soviel festgesetzt sein soll, dass

$$(9) \qquad \sqrt{e(r^n)} = \sqrt{e(r^{-n})}$$

sei.

Nach (5) ist alsdann $\sqrt{e(r^n)}\sqrt{e(r)}^{-n}$ eine Zahl des Körpers Ω_m. Bilden wir nun aus (8) das Product $\psi_n\psi_{-n}$, so folgt nach § 2, n° 5

$$\rho_n\rho_{-n} = \frac{\psi_n\psi_{-n}}{e(r^n)a_n a_{-n}\Pi(\pm p)^a} \tag{10}$$

also eine Zahl des Körpers Ω_n, und zwar eine *reelle Zahl.* Da aber $\rho_n\rho_{-n}$ eine Einheitswurzel ist, so kann diese Zahl nur $= \pm 1$ sein, und da sich hiernach der Wert der rechten Seite von (10) durch die Permutationen des Körpers Ω_n nicht ändert, so folgt:

$$\rho_n\rho_{-n} = \rho_1\rho_{-1} = \pm 1. \tag{11}$$

Es ist nun aber ebenso:

$$\rho_n\rho_1^{-n}\sqrt{e(r^n)}\sqrt{e(r)}^{-n} = \frac{\psi_n\psi_1^{-n}}{a_n a_1^{-n}\overset{p}{\Pi}(r^{m_2 n}, \eta_0)^a(r^{m_2}, \eta_0)^{-an}} \tag{12}$$

also gleichfalls eine Zahl in Ω_n und zwar eine Einheit, die wir

$$= r^k\mathfrak{E}(r) \tag{13}$$

setzen, indem wir unter $\mathfrak{E}(r)$ eine reelle Einheit verstehen. Ebenso ergiebt sich

$$\rho_{-n}\rho_{-1}^{n}\sqrt{e(r^n)}\sqrt{e(r)}^{-n} = \frac{\psi_{-n}\psi_{-1}^{-n}}{a_{-n}a_{-1}^{-n}\cdot\overset{p}{\Pi}(r^{-m_2 n}, \eta_0)^a(r^{-m_2}, \eta_0)^{-an}} \tag{14}$$

und da die rechte Seite von (14) aus der rechten Seite von (12) durch die Permutation (r, r^{-1}) entsteht, so folgt ihr Wert

$$= r^{-k}\mathfrak{E}(r). \tag{15}$$

Multipliciert man also (12) mit (14), so ergiebt sich mit Rücksicht auf (11)

$$e(r^n)e(r)^{-n} = \mathfrak{E}(r)^2 \tag{16}$$

woraus, da $\mathfrak{E}(r)$ reell, also $\mathfrak{E}(r)^2$ positiv ist, nach dem Satz A in § 6 der zweiten Abhandlung folgt, *dass $e(r)$ das Quadrat einer Einheit in Ω_m ist.* Damit ist aber durch die Formel (8) für diesen Fall der KRONECKER'sche Satz bewiesen.

Was die Einheitswurzeln ρ_n betrifft, so ergiebt sich für dieselben aus (12), wenn θ irgend eine m^{te} Einheitswurzel bedeutet:

$$\rho_{n\nu} = \theta^{\nu}\rho_{\nu}^{n}, \tag{17}$$

und durch wiederholte Anwendung dieser Formel

$$\rho_{n^k} = \theta^{kn^{k-1}}\rho^{n^k}. \tag{18}$$

Setzt man hierin $n = 5$, $k = \frac{1}{4}m$, so schliesst man hieraus, dass die Ordnung der Einheitswurzel ρ *höchstens die* $4m^{te}$ sein kann.

§ 4. *Beweis eines Hilfssatzes.*

Wir schicken unseren weiteren Betrachtungen den Beweis eines einfachen Lemma's voraus, welches wir so aussprechen:

Es sei

$$m = q^k$$

eine Potenz einer *ungeraden* Primzahl und es bedeute $E(x)$ die *grösste in* x *enthaltene ganze Zahl*, t bedeute jede positive ganze Zahl, *relativ prim* zu m und *kleiner* als m; t' eine ebensolche Zahl, die aus der Bedingung

$$tt' \equiv 1 \pmod{m} \tag{1}$$

bestimmt ist.

