JOURNAL OF THE COLLEGE OF SCIENCE, TOKYO IMPERIAL UNIVERSITY.
VOL. XLI., ARTICLE 9.

Ueber eine Theorie des relativ Abel'schen Zahlkörpers.

Von

Teiji TAKAGI, *Rigakuhakushi,*

Professor der Mathematik an der Kaiserl. Universität zu Tokyo.

Der vorliegende Aufsatz ist die ausführliche Darlegung einer Theorie des relativ Abel'schen Zahlkörpers, deren Umriss vor einigen Jahren in den *Proceedings* der hiesigen Mathematisch-Physikalischen Gesellschaft sehr knapp und mangelhaft skizzirt worden ist.

Diese Theorie stützt sich auf den verallgemeinerten Begriff der Idealclassen, welcher sich in der modernen Theorie der algebraischen Zahlen allmählich entwickelt, und durch Heinrich Weber eine explicite Formulirung in der sehr allgemeinen Form gefunden hat. Es werden danach zwei Ideale eines algebraischen Körpers nur dann als aequivalent betrachtet und in dieselbe Idealclasse gerechnet, wenn ihr Quotient durch eine Zahl dargestellt werden kann, welche gewisser Congruenzbedingung nach einem vorgeschriebenen Idealmodul des Körpers genügt. Es existirt alsdann zu einem beliebigen algebraischen Zahlkörper ein bestimmter relativ Abel'scher Oberkörper von der folgenden Beschaffenheit:

1) Die Relativdiscriminante des Oberkörpers enthält die und nur die Primideale als Factor, welche in den Idealmodul des Grundkörpers aufgehen, der der Classeneinteilung in demselben zu Grunde gelegt wird.

2) Die Galois'sche Gruppe des Oberkörpers in Bezug auf den Grundkörper ist holoedrisch isomorph mit der Classengruppe (im verallgemeinerten Sinne) des Grundkörpers.

3) Diejenigen Primideale des Grundkörpers, welche der Hauptclasse (im verallgemeinerten Sinne) angehören und nur diese erfahren im Oberkörper eine Zerlegung in die Primfactoren der ersten Relativgrade; allgemeiner hängt die weitere Zerlegung der Primideale des Grundkörpers in dem Oberkörper nur von der Classe ab, der die Primideale im Grundkörper angehören.

Es ist dies eine naturgemässe Verallgemeinerung der Grundeigenschaften des Classenkörpers, welcher zuerst von D. Hilbert eingeführt wurde und die Theorie desselben von Ph. Furtwängler weiter fortgeführt worden ist. Jener Oberkörper sei daher als der allgemeine Classenkörper für die zugehörigen Idealengruppe des Grundkörpers bezeichnet, welche Gruppe die Hauptclasse (im verallgemeinerten Sinne) des Grundkörpers bildet.

Eine wichtige Tatsache in der Theorie des relativ Abel'schen Zahlkörpers ist nun die, dass umgekehrt zu jedem relativ Abel'schen Oberkörper eine bestimmte Classengruppe nach einem geeignet gewählten Idealmodul in dem Grundkörper existirt, welcher jener Oberkörper als Classenkörper zugeordnet ist, so dass die relativ Abel'schen Oberkörper einerseits und die Idealengruppen in dem Grundkörper anderseits einander characterisirend in wechselseitig eindeutiger Beziehung stehen.

Ich habe so weit als möglich diese Theorie ohne die üblichen Voraussetzung entwickelt, dass der Grundkörper die Einheitswurzeln enthalte; hierbei haben sich die von Hilbert eingeführten, einem Primideal in relativ normalen Körper zugehörigen Körper, welche die weitere Zerlegung des Primideals des Grundkörpers beherrschen, als ein sehr nützliches Hülfsmittel erwiesen.

Unter den Anwendungen dieser Theorie sei der Existenzbeweis für die unendlichvielen Primideale ersten Grades in jeder Classe (im verallgemeinerten Sinne) eines beliebigen algebraischen Zahlkörpers hervorgehoben; es ist dies eine schöne Verallgemeinerung des classischen Dirichlet'schen Satzes über die Primzahlen in einer arithmetischen Reihe.

Als ein Beispiel und eine naheliegende Anwendung der allgemeinen Theorie habe ich die der relativ Abel'schen Körper

in Bezug auf einen imaginären quadratischen Körper in einem besonderen Capitel behandelt. Es gelang die Bestätigung der berühmten Kronecker'schen Vermutung über die aus der Theorie der complexen Multiplication der elliptischen Functionen entspringenden Körper vollständig durchzuführen, was durch H. Weber und R. Fueter (in der unten citirten Abhandlung) nur zum Teil geschehen ist.

In Verzicht auf die vollständige Litteraturangabe seien die folgenden Werke angeführt, die, sei es als Grundlage, sei es als Anregung, für diese Untersuchung von Wichtigkeit gewesen sind:

H. Weber, Ueber Zahlengruppen in algebraischen Körpern. Math. Ann. 48, 49, 50. (1897–1898).

H. Weber, Lehrbuch der Algebra, III. (1908).

D. Hilbert, Die Theorie der algebraischen Zahlkörper. Bericht, erstattet der Deutschen Mathematiker-Vereinigung, 1897.

D. Hilbert, Ueber die Theorie des relativ quadratischen Zahlkörpers, Math. Ann. 51 (1898).

D. Hilbert, Ueber die Theorie der relativ Abel'schen Zahlkörper. Nachrichten von der Kgl. Gesellschaft der Wissenschaften in Göttingen, 1898.

Ph. Furtwängler, Allgemeiner Existenzbeweis für den Classenkörper eines beliebigen algebraischen Zahlkörpers. Math. Ann. 63 (1907).

R. Fueter, Abel'sche Gleichungen in quadratisch-imaginären Zahlkörpern, Math. Ann. 75 (1914).

CAPITEL I.

Der allgemeine Classenkörper.

§. 1.

Verallgemeinerung des Classenbegriffs.

Bekanntlich heissen zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ in einem algebraischen Körper k äquivalent, wenn es in k eine ganze oder gebrochene Zahl $\varkappa$ gibt, so dass die Gleichheit besteht:

$$\mathfrak{a} = \varkappa\, \mathfrak{b}.$$

Die Gesamtheit aller Ideale, welche einem gegebenen aequivalent sind, fassen wir in eine Idealclasse zusammen. Dann ist die Anzahl h der Idealclassen im Körper k endlich. Diese Classen lassen sich durch Multiplication zusammensetzen: sind nämlich A, B irgend zwei Classen, $\mathfrak{a}$, $\mathfrak{b}$ beliebige Ideale dieser Classen, dann gehört das Product $\mathfrak{a}\,\mathfrak{b}$ einer durch die Classen A, B eindeutig bestimmte, von der Wahl der Representanten $\mathfrak{a}$, $\mathfrak{b}$ unabhängige Classe AB. Die h Classen bilden in der Tat eine Abel'sche Gruppe, in welcher die Multiplication als die Regel der Zusammensetzung gilt, und die Hauptclasse die Stelle des Hauptelementes einnimmt.

Man kann auch die Gesamtheit der ganzen und gebrochenen Ideale des Körpers k als eine (unendliche) Abel'sche Gruppe G auffassen, indem wir die Ideale durch Multiplication zusammensetzen. Dann bilden eben die Gesamtheit der ganzen oder gebrochenen Hauptideale eine Untergruppe o vom Index h; sind $\mathfrak{a}_1, \mathfrak{a}_2, \ldots \mathfrak{a}_h$ ein System der Representanten der h Classen, dann ist in einer, in der Gruppentheorie üblichen, Bezeichnungsweise:

$$G = o\,\mathfrak{a}_1 + o\,\mathfrak{a}_2 + \cdots + o\,\mathfrak{a}_h. \qquad (1)$$

Eine engere Fassung des Classenbegriffs hat sich bei den verschiedenen Problemen als von Nutzen erwiesen. Es werden die Ideale $\mathfrak{a}$, $\mathfrak{b}$ nur dann als aequivalent aufgefasst und in eine und dieselbe Classe gerechnet, wenn ihr Quotient einem Hauptideale $(\varkappa)$ gleich ist, wo $\varkappa$ gewisser Bedingungen betreffs des Vorzeichens unterworfen ist. Es ist zum Beispiel verlangt, dass $\varkappa$ positive Norm habe[1], oder dass $\varkappa$ total positiv sei,[2] d.h. die mit $\varkappa$ conjugirten Zahlen in den sämtlichen mit k conjugirten reellen Körpern $k_1, k_2 \ldots k_r$ positiv seien. Solche Vorzeichenbedingungen lassen sich in allgemeinster Weise wie folgt auffassen: Das System der Vorzeichen, welche die mit $\varkappa$ conjugirten Zahlen in $k_1 k_2 \ldots k_r$ aufweisen, sei mit

$$(\varepsilon_1, \varepsilon_2, \ldots\ldots \varepsilon_r)$$

bezeichnet, wo $\varepsilon = \pm 1$ ist; wir wollen es kurz die *Vorzeichencom-*

1) Vgl. Hilbert, Bericht, § 24.
2) Hilbert, Relativ Abel. Zahlkörper, § 5.

bination der Zahl $\varkappa$ nennen. Dann bilden die 2^r möglichen Vorzeichencombinationen eine Gruppe nach Multiplication, welche mit der Gruppe der entsprechenden Zahlen homomorph ist, d.h., ist

$$(\varepsilon_1', \varepsilon_2', \cdots\cdots \varepsilon_r')$$

die Vorzeichencombination von $\varkappa'$, dann ist die Vorzeichencombination der Zahl $\varkappa\varkappa'$ das *Product*

$$(\varepsilon_1\varepsilon_1', \varepsilon_2\varepsilon_2', \cdots\cdots \varepsilon_r\varepsilon_r').$$

Sei nun $\mathfrak{H}$ eine Untergruppe dieser Gruppe der sämtlichen 2^r Vorzeichencombinationen, und verlangt man, dass die Idealquotient $\varkappa$ eine Vorzeichencombination dieser Gruppe $\mathfrak{H}$ haben soll, dann ist damit ein engerer Classenbegriff definirt, wobei die Hauptclasse diejenige Untergruppe $\mathfrak{o}'$ der Gruppe $\mathfrak{o}$ der sämtlichen Hauptideale des Körpers k ist, welche nur die Hauptideale $(\varkappa)$ enthält, welche durch die Zahlen $\varkappa$ mit den Vorzeichencombinationen von $\mathfrak{H}$ erzeugt werden. An Stelle von (1) hat man nunmehr die neue Classeneinteilung:

$$\mathfrak{G} = \mathfrak{o}'\mathfrak{a}_1 + \mathfrak{o}'\mathfrak{a}_2 + \cdots\cdots \mathfrak{o}'\mathfrak{a}_{h'},$$

wo h' die Classenzahl von k im neuen, engeren Sinne ist, und es zerfällt jede Classe $\mathfrak{o}\mathfrak{a}$ im alten, weiteren Sinne in eine dieselbe Anzahl $\frac{h'}{h}$ von den Classen $\mathfrak{o}'\mathfrak{a}$ im engeren Sinne, wo die Zahl $\frac{h'}{h}$ offenbar ein Teiler von dem Index der Gruppe $\mathfrak{H}$, d.h. von 2^{r-r_0} ist, wenn 2^{r_0} die Ordnung der Gruppe $\mathfrak{H}$ ist.

Eine andere Erweiterung des Classenbegriffs erblicken wir in die sogenannten Ringclassen.[1] Es sei $\mathfrak{R}$ ein Zahlring im Körper k, $\mathfrak{f}$ der Führer desselben. Zwei zum Führer $\mathfrak{f}$ relativ prime Ringideale $\mathfrak{a}_\mathfrak{R}$ und $\mathfrak{b}_\mathfrak{R}$ werden dann aequivalent genannt, und danach die Ringclassen definirt, wenn

$$\mathfrak{a}_\mathfrak{R} = \varkappa\, \mathfrak{b}_\mathfrak{R},$$

wo $\varkappa$ eine Körperzahl ist, mit oder ohne Vorzeichenbedingung.

1) Vgl. Hilbert, Bericht, §§ 33, 34.

Ist nun α eine Zahl in $\mathfrak{a}_R$, dann muss in $\mathfrak{b}_R$ eine Zahl β geben, derart, dass

$$\alpha = \varkappa\beta, \quad \text{oder} \quad \varkappa = \frac{\alpha}{\beta};$$

so erscheint $\varkappa$ als Quotient zweier zu $\mathfrak{f}$ primen Ringzahlen. Wenn umgekehrt $\mathfrak{a}$, $\mathfrak{b}$ zwei zu $\mathfrak{f}$ prime Körperideale sind, und besteht zwischen ihnen die Gleichung:

$$\mathfrak{a} = \varkappa\,\mathfrak{b},$$

wo $\varkappa$ ein Quotient der Ringzahlen ist, dann besteht für die zugeordneten Ringideale die Relation:

$$\mathfrak{a}_R = \varkappa\,\mathfrak{b}_R.$$

Es kommt daher auf dasselbe hinaus, wenn man unter G die Gesamtheit der zu $\mathfrak{f}$ primen ganzen oder gebrochenen Körperideale versteht, unter o die Gesamtheit der Hauptideale, welche durch die Quotienten der zu $\mathfrak{f}$ primen Ringzahlen, eventuell mit Vorzeichenbedingungen, erzeugt werden, und die Gruppe G nach dieser Untergruppe o in die Complexe der Form $o\mathfrak{a}$ zerlegt: die Ringideale einer und derselben Ringclasse werden den Körperidealen eines und desselben Complexes $o\mathfrak{a}$ zugeordnet, und umgekehrt.

Ein weiterer Schritt wurde durch Heinrich Weber[1] getan. Wir betrachten nach ihm die Gruppe G der sämtlichen Ideale des Körpers k, welche (in Zähler und Nenner) zu einem gegebenen Ideal $\mathfrak{m}$, dem Exkludenten, relativ prim sind. Ist dann H eine beliebige Untergruppe von G vom endlichen Index h, und zerlegen wir G in die h Complexe der Form $H\mathfrak{a}$, dann sollen die Ideale eines und desselben Complexes in eine Classe, speciell die der Gruppe H selbst in die Hauptclasse, gerechnet werden; zwei Ideale von G sind demnach aequivalent nach H genannt, wenn ihr Quotient der Idealengruppe H angehört. Offenbar ist der Classenbegriff im gewöhnlichen, *absoluten* Sinne ein sehr specieller Fall dieses *allgemeinen* Classenbegriffs.

1) H. Weber. Ueber Zahlengruppen in algebraischen Körpern, Math. Ann. 48–50. Lehrbuch der Algebra, III., § 161.

Die Hauptideale, welche in $\mathfrak{H}$ enthalten sind, bilden für sich eine Gruppe $\mathfrak{H}_0$, offenbar vom endlichen Index. Definiren wir dann die Classen nach $\mathfrak{H}_0$, so sind die Classen nach $\mathfrak{H}$ nichts anders als die Zusammenfassung einer gleichen Anzahl der Classen nach $\mathfrak{H}_0$; mit anderen Worten, die Classengruppe nach $\mathfrak{H}$ ist die complementäre Gruppe $\mathfrak{G}/\mathfrak{H}$, wenn die Classen nach $\mathfrak{H}_0$ zu Grunde gelegt werden.

Jedem Hauptideal (a) von $\mathfrak{H}_0$ entspricht nun ein System von associrten Zahlen εa, wo ε Einheiten von k bedeutet. Betrachten wir nun diese Zahlen einzeln für sich, dann bilden sie in ihrer Gesamtheit eine unendliche Abel'sche Gruppe, deren Elemente einzelne Zahlen sind, und in welcher die Multiplication die Compositionsregel abgibt. Daher kann man mit Weber zur Definition des Classenbegriffs eine *Zahlengruppe* zu Grunde legen.

Die Gesamtheit z der ganzen und gebrochenen, zu dem gegebenen Ideal $\mathfrak{m}$ primen Zahlen des Körpers k ist eine Gruppe; es sei o eine Untergruppe derselben, von welcher der Index $(z : o)$ endlich ist. Jede Zahl von o definirt ein zu $\mathfrak{m}$ primes Hauptideal, die Gesamtheit desselben ist dann eine Idealengruppe, die wir vorübergehend mit $\bar{o}$ bezeichnen wollen. Dann bilden nach Weber die Ideale eines Complexes $\bar{o}a$ eine Idealclasse nach o, also speciell die Ideale von $\bar{o}$ die Hauptclasse.

So werden die sämtlichen zu $\mathfrak{m}$ primen Idealen von k in Classen verteilt. Die Beschränkung, dass nur die zu $\mathfrak{m}$ primen Ideale in Betracht gezogen werden, ist für die Classeneinteilung ohne Belang, denn jede Idealclasse im absoluten Sinne enthält die zu $\mathfrak{m}$ primen Ideale. Erst durch die Einführung der Zahlengruppe o wird jede absolute Idealclasse in eine dieselbe Anzahl d von den Classen nach o zerlegt. Diese Anzahl d bestimmt sich nach Weber durch die Formel[1]

$$d = \frac{(z : o)}{(\mathfrak{E} : \mathfrak{E}_0)},$$

wenn $\mathfrak{E}$ die Gruppe der sämtlichen Einheiten in k, $\mathfrak{E}_0$ diejenige der Einheiten in o, und allgemein $(\mathfrak{A} : \mathfrak{B})$ den Gruppenindex bedeutet.

1) H. Weber, Math. Ann. Bd. 48, S. 443. Lehrbuch, III, S. 598.

§. 2.

Congruenz-classengruppen.

Von einer besonderen Wichtigkeit ist nun der Fall, wo die Zahlengruppe o die folgende Bedingung erfüllt:[1]

Es sei $\mathfrak{a}$ ein beliebiges ganzes Ideal in G, und $T(t)$ die Anzahl der in $\bar{o}$ enthaltenen durch $\mathfrak{a}$ teilbaren ganzen Hauptideale, deren Norm nicht grösser als die positive Grösse t ist. Dann soll

$$T=\frac{gt}{\mathrm{N}(\mathfrak{a})}+Mt^{1-\delta},$$

und folglich

$$\lim_{t=\infty}\frac{T}{t}=\frac{g}{\mathrm{N}(\mathfrak{a})}$$

sein, worin g eine endliche von Null verschiedene positive Grösse ist, die nur von den Gruppen G und o, aber nicht von t und von der Wahl des Ideals $\mathfrak{a}$ abhängt, während M eine Function von t ist, welche mit unendlich wachsendem t nicht unendlich wird, und δ endlich eine nur von dem Körper k abhängende positive Grösse bedeutet, die kleiner als 1 ist.

Unter dieser Voraussetzung folgt, wenn für ein variables $s>1$

$$A(s)=\sum\frac{1}{\mathrm{N}(\mathfrak{j})^s}$$

gesetzt wird, worin $\mathfrak{j}$ die sämtlichen ganzen Ideale einer Classe A nach o durchläuft,

$$A(s)=\frac{g}{s-1}+G(s),$$

wo $G(s)$ eine Function ist, welche für $s=1$ in einen endlichen Grenzwert übergeht.[2]

Hieraus folgt zunächst, dass die Classenzahl nach o endlich ist.[3]

---

1) H. Weber, Ueber die Zahlengruppen usw., Math. Ann. 49., S. 84.
2) Do. S. 85.
3) Die Voraussetzung 2. bei Weber, a. a. O. ist in der Voraussetzung 3. enthalten.

Es sei nun H eine Untergruppe der Classengruppe nach O vom Index h. Dann gibt es bekanntlich h Systeme der Gruppencharactere

$$\chi_1, \chi_2, \cdots\cdots \chi_h,$$

welche für die Classen in H den Wert 1 haben. Dementsprechend definiren wir nach Weber die h Functionen $Q_i(s)$ durch die unendlichen Reihen:

$$Q_i(s) = \sum_{A}' \chi_i(A) A(s) = \sum_{j}' \frac{\chi_i(j)}{N(j)^s}, \quad (i=1, 2, \cdots\cdots h)$$

wo sich die erste Summe auf die h Classen A, die zweite auf die sämtlichen ganzen Ideale von G erstreckt. Diese Reihen convergiren absolut wenn $s>1$. Ist χ_1 der Hauptcharacter, dann geht für $s=1$

$$(s-1)\, Q_1(s)$$

in den endlichen von Null verschiedenen Grenzwert gh über; für die $h-1$ anderen Charactere gehen die Functionen

$$Q_i(s) \qquad (i=2, 3, \cdots\cdots h)$$

gleichfalls für $s=1$ in die endliche Grenzwerte über, die jedoch auch verschwinden können.

Die Functionen $Q_i(s)$ lassen sich, so lange $s>1$, in unendliche Producte entwickeln:

$$Q_i(s) = \prod_{p}' \frac{1}{1-\frac{\chi_i(p)}{N(p)^s}},$$

wo p die sämtlichen Primideale von G durchläuft.

Definiren wir demnach die Function $\log Q_i(s)$ durch die ebenfalls für $s>1$ unbedingt convergente Reihe:

$$\log Q_i(s) = -\sum_{p}' \log\left(1-\frac{\chi_i(p)}{N(p)^s}\right)$$

$$= \sum_{p}' \frac{\chi_i(p)}{N(p)^s} + \frac{1}{2} \sum_{p}' \frac{\chi_i(p)^2}{N(p)^{2s}} + \cdots\cdots,$$

so erhalten wir, indem wir nach i summiren

$$\log \prod_i Q_i(s) = h \sum' \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s} + \frac{h}{2} \sum' \frac{1}{\mathrm{N}(\mathfrak{p}_2)^{2s}} + \cdots\cdots,$$

wo links unter log. der reelle Wert des Logarithmus zu verstehen ist, und wo die erste Summe rechts sich auf die sämtlichen in $\mathfrak{H}$ enthaltenen Primideale $\mathfrak{p}_1$ erstreckt, während sich die zweite Summe auf alle Primideale $\mathfrak{p}_2$ erstreckt, von welchen erst die zweite Potenz in $\mathfrak{H}$ enthalten sind, usw.