Es ist zu beweisen, *dass man eine durch* q *nicht teilbare ganze Zahl* n *so annehmen kann, dass*

$$\sum^{t} t' E\left(\frac{tn}{m}\right) \tag{2}$$

durch q *nicht teilbar ist.*

Die Richtigkeit dieses Satzes ist zunächst leicht einzusehen, wenn $m = q$ eine Primzahl ist; denn bedeutet n eine beliebige positive ganze Zahl, kleiner als q, so ist

$$E\left(\frac{nt}{q}\right) + E\left(\frac{(q-n)t}{q}\right) = t - 1, \tag{3}$$

und wenn man mit t' multipliciert und die Summe nimmt, so folgt, da $\Sigma t' \equiv 0 \pmod q$:

$$\Sigma t' E\left(\frac{nt}{q}\right) + \Sigma t' E\left(\frac{(q-n)t}{q}\right) \equiv -1 \pmod q. \tag{4}$$

Es können also nicht *beide* Summen auf der linken Seite dieser Gleichung durch q teilbar sein, und wir dürfen also annehmen, es sei

$$\Sigma t' E\left(\frac{nt}{q}\right) \text{ nicht durch } q \text{ teilbar.} \tag{5}$$

Es lässt sich nun zeigen, dass diese selbe Zahl n, in die allgemeine Summe (2) eingesetzt, diese durch q unteilbar macht. Wir setzen zu diesen Zweck

$$m = qm', \qquad m' \geqq q$$

$$t = t_1 + qt_2; \qquad \begin{pmatrix} t_1 = 1, 2, \ldots, q-1 \\ t_2 = 0, 1, \ldots, m'-1 \end{pmatrix} \tag{6}$$

$$t_1 t_1' \equiv 1 \pmod q, \qquad tt' \equiv 1 \pmod m.$$

Es ist alsdann

$$t' \equiv t_1' \pmod q. \tag{7}$$

Darnach wird die Summe (2)

$$\sum^{t} t' E\left(\frac{tn}{m}\right) \equiv \sum^{t_1} t_1' \sum^{t_2} E\left(\frac{nt_2}{m'} + \frac{nt_1}{m}\right) \pmod q. \tag{8}$$

Da nun $nt_1 < m$, so folgt

$$E\left(\frac{nt_2}{m'} + \frac{nt_1}{m}\right) \text{ entweder } = E\left(\frac{nt_2}{m'}\right) \tag{9}$$

$$\text{oder } = E\left(\frac{nt_2}{m'}\right) + 1; \tag{10}$$

(10) tritt jedesmal dann ein, wenn zwischen

$$\frac{nt_2}{m'} \quad \text{und} \quad \frac{nt_2}{m'} + \frac{nt_1}{m}$$

eine ganze Zahl liegt, d. h. wenn

$$E\left(\frac{nt_2}{m'}\right) + 1 - \frac{nt_2}{m'} < \frac{nt_1}{m}. \tag{11}$$

Die linke Seite von (11) stellt lauter positive, die Einheit nicht übersteigende Brüche dar mit dem Nenner m', von denen, wenn t_2 die Zahlenreihe 0, 1, ..., $m'-1$ durchläuft, nicht zwei einander gleich sind. Es durchläuft daher die linke Seite von (11) in irgend einer Reihenfolge die Reihe der Zahlen

$$\frac{1}{m'}, \frac{2}{m'}, \ldots, \frac{m'-1}{m'}, 1, \tag{12}$$

und wenn nun α einen beliebigen positiven echten Bruch bedeutet, so ist $E(m'\alpha)$ die Anzahl derjenigen Zahlen der Reihe (12), welche nicht grösser als α sind.

Die Anzahl der Werte von t_2, für welche die Ungleichung (11) statt hat ist daher

$$= E\left(\frac{nt_1}{q}\right)$$

und ebenso oft tritt also auch der Fall (10) ein. Wenn wir daher die Summe der linken Seite von (9), (10) bilden, so folgt:

$$\sum^{t_2} E\left(\frac{nt_2}{m'} + \frac{nt_1}{m}\right) = E\left(\frac{nt_1}{q}\right) + \sum^{t_2} E\left(\frac{nt_2}{m'}\right). \tag{13}$$[1]

Setzen wir dies in (8) ein und beachten dass $\Sigma t_1' \equiv 0 \pmod q$ ist, so folgt

$$\sum^{t} t' E\left(\frac{tm}{m}\right) \equiv \sum^{t_1} t_1' E\left(\frac{nt_1}{q}\right) \pmod q, \tag{14}$$

wodurch nach (5) der Hilfssatz bewiesen ist.

§ 5. *Untersuchung des Falles, wo m eine ungerade Zahl ist.*

Es kommt nun vor allen Dingen darauf an, nachzuweisen, dass auch im Falle eines ungeraden m aus den Bedingungen a), b) am Schluss des § 2 *folgt, dass die* $\mathfrak{a}_m$ *Hauptideale sind.*

[1] Diese Formel ist eine leichte Verallgemeinerung einer von HERMITE (Acta mathematica, B. 5, S. 315) bewiesenen Formel. Man vgl. auch den Beweis der letzteren von STERN, Acta mathematica, B. 8, S. 94.