Da nun $(s-1)\prod_i Q_i(s)$ für $s=1$ endlich ist, so erhalten wir die für $s>1$ geltende fundamentale Beziehung

$$\sum' \frac{1}{\mathrm{N}(\mathfrak{p})^s} = \frac{1}{h} \log \frac{1}{s-1} + f(s), \qquad (1)$$

wo sich die unendliche Summe auf die sämtlichen in $\mathfrak{H}$ enthaltene Primideale $\mathfrak{p}$ erstreckt, und wo $f(s)$ eine Function von s ist, welche für $s=1$ nicht positiv unendlich wird.[1]

Die oben für die Zahlengruppe $\mathfrak{o}$ gestellte Forderung wird erfüllt, wenn $\mathfrak{o}$ die Gruppe der zu $\mathfrak{m}$ primen Zahlclassen nach dem Modul $\mathfrak{m}$ ist, mit oder ohne Vorzeichenbedingung von der in § 1 erwähnten Art, und dementsprechend $\mathfrak{G}$ die Gesamsheit der zu $\mathfrak{m}$ primen Ideale des Körpers ist. In dem Falle, wo $\mathfrak{o}$ die Gruppe der sämtlichen Zahlen α ist, welche die Congruenz

$$\alpha \equiv 1, \quad (\mathfrak{m})$$

befriedigen, also aus einer einzigen Zahlclasse mod. $\mathfrak{m}$ besteht, dem Falle, worauf es im Wesentlichen ankommt, bestätigt man durch die bekannte Methode der Volumenbestimmung,[2] dass

$$g = \frac{2^{\nu}\pi^{n-\nu}L}{w\mathrm{N}(\mathfrak{m})\sqrt{|d|}}, \qquad \delta = 1 - \frac{1}{n},$$

wo n den Grad des Körpers k, ν die Anzahl der Paare conjugirt imaginären unter den mit k conjugirten Körpern, d die

1) Diese Schlüsse bleibt offenbar gültig, wenn nur die Primideale ersten Grades in die Summe aufgenommen werden.

2) Vgl. H. Weber, Lehrbuch der Algebra, II. 20 und 21 Absch., auch Zahlengruppen, Math. Ann 49 S. 90–94.

Discriminante des Körpers k, N(m) die Norm des Ideals m im Körper k, w die Anzahl der Einheitswenzeln in o, L den Regulator[1] des Systems der Fundamentaleinheiten in o bedeuten; es ist vorausgesetzt, dass für die Zahlen in o alle Vorzeichencombinationen zugelassen werden.

Eine Idealclasse nach o, d.h. die Gesamtheit der Ideale

$$\alpha \mathfrak{j},$$

wo j ein gegebenes zu m primes Ideal, α eine ganze oder gebrochene zu m prime Körperzahl ist, derart, dass

$$\alpha \equiv 1, \quad (\mathfrak{m})$$

nennen wir eine *Congruenzclasse* nach dem Modul m, ein System solcher Classen, welche sich durch Multiplication und Division reproduciren eine *Congruenzclassengruppe.*

Jedoch sind wir berechtigt, auch eine beliebige Congruenzclassengruppe H einfach als eine Classe, als die *Hauptclasse,* zu betrachten, und demnach den Classencomplex HC als eine *Classe* zu bezeichnen. Diese Erweiterung des Classenbegriffs ist besonders von Statten, wenn H aus lauter Hauptidealen besteht; es kommt dann auf dasselbe hinaus, wie wenn in der Zahlengruppe o mehrere Zahlclassen nach m aufgenommen werden. Zum Beispiel sind die Ringclassen Congruenzclassen in dem erweiterten Sinne, wenn für den Modul der Führer des Ringes angenommen wird. Wenn m das Einheitsideal (1) ist, dann fallen wir in den Klassenbegriff im absoluten Sinne zurück. Da in der Folge ausschliesslich von den Congruenzclassen die Rede sein wird, lassen wir den Zusatz „Congruenz" weg.

Die in der Formel (1) ausgedrückte Tatsache formuliren wir als

Satz 1. *Ist* H *eine Classengruppe vom Index* h[2] *in einem Körper* k, *und durchläuft* $\mathfrak{p}$ *die sämtlichen in* H *enthaltenen Primideale (vom ersten Grade) des Körpers* k, *dann ist für* $s>1$

$$\sum \frac{1}{N(\mathfrak{p})^s} = \frac{1}{h} \log \frac{1}{s-1} + f(s),$$

1) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Aufl. S. 597.

2) Gemeint ist der Index von H in Bezug auf die Gruppe der sämtlichen Classen von k, eine abkürzende Bezeichnung, die in den folgenden durchgehend beibehalten wird.

wo $f(s)$ eine Function der reellen Veränderlichen s ist, welche nicht positiv unendlich wird, wenn sich s abnehmend der Grenze 1 nähert.

Ist nun $\mathfrak{a}$ ein zu $\mathfrak{m}$ relativ primes Ideal, dann gibt es in der Zahlengruppe $\mathfrak{o}$ eine durch $\mathfrak{a}$ teilbare ganze Zahl α von der Art, dass $\alpha:\mathfrak{a}$ relativ prim zu einem beliebig vorgeschriebenen Ideal $\mathfrak{c}$ ausfällt. Denn sind $\mathfrak{q}, \mathfrak{q}', \ldots$ die von einander verschiedenen Primfactoren von $\mathfrak{c}$, welche nicht in $\mathfrak{m}$ aufgehen, dann gibt es bekanntlich eine durch $\mathfrak{a}$ teilbare ganze Zahl α_0 derart dass $\alpha_0:\mathfrak{a}$ durch keines der Ideale $\mathfrak{q}, \mathfrak{q}', \ldots$ teilbar sind. Bestimmt man dann α aus den Congruenzen

$$\left.\begin{aligned} \alpha &\equiv \alpha_0, \quad (\mathfrak{a}\mathfrak{q}\mathfrak{q}'\cdots), \\ \alpha &\equiv \rho, \quad (\mathfrak{m}), \end{aligned}\right\}$$

wo ρ eine in $\mathfrak{o}$ enthaltene, folglich zu $\mathfrak{m}$ prime Zahl bedeutet, dann befriedigt α die gestellten Forderungen.

Aus dieser Tatsache folgt unmittelbar, dass jedes zu $\mathfrak{m}$ prime Ideal $\mathfrak{a}$ als den grössten gemeinsamen Divisor zweier in $\mathfrak{o}$ enthaltenen ganzen Zahlen $\varkappa$, ρ dargestellt werden kann. Ist nämlich $\varkappa$ eine durch $\mathfrak{a}$ teilbare Zahl in $\mathfrak{o}$, ρ ebenfalls eine solche Zahl, dass jedoch $\rho:\mathfrak{a}$ prim zu $\varkappa:\mathfrak{a}$ ausfällt, dann ist in der Tat

$$\mathfrak{a}=(\varkappa, \rho).$$

Ferner folgern wir noch die folgende wichtige Tatsache:

Satz 2. *In jeder Classe $\mathfrak{A}$ nach $\mathfrak{o}$ gibt es Ideale, die zu einem beliebig gegebenen Ideale $\mathfrak{c}$ relativ prim sind.*

Beweis. Sei $\mathfrak{a}$ ein beliebiges Ideal in der zu $\mathfrak{A}$ reciproke Classe $\mathfrak{A}^{-1}$, α eine durch $\mathfrak{a}$ teilbare Zahl in $\mathfrak{o}$:

$$\alpha=\mathfrak{a}\,\mathfrak{b},$$

derart, dass $\mathfrak{b}$ prim zu $\mathfrak{c}$ ausfällt. Da dann $\mathfrak{b}$ der Classe $\mathfrak{A}$ angehört, so ist der Satz bewiesen.

Wenn daher von den Idealen jeder Classe einer Classengruppe $\mathfrak{H}$ nach dem Modul $\mathfrak{m}$, nur die beibehalten werden, welche relativ prim zu einem beliebigen Ideal $\mathfrak{c}$ sind, dann bleiben die Classenzahl ungeändert. Eine solche Classengruppe kann aber auch aufgefasst werden, als eine Classengruppe nach dem Modul

$\mathfrak{m}'$, wo $\mathfrak{m}'$ das durch $\mathfrak{m}$ teilbare Ideal bedeutet, welches dadurch aus $\mathfrak{m}$ entsteht, wenn demselben alle in $\mathfrak{c}$ enthaltenen Primideale als Factoren hinzugefügt werden, die nicht in $\mathfrak{m}$ enthalten waren. In diesem Sinne ist eine Classengruppe nach dem Modul $\mathfrak{m}$ zugleich eine Classengruppe nach jedem durch $\mathfrak{m}$ teilbaren Modul $\mathfrak{m}'$; nur spielen dabei einige Factoren von $\mathfrak{m}'$ die Rolle der zur Classeneinteilung unwesentlichen *Excludenten*.

Ist allgemein $\mathfrak{H}$ eine Classengruppe sowohl nach dem Modul $\mathfrak{m}_1$ als nach $\mathfrak{m}_2$, und ist $\mathfrak{m}$ der grösste gemeinsame Divisor von $\mathfrak{m}_1$ und $\mathfrak{m}_2$, dann ist $\mathfrak{H}$ eine Classengruppe nach $\mathfrak{m}$. Denn sei α_0 eine zu $\mathfrak{m}_1$ und $\mathfrak{m}_2$ prime Zahl, die der Congruenz:

$$\alpha_0 \equiv 1, \quad (\mathfrak{m}) \tag{2}$$

genügt, also

$$\alpha_0 = 1 + \mu,$$

wo μ durch $\mathfrak{m}$ teilbar, folglich in der Form darstellbar ist:

$$\mu = \eta_1 + \eta_2,$$

wenn mit η_1 und η_2 bez. durch $\mathfrak{m}_1$ und $\mathfrak{m}_2$ teilbare Zahlen bezeichnet werden. Setzt man daher

$$\alpha = 1 + \eta_2,$$

dann bestehen die Congruenzen

$$\alpha \equiv \alpha_0, \ (\mathfrak{m}_1); \ \alpha \equiv 1, \ (\mathfrak{m}_2);$$

folglich ist α prim zu $\mathfrak{m}_1$ und zu $\mathfrak{m}_2$. Nach der zweiten Congruenz ist das Ideal (α) gewiss in $\mathfrak{H}$ enthalten, und weil $\mathfrak{H}$ auch eine Classengruppe nach dem Modul $\mathfrak{m}_1$ ist, so folgt aus der ersten Congruenz, dass (α_0) in $\mathfrak{H}$ enthalten sein muss. Da aber α_0 eine beliebige der Congruenz (2) genügende Zahl ist, so ist unsere Behauptung nachgewiesen.

Demnach gibt es unter allen Moduln $\mathfrak{m}$, die dieselbe Classengruppe $\mathfrak{H}$ definiren, einen bestimmten von kleinster Norm. Derselbe nennen wir der **Führer der Classengruppe** $\mathfrak{H}$.

§. 3.

Ein Fundamentalsatz über die relativ normalen Körper.

Satz 3. *Wenn* K *ein relativ normaler Körper vom Relativgrade* n *in Bezug auf dem Körper* k *ist, und wenn* $\mathfrak{p}_1$ *alle Primideale vom Grundkörper* k *durchläuft, welche in* K *in die von einander verschiedenen Primideale des ersten Relativgrades zerfallen, dann ist für* $s>1$

$$\sum^{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s} = \frac{1}{n} \log \frac{1}{s-1} + F(s),$$

wo $F(s)$ *eine Function des reellen Veränderlichen* s *ist, die endlich bleibt, wenn sich* s *abnehmend der Grenze 1 nähert.*[1]

Beweis. Das für $s>1$ absolut convergente, auf alle Primideale $\mathfrak{P}$ von K mit Ausschluss von den endlichvielen, in die Relativdifferente von K/k aufgehenden, zu erstreckende unendliche Product

$$\prod^{\mathfrak{P}} \frac{1}{1-\mathrm{N}_K(\mathfrak{P})^{-s}},$$

wo N_K die Norm im Körper K bezeichnet, lässt sich wie folgt umformen:

$$\prod^{\mathfrak{P}} \frac{1}{1-\mathrm{N}_K(\mathfrak{P})^{-s}} = \left(\prod^{\mathfrak{p}_1} \frac{1}{1-\mathrm{N}(\mathfrak{p}_1)^{-s}}\right)^n \prod^{f} \left(\prod^{\mathfrak{p}_f} \frac{1}{1-\mathrm{N}(\mathfrak{p}_f)^{-s}}\right)^e,$$

wo sich das erste Product rechts auf alle Primideale $\mathfrak{p}_1$ von k, das Product $\prod^{\mathfrak{p}_f}$ auf alle Primideale $\mathfrak{p}_f$ von k, welche in K in e von einander verschiedene Primideale des $f$ten Relativgrades zerfallen, wo $f = \frac{n}{e} > 1$, endlich das Product $\prod^{f}$ sich auf alle von 1 verschiedenen Teiler f von n erstreckt. Geht man in die Logarithmus über, so erhält man

$$\log \prod^{\mathfrak{P}} \frac{1}{1-\mathrm{N}_K(\mathfrak{P})^{-s}} = n \sum^{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s} + S,$$

---

1) Für den absolut normalen Körper, vgl. Hilbert, Bericht, S. 265 (Satz 84). Dieser Satz bleibt auch gültig, wenn nur die Primideale $\mathfrak{p}_1$ vom ersten (absoluten) Grade in die Summe aufgenommen werden, worauf es im wesentlichen ankommt; vgl. die Fussnote [1]) auf S. 10.

wo

$$S=n\Big(\frac{1}{2}\sum\frac{1}{N(\mathfrak{p}_1)^{2s}}+\frac{1}{3}\sum\frac{1}{N(\mathfrak{p}_1)^{3s}}+\cdots\cdots\Big)$$
$$+\sum^{e}e\Big(\sum\frac{1}{N(\mathfrak{p}_{f'}{}^{f's}}+\frac{1}{2}\sum\frac{1}{N(\mathfrak{p}_f)^{2fs}}+\cdots\cdots\Big)$$
$$<n\Big(\sum^{\mathfrak{j}}\frac{1}{N(\mathfrak{j})^{2s}}+\sum^{\mathfrak{j}}\frac{1}{N(\mathfrak{j})^{3s}}+\cdots\cdots\Big)$$
$$=n\sum^{\mathfrak{j}}\frac{1}{N(\mathfrak{j})^{s}\{N(\mathfrak{j})^{s}-1\}}<2n\sum^{\mathfrak{j}}\frac{1}{N(\mathfrak{j})^{2s}},$$

wenn $\sum$ eine über alle von dem Einheitsideal verschiedenen ganzen Ideale von k zu erstreckende Summe bedeutet. S ist also eine für $s>\frac{1}{2}$ absolut convergente Dirichlet'sche Reihe, und geht für $s=1$ in einen endlichen Grenzwert über.

Da bekanntlich

$$\operatorname*{Lim}_{s=1+0}\Big\{\log\prod\frac{1}{1-N_K(\mathfrak{P})^{-s}}-\log\frac{1}{s-1}\Big\}$$

endlich ist, so ist unser Satz bewiesen.

Von diesem Satz machen wir eine Anwendung auf einen Specialfall, um eine Tatsache herzuleiten, die wir später einmal benutzen werden.

Sei K relativ Abel'sch über k vom Relativgrade l^t, welcher aus t von einander unabhängigen relativ cyclischen Körpern vom Primzahlgrade l zusammengesetzt ist.

Sehen wir von den in einer endlichen Anzahl vorhandenen, in die Relativdiscriminante aufgehenden Primidealen ab, dann zerfällt ein Primideal von k in K entweder in l^t von einander verschiedenen Primideale vom ersten Relativgrade oder in l^{t-1} vom l ten Relativgrade; dieses letztere zerfällt dann in einem Unterkörper K′ vom Relativgrade l^{t-1} in die Primideale vom ersten Relativgrade; es ist nämlich K′ der Zerlegungskörper für jedes der l^{t-1} relativconjugirten Primideale von K (K muss relativ cyclisch in Bezug auf K′, also hier vom Relativgrade l sein).

Bezeichnen wir die Primideale der ersten Art durchweg mit $\mathfrak{p}_1$, die der zweiten Art, welche einem bestimmten Körper K′

entsprechen, mit $\mathfrak{p}_2$, dann folgt aus Satz 3, angewandt auf K und K′, dass

$$\sum^{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s} - \frac{1}{l} \log \frac{1}{s-1},$$

$$\left(\sum^{\mathfrak{p}_1} \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s} + \sum^{\mathfrak{p}_2} \frac{1}{\mathrm{N}(\mathfrak{p}_2)^s}\right) - \frac{1}{l^{t-1}} \log \frac{1}{s-1},$$

folglich auch

$$\sum^{\mathfrak{p}_2} \frac{1}{\mathrm{N}(\mathfrak{p}_2)^s} - \frac{l-1}{l^t} \log \frac{1}{s-1}$$

endlich bleiben, wenn sich der reelle Veränderliche s abnehmend der Grenze 1 nähert. Die Primideale $\mathfrak{p}_1$ sowie $\mathfrak{p}_2$ sind daher in unbegrenzter Anzahl vorhanden.

Enthält k die primitive l^{te} Einheitswurzel, dann lässt sich dieses Ergebnis wie folgt ausdrücken:

Es seien $a_1, a_2, \ldots\ldots a_t$ ganze Zahlen des Körpers k, welche die primitive l^{te} Einheitswurzel enthält, wo l eine natürliche Primzahl ist, von der Art, dass keine der $l^t - 1$ Producte

$$a_1^{m_1} a_2^{m_2} \ldots\ldots\ldots a_t^{m_t},$$

die man erhält, wenn man jeden der Exponenten die Werte 0, 1, 2, $\ldots\ldots l-1$ durchlaufen lässt, mit Ausschluss eines Wertsystems $m_1 = m_2 = \ldots = m_t = 0$, die l^{te} Potenz einer Zahl in k wird. Sind dann $\xi_1, \xi_2, \ldots\ldots \xi_t$ beliebig vorgeschriebene l^{te} Einheitswurzeln, dann gibt es in k stets unendlichviele Primideale $\mathfrak{p}$ vom ersten Grade, für welche

$$\left(\frac{a_1}{\mathfrak{p}}\right) = \xi, \left(\frac{a_2}{\mathfrak{p}}\right) = \xi_2^e, \ldots\ldots \left(\frac{a_t}{\mathfrak{p}}\right) = \xi_t^e,$$

wo $\left(\frac{a}{\mathfrak{p}}\right)$ den l^{ten} Potenzcharacter und e eine gewisse von $\mathfrak{p}$ abhängige nicht durch l teilbare ganze rationale Zahl ist.[1]

In der Tat, wenn zunächst $\xi_1, \xi_2 \ldots\ldots \xi_t$ sämtlich gleich 1 sind, werden durch die gestellte Forderung diejenige Primideale von k characterisirt, die im relativ Abel'schen Oberkörper $\mathrm{K} = \mathrm{k}(\sqrt[l]{a_1}, \sqrt[l]{a_2}, \ldots\ldots \sqrt[l]{a_t})$ vom Relativgrade l^t in die Primideale vom ersten

1) Vgl. Hilbert, Bericht, Satz 152.

Relativgrade zerfallen. Ist dagegen etwa $\xi_1 \neq 1$, dann bestimme man $t-1$ ganze rationale Zahlen $n_2, \ldots\ldots n_t$ so, dass

$$\xi_1^{n_2}\xi_2=1, \ldots\ldots \xi_1^{n_t}\xi_t=1,$$

und setze dementsprechend

$$\alpha_1^{n_2}\alpha_2=\beta_2, \ldots\ldots \alpha_1^{n_t}\alpha_t=\beta_t.$$

Dann lässt sich die gestellte Forderung umformen in:

$$\left(\frac{\alpha_1}{\mathfrak{p}}\right)\neq 1, \quad \left(\frac{\beta_2}{\mathfrak{p}}\right)=1, \ldots\ldots\ldots \left(\frac{\beta_t}{\mathfrak{p}}\right)=1.$$

Sie werden durch diejenige Primideale $\mathfrak{p}$ von k erfüllt, welche in dem relativ Abel'schen Körper $K'=k(\sqrt[l]{\beta_2}, \ldots\ldots \sqrt[l]{\beta_t})$ vom Relativgrade l^{t-1}, nicht aber in K, in die Primideale vom ersten Relativgrade zerfallen. Die über diese Primideale erstreckte Summe $\Sigma\frac{1}{N(\mathfrak{p})^s}$ wird daher nach Satz 3, für $s=1$ unendlich wie

$$\left(\frac{1}{l^{t-1}}-\frac{1}{l^t}\right)\log\frac{1}{s-1},$$

womit unsere Behauptung bestätigt wird.

§. 4.

Der Classenkörper.

Es sei K ein relativ normaler Oberkörper von k vom Relativgrade n; die Idealclassen in k seien nach dem Modul $\mathfrak{m}$ definirt. Die Gesamtheit derjenigen Classen von k, welche Relativnormen der zu $\mathfrak{m}$ primen Ideale des Oberkörpers K enthalten, bildet dann eine Classengruppe, die wir mit $\mathfrak{H}$ bezeichnen, und es sei h der Index von $\mathfrak{H}$ in Bezug auf die vollständige Classengruppe von k. Der Körper K und die Classengruppe $\mathfrak{H}$ bezeichnen wir als einander *zugeordnet*.

Die zu $\mathfrak{m}$ primen Primideale von k, welche in K in die Primideale des ersten Relativgrades zerfallen, sind demnach sämtlich in den Classen von $\mathfrak{H}$ enthalten, womit nicht gesagt wird, dass umgekehrt jedes in einer Classe von $\mathfrak{H}$ enthaltene Primideal

von k in die Primideale des ersten Relativgrades in K zerfällt.