Wir behalten die bisherige Bezeichnung bei, indem wir

$$m = m_1 m_2 = q^k \tag{1}$$

setzen, unter m_1, welches > 1 vorausgesetzt ist, den grössten gemeinschaftlichen Teiler von m und $p - 1$ verstehen und mit t, t' resp. t_1, t_1' die Reihe der durch q nicht teilbaren positiven Zahlen, $< m$ resp. $< m_1$ bezeichnen, welche den Bedingungen

$$tt' \equiv 1 \pmod{m}, \qquad t_1 t_1' \equiv 1 \pmod{m_1} \tag{2}$$

genügen, und zwar sei stets

$$t \equiv t_1 \pmod{m_1}, \tag{3}$$

folglich auch

$$t' \equiv t_1' \pmod{m_1}. \tag{4}$$

Wir bezeichnen endlich noch mit (x) den *kleinsten positiven Rest* einer ganzen Zahl x nach dem Modul m, so dass $x = mE\left(\frac{x}{m}\right) + (x)$ ist.

Die Primzahl p gehört nach dem Modul m zum Exponenten m_2, d. h. p^{m_2} ist die niedrigste Potenz von p welche nach dem Modul m der Einheit congruent ist, und daher sind die Potenzen von p

$$1, \quad p, \quad p^2, \quad \ldots, \quad p^{m_2-1}$$

sämmtlich modulo m verschieden, und sämmtlich $\equiv 1 \pmod{m_1}$. Es ist also auch jede der Zahlen t einer und nur einer der Zahlen

$$t_1, \quad t_1 p, \quad t_1 p^2, \quad \ldots, \quad t_1 p^{m_2-1}$$

nach dem Modul m congruent und es lässt sich λ so bestimmen, dass

$$t = (p^\lambda t_1) \tag{5}$$

wird.

Nun zerfällt p im Körper Ω_m in $\varphi(m_1)$ von einander verschiedene Primideale $\mathfrak{p}_t$, und in ebensoviele Primideale $\mathfrak{P}_{t_1}$ zerfällt p im Körper Ω_{m_1} so dass (I, § 7, n° 4 und n° 8):

$$\mathfrak{p}_t = \mathfrak{p}_{t_1} = \mathfrak{o}\mathfrak{P}_{t_1}, \tag{6}$$

und wir betrachten nun das Idealproduct

$$\mathfrak{d} = \prod_{t'}^{t} \mathfrak{p}_{t'}^{t} \tag{7}$$

welches in Folge von (4), (5), (6) sich auch so darstellen lässt:

$$\mathfrak{d} = \prod_{t_1'}^{t_1} \mathfrak{p}_{t_1'}^{t_1+(pt_1)+\ldots+(p^{m_2-1}t_1)} = \prod_{t_1'}^{t_1} \mathfrak{p}_{t_1'}^{\sum^{\lambda}(p^{\lambda}t_1)}. \tag{8}$$

Das Ideal $\mathfrak{d}$ gehe durch die Substitution (r, r^n) in $\mathfrak{d}_n$ über. *Ein solches Ideal* $\mathfrak{d}$ *kann aus jedem Ideal* $\mathfrak{p}$ *des Körpers* Ω_m *hergeleitet werden, wenn nur die zugehörige Primzahl* $p \equiv 1 \pmod q$ *ist.* Nun ist aber für jeden Exponenten λ, wenn h_λ eine passend bestimmte ganze Zahl ist, für ein festes t_1

$$(p^{\lambda}t_1) - t_1 = m_1 h_\lambda, \tag{9}$$

und hierin ist:

1. h_λ nicht negativ, weil eine Zahl für den Modul m_1 keinen grösseren Rest haben kann als für den Modul m,

2. $h_\lambda < m_2$, weil $(p^{\lambda}t_1) < m$ ist, und

3. h_λ von $h_{\lambda'}$ verschieden, wenn $\lambda' \pmod{m_2}$ von λ verschieden ist (da sonst $p^{\lambda} \equiv p^{\lambda'} \pmod m$ sein müsste).