Wenn der Relativgrad des relativ normalen Körpers K und der Index der zugeordneten Classengruppe $\mathfrak{H}$ von k einander gleich sind, dann soll K der **Classenkörper für die Classengruppe** $\mathfrak{H}$ genannt werden.

Mit Hülfe der Sätze 1 und 3 folgt aus der obigen Definition der folgende Satz, welcher in der Folge von einer fundamentaler Bedeutung ist.

Satz 4. *Der Relativgrad des relativ normalen Körpers ist niemals kleiner als der Index der zugeordneten Classengruppe des Grundkörpers.*

Beweis. Nach Satz 1 ist, wenn $\mathfrak{p}$ die sämtlichen in der Classengruppe $\mathfrak{H}$ enthaltenen Primideale von k durchläuft,

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} = \frac{1}{h} \log \frac{1}{s-1} + f(s), \qquad (s>1)$$

wo h der Index der Classengruppe $\mathfrak{H}$ ist, und $f(s)$ eine Function der reellen Veränderlichen s, welche für $s=1$ unter einer endlichen positiven Schranke bleibt. Die sämtlichen zu $\mathfrak{m}$ primen Primideale von k, welche in K in die von einander verschiedenen Primideale vom ersten Relativgrade zerfallen, die wir durchweg mit $\mathfrak{p}_1$ bezeichnen, sind in $\mathfrak{H}$ enthalten; wir bezeichnen die übrigen in $\mathfrak{H}$ enthaltenen Primideale durchweg mit $\mathfrak{p}'$. Dann ist

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^s} + \sum_{\mathfrak{p}'} \frac{1}{N(\mathfrak{p}')^s},$$

und nach Satz 3

$$\sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^s} = \frac{1}{n} \log \frac{1}{s-1} + F(s), \qquad (s>1)$$

wo n der Relativgrad von K/k ist und $F(s)$ eine Function von s, die für $s=1$ endlich bleibt.

Demnach hat man

$$\sum_{\mathfrak{p}'} \frac{1}{N(\mathfrak{p}')^s} = \left(\frac{1}{h} - \frac{1}{n}\right) \log \frac{1}{s-1} + f(s) - F(s) \geqq 0$$

für $s>1$. Da $f(s)-F(s)$ nicht positiv unendlich wird, wenn sich s abnehmend der Grenze 1 nähert, so folgt hieraus

$$\frac{1}{h} - \frac{1}{n} \geqq 0,$$

oder

$$n \geqq h,$$

womit der Satz bewiesen ist.

Dieser Schluss bleibt, wie man sofort erkennt, auch dann gültig, wenn nur vorausgesetzt wird, dass die in $\mathfrak{H}$ enthaltenen Primideale vom (absolut) ersten Grade in die Primideale vom ersten Grade in K zerfallen, sogar mit einer endlichen Anzahl Ausnahme, oder unendlichvielen, wenn nur die über diese Ausnahme-ideale erstreckte Summe $\Sigma \frac{1}{N(\mathfrak{p})^s}$ für $s=1$ endlich bleibt.

Eine wichtige Folgerung des obigen Beweises ist die, dass, wenn $n=h$, also wenn K Classenkörper für die Classengruppe $\mathfrak{H}$ ist, die Function $f(s)$ notwendig für $s=1$ endlich bleibt. Dann sind die Grenzwerte für $s=1$ von den Reihen

$$Q_i(s) \qquad (i=2, 3, \cdots\cdots h)$$

(§ 2, S. 9) von Null verschieden, und hieraus folgt, die folgende wichtige Tatsache[1]:

Satz 5. *In einem beliebigen algebraischen Körper existirt in jeder Classe nach dem Modul* $\mathfrak{m}$ *eine unbegrenzte, asymptotisch gleiche,*[2] *Anzahl von Primidealen ersten Grades; speciell existiren, wenn* μ *eine beliebige,* a *eine zu* μ *prime, ganze Zahl des Körpers ist, unendlichviele ganze Zahlen* ϖ *in dem Körper, die der Congruenz*

$$\varpi \equiv a, \qquad (\mu)$$

genügen, und von der Art sind, dass (ϖ) *unendlichviele Primideale des ersten Grades darstellen;*

(dies unter der vorläufigen Annahme, dass es für jede Classengruppe $\mathfrak{H}$ eines beliebigen Körpers einen entsprechenden Classenkörper gebe, was tatsächlich der Fall ist, wie in der Folge bewiesen werden wird).

Wir fügen hier noch einen Hülfssatz hinzu, den wir später nicht wohl entbehren können.

1) H. Weber, Zahlengruppen, Math. Ann. 49, S. 89.

2) E. Landau, Ueber die Verteilung der Primideale in den Idealklassen eines algebraischen Zahlkörpers, Math. Ann. 63, S. 196-197.

Hülfssatz. Sei K/k ein relativ normaler Körper vom Relativgrade n, H eine Classengruppe in k vom Index h, welche nicht dem Körper K zugeordnet zu sein braucht. Dann gibt es in k unendlichviele Primideale (ersten Grades), die nicht einer Classe vom H angehören, und auch nicht in K in die Primideale vom ersten Relativgrade zerfallen.[1]

Beweis. Wir beweisen diesen Satz nur in dem Falle, wo $h>2$, weil wir ihn später nur für eine Classengruppe eines ungeraden Primzahlindex anwenden werden. Nach Satz 1 gilt für die über alle nicht in H enthaltene Primideale erstreckte Summe

$$\sum \frac{1}{\mathrm{N}(\mathfrak{p})^s} = \frac{h-1}{h} \log \frac{1}{s-1} + \Phi(s),$$

wo $\Phi(s)$ für $s=1$ endlich oder *positiv* unendlich wird. Anderseits ist

$$\sum \frac{1}{\mathrm{N}(\mathfrak{p}_1)^s} = \frac{1}{n} \log \frac{1}{s-1} + F(s),$$

wo $F(s)$ für $s=1$ in einen endlichen Grenzwert übergeht, wenn die Summe auf alle Primideale $\mathfrak{p}_1$ erstreckt wird, die in K in die Primideale des ersten Relativgrades zerfallen.

Wenn nun $h>2$, dann ist jedenfalls

$$\frac{h-1}{h} > \frac{1}{n},$$

woraus der Satz folgt.

§. 5.

Eindeutigkeit des Classenkörpers.

Satz 6. *Seien* H, H′ *Classengruppen in* k; K, K′ *bez. die Klassenkörper für dieselben. Ist dann* H′ *Untergruppe von* H, *dann ist* K′ *Oberkörper von* K. *Für eine Classengruppe kann es daher nicht mehr als einen Classenkörper geben.*

Beweis. Seien K/k, K′/k bez. vom Relativgrade n, n'; der

1) Vgl. Ph. Furtwängler, Math. Annalen 63, S. 23.

aus K und K′ zusammengesetzte Körper K^* ist dann wieder relativ normal, er sei vom Relativgrade n^*.

Seien ferner S_1, S_2, S_3 die auf die Primideale $\mathfrak{p}$ von k erstreckten Summen

$$\sum' \frac{1}{\mathfrak{N}(\mathfrak{p})^s},$$

und zwar erstrecke sich S_1 auf die sämtlichen Primideale, die sowohl in K als auch in K′, folglich in K^* in die Primideale des ersten Relativgrades, S_2 auf die, welche in K aber nicht in K′, S_3 auf die, welche in K′ aber nicht in K, in die Primideale des ersten Relativgrades zerfallen. Dann ist nach Satz 3

$$S_1 = \frac{1}{n^*} \log \frac{1}{s-1} + F_1(s),$$

$$S_1 + S_2 = \frac{1}{n} \log \frac{1}{s-1} + F_2(s),$$

$$S_1 + S_3 = \frac{1}{n'} \log \frac{1}{s-1} + F_3(s),$$

wo die Functionen $F(s)$ für $s=1$ endlich bleiben. Hieraus erhält man

$$S_1 + S_2 + S_3 = \left(\frac{1}{n} + \frac{1}{n'} - \frac{1}{n^*} \right) \log \frac{1}{s-1} + G(s), \qquad (1)$$

wo auch $G(s)$ für $s=1$ endlich ist.

Anderseits ist, nach Annahme, die Classengruppe H vom Index n; ferner soll H alle oben in die Summen S_1, S_2, S_3 aufgenommenen Primideale, und möglicherweise noch die anderen, enthalten, von welchen letzteren auf einer ähnlichen Weise die Summe S' gebildet sein möge. Alsdann ist nach Satz 1.

$$S_1 + S_2 + S_3 + S' = \frac{1}{n} \log \frac{1}{s-1} + f(s), \qquad (2)$$

wo $f(s)$ eine Function von s ist, welche unterhalb einer endlichen positiven Schranke bleibt, wenn s abnehmend der Grenze 1 zustrebt.

Aus (1) und (2) folgt, für $s>1$

$$S'=\left(\frac{1}{n^*}-\frac{1}{n'}\right)\log\frac{1}{s-1}+f(s)-G(s)\geqq 0,$$

woraus zu schliessen ist, dass

$$\frac{1}{n^*}-\frac{1}{n'}\geqq 0,$$

oder

$$n'\geqq n.^*$$

Da aber $n^*\geqq n'$, so erhält man

$$n^*=n'.$$

Also fällt der Körper K* mit K′ zusammen, d. h. K ist in K′ enthalten.

Wenn nun K′ auch der Classenkörper für H ist, dann muss nach dem eben bewiesenen K′ in K enthalten sein. Daher fällt K′ mit K zusammen: es kann daher nicht mehr als einen Classenkörper für H geben.

Wir bemerken noch, dass die obigen Schlüsse gültig bleiben, wenn nur vorausgesetzt wird, dass die Primideale von k, welche bez. in den relativ normalen Körpern K und K′ in die Primideale vom ersten Relativgrade zerfallen *mit endlicher Anzahl Ansnahme* bez. in H und H′ enthalten sind. Dasselle gilt auch dann noch, wenn nur die Primideale *ersten Grades* von k in Betracht gezogen werden.

CAPITEL II.

Die Geschlechter im relativ cyclischen Körper vom Primzahlgrade.

§ 6.

Einige allgemeine Sätze über die relativ Abel'schen Zahlkörper.

In diesem Artikel fassen wir einige Sätze über die relativ Abel'schen Körper zusammen, die wir in der Folge wiederholt

anzuwenden haben. Es sind die Sätze, welche die Zerlegungs- Trägheits- und Verzweigungs-körper eines Primideals betreffen, die zuerst von D. Hilbert[1] für die absolut normalen (Galois'schen) Körper aufgestellt, und von H. Weber[2] für die relativ normalen Körper verallgemeinert worden sind, und die wir hier für die relativ Abel'schen Körper specializiren werden.

Sei K/k relativ Abel'sch vom Relativgrade n. Ein Primideal $\mathfrak{p}$ vom Grundkörper k wird in K auf einer folgenden Weise in die Primfactoren zerlegt:

$$\mathfrak{p}=(\mathfrak{P}_1\,\mathfrak{P}_2\cdots\cdots\mathfrak{P}_e)^g,$$

wo

$$n=e\,g\,f',$$

und f' der Relativgrad[3] von jedem der relativ conjugirten Ideale $\mathfrak{P}_1, \mathfrak{P}_2, \ldots\ldots \mathfrak{P}_e$ von K in Bezug auf k ist.

Die Zerlegungskörper von diesen relativ conjugirten Primidealen in Bezug auf k sind, wenn K relativ Abel'sch ist, ein und derselbe Oberkörper von k, so dass wir berechtigt sind, ihn als der Zerlegungskörper für das Primideal $\mathfrak{p}$ im Oberkörper K zu bezeichnen. Gleiches gilt für den Trägheits-, und Verzweigungs-körper.

Der Zerlegungskörper K_z für $\mathfrak{p}$ ist vom Relativgrade e in Bezug auf k, er ist der grösste in K enthaltene Oberkörper von k, in welchem $\mathfrak{p}$ in die von einander verschiedenen Primideale des ersten Relativgrades zerfällt.

Der Trägheitskörper K_t für $\mathfrak{p}$ ist vom Relativgrade ef' in Bezug auf k, und relativ cyclisch vom Grade f' in Bezug auf den Zerlegungskörper K_z. Er ist der grösste in K enthaltene Oberkörper von k, dessen Relativdiscriminante prim zu $\mathfrak{p}$ ausfällt.

Der Verzweigungskörper K_v für $\mathfrak{p}$ ist relativ cyclisch in Bezug auf den Trägheitskörper K_t, dessen Relativgrad ein Teiler von $p^{ff'}-1$ ist, wo p^f die Norm von $\mathfrak{p}$ in k, also $p^{ff'}$ die Norm von $\mathfrak{P}$ in K ist; dieser Relativgrad ist als der grösste Teiler von g bestimmt, welcher

1) D. Hilbert, Grundzüge einer Theorie des Galois'schen Zahlkörpers, Göttinger Nachrichten, 1894; vgl. auch Bericht, §§ 39–47.

2) H. Weber, Lehrbuch der Algebra, II. (2 Aufl.) 19. Abschnitt.

3) H. Weber, l. c. S. 645.

prim zu p ist. Wenn g durch p teilbar ist, dann sind zwischen K_v und K die Verzweigungskörper höheren Grades K_v', K_v'',.....einzuschalten; die Relativkörper K_v'/K_v, K_v''/K_v',..... sind relativ Abel'sch und aus nicht mehr als ff' von einander unabhängigen relativ cyclischen Körpern p^{ten} Grades zusammengesetzt. Es ist $\mathfrak{P}^g$ ein Primideal in K_t, dasselbe wird in K/K_t in die g te Potenz eines Primideals $\mathfrak{P}$ zerlegt, welches vom ersten Relativgrade in Bezug auf K_t ist. Wir heben speciell die folgenden Sätzen hervor.

Satz 7. *Ist* K/k *relativ cyclisch vom Primzahlpotenzgrade* l^h, *und geht ein zu* l *primes Primideal* $\mathfrak{p}$ *von* k *in die Relativdiscriminante des in* K *enthaltenen relativ cyclischen Oberkörper von* k *vom Relativgrade* l *auf, dann ist die Relativdiscriminante von* K/k *genau durch die* l^h—1^{te} *Potenz von* $\mathfrak{p}$ *teilbar; ferner ist*

$$\mathrm{N}\,(\mathfrak{p}) \equiv 1, \qquad (l^h),$$

wo N *die in* k *genommene Norm bedeutet.*

Satz 8. *Es sei* K/k *relativ cyclisch vom Primzahlgrade* l, *ferner sei* $\mathfrak{l}$ *ein in* l *aufgehendes Primideal von* k. *Wenn dann die Relativdiscriminante von* K/k *durch* $\mathfrak{l}$ *teilbar, dann ist sie genau durch die* $(v+1)(l-1)$ *te Potenz von* $\mathfrak{l}$ *teilbar, wo* $v > 0$. *Die Zahl* v *ist dadurch characterisirt, dass für jede ganze Zahl* A *von* K *die Congruenz besteht:*

$$\mathrm{s}\,A \equiv A, \qquad (\mathfrak{L}^{v+1})$$

wo s *eine erzeugende Substitution der Galois'schen Gruppe des Relativkörpers* K/k, sA *die relativ conjugirte Zahl von* A, *und* $\mathfrak{L}$ *das in* $\mathfrak{l}$ *aufgehendes Primideal von* K *bedeutet. Speciell ist, wenn* A *genau durch die erste Potenz von* $\mathfrak{L}$ *teilbar ist,* sA–A *genau durch die* $v+1^{te}$ *Potenz von* $\mathfrak{L}$ *teilbar.*[1]

Für die Zahl v *gilt die Beziehung*

$$\frac{s\,l}{l-1} \geqq v \geqq 1,$$

wenn s *der Exponent der höchsten in* l *aufgehenden Potenz von* $\mathfrak{l}$ *ist. Ferner ist* v *nur dann durch* l *teilbar, wenn*

1) Hilbert, Bericht, § 44, 47; es ist $v+1$ der dort mit L bezeichnete Exponent.

$$v=\frac{sl}{l-1},$$

(also wenn s durch $l-1$ teilbar ist).

Beweis. Es genügt, den zweiten Teil des Satzes zu beweisen. Sei A eine genau durch die erste Potenz von $\mathfrak{L}$ teilbare Zahl von K. Ist dann A genau durch $\mathfrak{L}^e$ teilbar, dann kann man eine zu $\mathfrak{L}$ prime Zahl B so bestimmen, dass

$$A\equiv BA^e, \qquad (\mathfrak{L}^u), \tag{1}$$

wo u ein beliebig grosser Exponent sein kann. Ist nun $e\not\equiv 0$, (l), dann ist $\mathrm{s}A^e-A^e$ genau durch $\mathfrak{L}^{v+e}$ teilbar, daher auch

$$\mathrm{s}A-A\equiv B(\mathrm{s}A^e-A^e)+(\mathrm{s}B-B)\mathrm{s}A^e, \qquad (\mathfrak{L}^u)$$

genau durch $\mathfrak{L}^{v+e}$ teilbar, weil das zweite Glied rechts wenigstens durch $\mathfrak{L}^{v+e+1}$ teilbar und nach Annahme $u>v+e$ ist. Ist aber $e\equiv 0$, (l), dann kann man in (1) A^e durch eine Zahl λ von k ersetzen, welche genau durch die $e:l^{\text{te}}$ Potenz von $\mathfrak{l}$ teilbar ist; man erhält dann

$$\mathrm{s}A-A\equiv(\mathrm{s}B-B)\lambda, \qquad (\mathfrak{L}^u),$$

folglich ist $\mathrm{s}A-A$ gewiss durch eine höhere als die $v+e^{\text{te}}$ Potenz von $\mathfrak{L}$ teilbar.

Bildet man daher aus der Zahl $A_1=\mathrm{s}A-A$ wieder die Zahl $A_2=\mathrm{s}A_1-A_1$, und so fort, bis man erhält $A_n=\mathrm{s}A_{n-1}-A_{n-1}$, welche letztere Zahl A_n symbolisch mit

$$(\mathrm{s}-1)^n A$$

bezeichnet sein möge, dann ist dieselbe genau durch die $e+nv^{\text{te}}$ Potenz von $\mathfrak{L}$ teilbar, wenn keine der n Zahlen e, $e+v$, $e+2v$, ... $e+(n-1)v$ durch l teilbar ist, andernfalls aber gewiss durch eine höhere als die $e+nv^{\text{te}}$ Potenz von $\mathfrak{L}$ teilbar.

Vermöge der Identität

$$1+x+x^2+\cdots\cdots+x^{l-1}=l+\binom{l}{2}(x-1)+\binom{l}{3}(x-1)^2+\cdots\cdots$$
$$+l(x-1)^{l-2}+(x-1)^{l-1}$$

schreiben wir nun die Relativspur von A in der Form:

$$S(A)=(1+s+s^2+\cdots\cdots+s^{l-1})A$$
$$=lA+\binom{l}{2}(s-1)A+\binom{l}{3}(s-1)^2A+\cdots\cdots+(s-1)^{l-1}A.$$

Das erste Glied auf der rechten Seite ist genau durch die $sl+1^{te}$, alle folgenden Glieder bis auf das letzte durch höhere Potenzen von $\mathfrak{L}$ teilbar; das letzte Glied aber möge genau durch $\mathfrak{L}^a$ teilbar sein. Nach dem vorhin Bemerkten ist dann

$$a>1+v(l-1),$$

ausser wenn $v\equiv 0$ oder $\equiv 1$ (l). Da der Exponent der höchsten in $S(A)$ aufgehenden Potenz von $\mathfrak{L}$ durch l teilbar sein muss, so ist jedenfalls

$$sl+1\geqq a. \qquad (2)$$

Hieraus folgt für $v\not\equiv 0,\ \not\equiv 1,\ (l)$,

$$sl>v(l-1).$$

Dasselbe muss aber auch für $v\equiv 1,\ (l)$ gelten, weil dann

$$a=1+v(l-1)$$

durch l teilbar, folglich das Gleichheitszeichen in (2) ausgeschlossen ist. Wenn endlich $v\equiv 0,\ (l)$, so ist $a=1+v(l-1)$ nicht durch l teilbar, daher muss in (2) notwendig das Gleichheitszeichen gelten, also

$$sl=v(l-1),$$

womit der Satz bewiesen ist.

Wenn k die primitive l^{te} Einheitswurzel ζ enthält, und wenn ein Primideal $\mathfrak{l}$ genau zur σ^{ten} Potenz in $(1-\zeta)$ aufgeht, dann ist $s=\sigma(l-1)$. Ist dann μ eine Zahl von k die genau durch eine Potenz von $\mathfrak{l}$ teilbar ist, deren Exponent zu l prim ist, dann geht $\mathfrak{l}$ in die Relativdiscriminante des relativ cyclischen Körpers $K=k(\sqrt[l]{\mu})$ auf, und die entsprechende Zahl v nimmt den grösstmöglichen Wert σl an. Wenn dagegen μ nicht durch l teilbar ist und m der höchste Exponent bedeutet, für den es eine Zahl a in k gibt, so dass $\mu\equiv a^l\ (\mathfrak{l}^m)$, dann ist die Relativdiscriminante von $K=k(\sqrt[l]{\mu})$ nur dann durch $\mathfrak{l}$ teilbar, wenn $m<\sigma l$. In diesem

Falle ist aber m notwendig prim zu l. Für die entsprechende Zahl v erhält man den Wert $v=\sigma l-m$. Denn die Zahl $A=\alpha-\sqrt[l]{\mu}$ von K ist genau durch $\mathfrak{L}^m$, und $sA-A=(1-\zeta)\sqrt[l]{\mu}$ genau durch $\mathfrak{L}^{\sigma l}$ teilbar, so dass $\sigma l=m+v$. [1]

Endlich sei noch das folgende bemerkt: Ist K/k relativ cyclisch vom Grade l^h, und wird mit $K^{(\nu)}$ der in K enthaltene relativ cyclische Oberkörper von k vom Relativgrade l^ν ($\nu=1, 2, \cdots h$) bezeichnet, und geht $\mathfrak{l}$ in die Relativdiscriminante von $K^{(1)}/k$ auf, dann zerfällt $\mathfrak{l}$ in K in die $l^{h\,\text{te}}$ Potenz eines Primideals; die Relativdiscriminante von K/k enthält dann $\mathfrak{l}$ genau zu der Potenz mit dem Exponenten:

$$l^{h-1}(v+1)(l-1)+l^{h-2}(v_1+1)(l-1)+\cdots\cdots+(v_{h-1}+1)(l-1)$$
$$=l^h-1+(l-1)\{vl^{h-1}+v_1l^{h-2}+\cdots\cdots+v_{h-1}\},$$

wo v_1, v_2, ... dieselbe Bedeutung für $K^{(2)}/K^{(1)}$, $K^{(3)}/K^{(2)}$, ... haben, wie v für $K^{(1)}/k$, und es ist

$$1\leqq v<v_1<v_2<\cdots\cdots<v_{h-1}\leqq\frac{sl^h}{l-1}.$$

§. 7.

Über die Normenreste des relativ cyclischen Körpers vom Primzahlgrade.

Es sei k ein beliebiger algebraischer Körper, K ein relativ cyclischer Oberkörper von k vom Relativgrade l, wo l eine gerade oder ungerade natürliche Primzahl ist. Eine Zahl α in k heisse dann ein **Normenrest** des Relativkörpers K nach einem Idealmodul $\mathfrak{j}$ in k, wenn es eine Zahl A in K gibt, für die

$$N(A)\equiv\alpha,\quad(\mathfrak{j}),$$

wo mit N die Relativnorm in Bezug auf k bezeichnet wird.

---

1) Vgl. Hilbert, Bericht, Satz 148, wo die hier angedeuteten Tatsachen für den Kreiskörper k bewiesen wird; dieser Beweis ist leicht auf den allgemeinen Körper k zu übertragen.

Ueber die Normenreste nach Primidealpotenzen in k gilt der folgende fundamentale Satz.

Satz. 9. *Es sei* K/k *relativ cyclisch vom Primzahlgrade* l. (I) *Wenn dann* $\mathfrak{p}$ *ein Primideal in* k *ist, welches nicht in die Relativdiscriminante von* K/k *aufgeht, dann ist jede zu* $\mathfrak{p}$ *prime Zahl in* k *Normenrest des Körpers* K *nach jeder Potenz von* $\mathfrak{p}$. (II) *Wenn dagegen* $\mathfrak{p}$ *in die Relativdiscriminante aufgeht, jedoch* $\mathfrak{p}$ *prim zu* l *ist, dann ist, von allen zu* $\mathfrak{p}$ *primen und einander nach* $\mathfrak{p}$ *incongruenten Zahlen in* k *genau der* l^{te} *Teil Normenreste nach* $\mathfrak{p}$, *hier bedeutet* e *eine beliebige natürliche Zahl.* (III) *Dasselbe gilt auch für die Potenz* $\mathfrak{l}^e$ *eines in* l *aufgehendes Primideals* $\mathfrak{l}$ *von* k, *falls* $\mathfrak{l}$ *zur Potenz* $\mathfrak{l}^{(v+1)(l-1)}$ *in die Relativdiscriminante aufgeht, und* $e>v$ *ist. Dagegen ist jede zu* $\mathfrak{l}$ *prime Zahl in* k *Normenrest nach* $\mathfrak{l}^e$, *wenn* $e \leqq v$ *ist. Hier hat die Zahl* v *die in Satz 8 angegebene Bedeutung.*[1]

Beweis (I). Wir unterscheiden vier Fälle, jenachdem $\mathfrak{p}$ in l aufgeht oder nicht, und $\mathfrak{p}$ in K zerfällt oder nicht.

Zunächst sei $\mathfrak{p}$ prim zu l, und es zerfalle $\mathfrak{p}$ in K in l von einander verschiedene Primideale:

$$\mathfrak{p}=\mathfrak{P}\mathfrak{P}'\ldots\ldots\mathfrak{P}^{(l-1)}$$

Sei f der Grad des Primideals $\mathfrak{p}$ in k, also auch der Primideale $\mathfrak{P}, \mathfrak{P}', \ldots\ldots$ in K, und es sei ρ eine Primitivzahl nach $\mathfrak{p}$. Jede Zahl a in k, die zu $\mathfrak{p}$ prim ist, genügt dann offenbar einer Congruenz der Form

$$a \equiv a_0 \rho^n, \quad (\mathfrak{p}^e),$$

wo n eine Zahl aus der Reihe $0, 1, 2, \ldots\ldots p^f-2$, und a_0 eine ganze Zahl in k ist, welche die Congruenz

$$a_0 \equiv 1, \quad (\mathfrak{p})$$

befriedigt. Demnach ist a_0 ein l ter Potenzrest nach $\mathfrak{p}^e$:

$$a_0 \equiv \gamma^l, \quad (\mathfrak{p}^e).$$

Ferner sei eine Zahl P in K so bestimmt, dass

1) Vgl. Hilbert, Bericht, §130, wo der Satz für den Kreiskörper der l^{ten} Einheitswurzeln aufgestellt ist, allerdings ohne genaue Angabe des critischen Wertes des Exponenten e in (III.)

$$P\equiv\rho,\quad(\mathfrak{P}^e),\quad\equiv 1,\quad(\mathfrak{P}'^e\mathfrak{P}''^e\ldots\ldots);$$

dann ist

$$\mathrm{N}(P)\equiv\rho,\quad(\mathfrak{p}^e),$$

demnach

$$\alpha\equiv\mathrm{N}(\gamma P^n),\quad(\mathfrak{p}^e),$$

womit der Satz im vorliegenden Falle bewiesen ist.

Zweitens sei $\mathfrak{p}$ prim zu l, und es bleibe $\mathfrak{p}=\mathfrak{P}$ prim in K. Ist dann P eine Primitivzahl nach $\mathfrak{P}$ in K, dann ist

$$\rho=\mathrm{N}(P)\equiv P^{1+p^f+p^{2f}+\ldots\ldots+p^{(l-1)f}}\qquad(\mathfrak{P})$$

offenbar eine Primitivzahl nach $\mathfrak{p}$ in k. Da jede zu $\mathfrak{p}$ prime Zahl α in k einer Congruenz der Form

$$\alpha\equiv\alpha_0\rho^n,\quad(\mathfrak{p}^e)$$

genügt, wo $\alpha_0\equiv 1\ (\mathfrak{p})$ und folglich $\alpha_0\equiv\gamma^l,\ (\mathfrak{p}^e)$, in k, so ist auch in diesem Falle

$$\alpha\equiv\mathrm{N}(\gamma P^n),\quad(\mathfrak{p}^e).$$

Drittens, sei $\mathfrak{p}=\mathfrak{l}$ ein in l aufgehehendes Primideal von k, welches in K in l von einander verschiedene Primideale zerfällt,

$$\mathfrak{l}=\mathfrak{L}\mathfrak{L}'\mathfrak{L}''\ldots\ldots\mathfrak{L}^{(l-1)}.$$

Da jede zu $\mathfrak{l}$ prime Zahl in k offenbar l^{ter} Potenzrest von $\mathfrak{l}$ ist, so ist unser Satz richtig für die erste Potenz von $\mathfrak{l}$.

Angenommen nun, es sei eine zu $\mathfrak{l}$ prime Zahl α Normenrest nach $\mathfrak{l}^e$. Wir setzen

$$\mathrm{N}(A)\equiv\alpha+\beta\lambda^e,\quad(\mathfrak{l}^{e+1}),$$

wo λ eine genau durch die erste Potenz von $\mathfrak{l}$ teilbare Zahl in k ist. Bestimmt man dann eine Zahl θ in K gemäss den Congruenzen:

$$\theta\equiv 1,\quad(\mathfrak{L}),\quad\equiv 0,\quad(\mathfrak{L}'\mathfrak{L}''\ldots\ldots),$$

so dass für die Relativspur von θ gilt:

$$\mathrm{S}(\theta)\equiv 1,\quad(\mathfrak{l}),$$

dann ist

$$\mathrm{N}(1+\xi\theta\lambda^e)\equiv 1+\xi\lambda^e,\quad(\mathfrak{l}^{e+1}),$$

wenn ξ eine beliebige Zahl in k ist.

Demnach hat man

$$N\{A(1+\xi\theta\lambda^e)\} \equiv \alpha+(\beta+\alpha\xi)\lambda^e, \quad (\mathfrak{l}^{e+1}).$$

Da man nun ξ gemäss der Bedingung

$$\beta+\alpha\xi \equiv 0, \quad (\mathfrak{l})$$

bestimmen kann, so ist erwiesen, dass α Normenrest nach der höheren Potenz $\mathfrak{l}^{e+1}$ von $\mathfrak{l}$ ist, und hiermit ist der Satz bewiesen.

Zuletzt, sei $\mathfrak{l}$ ein Primfactor von $\mathfrak{l}$ in k, und $\mathfrak{l}=\mathfrak{L}$ prim in K. Der Beweis verlaüft genau wie im vorhergehenden Falle; nur muss die Existenz einer Zahl θ in K, deren Relativspur prim zu $\mathfrak{l}$ ausfällt, besonders bewiesen werden. Sei also P eine Primitivzahl nach $\mathfrak{L}$ und

$$P^l+a_1P^{l-1}+\cdots\cdots+a_l=0$$

die Gleichung l^{ten} Grades in k, welche durch P befriedigt wird. Wäre nun $S(P^n)$ für $n=1, 2, \cdots\cdots l-1$ durch $\mathfrak{l}$ teilbar, dann musste, nach der Newton'schen Formel für die Potenzsummen, die Coefficienten $a_1, a_2, \cdots\cdots a_{l-1}$ durch $\mathfrak{l}$ teilbar sein, also

$$P^l \equiv N(P), \quad (\mathfrak{l}).$$

Alsdann wäre

$$P^l \equiv P^{1+lf+l^2f+\cdots\cdots+l^{(l-1)f}}, \quad (\mathfrak{L}),$$

wo f der Grad von $\mathfrak{l}$ in k, also lf der Grad von $\mathfrak{L}$ in K ist, folglich

$$l \equiv 1+l^f+l^{2f}+\cdots\cdots+l^{(l-1)f}, \quad (l^{lf}-1),$$

was offenbar unmöglich ist. Daher gibt es in der Tat eine Zahl θ in K derart, dass

$$S(\theta) \equiv 1, \quad (\mathfrak{l}).$$

Hiermit ist der Teil (I) unseres Satzes vollständig bewiesen.

Beweis (II.) Sei $\mathfrak{p}$ ein zu l primer Primfactor der Relativdiscriminante. Dann ist

$$\mathfrak{p}=\mathfrak{P}^l,$$

wo $\mathfrak{P}$ ein Primideal in K, und

$$\Phi(\mathfrak{P}^e)=\varphi(\mathfrak{p}^e)=p^{(e-1)f}(p^f-1),$$

wenn Φ bez. φ die Euler'sche Function bez. in K und k, und f der Grad des Primideals $\mathfrak{p}$ in k ist. Daher ist jede zu $\mathfrak{p}$ prime Zahl A in K nach jeder Potenz von $\mathfrak{P}$ einer Zahl a in k congruent,

$$A\equiv a, \quad (\mathfrak{P}^{el}),$$

woraus

$$\mathrm{N}(A)\equiv a^l, \quad (\mathfrak{p}^e),$$

d. h. jeder Normenrest nach $\mathfrak{p}^e$ ist ein l^{ter} Potenzrest von $\mathfrak{p}^e$, und umgekehrt.

Ist nun ρ eine Primitivzahl nach $\mathfrak{p}$, dann ist für jede zu $\mathfrak{p}$ prime Zahl a in k

$$a\equiv a_0\rho^n, \quad (\mathfrak{p}^e),$$

wo $a_0\equiv 1, (\mathfrak{p})$, und n eine Zahl aus der Reihe 0, 1, 2, ... p^f-2 ist. Es ist nun a_0 offenbar ein l^{ter} Rest von $\mathfrak{p}^e$. Da nach Satz 7. $p^f-1\equiv 0, (l)$, so ist ρ^n dann und nur dann ein l^{ter} Rest nach $\mathfrak{p}^e$, wenn n durch l teilbar ist. Hiermit ist der Teil (II) unseres Satzes bewiesen.

Beweis (III). Sei $\mathfrak{l}$ ein Primfactor von l in k, welcher zur $(v+1)(l-1)$ten Potenz in die Relativdiscriminante von K/k aufgeht, ferner sei $\mathfrak{l}=\mathfrak{L}^l$, wo $\mathfrak{L}$ Primideal in K ist. Wir bezeichnen in den Folgenden durchweg mit λ_e und Λ_e eine genau durch die e te Potenz bez. von $\mathfrak{l}$ und $\mathfrak{L}$ teilbare Zahl von k und K. Für die Relativspur von Λ_e erhält man dann, wie beim Beweise des Satzes 8

$$\mathrm{S}(\Lambda_e)=l\Lambda_e+\binom{l}{2}(\mathrm{s}-1)\Lambda_e+\binom{l}{3}(\mathrm{s}-1)^2\Lambda_e+\cdots\cdots+(\mathrm{s}-1)^{l-1}\Lambda_e.$$

Das erste Glied rechts ist nun genau durch die $sl+e^{\text{te}}$ Potenz von $\mathfrak{L}$, alle folgende Glieder bis auf das letzte durch die höheren Potenzen, das letzte Glied aber wenigstens durch die $e+v(l-1)^{\text{te}}$ Potenz von $\mathfrak{l}$ teilbar. Daher erhält man, wenn man die Relation:

$$sl\geqq v(l-1)$$

berücksichtigt (Satz 8),

$$\left.\begin{array}{lll} \text{wenn} \quad e<v: & \mathrm{S}(\Lambda_e)\equiv 0, & (\mathfrak{l}^{e+1}), \\ & \mathrm{S}(\Lambda_v)\equiv 0, & (\mathfrak{l}^{v}), \\ e>v: & \mathrm{S}(\Lambda_e)\equiv 0, & (\mathfrak{l}^{v+1}). \end{array}\right\} \tag{1}$$

Hieraus ist nun auf das folgende zu schliessen:

$$\text{wenn} \quad e<v: \qquad \mathrm{N}(1+\Lambda_e)=1+\lambda_e, \tag{2}$$

$$\mathrm{N}(1+\Lambda_v)\equiv 1+\mathrm{S}(\Lambda_v)+\mathrm{N}(\Lambda_v), \quad (\mathfrak{l}^{v+1}), \tag{3}$$

$$\text{wenn} \quad e>v: \qquad \mathrm{N}(1+\Lambda_e)\equiv 1, \quad (\mathfrak{l}^{v+1}). \tag{4}$$

Dies geschieht am einfachsten dadurch, dass man mit Hülfe der Newton'schen Formel über die Potenzsummen die Teilbarkeit der elementarsymmetrischen Functionen von Λ_e, $\mathrm{s}\Lambda_e, \cdots\cdots \mathrm{s}^{l-1}\Lambda_e$ durch die entsprechenden Potenzen von $\mathfrak{l}$ nach (1) bestätigt. Nach (2) und (3) folgt nun, dass

$$\mathrm{N}(1+\Lambda_e)\equiv 1, \quad (\mathfrak{l}^{v}),$$

dann und nur dann, wenn

$$e \geqq v,$$

woraus weiter, dass für zwei zu $\mathfrak{L}$ prime Zahlen A, B

$$\mathrm{N}(A)\equiv \mathrm{N}(B), \quad (\mathfrak{l}^{v}),$$

dann und nur dann, wenn

$$A \equiv B, \quad (\mathfrak{L}^{v}).$$

Berücksichtigt man daher die Relation

$$\Phi(\mathfrak{L}^{v})=\varphi(\mathfrak{l}^{v}),$$

dann ersieht man, dass jede zu $\mathfrak{l}$ prime Zahl in k, Normenrest nach $\mathfrak{l}^{v}$ und folglich nach jeder niederen Potenz von $\mathfrak{l}$ ist.

Da, nach (4), auch für den Modul $\mathfrak{l}^{v+1}$, aus der Congruenz

$$A \equiv B, \quad (\mathfrak{L}^{v+1}),$$

die andere:

$$\mathrm{N}(A)\equiv \mathrm{N}(B), \quad (\mathfrak{l}^{v+1})$$

zu folgern ist, so wird unser Satz für $\mathfrak{l}^{\nu+1}$ bewiesen sein, wenn nachgewiesen wird, dass die Bedingung

$$\mathrm{N}(A)\equiv 1, \quad (\mathfrak{l}^{\nu+1}) \tag{5}$$

durch genau l einander nach $\mathfrak{l}^{\nu+1}$ incongruenten Zahlen befriedigt wird. Nach (2) kommt hierzu nur die Zahlen von der Form

$$1+A_\nu \tag{6}$$

in Frage. Es gibt nun in der Tat eine Zahl von dieser Gestalt, welche der Congruenz (5) genügt. Es ist nämlich $A_1-\mathrm{s}\,A_1$ genau durch $\mathfrak{L}^{\nu+1}$ teilbar. Bringt man daher den Bruch $\mathrm{s}\,A_1 : A_1$ in die Gestalt

$$\frac{\mathrm{s}\,A_1}{A_1}=\frac{A_0}{\alpha},$$

wo α und A_0 zu $\mathfrak{L}$ prime ganze Zahlen bez. in k und K sind, und worin $\alpha\equiv 1$ nach einer beliebig hohen Potenz von $\mathfrak{l}$ angenommen werden kann, dann ist

$$\mathrm{N}(A_0)=\alpha^l\equiv 1, \quad (\mathfrak{l}^{\nu+1}).$$

Anderseits folgt aus

$$\alpha\,\mathrm{s}\,A_1=A_0\,A_1,$$

oder

$$A_1(A_0-\alpha)=\alpha(\mathrm{s}\,A_1-A_1),$$

dass $A_0-\alpha$ genau durch $\mathfrak{L}^\nu$ teilbar ist, demnach nach Annahme über α

$$A_0=1+A_\nu^{(0)}.$$

Nach (3) genügt diese besondere Zahl $A_\nu^{(0)}$ der Congruenz

$$\mathrm{S}(A_\nu^{(0)})+\mathrm{N}(A_\nu^{(0)})\equiv 0, \quad (\mathfrak{l}^{\nu+1}). \tag{7}$$

Für jede Zahl A von der Form (6) gilt nun

$$A\equiv 1+\rho\,A_\nu^{(0)}, \quad (\mathfrak{L}^{\nu+1}), \tag{8}$$

also nach (4) und (3)

$$\mathrm{N}(A)\equiv 1+\rho\,\mathrm{S}(A_\nu^{(0)})+\rho^l\,\mathrm{N}(A_\nu^{(0)}), \quad (\mathfrak{l}^{\nu+1}).$$

Daher ist

$$N(A)\equiv 1, \quad (\mathfrak{l}^{v+1})$$

dann und nur dann, wenn

$$\rho\, S(A_v^{(v)})+\rho^l N(A_v^{(v)})\equiv 0, \quad (\mathfrak{l}^{v+1}),$$

oder nach (7), wenn

$$\rho(\rho^{l-1}-1)\, N(A_v^{(v)})\equiv 0, \quad (\mathfrak{l}^{v+1}),$$

oder

$$\rho(\rho^{l-1}-1)\equiv 0, \quad (\mathfrak{l}),$$

was dann und nur dann der Fall ist, wenn ρ einer rationalen Zahl nach $\mathfrak{l}$ congruent ist. Die Congruenz (5) wird daher genau durch l nach $\mathfrak{l}^{v+1}$ incongruente Zahlen befriedigt, die man erhält, wenn in (8) $\rho=0, 1, 2, \ldots\ldots l-1$ gesetzt wird, wie zu beweisen war.

Ferner ist, wenn t eine positive ganze rationale Zahl, ρ eine zu $\mathfrak{l}$ prime Zahl in k ist,

$$N(1+\rho\lambda_t A_v)\equiv 1+\rho\lambda_t S(A_v), \quad (\mathfrak{l}^{v+t+1}),$$

also, da nach (7), $S(A_v)$ genau durch $\mathfrak{l}^v$ teilbar ist,

$$N(1+\rho\lambda_t A_v)=1+\rho\lambda_{v+t}. \tag{9}$$

Ist also α Normenrest nach $\mathfrak{l}^{v+1}$, und zwar

$$N(A)\equiv\alpha+\beta\lambda_{v+t}. \quad (\mathfrak{l}^{v+t+1}),$$

wo β zu $\mathfrak{l}$ prim, und für λ_{v+} dieselbe Zahl wie in (9) angenommen wird, dann ist

$$N\{A(1+\rho\lambda_{t+v})\}\equiv\alpha+(\alpha\rho+\beta)\lambda_{v+t}, \quad (\mathfrak{l}^{v+t+1}).$$

Da man ρ aus

$$\alpha\rho+\beta\equiv 0, \quad (\mathfrak{l})$$

bestimmen kann, so ist α Normenrest nach $\mathfrak{l}^{v+t+1}$. Jeder Normenrest nach $\mathfrak{l}^{v+t}$ ist daher Normenrest nach jeder höheren Potenz von $\mathfrak{l}$, und weil jeder Normennichtrest nach $\mathfrak{l}^{v+1}$ umsomehr Normennichtrest nach jeder höheren Potenz von $\mathfrak{l}$ ist, so ist hiermit unser Satz in allen seinen Teilen vollständig bewiesen.