Mithin durchläuft h_λ zugleich mit λ, wenn auch in anderer Reihenfolge, die Zahlen 0, 1, 2, ..., $m_2 - 1$ und demnach ergiebt sich aus (9)

$$\sum^{\lambda}(p^{\lambda}t_1) = m_2 t_1 + \frac{1}{2} m(m_2 - 1)$$

woraus nach (8)

$$\mathfrak{d} = p^{\frac{1}{2}m(m_2-1)} \prod^{t_1} (\mathfrak{p}_{t_1'}^{t_1})^{m_2}. \tag{10}$$

Es ist daher, wenn wir die Bezeichnung § 2, (13), (14) beibehalten, nach dem KUMMER'schen Theorem (I, § 8):

$$\mathfrak{d} = \mathfrak{v} p^{\frac{1}{2}m(m_2-1)} (r^{m_2}, \eta_0)^m. \tag{11}$$

Daraus ergiebt sich nun, *dass nicht nur* $\mathfrak{d}$ *ein Hauptideal ist, sondern dass auch die Producte* $\mathfrak{d}_1^{-n}\mathfrak{d}_n$ m^{te} *Potenzen von Hauptidealen sind.* (§ 2, n° 5.)

Auf Grund hiervon lässt sich nun beweisen, dass, wenn die Bedingungen erfüllt sind:

$$\text{a)} \quad \mathfrak{a}_n^m \qquad \text{b)} \quad \mathfrak{a}_n \mathfrak{a}_1^{-n} \quad \text{sind Hauptideale,}$$

die conjugierten Ideale $\mathfrak{a}_n$ selbst *Hauptideale* sein müssen.

Dieser Beweis setzt sich aus zwei Teilen zusammen:

1. Es werde angenommen, dass in dem Ideale $\mathfrak{a}$ *nur* die Primfactoren solcher Primzahlen p vorkommen, welche $\equiv 1 \pmod q$ sind, auf welche also die Formel (11) und die daran geknüpfte Folgerung Anwendung findet.

Unter dieser Voraussetzung ist wegen (7) und (11)

$$\mathfrak{a} = \prod_t^t \mathfrak{a}_{t'}^t \quad \text{ein Hauptideal.} \tag{12}$$

Es ist aber ferner

$$\mathfrak{a}_n = \prod_t^t \mathfrak{a}_{nt'}^t = \prod_t^t \mathfrak{a}_{t'}^{(nt)}$$

und folglich

$$\mathfrak{a}_n^{-1} \mathfrak{a}_1^n = \left(\prod_t^t \mathfrak{a}_{t'}^{E\left(\frac{nt}{m}\right)} \right)^m, \tag{13}$$

was nach (11) die m^{te} Potenz eines Hauptideals ist. Also

$$\prod_t^t \mathfrak{a}_{t'}^{E\left(\frac{nt}{m}\right)} \quad \text{ein Hauptideal.} \tag{14}$$

Nach der Voraussetzung b) ist aber $\mathfrak{a}_{t'}$ äquivalent $\mathfrak{a}^{t'}$, und also nach (14) auch

$$\mathfrak{a}^{\sum_t^t t' E\left(\frac{nt}{m}\right)} \quad \text{ein Hauptideal.} \tag{15}$$

Nach dem Hilfssatz § 4 kann man aber die ganze Zahl n so annehmen, dass $\sum_t^t t' E\left(\frac{nt}{m}\right)$ *nicht teilbar ist durch* q und mithin folgt aus a) *und* (15) *dass* $\mathfrak{a}$ *ein Hauptideal ist.*

2. Es sei jetzt p eine $(\text{mod } m)$ zum Exponenten f gehörige Primzahl, und

$$\varphi(m) = ef,$$

jedoch sei p nicht $\equiv 1 \pmod q$, mithin f nicht eine Potenz von q und e

nicht durch $q - 1$ teilbar. Eine solche Primzahl p zerfällt in Ω_m in e verschiedene Primideale f^{ten} Grades. Wir legen eine primitive Wurzel c von m zu Grunde und lassen ξ nach dem Modul m die Reihe der Zahlen

$$c^0,\ c^1,\ \ldots,\ c^{e-1} \tag{16}$$

durchlaufen; bezeichnen wir dann mit $\mathfrak{p}_\xi$ die in p aufgehenden Primideale, so ist:

$$\mathfrak{o}p = \prod_{\xi}^{\xi} \mathfrak{p}_\xi, \tag{17}$$

und die Bezeichnung kann so gewählt werden, dass durch die Substitution (r, r^n), $\mathfrak{p}_\xi$ in $\mathfrak{p}_{n\xi}$ übergeht. Es enthalte jetzt unser Ideal $\mathfrak{a}$ Primideale f^{ten} Grades und die Richtigkeit des zu beweisenden Satzes werde vorausgesetzt *für alle diejenigen Ideale, welche keine Primideale f^{ten} Grades, und keine Primideale von anderen Graden wie $\mathfrak{a}$ enthalten.*