In der Folge benutzen wir den Satz 9 in der folgenden verallgemeinerten Form:

Satz 10. *Sei* K/k *relativ cyclisch vom Primzahlgrade* l, *die Relativdiscriminante* $\mathfrak{d}$ *von* K/k *enthalte* d *von einander verschiedene Primideale von* $\mathfrak{k}$ *als Factor, derart, dass*

$$\mathfrak{d}=\mathfrak{f}^{l-1}, \quad \mathfrak{f}=\Pi\mathfrak{p}.\ \Pi\mathfrak{l}^{v+1},$$

wo die Producte $\Pi\mathfrak{p}$, $\Pi\mathfrak{l}^{v+1}$ *bez. auf die zu* l *primen und in* l *aufgehenden Primfactoren von* $\mathfrak{d}$ *zu erstrecken sind. Ist dann* $\mathfrak{m}$ *ein beliebiges durch* $\mathfrak{f}$ *teilbares Ideal von* k, *dann ist, von allen zu* $\mathfrak{m}$ *primen und einander nach* $\mathfrak{m}$ *incongruenten Zahlen von* k, *genau der* l^d *te Teil Normenrest des Körpers* K *nach dem Modul* $\mathfrak{m}$.

§. 8.

Einheiten im relativ cyclischen Körper.

Im relativ cyclischen Körper K/k vom Primzahlgrade l, sei eine Zahlengruppe O vorgelegt, welche eine Congruenzgruppe ist mit oder ohne Vorzeichenbedingung, und welche gegenüber der Substitution s des Relativkörpers invariant ist, d.h. von der Art, dass mit einer Zahl A zugleich die relativ conjugirte A^s darin enthalten ist. Die Gesamtheit der Zahlen von O, welche im Grundkörper k enthalten sind, bildet dann eine Zahlengruppe o in k, welche auch eine Congruenzgruppe ist.

Wenn mit R, r bez. die Anzahl der Grundeinheiten in K, k also auch in O, o bezeichnet wird, dann ist, wenn l ungerade ist

$$R-r=(l-1)(r+1), \tag{1}$$

dagegen, wenn $l=2$, also $K=k(\sqrt{\mu})$ relativ quadratisch ist,

$$R-r=r+1-\nu, \tag{2}$$

wenn ν die Anzahl derjenigen reellen mit k conjugirten Körper bedeutet, worin die mit μ conjugirten Zahlen negativ ausfallen.

Satz 11. *In der Zahlengruppe* O *lassen sich stets ein System von* n *Einheiten* $H_1, H_2, \ldots H_n$ *finden, derart, dass sich jede Einheit* E *in* O *in der Form:*

$$E=H_1^{u_1}H_2^{u_2}\cdots\cdots H_n^{u_n}H^{1-s}[\xi] \qquad (3)$$

darstellen lässt, wo die Exponenten u_1, u_2, ... *Zahlen aus der Reihe* 0, 1, 2, ... $l-1$ *sind,* H *eine Einheit in* O, $[\xi]$ *eine Einheit in* o *oder aber eine Einheit in* O, *deren* l^{te} *Potenz in* o *liegt, bedeutet. Die Einheiten* H_1, H_2, ... H_n *sind in dem Sinne von einander unabhängig, dass eine Einheit von der Gestalt* (3) *nur dann gleich* 1 *sein kann, wenn* $u_1=u_2=\cdots\cdots=u_n=0$.

Die Zahl n *hat den folgenden Wert:*

$$n=r+1, \qquad \text{wenn } l \text{ ungerade ist,}$$
$$n=r+1-\nu, \qquad \text{wenn } l=2.$$

Beweis. Die Einheiten

$$H^{1-s}[\xi]$$

bilden in ihrer Gesamtheit eine Untergruppe der Gruppe der sämtlichen Einheiten in O, von einem endlichen Index l^n, weil die l^{te} Potenz jeder Einheit in O darin enthalten ist. Letzteres folgt unmittelbar aus der Identität:

$$1+s+s^2+\cdots\cdots+s^{l-1}=l+(1-s)\,Q(s), \qquad (4)$$

wo

$$Q(s)=(1-s)^{l-2}-l\,(1-s)^{l-3}+\cdots\cdots+\binom{l}{3}(1-s)-\binom{l}{2},$$

speciell

$$Q(s)=-1, \quad \text{wenn } l=2.$$

Hiernach ist die Existenz eines Systems von Einheiten mit der im Satz angegebenen Eigenschaften ohne weiteres klar; es handelt sich nur noch darum, die Anzahl n dieser Einheiten zu finden, was auf der folgenden Weise geschieht.

Da sich die Einheit H auf der rechten Seite von (3) wieder in der Form:

$$H=H_1^{u_1'}H_2^{u_2'}\cdots\cdots H_n^{u_n'}H'^{1-s}[\xi']$$

darstellen lässt, so kann man setzen

$$E=H_1^{u_1+u_1'(1-s)}\cdots\cdots H_n^{u_n+u_n'(1-s)}H^{(1-s)^2}[\xi],$$

wenn man sich bedenkt, dass $[\xi']^{1-s}=1$ oder $=\zeta$, wo ζ eine primitive l^{te} Einheitswurzel bedeutet, letzteres nur dann, wenn

$$K=k([\xi']),$$

und folglich $\zeta=[\xi']^{1-s}$ in o enthalten ist.

Indem wir auf diese Weise fortfahren, erhalten wir

$$E=H_1^{F_1(s)}\cdots\cdots H_n^{F_n(s)}H^{(1-s)^{l-1}}[\xi], \tag{5}$$

wo

$$F_1(s)=u_1+u_1'(1-s)+\cdots\cdots+u_1^{(l-2)}(1-s)^{l-2},\cdots\cdots$$

und die Coefficienten u_1, u_1'.....sämtlich Zahlen aus der Reihe: 0, 1, 2,.....$l-1$ sind.

Wir untersuchen nun die Annahme: es sei

$$1=H_1^{F_1(s)}\cdots\cdots H_n^{F_n(s)}H^{(1-s)^{l-1}}[\xi]. \tag{6}$$

Aus der Bedeutung des Einheitensystems H_1, H_2,.....H_n folgt zunächst

$$u_1=u_2=\cdots\cdots=u_n=0,$$

so dass, für $l=2$, schon

$$F_1(s)=0,\cdots\cdots F_n(s)=0,$$

und für ein ungerades l,

$$1=\left(H_1^{G_1(s)}\cdots\cdots H_n^{G_n(s)}H^{(1-s)^{l-2}}\right)^{1-s}[\xi], \tag{7}$$

wo

$$G_1(s)=u_1'+u_1''(1-s)+\cdots\cdots+u_1^{(l-2)}(1-s)^{l-3},\cdots\cdots$$

Eine Relation von der Gestalt

$$H^{1-s}=[\xi],$$

wo H eine Einheit in O bedeutet, ist aber offenbar nur dann möglich, wenn $N([\xi])=[\xi]^l=1$, so dass $[\xi]$ eine l^{te} Einheitswurzel ist. Ist $[\xi]=1$, dann ist H selbst, ist aber $[\xi]=\zeta$ eine primitive l^{te} Einheitswurzel, H^l eine Einheit in o; jedenfalls ist H selbst

eine Einheit, die wir mit $[\xi]$ bezeichnen können. Demnach kann man statt (7) einfach setzen:

$$1=H_1^{G_1(s)}\cdots\cdots H_n^{G_n(s)}H^{(1-s)^{l-2}}[\xi].$$

Die Einheit H auf der rechten Seite bringen wir wieder auf die Form

$$H=H_1^{v_1}\cdots\cdots H_n^{v_n}H'^{1-s}[\xi'],$$

so dass wir erhalten

$$1=H_1^{F_1'(s)}\cdots\cdots H_n^{F_n'(s)}H^{(1-s)^{l-1}}[\xi],$$

wo

$$F_1'(s)=u_1'+u_1''(1-s)+\cdots\cdots+u_1^{(l-2)}(1-s)^{l-3}+v_1(1-s)^{l-2},\cdots\cdots$$

ähnliche Bedeutung wie $F_1(s)$.....haben. Daher folgt weiter

$$u_1'=u_2'=\cdots\cdots\cdots u_n'=0.$$

So fortfahrend sieht man ein, dass, auch für ungerades l, aus (6) notwendig folgt:

$$F_1(s)=0,\cdots\cdots\cdots F_n(s)=0.$$

Daher sind die $n(l-1)$ Einheiten

$$H_1,\ H_1^{1-s},\cdots\cdots H_1^{(1-s)^{l-2}};\cdots\cdots H_n,\ H_n^{1-s},\cdots\cdots H_n^{(1-s)^{l-2}}$$

unabhängig in Bezug auf die Gruppe der Einheiten:

$$H^{(1-s)^{l-1}}[\xi].$$

Diese Gruppe ist aber identisch mit der Gruppe der Einheiten:

$$H^l[\xi],$$

weil

$$(1-s)^{l-1}\equiv 1+s+\cdots\cdots\cdots+s^{l-1},\ (l),$$

und anderseits

$$(1-s)^{l-1}\varphi(s)+(1+s+\cdots\cdots+s^{l-1})\psi(s)=l,$$

wo $\varphi(s)$, $\psi(s)$ ganzzahlige ganze rationale Functionen von s sind.[1]

1) Für $\psi(s)$ kann man die $l-1$ ersten Glieder der formalen Entwickelung von $l/(1+s+\cdots\cdots+s^{l-1})$ nach steigenden Potenzen von $1-s$ nehmen.

Daher lässt sich jede Einheit E von O in der Gestalt

$$E=H_1^{F_1(s)}\ldots\ldots H_n^{F_n(s)}H^t[\xi]$$

darstellen, wo $F_1(s),\ldots\ldots F_n(s)$ mit E eindeutig bestimmt sind.

Da die sämtlichen Einheiten in O und die Einheiten $[\xi]$ H^t bez l^{R+1} und l^{r+1}, oder l^R und l^r Einheitenverbände [1] in O ausmachen, jenachdem eine Einheitswurzel, deren Ordnung eine Potenz von l ist, in O vorkommt oder nicht, so ergibt sich

$$R-r=n(l-1).$$

Wenn man hierin den Wert von $R-r$ nach (2) oder (3) einträgt, so erhält man den im Satz angegebenen Wert von n.

Satz 12. *Machen die Relativnormen sämtlicher Einheiten in* O l^{v_0} *Einheitenverbände in* o *aus, dann gibt es in* O ρ *Einheiten* E_1, $E_2,\ldots\ldots E_\rho$ *mit der Relativnorm* 1, *von der Beschaffenheit, dass jede Einheit in* O *mit der Relativnorm* 1 *in der Form:*

$$E_1^{u_1}E_2^{u_2}\ldots\ldots E_\rho^{u_\rho}H^{1-s} \qquad (8)$$

darstellbar ist, wo u_1, $u_2,\ldots\ldots u_\rho$ *Zahlen aus der Reihe* 0, 1, 2,..... $l-1$ *sind, und* H *eine Einheit in* O *bedeutet; diese Einheiten* E_1, $E_2,\ldots\ldots E_\rho$ *sind in dem Sinne von einander unabhängig, dass eine Einheit der Form* (8) *nur dann gleich* 1 *sein kann, wenn* $u_1=u_2=\ldots\ldots=u_n=0$.

Die Zahl ρ *hat den Wert:*

$$\rho=r+1+\delta-v_0, \qquad \text{wenn } l \text{ ungerade ist,}$$
$$\rho=r+1+\delta-\nu-v_0, \qquad \text{wenn } l=2,$$

wo $\delta=1$ *oder* $\delta=0$ *zu setzen ist, jenachdem die primitive* l^{te} *Einheitswurzel in* o *vorkommt oder nicht.*

Beweis. Hier wiederum handelt es sich nur um die Bestätigung des für ρ angegebenen Wertes, da die Existenz des Einheitensystems E_1, $E_2,\ldots\ldots E_\rho$ mit der im Satz angegebenen

1) Unter einem Einheitenverband in O verstehen wir ein System der Einheiten in O von der Form EH^t, wo E eine gegebene Einheit in O ist, und H alle Einheiten von O durchläuft. Vgl. Hilbert, Math. Ann. 51, S. 21.

Eigenschaften ohne weiteres klar ist. Wir unterscheiden nun drei Fälle:

Erstens sei vorausgesetzt: die primitive l^{te} Einheitswurzel ζ kommt nicht in o vor. Dann kann die Einheit $[\xi]$ in (3) nur die Einheiten in o bedeuten, und weil es keine Einheit in o gibt, ausser der Einheit 1, mit der Relativnorm 1, so kann man E_1, $E_2, \ldots\ldots E_\rho$ für ρ der Einheiten H_1, $H_2, \ldots\ldots H_n$ in (3) nehmen, es seien diese $H_{n-\rho+1}, \ldots\ldots H_n$, sodass jede Einheit in O in der Form:

$$E=H_1^{u_1}\cdots\cdots H_{n-\rho}^{u_{n-\rho}}E_1^{v_1}\cdots\cdots E_\rho^{v_\rho}H^{1-s}[\xi] \quad (0\leqq u, v<l)$$

darstellbar ist, und zwar so, dass die Relativnorm der Einheit E nicht gleich 1 sein kann, ausser wenn $u_1=u_2=\cdots\cdots=u_{n-\rho}=0$. Setzt man daher

$$\eta_1=\mathrm{N}(H_1),\cdots\cdots\cdots\eta_{n-\rho}=\mathrm{N}(H_{n-\rho}),$$

dann ergibt sich für jede Einheit E in O

$$\mathrm{N}(E)=\eta_1^{u_1}\cdots\cdots\eta_{n-\rho}^{u_{n-\rho}}\xi^l, \qquad (0\leqq u<l)$$

und somit

$$v_o=n-\rho,$$

woraus nach Einsetzen des im Satz 11 angegebenen Wertes von n und Berücksichtigung von $\delta=0$ der gesuchte Wert von ρ sich ergibt.

Zweitens sei vorausgesetzt: es komme ζ in o vor, jedoch sei K nicht durch die l^{te} Wurzel einer Einheit in o erzeugt. Hier ist wieder die Einheit $[\xi]$ in (3) die Einheit in o, und es ist ζ in dem System der Einheiten $[\xi]$, nicht aber in H^{1-s} enthalten. Wir setzen demnach

$$E_1=H_{n-\rho+2},\cdots\cdots\cdots E_{\rho-1}=H_{n-1}; \quad E_\rho=\zeta,$$

sodass jede Einheit E in O sich in der Form

$$E=H_1^{u_1}\cdots\cdots H_{n-\rho+1}^{u_{n-\rho+1}}E_1^{v_1}\cdots\cdots E_\rho^{v_\rho}H^{1-s}[\xi] \quad (0\leqq u, v<l)$$

darstellen lässt, wo für jedes E das System der Exponenten u, v eindeutig bestimmt ist. Folglich

$$N(E)=\eta_1^{u_1}\cdots\cdots\eta_{n-\rho+1}^{u_{n-\rho+1}}\xi^l,$$

woraus

$$v_0=n-\rho+1.$$

Da hier $\delta=1$ zu setzen ist, so ist in diesem Falle unser Satz bewiesen.

Zuletzt sei vorausgesetzt: es komme ζ in o vor, und $K=k(\sqrt[l]{\eta_0})$, wo η_0 eine Einheit in o ist. Setzt man nun

$$H_0=\sqrt[l]{\eta_0},$$

dann kann in (3) die Einheiten $[\xi]$ durch $H_0^{u_0}$ ersetzt werden, wenn u_0 eine Zahl aus der Reihe: 0, 1, 2,.....$l-1$ und ξ eine Einheit in o bedeutet. Ferner ist ζ in dem System H^{1-s} enthalten, es ist nämlich $\zeta=H_0^{1-s}$. Demnach kann man setzen

$$E_1=H_{n-\rho+1},\cdots\cdots E_\rho=H_n,$$

so dass jede Einheit E in O auf einer einzigen Weise in der Form:

$$E=H_0^{u_0}H_1^{u_1}\cdots\cdots H_{n-\rho}^{u_{n-\rho}}E_1^{v_1}\cdots\cdots E_\rho^{v_\rho}\xi \qquad (0\leqq u, v<l)$$

darstellbar ist; und es ist

$$N(E)=\eta_0^{u_0}\eta_1^{u_1}\cdots\cdots\eta_{n-\rho}^{u_{n-\rho}}\xi^{l}.^{1)}$$

Daher ist

$$v_0=n-\rho+1,$$

woraus mit $\delta=1$ der gesuchte Wert von ρ sich ergibt.

§. 9.

Formulirung eines Fundamentalsatzes.

Nachdem in den vorhergehenden die vorbereitenden Sätze erledigt worden, sind wir nun im Stande, einen Fundamentalsatz zu formuliren, dessen Beweis das Hauptzweck der nachfolgenden Paragraphen dieses Capitels sein soll.

1) Wenn $l=2$, ist η_0 durch $-\eta_0$ zu ersetzen.

Satz 13. *Die Relativdiscriminante des relativ cyclischen Körpers* K/k *vom ungeraden Primzahlgrade* l *sei* $\mathfrak{d}=\mathfrak{f}^{l-1}$, *wo*

$$\mathfrak{f}=\Pi\mathfrak{p}.\ \Pi\mathfrak{l}^{v+1},$$

wo $\mathfrak{p}$ *ein zu* l *primes, und* $\mathfrak{l}$ *ein in* l *aufgehendes Primideal von* k *bedeutet. Die Idealclassen von* k *seien nach einer Zahlengruppe* $\mathfrak{o}$ *definirt, welche aus den Zahlen* α *besteht, die der Congruenz:*

$$\alpha\equiv 1,\ (\mathfrak{m})$$

genügen, wo der Modul $\mathfrak{m}$ *ein beliebiges durch* $\mathfrak{f}$ *teilbares Ideal von* k *ist. Dann sind die Relativnormen aller zu* $\mathfrak{m}$ *primen Ideale von* K *in einer Classengruppe vom Index* l *in* k *enthalten.*

Dasselbe gilt auch für den relativ quadratischen Körper $K=k(\sqrt{\mu})$, *wenn an Stelle von* $\mathfrak{o}$ *eine Zahlengruppe* $\bar{\mathfrak{o}}$ *mit gewisser Vorzeichenbedingung angenommen wird. Es soll nämlich nur diejenigen Zahlen von* $\mathfrak{o}$ *in* $\bar{\mathfrak{o}}$ *aufgenommen werden, welche wenigstens in allen denjenigen mit* k *conjugirten reellen Körpern, worin* μ *negativ ausfällt, positiv sind.*[1]

Mit andern Worten:

Jeder relativ Abel'sche Körper vom Primzahlgrade l *mit der Relativdiscriminante* $\mathfrak{f}^{l-1}$ *ist der Classenkörper für eine Classengruppe nach dem Modul* $\mathfrak{f}$.[2]

§. 10.

Die Anzahl der ambigen Classen im relativ cyclischen Körper eines ungeraden Primzahlgrades.

Es sei K/k ein relativ cyclischer Körper von einem ungeraden Primzahlgrade l, und es sei s eine erzeugende Substitution der Galois'schen Gruppe des Relativkörpers K/k. Eine Idealclasse C des Körpers K heisst **ambig**, wenn sie mit der relativ conjugirten Classe sC identisch ist; im Zeichen:

$$C^{1-s}=1.$$

1) Wenn k_1 ein mit k conjugirter reeller Körper ist, dann soll eine Zahl α von k abkürzend als „positiv oder negativ in k_1" bezeichnet werden, wenn die mit α conjugirte Zahl in k_1 positiv bez. negativ ausfällt, ungeachtet des Vorzeichens von α selbst oder auch wenn α selbst imaginär ist; diese Abkürzung wird in den folgenden durchgehend beibehalten werden.

2) Vgl. § 4.

Eine Classe ist ambig, wenn sie ein Ideal des Grundkörpers k, oder ein ambiges Ideal des Relativkörpers K/k, oder aber ein Product eines ambigen Ideals und eines Ideals in k enthält, nicht aber umgekehrt.

Ueber die Anzahl der ambigen Classen im Körper K gibt der folgende Satz Aufschluss.

Satz 14. *Wenn*

h *die Classenzahl des Körpers* k,

r *die Anzahl der Grundeinheiten in* k,

δ *die Zahl* 1 *oder* 0, *jenachdem* k *die primitive* l^{te} *Einheitswurzel* ζ *enthält oder nicht,*

d *die Anzahl der von einander verschiedenen ambigen Primideale des Körpers* K/k,

l^v *die Anzahl der Einheitenverbände in* k, *die durch die Relativnormen von Einheiten und von gebrochenen Zahlen des Körpers* K *gebildet sind,*

a *die Anzahl der ambigen Classen des Körpers* K *ist, dann wird*

$$a = hl^{d+v-(r+1+\delta)}$$

In diesem Satze sollen die Idealclassen der Körper K *und* k *im absoluten Sinne genommen werden.*

Beweis. Wir zählen zunächst diejenigen ambigen Classen des Körpers K ab, welche durch die ambigen Ideale von K/k und die Ideale von k erzeugt werden. Die Ideale

$$\mathfrak{D}\mathfrak{j},$$

wo $\mathfrak{D}$ ein ambiges Ideal von K/k (oder das Ideal 1), und $\mathfrak{j}$ ein Ideal in k bedeutet, bilden, weil $\mathfrak{D}^l$ ein Ideal in k ist, in ihrer Gesamtheit eine Gruppe der Ordnung $l^d h$, worin der Inbegriff der ganzen und gebrochenen monomischen (Haupt-) Ideale von k das Hauptelement der Gruppe ist. Diese Gruppe sei mit D bezeichnet. Diejenigen der Elemente dieser Gruppe, welche in K in die Hauptclasse übergehen, bilden dann eine Untergruppe D_0 von D. Dann ist offenbar die Anzahl a_0 der aus $\mathfrak{D}$ und $\mathfrak{j}$ entspringenden ambigen Classen von K gleich dem Gruppenindex $(D : D_0)$.

Es seien nun, wie in Satz 12, wo jetzt O und o sämtliche Zahlen des Körpers K bez. k umfassen sollen,

$$E_1, E_2, \cdots\cdots E_\rho$$

die Einheiten des Körpers K mit der Relativnorm 1, von der folgenden Beschaffenheit:

1°. Jede Einheit E von K mit der Relativnorm 1 ist in der Form darstellbar:

$$E=E_1^{u_1}E_2^{u_2}\cdots\cdots E_\rho^{u_\rho}H^{l-s},$$

wo $u_1, u_2, \ldots\ldots u_\rho$ Zahlen aus der Reihe: 0, 1, 2, $\ldots\ldots l-1$ sind, und H eine Einheit von K bedeutet.

2°. Diese ρ Einheiten sind in dem Sinne von einander unabhängig, dass niemals eine Beziehung von der Form

$$1=E_1^{u_1}E_2^{u_2}\cdots\cdots E_\rho^{u_\rho}H^{l-s} \qquad (0\leqq u<l)$$

bestehen kann, ausser wenn $u_1=u_2=\ldots\ldots=u_\rho=0$.

Da $N(E_i)=1$ ist, so gibt es ganze Zahlen A_i in K, derart, dass[1]

$$E_i=A_i^{l-s} \qquad (i=1, 2, \cdots\cdots \rho)$$

und zwar ist nach 2° A_i nicht eine Einheit in K. Das Hauptideal (A_i) ist daher von der Form $\mathfrak{D}\mathfrak{j}$ und es ist $(\mathfrak{D}\mathfrak{j})^l=N(A_i)$ ein Hauptideal in k.

Da eine Beziehung von der Form:

$$A_1^{u_1}A_2^{u_2}\cdots\cdots A_\rho^{u_\rho}=Ha, \qquad (0\leqq u<l)$$

wo H eine Einheit in K, a eine Zahl in k bedeutet, die andere:

$$E_1^{u_1}E_2^{u_2}\cdots\cdots E_\rho^{u_\rho}=H^{l-s}$$

nach sich zieht, so bedingt sie, dass die Exponenten $u_1, u_2, \ldots\ldots u_\rho$ sämtlich verschwinden. Setzt man also

$$(A_i)=\mathfrak{D}_i\mathfrak{j}_i \qquad (i=1, 2, \cdots\cdots \rho)$$

so erzeugen diese Ideale genau l^ρ Elemente der Gruppe D_0.

Ist aber umgekehrt

$$\mathfrak{D}\mathfrak{j}=(A)$$

ein Hauptideal in K, so ist

$$A^{l-s}=E,$$

1) Vgl. Hilbert, Bericht, Satz 90.

wo E eine Einheit in K ist, für welche

$$\mathrm{N}(E)=1$$

ausfällt. Daher ist nach 1°

$$E=E_1^{u_1}\,E_2^{u_2}\cdots\cdots E_\rho^{u_\rho}\,H,^{1-s} \qquad (0\leqq u<l)$$

wo H eine Einheit in K ist, oder

$$A^{1-s}=(A_1^{u_1}\,A_2^{u_2}\cdots\cdots A_\rho^{u_\rho}\,H)^{1-s},$$

folglich

$$A=A_1^{u_1}\,A_2^{u_2}\cdots\cdots A_\rho^{u_\rho}\,H\alpha,$$

wo α eine Zahl in k bedeutet. Das Ideal $\mathfrak{Dj}$ ist daher unter den oben erwähnten l^ρ Elementen der Gruppe D_0 enthalten.

Hiermit ist nachgewiesen, dass die Gruppe D_0 von der Ordnung l^ρ ist; für den Gruppenindex $a_0=(D: D_0)$ ergibt sich daher

$$a_0=hl^{n-\rho} \qquad (1)$$

Wenn mit v_0 die Anzahl der Einheitenverbände in k, die aus den sämtlichen Relativnormen der Einheiten von K bestehen, bezeichnet wird, dann gibt es nach Annahme noch $v-v_0$ unabhängigen Einheiten in k, welche Relativnormen der gebrochenen Zahlen von K sind:

$$\varepsilon_1=N(\theta_1),\cdots\cdots\varepsilon_{v-v_0}=\mathrm{N}(\theta_{v-v_0}),$$

von der Art, dass jede Einheit ε von k, welche Relativnorm einer gebrochenen Zahl von K ist, in der Form darstellbar ist:

$$\varepsilon=\varepsilon_1^{u_1}\,\varepsilon_2^{u_2}\cdots\cdots\mathrm{N}(H), \qquad (0\leqq u<l)$$

wo H eine Einheit in K bedeutet, und dass eine Beziehung

$$1=\varepsilon_1^{u_1}\,\varepsilon_2^{u_2}\cdots\cdots\mathrm{N}(H) \qquad (0\leqq u<l)$$

niemals bestehen kann, ausser wenn die $v-v_0$ Exponenten $u_1, u_2,\ldots\ldots$ sämtlich verschwinden.

Sei nun

$$\theta_1=\Pi\mathfrak{p}^{F(\mathfrak{p})}$$

die Zerlegung der gebrochenen Zahl θ_1 in die Primideale von K,

wo also der Exponent $F(s)$ der symbolischen Potenz eine ganzzahlige ganze rationale Function vom Grade $l-1$ in s bedeutet, und das Product auf alle mit θ_1 verwandten, einander nicht relativ conjugirten Primideale $\mathfrak{p}$ erstreckt werden soll. Da aber $N(\theta_1)$ gleich einer Einheit ist, so folgt, dass

$$F(s)(1+s+s^2+\cdots\cdots+s^{l-1})$$

durch $1-s^l$, folglich $F(s)$ selbst durch $1-s$ teilbar ist. Wir können demnach setzen:

$$\theta_i=\mathfrak{A}_i^{1-s} \qquad (i=1, 2, \cdots\cdots v-v_0)$$

wo $\mathfrak{A}_i$ ein ganzes oder gebrochenes Ideal von K ist. Die l^{te} Potenz dieses Ideals $\mathfrak{A}_i$ ist in K mit einem Ideal $\mathfrak{a}_i$ von k, nämlich der Relativnorm von $\mathfrak{A}_i$ aequivalent:

$$\mathfrak{A}_i^l=N(\mathfrak{A}_i)\mathfrak{A}_i^{(1-s)Q(s)}=\theta_i^{Q(s)}\mathfrak{a}_i,$$

wo $Q(s)$ die bekannte Bedeutung hat.[1] Es kann aber eine Beziehung von der Form

$$\mathfrak{A}_1^{u_1}\,\mathfrak{A}_2^{u_2}\cdots\cdots=\mathfrak{D}\mathfrak{j}A, \qquad (0\leqq u<l)$$

wo A eine Zahl von K bedeutet, niemals bestehen, ausser wenn die $v-v_0$ Exponenten $u_1, u_2, \ldots\ldots$ sämtlich verschwinden; denn aus dieser Idealgleichheit folgt, durch das Erheben in die symbolische $1-s^{te}$ Potenz,

$$\theta_1^{u_1}\,\theta_2^{u_2}\cdots\cdots=HA,^{1-s}$$

wo H eine Einheit in K ist, und daraus ferner, indem wir in die Relativnorm übergehen,

$$\varepsilon_1^{u_1}\,\varepsilon_2^{u_2}\cdots\cdots=N(H),$$

was das Verschwinden der Exponenten $u_1, u_2, \ldots\ldots$ bedingt.

Mit anderen Worten: die Ideale $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots$ erzeugen $v-v_0$ ambigen Classen von K, die sowohl von einander als von den durch die Ideale $\mathfrak{D}\mathfrak{j}$ erzeugten unabhängig sind.

Anderseits ist jedes Ideal $\mathfrak{A}$ aus einer ambigen Classe von K in der Form darstellbar:

---

1) Vgl. S. 36.

$$\mathfrak{A}=\mathfrak{A}_1^{u_1}\mathfrak{A}_2^{u_2}\cdots\cdots\mathfrak{D}\mathfrak{j}A, \qquad (0\leqq u<l)$$

wo A eine Zahl von K bedeutet.

Denn aus $\mathfrak{A}\overset{1-s}{=}\theta$, folgt $\mathrm{N}(\theta)=\varepsilon$, wo ε eine Einheit in k ist, und hieraus der Reihe nach:

$$\varepsilon=\varepsilon_1^{u_1}\,\varepsilon_2^{u_2}\cdots\cdots\mathrm{N}(H), \qquad \text{wo } H \text{ eine Einheit in K ist,}$$

$$\mathrm{N}(\theta)=\mathrm{N}(\theta_1^{u_1}\,\theta_2^{u_2}\cdots\cdots H),$$

$$\theta=\theta_1^{u_1}\,\theta_2^{u_2}\cdots\cdots HA, \qquad \text{wo } A \text{ eine Zahl von K ist,}$$

$$\mathfrak{A}\overset{1-s}{=}(\mathfrak{A}_1^{u_1}\mathfrak{A}_2^{u_2}\cdots\cdots A),$$

$$\mathfrak{A}=\mathfrak{A}_1^{u_1}\mathfrak{A}_2^{u_2}\cdots\cdots A\mathfrak{D}\mathfrak{j}.$$

Demnach ist

$$a=a_0\,l^{v-v_0},$$

also nach (1)

$$a=hl^{d+v-(\rho+v_0)}.$$

Da nach Satz 12

$$\rho=r+1+\delta-v_0,$$

so ist

$$a=hl^{d+v-(r+1+\delta)}$$

wie zu beweisen war.

§. 11.

Die Anzahl der ambigen Classen im relativ quadratischen Körper.

Satz 15. *Wenn* $\mathrm{K}=\mathrm{k}(\sqrt{\mu})$ *relativ quadratisch in Bezug auf* k *ist, und wenn* ν *die Anzahl derjenigen mit* k *conjugirten reellen Körper ist, worin die Conjugirten von* μ *negativ ausfallen, dann ist, unter Beibehaltung der übrigen Bezeichnungsweise von Satz 14.*

$$a=hl^{d+v+\nu-(r+\delta)}$$

Die Classen in K *wie in* k *sollen wiederum im absoluten Sinne genommen werden.*

Der Beweis verläuft genau wie bei Satz 14; nur soll am Schlusse für die Zahl ρ der im gegenwärtigen Falle gültige Wert:

$$r+2-\nu-v_0$$

eingesetzt werden (vgl. Satz 12).

Es sei noch bemerkt, dass im Falle, wo die mit k conjugirten Körper sämtlich imaginär sind, dieser Satz genau mit Satz 14 zusammenfällt, weil dann $\nu=0$ und die Zahl δ in Satz 14 gleich 1 zu setzen ist, da die Einheitswurzel -1 in k vorkommt.

§. 12.

Die Geschlechter im relativ cyclischen Körper eines ungeraden Primzahlgrades.

Es sei K/k relativ cyclisch vom ungeraden Primzahlgrade l, $\mathfrak{d}=\mathfrak{f}^{l-1}$ die Relativdiscriminante desselben, o die Zahlengruppe in k, die aus der Gesamtheit der zu $\mathfrak{f}$ primen *Normenreste des Körpers* K/k *nach* $\mathfrak{f}$ besteht. Die Idealclassen in k seien nach o definirt, so dass zwei Ideale $\mathfrak{j}_1$ und $\mathfrak{j}_2$ in k dann und nur dann aequivalent sind, wenn die Idealgleichheit besteht:

$$\mathfrak{j}_1=\mathfrak{j}_2\alpha \text{ und } \alpha\equiv \mathrm{N}(A), \ (\mathfrak{f}),$$

wo α und A zu $\mathfrak{f}$ prime ganze oder gebrochene Zahlen von k bez. K sind.

Wenn dann zwei Ideale $\mathfrak{J}_1$ und $\mathfrak{J}_2$ von K im absoluten Sinne aequivalent sind, und einer Classe (im absoluten Sinne) C von K angehören, dann fallen die Relativnormen dieser Ideale in eine und dieselbe Classe c nach o hinein; diese Classe c heisse die Relativnorm der Classe C; im Zeichen

$$\mathrm{c}=\mathrm{N}(\mathrm{C}).$$

Da o eine Congruenzgruppe nach dem Modul $\mathfrak{f}$ ist, so ist Satz 4 anwendbar, demzufolge die Classengruppe von k, welche sämtliche Relativnormen der Classen von K enthält, von einem Index i sein muss, welcher den Relativgrad l des Relativkörpers K/k nicht übertreffen kann:

$$i\leqq l. \qquad (1)$$

Sei G die Gruppe der sämtlichen Classen von K, H die Untergruppe von G, welche aus der Gesamtheit derjenigen Classen

von K besteht, deren Relativnormen die Hauptclasse nach o sind. Dann ist der Gruppenindex (G:H) offenbar gleich der Ordnung derjenigen Classengruppe von k nach o, welche aus der sämtlichen Relativnormen der Classen von K besteht. Daher folgt aus (1)

$$(G:H)=\frac{h'}{i}\geqq\frac{h'}{l}, \tag{2}$$

wenn h' die Classenzahl von k nach o bedeutet.

Ferner sei H_0 die Gruppe der Classen von K, welche symbolische $1-s^{te}$ Potenzen der Classen von K sind, so dass der Gruppenindex

$$(G:H_0)=a,$$

der Anzahl der ambigen Classen von K ist.

Da offenbar H_0 eine Untergruppe von H ist, so folgt nach (2)

$$a=(G:H_0)\geqq(G:H)\geqq\frac{h'}{l}, \tag{3}$$

Nach Satz 14 ist nun[1]

$$a=hl^{d+v-(r+1+\delta)} \tag{4}$$

wenn h die Classenzahl von k im absoluten Sinne bedeutet.

Anderseits ist, wenn o' die Gruppe der sämtlichen zu $\mathfrak{f}$ primen Zahlen in k bedeutet, nach Satz 10

$$(o':o)=l^d, \tag{5}$$

wo d die Anzahl der von einander verschiedenen in $\mathfrak{f}$ aufgehenden Primideale in k ist, also dieselbe Bedeutung hat, wie in (4).

Ist ferner E' die Gruppe der sämtlichen Einheiten in k, und E die der Einheiten in o, dann ist offenbar

$$(E':E)=l^{r+\delta-n}, \tag{6}$$

wenn r und δ dieselbe Bedeutung haben, wie in (4), und l^n die Anzahl der Einheitenverbände in o ist.

Demnach ist[2] nach (5) und (6)

1) Die Beschränkung, dass wir hier nur die zu $\mathfrak{f}$ primen Ideale von K in Betracht ziehen, hat keinen Einfluss auf die Anzahl a gewisser Classen von K, die ja im absoluten Sinne genommen wird, vgl. Satz 2.

2) Vgl. § 1, S. 7.

$$h'=h\frac{(\mathfrak{o}':\mathfrak{o})}{(\mathfrak{E}':\mathfrak{E})}=hl^{d+n-(r+\delta)} \tag{7}$$

Aus (3), (4), und (7) folgt

$$d+v-(r+1+\delta)\geqq d+n-(r+\delta)-1,$$

oder

$$0\geqq n-v.$$

Da offenbar $n-v\geqq 0$, so erhält man

$$n=v. \tag{8}$$

Dies hat zur Folge, dass in (3) und somit auch in (2) und (1) notwendig das Gleichheitszeichen gelten muss. Demnach ergibt sich

$$a=\frac{h'}{l}, \tag{9}$$

$$\mathfrak{H}=\mathfrak{H}_0, \tag{10}$$

$$i=l. \tag{11}$$

Hiermit ist der Fundamentalsatz 13 für einen relativ cyclischen Körper vom ungeraden Primzahlgrade bewiesen, denn wenn die Classen von k nach einem beliebigen durch $\mathfrak{f}$ teilbaren Ideale $\mathfrak{m}$ definirt werden, so mag sich jede Classe nach $\mathfrak{o}$ in gleichviele Classen nach $\mathfrak{m}$ auflösen, jedoch ohne dass der *Index* einer Classengruppe verändert wird.

Aus dem vorhergehenden Beweis von Satz 13 ziehen wir noch einige wichtige Schlüsse:

Alle diejenige Classe von K, deren Relativnorm eine und dieselbe Classe von k nach der Gruppe $\mathfrak{o}$ der Normenreste nach $\mathfrak{f}$ ist, fassen wir in ein **Geschlecht** zusammen, und definiren speciell das *Hauptgeschlecht* als den Inbegriff derjenigen Classen von K, deren Relativnormen die Hauptclasse von k nach $\mathfrak{o}$ sind. Das Hauptgeschlecht ist also die Classengruppe $\mathfrak{H}$, und das Geschlecht, welchem eine Classe C angehört der Classencomplex $\mathfrak{H}C$. Also folgt aus (9) und (10):

Satz 16. *Die Anzahl der Geschlechter in* K *ist gleich dem* l^{ten} *Teil der Classenzahl von* k *nach* $\mathfrak{o}$.

Satz 17. *Jede Classe des Hauptgeschlechts in* K *ist die symbolische* $l-s^{te}$ *Potenz einer Classe von* K.

Ferner gilt

Satz 18. *Wenn eine Einheit in* k, *oder eine Zahl in* k, *die* l^{te} *Potenz eines Ideals von* k *ist, Normenrest des Körpers* K/k *nach dem Ideale* $\mathfrak{f}$ *ist, dann ist sie wirkliche Relativnorm einer ganzen oder gebrochenen Zahl von* K.

Beweis. Was die Einheiten betrifft ist dieser Satz schon in (8) enthalten. Sei also $(\nu)=\mathfrak{j}^l$, und ν Normenrest des Körpers K/k nach $\mathfrak{f}$. Da $N(\mathfrak{j})=\mathfrak{j}^l=(\nu)$, und ν der Zahlengruppe o angehört, so ist das Ideal $\mathfrak{j}$ in einer Classe des Hauptgeschlechts von K enthalten. Daher ist nach Satz 17

$$\mathfrak{j}=\mathfrak{J}^{1-s}\theta,$$

wo $\mathfrak{J}$ ein Ideal, θ eine Zahl in K bedeutet. Bildet man beiderseits die Relativnormen, so erhält man

$$\nu=\varepsilon N(\theta),$$

wo ε eine Einheit in k ist. Da nun ν Normenrest nach $\mathfrak{f}$ ist, so gilt dasselbe auch von ε; folglich ist nach (8) ε eine wirkliche Relativnorm. Setzt man daher

$$\varepsilon=N(A),$$

dann folgt

$$\nu=N(A\theta).$$

§. 13.

Die Geschlechter im relativ quadratischen Körper.

Wenn $K=k(\sqrt{\mu})$ relativ quadratisch in Bezug auf k ist, und wenn ν die Anzahl derjenigen mit k conjugirten reellen Körper ist, worin die Conjugirten von μ negativ ausfallen, dann rechnen wir nur diejenigen Normenreste nach $\mathfrak{f}$, welche in diesen ν Körpern *positiv* ausfallen, in die Zahlengruppe o^+, und legen dieselbe der Classeneinteilung in k zu Grunde.

Da die Relativnormen der zu $\mathfrak{f}$ primen Zahlen von K offenbar der Zahlengruppe o^+ angehören, so fallen die Relativnormen aller

Ideale einer Classe (im absoluten Sinne) C von K in eine und dieselbe Classe c von k nach o^+; dieselbe nennen wir demnach die Relativnorm der Classe C von K: $c=N(C)$.

Die Betrachtungen, die wir im vorhergehenden Paragraphen angestellt haben, werden mit geringen Modificationen auch im gegenwärtigen Falle genau dieselben Resultaten ergeben. Indem wir uns durchweg die Bezeichnungsweise des vorigen Artikels bedienen, ist zunächst h' die Classenzahl von k nach o^+, so dass

$$h'=h\frac{(o':o^+)}{(E':E^+)},$$

wo E^+ die Gruppe der Einheiten in o^+ bedeutet. Es ist also nach Satz 10

$$(o':o^+)=2^{d+\nu},$$

weil die Congruenzbedingung, Normenrest nach $\mathfrak{f}$ zu sein, welcher eine Zahl von k zu genügen hat, unabhängig ist von der Vorzeichencombination dieser Zahl in den ν oben specifirten Körpern.

Sodann ist

$$(E':E)=2^{r+1-n},$$

wenn 2^n die Anzahl der Einheitenverbände in o^+ bedeutet.

Daher ist

$$h'=h.\ 2^{d+\nu+n-(r+1)},$$

Die Bedingung

$$a\geqq\frac{h'}{2}$$

ergibt, wenn man darin für a den in Satz 15 angegebenen Wert

$$a=h\,2^{d+v+\nu-(r+2)}$$

einsetzt,

$$d+v+\nu-(r+2)\geqq d+\nu+n-(r+1)-1,$$

oder

$$0\geqq n-v,$$

woraus wie vorhin

$$n=v,$$

und folglich

$$a=\frac{h'}{2},$$

$$H=H_0,$$

$$i=2.$$

Die letzte Gleichheit beweist Satz 13 für einen relativ quadratischen Körper.

Wenn die Gesamtheit derjenigen Classen von K, deren Relativnormen eine und dieselbe Classe von k nach o^+ sind, in ein **Geschlecht,** diejenigen, deren Relativnormen die Hauptclasse von k nach o^+ sind, in das *Hauptgeschlecht* gerechnet werden, dann gelten die Sätze:

Satz 19. *Die Anzahl der Geschlechter in einem relativ quadratischen Körper ist gleich der Hälfte der Classenzahl von* k *nach* o^+.

Satz 20. *Jede Classe des Hauptgeschlechts in einem relativ quadratischen Körper ist die symbolische* $1-s^{te}$ *Potenz einer Classe von* K.

Ferner gilt.

Satz 21. *Wenn eine Einheit von* k *oder eine Zahl von* k, *welche Idealquadrat in* k *ist, positiv in den mit* k *conjugirten reellen Körpern worin die Zahl* μ *negativ ausfällt*[1] *und Normenrest des relativquadratischen Körpers* $K=k(\sqrt{\mu})$ *nach dem Ideal* $\mathfrak{f}$ $(=\mathfrak{d})$ *ist, dann ist sie wirklich Relativnorm einer Zahl von* K.