Die Ideale

$$\mathfrak{b} = \prod_{\xi}^{\xi} \mathfrak{a}_\xi, \qquad \mathfrak{b}_n = \prod_{\xi}^{\xi} \mathfrak{a}_{n\xi} \tag{18}$$

sind nun wegen (17) mit solchen Idealen *äquivalent* welche keine Primideale f^{ten} Grades enthalten und sonst keine anderen als solche die auch in $\mathfrak{a}_n$ vorkommen. Ausserdem ist aber nach a)

$$\mathfrak{b}_n^m \quad \text{ein Hauptideal} \tag{19}$$

und nach b)

$$\mathfrak{b}_n \quad \text{äquivalent} \quad \mathfrak{a}^{n^{\Sigma_\xi}}, \quad \text{äquivalent} \quad \mathfrak{b}^n, \tag{20}$$

d. h. die Voraussetzungen a), b) sind für das Ideal $\mathfrak{b}$ befriedigt, und daher ist n. V.

$$\mathfrak{b} \quad \text{ein Hauptideal.} \tag{21}$$

Es ist aber

$$\mathfrak{b} \quad \text{äquivalent} \quad \mathfrak{a}^{\Sigma_\xi}$$

und

$$\Sigma\xi \equiv \frac{c^e - 1}{c - 1} \pmod{m};$$

da nun e nicht durch $q-1$ teilbar ist, so ergiebt sich, dass auch $\Sigma\xi$ nicht durch q teilbar ist, und da also

$$\mathfrak{a}^m \quad \text{und} \quad \mathfrak{a}^{\Sigma\xi}$$

Hauptideale sind, so gilt das gleiche auch von $\mathfrak{a}$. Damit ist also der an die Spitze dieses Paragraphen gestellte Satz allgemein bewiesen.

§ 5. *Fortsetzung und Schluss.*

Mit Hilfe dieses Satzes lässt sich nun aus § 2, (18) folgern, wenn α eine Zahl, $\mathcal{E}(r)$ eine Einheit in Ω_m bedeutet:

$$\omega = \mathcal{E}(r)\alpha^m \overset{p}{\prod}(r^{m_2}, \eta_0)^{am}, \tag{1}$$

und die Einheit $\mathcal{E}(r)$ muss wegen § 1, n° 3; § 2, n° 5 der Bedingung genügen dass

$$\mathcal{E}^{-n}(r)\mathcal{E}(r^n)$$

die m^{te} Potenz einer Einheit ist.

Setzen wir nach I, § 9, n° 2

$$\mathcal{E}(r) = r^\nu e(r) \tag{2}$$

wo $e(r)$ eine *reelle* Einheit des Körpers Ω_m ist, also der Bedingung

$$e(r) = e(r^{-1}) \tag{3}$$

genügt, so ist auch

$$e(r^n)e(r)^{-n} = \varepsilon(r)^m$$

die m^{te} Potenz einer Einheit, und folglich (für $n = -1$)

$$e(r)^2 = \varepsilon(r)^m;$$

da m ungerade, so folgt hieraus, dass $e(r)$ selbst eine m^{te} Potenz ist, und wenn wir dieselbe mit α^m vereinigen, so kann (1) jetzt so geschrieben werden

$$\omega = r^\nu \alpha^m \overset{p}{\prod}(r^{m_2}, \eta_0)^{am}, \tag{4}$$

und durch Ausziehen der m^{ten} Wurzel, indem ρ eine mm^{te} Wurzel der Einheit bedeutet:

$$\psi = \rho\alpha\prod_{p}(r^{m_2}, \eta_0)^a. \tag{5}$$

Aus dem Umstand, dass $\psi_n\psi_1^{-n}$ dem Körper Ω_m angehört, schliesst man noch für die Einheitswurzel ρ_n, wenn θ irgend eine Potenz von r bedeutet:

$$\rho_{\nu n} = \theta^{\nu}\rho_{\nu}^{n},$$

und durch Anwendung dieser Formel auf $\nu = 1, n, \ldots, n^{\lambda}$:

$$\rho_{n^{\lambda}} = \theta^{\lambda n^{\lambda-1}}\rho^{n^{\lambda}}, \tag{6}$$

woraus, wenn man für n eine primitive Wurzel von q^2 und für λ den Wert $\varphi(m)$ setzt, sich schliessen lässt, dass ρ *höchstens* eine qm^{te} Einheitswurzel ist.

Durch die Formel (5) *ist nun der* Kronecker*'sche Satz auch für diesen Fall allgemein bewiesen.*

Marburg, im März 1886.