§. 14.

Eine Verallgemeinerung des Geschlechterbegriffs.

Es sei $\mathfrak{f}^{l-1}$ die Relativdiscriminante des relativ cyclischen Körpers K/k vom Primzahlgrade l, $\mathfrak{m}$ ein beliebiges durch $\mathfrak{f}$ teilbares Ideal in k, o die Zahlengruppe in k, welche aus der Gesamtheit derjenigen Zahlen ω in k besteht, die der Congruenz:

$$\omega\equiv 1, \quad (\mathfrak{m})$$

1) Vgl. Fussnote 1), S. 42.

genügen, und im Falle: $l=2$, überdies total positiv sind.

Wir legen diese Zahlengruppe o der Classeneinteilung im Grundkörper k zu Grunde, und verallgemeinern den Begriff der Geschlechter in K dahin, dass die Ideale in K nur dann in ein Geschlecht gerechnet werden, wenn ihre Relativnormen in eine und dieselbe Classe nach o hineinfallen. Insbesondere ist demnach das Hauptgeschlecht die Gesamtheit der Ideale $\mathfrak{J}$ in K, deren Relativnormen in der Hauptclasse nach o liegen, d. h.

$$\mathrm{N}(\mathfrak{J})=(\omega), \quad \text{wo} \quad \omega\equiv 1, \quad (\mathfrak{m}),$$

und, wenn $l=2$, überdies noch ω total positiv ist.

Dass die Anzahl der Geschlechter gleich dem l^{ten} Teil der Classenzahl nach o ist, dass also die Sätze 16 und 19 auch für die Geschlechter im verallgemeinerten Sinne gelten, ist einleuchtend, nach einer Bemerkung in § 12 (S. 50). Zweck dieses Artikels ist es nun, nachzuweisen, dass es möglich ist, eine geeignete Zahlengruppe O in K so zu bestimmen dass, wenn die Classen in K nach derselben definirt werden, jede Classe des Hauptgeschlechtes in K die symbolische $(1-s)^{\text{te}}$ Potenz einer Classe von K wird, dass also auch die Sätze 17 und 20 ihre Gültigkeit beibehalten werden. Wir müssen uns aber zunächst mit einigen Hulfssätzen beschäftigen.

Hülfssatz 1. *Ist* $\mathfrak{q}$ *ein Primideal in* k, *welches nicht in die Relativdiscriminante des relativ cyclischen Körpers* K/k *vom Primzahlgrade* l *aufgeht,* θ *eine Zahl in* K, *welche der Bedingung*

$$\mathrm{N}(\theta)\equiv 1, \quad (\mathfrak{q}^{e}) \qquad (1)$$

genügt, wo e *ein beliebiger positiver Exponent ist, dann gibt es in* K *eine zu* $\mathfrak{q}$ *prime Zahl* A, *derart, dass*

$$\theta\equiv \mathrm{A}^{1-s} \quad (\mathfrak{q}^{e}).$$

Beweis. Wir bedienen uns auch hier mit Vorteil des Gruppenbegriffs. Sei G die Gruppe der sämtlichen zu $\mathfrak{q}$ primen Zahlclassen von K nach dem Modul $\mathfrak{q}^{e}$, H diejenige der Zahlclassen, deren

Zahlen die Bedingung (1) befriedigen, endlich H_0 die der Zahlclassen, welche durch die Zahlen A^{1-s} representirt werden. Es ist dann zu beweisen, dass

$$H=H_0.$$

Da offenbar H_0 eine Untergruppe von H ist, so gilt für die Gruppenindices

$$(G:H) \leqq (G:H_0).$$

Berücksichtigt man nun, dass, wenn $\theta \equiv 1, (\mathfrak{q}^e)$, offenbar $N(\theta) \equiv 1, (\mathfrak{q}^e)$ ist, so sieht man ein, dass $(G:H)$ gleich der Anzahl der Normenrestclassen in k nach $\mathfrak{q}^e$, also nach Satz 9

$$(G:H)=\varphi(\mathfrak{q}^e).$$

Anderseits ist $(G:H_0)$ offenbar gleich der Anzahl der Zahlclassen, deren Zahlen der Bedingung

$$A^{1-s} \equiv 1, \quad (\mathfrak{q}^e) \qquad (2)$$

genügt. Unser Satz wird daher bewiesen sein, wenn gezeigt wird, dass jede Zahl A, welche der Congruenz (2) genügt, notwendig congruent einer Zahl in k nach dem Modul $\mathfrak{q}^e$ ausfallen muss.

Dies ist einleuchtend, wenn $\mathfrak{q}$ prim zu l ist, denn aus (2) folgt

$$A \equiv A^s \equiv A^{s^2} \cdots \equiv A^{s^{l-1}} \quad (\mathfrak{q}^e),$$

daher

$$lA \equiv S(A), \quad (\mathfrak{q}^e),$$

wo $S(A)$ die Relativspur von A, also eine Zahl in k ist. Da l prim zu $\mathfrak{q}$ ist, so folgt hieraus das Gesagte.

Wenn $\mathfrak{q}=\mathfrak{l}$ ein in $\mathfrak{l}$ aufgehendes Primideal ist, unterscheiden wir zwei Fälle, jenachdem $\mathfrak{l}$ in K in l von einander verschiedene Primideale zerfällt, oder prim bleibt.

Im ersten Falle, sei

$$\mathfrak{l}=\mathfrak{L}(s\,\mathfrak{L})\,(s^2\,\mathfrak{L})\cdots\cdots$$

Da dann $\Phi(\mathfrak{L}^e)=\Phi(s\mathfrak{L}^e)=\cdots\cdots=\varphi(\mathfrak{l})$ so ist für jede Zahl A in K

$$A\equiv a,\ (\mathfrak{L}^e),\ \equiv a',\ (s\mathfrak{L}^e)\cdots\cdots$$

wo a, a',……Zahlen in k sind. Ist also $A\equiv A^s$, $(\mathfrak{l}^e)$, dann muss, da $A^s\equiv a$, $(s\mathfrak{L}^e)$,…… $a\equiv a'$, $(s\mathfrak{L}^e)$, also $a\equiv a'$, $(\mathfrak{l}^e)$; ebenso $a'\equiv a''$, $(\mathfrak{l}^e)$, usw. Folglich ist

$$A\equiv a,\quad (\mathfrak{l}^e).$$

Zweitens sei $\mathfrak{l}=\mathfrak{L}$ prim in K. Ist dann $\mathfrak{l}$ Primideal f^{ten} Grades in k, also lf ten Grades in K, dann ist bekanntlich für jede zahl A in K

$$A^s\equiv A,^{l^f}\quad (\mathfrak{L}).$$

Ist daher $A\equiv A^s$ $(\mathfrak{L})$, dann ist

$$A\equiv A,^{l^f}\quad (\mathfrak{L}),$$

also, wenn A prim zu $\mathfrak{l}$ ist,

$$A^{l^f-1}\equiv 1,\quad (\mathfrak{L}).$$

Dies ist aber das Kriterium dafür, dass A einer Zahl a in k nach $\mathfrak{L}$ congruent sein soll.

Sei ferner

$$A\equiv A^s\quad (\mathfrak{L}^2),$$

dann kann man setzen

$$A\equiv a+\lambda B,\quad (\mathfrak{L}^2),$$

wo a eine Zahl in k, λ eine durch die erste Potenz von $\mathfrak{l}$ teilbare Zahl in k, und B eine Zahl in K ist. Dann folgt

$$B\equiv B,^s\quad (\mathfrak{L}).$$

also nach dem vorhergehenden

$$B\equiv\beta,\quad (\mathfrak{L}),$$

wo β eine Zahl in k ist. Es ist also auch

$$A\equiv a',\quad (\mathfrak{L}^2),$$

wo a' eine Zahl in k ist. So fortfahrend beweist man den Satz für jede beliebige Potenz von $\mathfrak{l}$ als Modul.

Es sei noch bemerkt, dass dieser Beweis für das Primideal $\mathfrak{l}$ auch für die zu l primen Primideale $\mathfrak{p}$ seine Gültigkeit beibehält.

Hülfssatz 2. *Es sei $\mathfrak{p}$ ein zu l primes Primideal in* k, *welches in die Relativdiscriminante des relativ cyclischen Körpers* K/k *vom Primzahlgrade l aufgeht, so dass $\mathfrak{p}$ die l^{te} Potenz eines Primideals $\mathfrak{P}$ in* K *ist. Ferner sei Θ eine Zahl in* K, *welche der Bedingung*

$$N(\Theta)\equiv 1, \quad (\mathfrak{p}^e)$$

genügt, wo e ein beliebiger positiver Exponent ist. Dann gibt es eine Zahl A in K, *derart, dass*

$$\Theta\equiv A,^{1-s} \quad (\mathfrak{P}^{(e-1)l+1}),$$

wenn für A auch eine durch $\mathfrak{P}$ teilbare Zahl zugelassen wird.

Dasselbe gilt auch dann, wenn $\mathfrak{p}=\mathfrak{l}$ in l aufgeht, vorausgesetzt, dass für den Modul der ersten Congruenz $\mathfrak{l}^{v+n}$, für den der zweiten $\mathfrak{L}^{v+nl}$ angenommen wird, wo n eine beliebige positive ganze rationale Zahl ist, und v die bisherige Bedeutung für das Primideal $\mathfrak{l}=\mathfrak{L}^l$ hat.[1]

Beweis. Es habe G, H, H_0 dieselbe Bedeutung wie bei dem Beweis des vorhergehenden Hülfssatzes. Wir bemerken zuvörderst, dass, wenn Π (bez. A) eine genau durch die erste Potenz von $\mathfrak{P}$ (bez. $\mathfrak{L}$) teilbare Zahl in K ist, Π^{1-s} (bez. A^{1-s}) offenbar eine Zahl ist, die der Gruppe H angehört, von der aber erst die l^{te} Potenz der Gruppe H_0 angehören kann, weil eine Congruenz

$$\Pi^{1-s}\equiv A,^{1-s} \ (\mathfrak{P}), \quad \text{bez.} \quad A^{1-s}\equiv A,^{1-s} \quad (\mathfrak{L}^{v+1})$$

unmöglich ist, wenn A prim zu $\mathfrak{P}$ (bez. $\mathfrak{L}$) sein soll.

Daher ist der Gruppenindex

$$(H : H_0)\geqq l.$$

Anderseits ist, weil aus $\Theta\equiv 1$, $(\mathfrak{P}^{(e-1)l+1})$ bez. $(\mathfrak{L}^{v+nl})$ offenbar folgt: $N(\Theta)\equiv 1$ $(\mathfrak{p}^e)$ bez. $(\mathfrak{l}^{v+n})$ [2], der Gruppenindex (G: H) gleich der Anzahl der Normenrestclassen in k nach $\mathfrak{p}^e$ bez. $\mathfrak{l}^{v+n}$, also nach Satz 9

1) Vgl. Satz 8, S. 24.

2) Vgl. S. 34, Gl. (9).

$$(G:H)=\frac{1}{l}\varphi(\mathfrak{p}^e) \text{ bez. } \frac{1}{l}\varphi(\mathfrak{l}^{v+n}).$$

Unser Satz wird daher bewiesen sein, wenn gezeigt wird, dass $(G:H_0)$ oder, was dasselbe ist, die Anzahl der zu $\mathfrak{P}$ bez. $\mathfrak{L}$ primen Zahlclassen nach dem Modul $\mathfrak{P}^{(e-1)l+1}$ bez. $\mathfrak{L}^{v+nl}$, deren Zahlen A der Congruenz

$$A\equiv A^s, \quad (\mathfrak{P}^{(e-1)l+1}),$$

bez.
$$A\equiv A^s, \quad (\mathfrak{L}^{v+nl}) \tag{3}$$

genügen, genau $\varphi(\mathfrak{p}^e)$ bez. $\varphi(\mathfrak{l}^{v+n})$ beträgt.

Für das zu l primes $\mathfrak{P}$ ist dies einleuchtend, wie beim Beweis des vorhergehenden Hülfssatzes. Um den Satz für das Primideal $\mathfrak{L}$ zu beweisen, sei Λ_t eine genau durch die t^{te} Potenz von $\mathfrak{L}$ teilbare Zahl. Setzt man eine Zahl A in der Form an:

$$A\equiv\alpha+\Lambda_t,$$

wo α eine Zahl in k ist, und t für gegebenes A den möglichst grossen Wert haben soll, so dass t nicht durch l teilbar ist, dann genügt A dann und nur dann der Congruenz (3), wenn

$$t>nl.$$

Diese Zahlen A werden also durch

$$A\equiv\alpha_0+\beta_1\Lambda^{nl+1}+\cdots\cdots+\beta_{v-1}\Lambda^{v+nl-1}, \quad (\mathfrak{L}^{v+nl}),$$

gegeben, wenn für α_0 die $\varphi(\mathfrak{l}^{n+1})$ einander nach $\mathfrak{l}^{n+1}$ incongruenten zu $\mathfrak{l}$ prime Zahlen in k, für $\beta_1,\cdots\cdots\beta_{v-1}$ je ein System der l^f einander nach $\mathfrak{l}$ incongruenten Zahlen in k gesetzt werden. Es ergibt sich also für die Anzahl in Frage der Wert

$$\varphi(\mathfrak{l}^{n+1}).\, l^{f(v-1)}=\varphi(\mathfrak{l}^{n+v}).$$

wie nachzuweisen war.[1]

1) Ohne Satz 9 zu benutzen, zeigt man leicht, wie aus der vorhergehenden Beweise einzusehen ist, dass der Normenrest nach $\mathfrak{p}^e$ bez. $\mathfrak{l}^{v+n}$ *höchstens* den l^{ten} Teil der sämtlichen Zahlclassen nach $\mathfrak{p}^e$ bez. $\mathfrak{l}^{v+n}$ ausmachen kann. Mit dieser Obergrenze für die Anzahl der Normenreste kommt man aber beim Beweis des Satzes 13 in §12 aus. Denn alsdann ist auf der rechten Seite von (5) (S. 49) $d+x$ statt d zu setzen, wo $x\geqq 0$. Dann erhält man zunächst $0\geqq n-v+x$, woraus notwendig $n-v=0$ und $x=0$ folgt. So wäre der Satz 10 auf diesem Umwege von neuem bewiesen sein. Diese Bemerkung füge ich zu, als eine Verificirung des Satzes 10.

In den Folgenden benutzen wir die Hülfssätze 1, 2 in der verallgemeinerten Fassung, die wie folgt lautet.

Hülfssatz 3. *Es sei* $\mathfrak{f}^{l-1}$ *die Relativdiscriminante des relativ cyclischen Körpers* K/k *vom Primzahlgrade* l, $\mathfrak{m}=\mathfrak{f}\mathfrak{a}$ *ein beliebiges durch* $\mathfrak{f}$ *teilbares Ideal in* k. *Entsprechend seien*

$$\mathfrak{F}=\Pi\mathfrak{P}.\,\Pi\mathfrak{Q}^{\nu+1},\quad \mathfrak{M}=\mathfrak{F}\mathfrak{a}$$

Ideale in K, *wo das Product* $\Pi\mathfrak{P}$ *auf alle von einander verschiedenen in* $\mathfrak{f}$ *aufgehenden und zu* l *primen Primideale von* K, *und das Product* $\Pi\mathfrak{Q}^{\nu+1}$ *auf alle diejenigen, welche in* l *aufgehen, zu erstrecken ist. Ist dann* θ *eine zu* $\mathfrak{M}$ *prime Zahl in* K, *welche der Bedingung*

$$\mathrm{N}(\theta)\equiv 1,\quad (\mathfrak{m})$$

genügt, dann gibt es in K *eine Zahl* A, *derart, dass*

$$\theta\equiv A^{1-s},\quad (\mathfrak{M})$$

wird. Die Zahl A *ist unter Umständen nicht prim zu* $\mathfrak{M}$, *ist aber von der Art, dass*

$$(A)=\mathfrak{A}^{1-s},$$

wo $\mathfrak{A}$ *ein zu* $\mathfrak{M}$ *primes Ideal in* K *ist, dass ferner, wenn* $l=2$, A *eine beliebig vorgeschriebene Vorzeichencombination in den mit* K *conjugirten Körpern haben kann.*

Beweis. Setzt man

$$\mathfrak{m}=\Pi\mathfrak{p}^{e}\,\Pi\mathfrak{l}'^{\pm u}\,\Pi\mathfrak{q}^{e'},$$

dann ist, nach Annahme

$$\mathfrak{M}=\Pi\mathfrak{P}^{(e-1)l+1}\,\Pi\mathfrak{Q}^{\nu+ul}\,\Pi\mathfrak{q}^{e'},$$

wo das erste und das zweite Product bei $\mathfrak{m}$ sowie bei $\mathfrak{M}$ die bekannte Bedeutung haben und das dritte Product auf alle in $\mathfrak{m}$ enthaltenen, zu $\mathfrak{f}$ primen Primideale zu erstrecken ist. Nach Hülfssätzen 1 und 2 ergibt daher für θ die Congruenzen

$$\Theta \equiv \Pi^{\alpha} A_1)^{1-s}, \quad (\mathfrak{P}^{(e-1)l+1}), \ldots\ldots$$

$$\equiv (A^{\beta} A_2)^{1-s} \quad (\mathfrak{Q}^{\nu+nl}), \ldots\ldots$$

$$\equiv A_3^{1-s}, \quad (\mathfrak{q}^{e'}), \ldots\ldots$$

wo Π bez. A genau durch die erste Potenz von $\mathfrak{P}$ bez. $\mathfrak{Q}$ teilbar, und $A_1, A_2, A_3, \ldots\ldots$bez. zu $\mathfrak{P}, \mathfrak{Q}, \mathfrak{q}, \ldots\ldots$prim, und ausserdem Π und $A_1 \equiv 1$, $(\mathfrak{M} : \mathfrak{P}^{(e-1)l+1})$, A und $A_2 \equiv 1$, $(\mathfrak{M} : \mathfrak{Q}^{\nu+nl})$, $A_3 \equiv 1$, $(\mathfrak{M} : \mathfrak{q}^{e})$, usw. angenommen sind, und die Exponenten $\alpha, \beta, \ldots\ldots$Zahlen aus der Reihe $0, 1, 2, \ldots\ldots l-1$ bedeuten.

Daher ist

$$\Theta \equiv A^{1-s}, \quad (\mathfrak{M}),$$

wenn

$$A = \Pi^{\alpha} A^{\beta} \; A_1 A_2 A_3 \ldots\ldots$$

gesetzt wird. Da $\mathfrak{M} = \mathfrak{M}^s$, so wird, wenn $A \equiv B$, $(\mathfrak{M})$, offenbar $A^{1-s} \equiv B^{1-s}$, $(\mathfrak{M})$. Ersetzt man daher nach Bedarf B durch

$$A^* = A + m\Gamma,$$

wo Γ, für $l=2$, eine Zahl in K mit einer vorgeschriebene Vorzeichencombination, und m eine durch $\mathfrak{M}$ teilbare positive rationale Zahl bedeutet, die hinlänglich gross angenommen werden mag, so dass A^* dieselbe Vorzeichencombination wie Γ hat, dann wird die Forderung betreffs der Vorzeichen erfüllt. Endlich ist, wenn

$$\Pi = \mathfrak{P}\mathfrak{A}_1, \ldots\ldots$$

$$A = \mathfrak{Q}\mathfrak{A}_2, \ldots\ldots$$

gesetzt wird, nach Annahme, $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots$prim zu $\mathfrak{M}$. Daher ist

$$(A^{1-s}) = \mathfrak{A}^{1-s},$$

wo $\mathfrak{A} = \mathfrak{A}_1^{\alpha} \mathfrak{A}_2^{\beta} A_1 A_2 A_3 \ldots\ldots$ein zu $\mathfrak{M}$ primes Ideal ist. Somit ist Hülfssatz 3 in allen seinen Teilen bewiesen.

Wir gehen jetzt zum Beweis des am Anfang dieses Artikels angedeuteten Satzes über, den wir wie folgt formuliren wollen:

Satz 22. *Es sei* K/k *relativ cyclisch vom Primzahlgrade* l, *es habe die Ideale* $\mathfrak{m}$, $\mathfrak{M}$ *die im Hülfssatz 3 erklärte Bedeutung; ferner seien* o *und* O *die Zahlengruppen in* k *bez.* K, *welche aus den Zahlen* ω *bez.* Ω *bestehen, welche bez. die Congruenzen:*

$$\omega \equiv 1, \quad (\mathfrak{m}); \qquad \Omega \equiv 1, \quad (\mathfrak{M})$$

befriedigen, und überdies, wenn $l=2$, *total positiv in Bezug auf* k *bez.* K *sind.*

Werden alsdann die Idealclassen in k *und* K *bez. nach* o *und* O *definirt, dann ist jede Classe des Hauptgeschlechts in* K *nach* O *eine symbolische* $(1-s)^{te}$ *Potenz einer Classe in* K *nach* O.

Beweis. Greifen wir zum Beweise des Satzes 13 in §12 und §13 zurück, so sehen wir ein, dass jener Satz gültig bleibt, wenn man in k die Classen nach der Gruppe der Normenreste nach $\mathfrak{m}$ definiren, in K aber die Classen im absoluten Sinne annehmen (nur sollen die nicht zu $\mathfrak{m}$ primen Ideale ausser Betracht gelassen sein, was der Classeneinteilung nicht beeinflusst). Demnach genügt es nachzuweisen, dass jedes Ideal der Form $\mathfrak{J}^{1-s}\theta$ in K, für welches

$$\mathrm{N}(\mathfrak{J}^{1-s}\theta)=(\omega) \tag{4}$$

ausfällt, notwendig von der Form $\mathfrak{J}'^{1-s}\Omega$ sein muss; hier bedeutet θ eine beliebige zu $\mathfrak{M}$ fremde Zahl in K, ω und Ω dagegen Zahlen bez. in o und O.

Aus (4) folgt nun

$$\mathrm{N}(\theta)=\varepsilon\omega, \tag{5}$$

wo ε eine Einheit in k ist, welche, weil $\omega\equiv 1$, $(\mathfrak{f})$, Normenrest nach $\mathfrak{f}$, folglich nach Satz 18 sich als eine wirkliche Zahlennorm erweist.

Sei also

$$\mathrm{N}(B)=\varepsilon, \quad \text{demnach} \quad (B)=\mathfrak{B}^{1-s}, \tag{6}$$

woraus

$$\mathrm{N}\left(\frac{\theta}{B}\right)=\omega. \tag{7}$$

Daher ist nach Hülfssatz 3,

$$\frac{\theta}{B}=A^{1-s}\varrho, \tag{8}$$

wo

$$(A^{1-s})=\mathfrak{A}^{1-s}.$$

Demnach folgt nach (6) und (8)

$$\theta=(\mathfrak{A}\mathfrak{B})^{1-s}\varrho,$$

woraus, in der Tat,

$$\mathfrak{J}^{1-s}\theta=\mathfrak{J}'^{1-s}\varrho,$$

wenn $\mathfrak{J}'=\mathfrak{A}\,\mathfrak{B}\,\mathfrak{J}$ gesetzt wird.

Wir haben oben die Vorzeichenbedingungen ausser Acht gelassen. Ist nun $K=k(\sqrt{\mu})$ relativ quadratisch, dann ist in (5) ω total positiv, also ε positiv in jedem mit k conjugirten reellen Körpern, worin μ negativ ausfällt. Daher gilt nach Satz 21 die Gleichheit (6) auch in diesem Falle. Da ferner nach (7), die Zahl $\frac{\theta}{B}$ dieselbe Vorzeichen in jedem Paare zu K conjugirten Oberkörpern von k′ hat, wo k′ ein beliebiger zu k conjugirter reeller Körper ist, in welcher μ positiv ausfällt, und weil A in (8), nach Hülfssatz 3, beliebig vorgeschriebene Vorzeichencombination haben kann, so kann man A so wählen, dass A^{1-s} dieselbe Vorzeichencombination wie $\frac{\theta}{B}$ bekommt, so dass die Zahl ϱ in (8) total positiv in Bezug auf K wird. Hiermit ist unser Satz in allen seinen Teilen vollständig bewiesen.

CAPITEL III.

Existenzbeweis für den allgemeinen Classenkörper.

§. 15.

Formulirung des Existenzsatzes.

Satz 23. *In einem algebraischen Körper* k *sei eine Classengruppe* H *nach dem Modul* $\mathfrak{m}$ *mit oder ohne Vorzeichenbedingung vorgelegt. Dann existirt stets ein Classenkörper* K *für diese Classengruppe* H, *welcher die folgenden Eigenschaften besitzt:*

1) K *ist relativ Abel'sch in Bezug auf* k.

2) *Die Galois'sche Gruppe des Relativkörpers* K/k *ist holoedrisch isomorph mit der complementären Gruppe* G/H, *wo* G *die Gruppe der sämtlichen Classen von* k *bedeutet.*

3) *Die Relativdiscriminante von* K/k *enthält kein Primideal als Factor, welches nicht in den Modul* $\mathfrak{m}$ *aufgeht.*

Dieser Satz ist die naturgemässe Verallgemeinerung des zuerst von D. Hilbert [1] für den Fall: $\mathfrak{m}=1$, also für den Classenkörper im absoluten Sinne ausgesprochenen Satzes, welcher von ihm in den einfachsten Specialfällen, dann später von Ph. Furtwängler [2] für beliebige Grundkörper k bewiesen worden ist. Der Beweis des oben aufgestellten Existenzsatzes für den *allgemeinen* Classenkörper gelingt durch die gehörige Erweiterung der Hilbert'schen Methode; eine grosse Erleichterung erzielen wir aber durch Zuhülfenahme des Fundamentalsatzes 13.

§. 16.

Rang der Gruppe der Zahlclassen.

Es sei l eine gerade oder ungerade natürliche Primzahl, $\mathfrak{l}$ ein Primideal des Körpers k, welches zur $s$ten Potenz in l aufgeht, und vom f^{ten} Grade ist. Es existirt alsdann in k ein System von ρ Zahlen $\gamma_1, \gamma_2, \ldots\ldots \gamma_\rho$, welche sämtlich $\equiv 1$, $(\mathfrak{l})$, und so beschaffen sind, dass für jede zu $\mathfrak{l}$ prime Zahl γ von k eine Relation von der Form

$$\gamma \equiv \gamma_1^{u_1} \gamma_2^{u_2} \ldots\ldots \gamma_\rho^{u_\rho} \xi^l, \quad (\mathfrak{l}^g),$$

besteht, wo g eine beliebige natürliche Zahl ist, und die Exponenten $u_1, u_2, \ldots\ldots u_\rho$ für gegebenes γ eindeutig bestimmte Zahlen aus der Reihe: 0, 1, 2, $\ldots\ldots l-1$ sind.

Die Zahl ρ ist der Rang von der Abel'schen Gruppe, der Ordnung $l^{(g-1)f}$, deren Elemente diejenigen Zahlclassen nach dem

1) D. Hilbert, Ueber die Theorie der relativ Abel'schen Zahlkörper, Göttinger Nachrichten, 1898.

2) Ph. Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper usw. Math. Ann. 63.

Modul $\mathfrak{l}^v$ sind, die aus den Zahlen $\equiv 1$, $(\mathfrak{l})$ bestehen. Daher bestimmt sich ρ daraus, dass l^ρ die Anzahl der einander nach $\mathfrak{l}^v$ incongruenten Lösungen der Congruenz:

$$\xi^l \equiv 1, \quad (\mathfrak{l}^v) \tag{1}$$

ist.

Hülfssatz.[1] *Es ist*

$$\rho = \left[g - \frac{g}{l}\right] f, \quad \textit{wenn} \quad \frac{sl}{l-1} \geqq g > 0;$$

$$\rho = sf + e, \quad \textit{wenn} \quad g > \frac{sl}{l-1},$$

(*speciell* $\rho = 0$, *wenn* $g = 1$), *wo* $e = 1$, *oder* $= 0$, *jenachdem die Congruenz*

$$l + \xi^{l-1} \equiv 0, \quad (\mathfrak{l}^{v+1})$$

in k *lösbar ist, oder nicht; das Zeichen* $[x]$ *hat die gewöhnliche Bedeutung der grössten ganzen rationalen Zahl, die* x *nicht übertrifft.*

Der Fall $e = 1$ *ist nur dann möglich, wenn*

$$s = \sigma(l-1)$$

durch $l-1$ *teilbar ist. Speciell ist* $e = 1$, *wenn der Körper* k *die primitive* l^{te} *Einheitswurzel* ζ *enthält, also stets, wenn* $l = 2$.

Beweis. Bezeichnet man allgemein mit λ_n eine genau durch die n^{te} Potenz von $\mathfrak{l}$ teilbare Zahl von k, dann ist, wie leicht nachzuweisen ist,

$$\text{wenn} \quad n < \frac{s}{l-1}, \quad (1+\lambda_n)^l = 1 + \lambda_{n'}, \tag{2}$$

$$\text{wenn} \quad n > \frac{s}{l-1}, \quad (1+\lambda_n)^l = 1 + \lambda_{s+n}, \tag{3}$$

$$\text{und wenn} \quad \frac{s}{l-1} = \sigma, \quad (1+\lambda_\sigma)^l \equiv 1 + l\lambda_\sigma + \lambda_\sigma^l, \quad (\mathfrak{l}^{\sigma l+1}). \tag{4}$$

Ist also

$$\frac{sl}{l-1} \geqq g > 0,$$

1) Vgl. T. Takenouchi, diese Journal, vol. 36, Art. 1.

dann ist, nach (2)

$$(1+\lambda_n)^l \equiv 1, \quad (\mathfrak{l}^g),$$

dann und nur dann, wenn

$$nl \geqq g, \quad \text{oder} \quad n \geqq g_0,$$

wo g_0 die kleinste natürliche Zahl ist, die noch $\geqq \frac{g}{l}$ ist. Die Lösungen der Congruenz (1) sind daher die Zahlen:

$$\xi \equiv 1, \quad (\mathfrak{l}^{g_0}),$$

welche nach dem Modul $\mathfrak{l}^g$ genau $l^{(g-g_0)f}$ incongruenten Zahlen abgeben. Daher ist in diesem Falle

$$\rho = (g-g_0)f = \left[g - \frac{g}{l}\right] f.$$

Ist zweitens

$$g > \frac{sl}{l-1},$$

aber s nicht durch $l-1$ teilbar, dann sind nach (3) die Lösungen der Congruenz (1) die Zahlen:

$$\xi \equiv 1, \quad (\mathfrak{l}^{g-s}). \tag{5}$$

Daher ist in diesem Falle

$$\rho = sf.$$

Wenn aber s durch $l-1$ teilbar, also

$$g > \sigma l,$$

dann kommen nach (4) ausserdem noch die Zahlen von der Form $1+\lambda_\sigma$ in Betracht, wenn für dieselben

$$l\lambda_\sigma + \lambda_\sigma^l \equiv 0, \quad (\mathfrak{l}^{\sigma l+1}),$$

oder

$$l + \lambda_\sigma^{l-1} \equiv 0, \quad (\mathfrak{l}^{\sigma+1})$$

ausfällt. Ist nun für eine dieser speciellen λ_σ

$$\alpha = 1+\lambda_\sigma, \qquad \alpha^l \equiv 1, \quad (\mathfrak{l}^{\sigma l+1}),$$

so kann man, wie leicht ersichtlich, in

$$\alpha' = \alpha(1+\eta\lambda_{\sigma+1})$$

η so bestimmen, dass $\alpha'^{l} \equiv 1 \, (\mathfrak{l}^{\sigma l+2})$ wird. So fortfahrend erhält man eine Zahl

$$\beta_0 = 1+\lambda_\sigma^{(0)},$$

welche für beliebig grosses g der Congruenz (1) genügt. Jede Zahl β von der Form $1+\lambda_\sigma$ kann aber in der Form dargestellt werden:

$$\beta \equiv 1+\gamma\lambda_\sigma^{(0)}, \quad (\mathfrak{l}^g).$$

Soll diese Zahl die Congruenz (1) befriedigen, so muss jedenfalls

$$l+(\gamma\lambda_\sigma^{(\sigma)})^{l-1} \equiv 0, \quad (\mathfrak{l}^{s+1}),$$

weil aber auch

$$l+\lambda_\sigma^{(0)l-1} \equiv 0, \quad (\mathfrak{l}^{s+1}),$$

so ist notwendig

$$\gamma^{l-1} \equiv 1, \quad (\mathfrak{l}),$$

folglich

$$\gamma \equiv c, \quad (\mathfrak{l}),$$

wo c eine zu l prime ganze rationale Zahl ist. Demnach ist

$$\beta \equiv \beta_0^c \quad (\mathfrak{l}^{\sigma+1}),$$

also

$$\beta \equiv \beta_0^c(1+\lambda_n) \quad (\mathfrak{l}^n),$$

wo $n > \sigma$. Damit diese Zahl β der Congruenz (1) genüge, ist aber nach (3) notwendig und hinreichend, dass

$$n \geqq g-s.$$

Man sieht, dass im gegenwärtigen Falle, alle Lösungen von (1) durch die Producte der Zahlen (5) mit einer der l Zahlen

$$1, \beta_0, \beta_0^2, \ldots\ldots \beta_0^{l-1}$$

gegeben werden. Es ergibt sich also

$$\rho = sf+1.$$

Wenn die primitive l^{te} Einheitswurzel ζ in k vorkommt, dann wird die Congruenz

$$l+\xi^{l-1}\equiv 0 \qquad (\mathfrak{l}^{s+1})$$

durch $\xi=1-\zeta$ (wenn $l=2$, durch $\xi=2$) befriedigt, weil

$$\frac{l}{(1-\zeta)^{l-1}}=\frac{(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{l-1})}{(1-\zeta)^{l-1}}=(1+\zeta)\cdots(1+\zeta+\cdots+\zeta^{l-2})$$
$$\equiv \underline{|l-1} \equiv -1, \qquad (\text{mod. } 1-\zeta).$$

In diesem Falle ist daher stets $e=1$.

§. 17.

Rang der Classengruppe.

Wenn die Idealclassen des Körpers k nach der Zahlengruppe o der Zahlen $\equiv 1$ $(\mathfrak{m})$ definirt werden, und ist die Ordnung der Gruppe $\mathfrak{G}$ der sämtlichen Classen von k, d.h. die Classenzahl von k nach o genau durch die h^{te} Potenz einer geraden oder ungeraden Primzahl l teilbar, dann bezeichnen wir mit $\mathfrak{G}_0$ die Untergruppe von $\mathfrak{G}$ von der Ordnung l^h, und mit $\mathfrak{D}$ den Inbegriff aller Classen, deren Ordnungen prim zu l sind, so dass

$$\mathfrak{G}=\mathfrak{G}_0\mathfrak{D}$$

das directe Product der beiden Gruppen $\mathfrak{G}_0$ und $\mathfrak{D}$ ist. Im folgenden spielt der Rang dieser Gruppe $\mathfrak{G}_0$ eine fundamentale Rolle.

Satz 24. *Sei t die Anzahl der in $\mathfrak{G}_0$ enthaltenen unabhängigen Idealclassen im absoluten Sinne; $\mathfrak{r}_1, \mathfrak{r}_2, \ldots\ldots \mathfrak{r}_t$ ein System der Repräsentanten dieser Classen, die prim zu $\mathfrak{m}$ sind; $\rho_1, \rho_2, \ldots\ldots \rho_t$ die niedrigsten Potenzen dieser Ideale, welche monomisch sind; $\varepsilon_1, \varepsilon_2, \ldots\ldots \varepsilon_{t+\delta}$ ein System der Grundeinheiten von* k, *zu welchem wir eine derjenigen Einheitswurzeln mitrechnen, deren Ordnung eine Potenz von l, und zwar die höchste in* k, *ist, so dass $\delta=1$ oder $\delta=0$, jenachdem die primitive l^{te} Einheitswurzel in* k *vorhanden ist oder nicht, und es sei l^n die Anzahl der l^{ten} Potenzreste nach $\mathfrak{m}$, welche in dem System von $l^{t+\delta+t}$ Zahlen:*

$$\varepsilon_1^{u_1} \cdots\cdots \varepsilon_{r+\delta}^{u_{r+\delta}} \rho_1^{v_1} \cdots\cdots \rho_t^{v_t} \tag{1}$$

$$(0 \leqq u,\ v < l)$$

enthalten sind. Dann ist der Rang der Classengruppe G_0

$$\overline{t} = d + \Sigma R(g) + n - (r+\delta), \tag{2}$$

wo d *die Anzahl der in* $\mathfrak{m}$ *aufgehenden, von einander verschiedenen zu* l *primen Primideale* $\mathfrak{p}$, *für welche* $\varphi(\mathfrak{p})$ *durch* l *teilbar ist,* $R(g)$ *der im Hülfssatz des* §16 *angegebene Rang der Zahlengruppe nach dem Modul* $\mathfrak{l}^v$ *ist, und die Summation über alle in* $\mathfrak{m}$ *aufgehenden Potenzen* $\mathfrak{l}^v$ *erstreckt werden soll.*

Beweis. Da nach Voraussetzung

$$N = d + \Sigma R(g) \tag{3}$$

unabhängige l^{te} Nichtreste nach $\mathfrak{m}$ gibt und

$$N' = r + \delta + t - n \tag{4}$$

von denselben durch die Zahlen des Systems (1) gegeben werden, so lässt sich ein System von N Zahlen

$$\gamma_1,\ \gamma_2, \cdots\cdots \gamma_{N-N'},\ \eta_1,\ \eta_2, \cdots\cdots \eta_{N'}$$

aufstellen, von denen die N' letzten aus dem System (1) entnommen werden sollen, derart, dass sich jede zu $\mathfrak{m}$ prime Zahl γ von k in der Form darstellen lässt:

$$\gamma \equiv \gamma_1^{x_1} \cdots\cdots \gamma_{N-N'}^{x_{N-N'}} \eta_1^{y_1} \cdots\cdots \eta_{N'}^{y_{N'}} \xi^l, \quad (\mathfrak{m})$$

oder

$$\gamma = \gamma_1^{x_1} \cdots\cdots \gamma_{N-N'}^{x_{N-N'}} \eta_1^{y_1} \cdots\cdots \eta_{N'}^{y_{N'}} \alpha\, \xi^l, \tag{5}$$

wo die Exponenten x, y für jedes gegebene γ eindeutig bestimmte Zahlen aus der Reihe: 0, 1, 2, $\ldots\ldots l-1$ sind, und α eine Zahl in o bedeutet: $\alpha \equiv 1$, $(\mathfrak{m})$.

Ist daher $\mathfrak{r}$ ein beliebiges zu $\mathfrak{m}$ primes Ideal von k, dann besteht eine Idealgleichheit von der Form

$$\mathfrak{r} = \mathfrak{r}_1^{a_1} \cdots\cdots \mathfrak{r}_t^{a_t}\, \gamma_1^{b_1} \cdots\cdots \gamma_{N-N'}^{b_{N-N'}}\, \alpha\, \mathfrak{j}^l, \tag{6}$$

$$(0 \leqq a,\ b < l)$$

wo j ein zu m primes ganzes oder gebrochenes Ideal von k bedeutet.

Ein Ideal von der Form (6) ist aber nur dann gleich 1, wenn die Exponenten $a_1, \ldots\ldots a_t$ sämtlich verschwinden, also eine Zahlengleichheit von der Form besteht:

$$1 = \gamma_1^{b_1} \cdots\cdots \gamma_{N-N'}^{b_{N-N'}}\ \alpha\,[\varepsilon, \rho]\,\xi^l,$$

oder

$$1 \equiv \gamma_1^{b_1} \cdots\cdots \gamma_{N-N'}^{b_{N-N'}}\ [\varepsilon, \rho]\,\xi^l, \quad (\mathfrak{m}),$$

wo mit $[\varepsilon, \rho]$ eine Zahl des Systems (1) bezeichnet wird. Da nun $\gamma_1, \gamma_2, \cdots\cdots \gamma_{N-N'}$ sowohl von einander als von $[\varepsilon, \rho]$ unabhängige Nichtreste sind, so bedingt diese Congruenz, dass auch die Exponenten $b_1, \ldots\ldots b_{N-N'}$ sämtlich verschwinden.

Hiermit ist gezeigt, dass für jedes gegebene Ideal $\mathfrak{r}$, die Exponenten a, b auf der rechten Seite von (6) eindeutig bestimmt sind, dass daher der gesuchte Rang der Gruppe G_0 gleich

$$\bar{t} = t + N - N'.$$

Wenn man hierin für N und N' die Werte (3) und (4) einsetzt, so erhält man die Formel (2).

Da offenbar $N \geqq N'$, so ist stets $\bar{t} \geqq t$, wie es sein musste.

Zusatz. *Wenn* $\mathfrak{v}$ *eine beliebig vorgeschriebene Gruppe der Vorzeichencombinationen*[1] *ist, und werden die Zahlen von* $\mathfrak{o}$ *mit den Vorzeichencombinationen dieser Gruppe* $\mathfrak{v}$ *in eine engere Zahlengruppe* $\mathfrak{o}'$ *zusammengefasst, nach welcher nun die Classen von* $\mathfrak{k}$ *zu definiren sind, dann wächst für* $l = 2$ *der Rang der Classengruppe* G_0 *um*

$$p = (r_1 - r_0) - (n - n_0), \qquad (7)$$

so dass an Stelle von (2)

$$\bar{t} = d + \Sigma R(g) + n_0 + r_1 - (r + r_0 + 1) \qquad (8)$$

1) Vgl. § 1. S. 4.

zu setzen ist; hierbei ist r_1 *die Anzahl der mit* k *conjugirten reellen Körper,* 2^{r_0} *die Anzahl der Vorzeichencombinationen von* v, *endlich bestimmt sich die Zahl* n_0 *dadurch, dass von den* 2^n *im System* (1) *enthaltenen quadratischen Reste nach* $\mathfrak{m}$ *genau* 2^{n_0} *die Vorzeichencombinationen von* v *besitzen.*

Denn nach Annahme lässt sich ein System der r_1-r_0 quadratischen Reste nach $\mathfrak{m}$:

$$\alpha_1,\cdots\cdots\alpha_p,\ \eta_1'',\cdots\cdots\eta''_{n-n_0}$$

aufstellen, welche die sämtlichen r_1-r_0 von v unabhängigen Vorzeichencombinationen aufweisen, und von denen die $n-n_0$ letzten dem System (1) angehören. Daher lässt sich der Ausdruck $\alpha\xi^l$ auf der rechten Seite von (5) durch den folgenden ersetzen:

$$\alpha_1^{c_1}\cdots\cdots\alpha_p^{c_p}\,\eta_1''^{d_1}\cdots\cdots\eta''^{d_{n-n_0}}_{n-n_0}\,\alpha'\xi^{2l}$$

wo die Exponenten c, d die Zahlen 0 oder 1 sind, und α' eine Zahl in $\mathfrak{o}'$ bedeutet. An Stelle von (6) kann man demnach setzen:

$$\mathfrak{r}=\mathfrak{r}_1^{a_1}\cdots\cdots\gamma_1^{b_1}\cdots\cdots\alpha_1^{c_1}\cdots\cdots\alpha_p^{c_p}\,\alpha'\mathfrak{j}^2,$$

$$(0\leqq a,\ b,\ c<2)$$

und es kann ein Ideal dieser Form nur dann gleich 1 sein, wenn wie vorhin die sämtlichen Exponenten a, b verschwinden, und

$$1=\alpha_1^{c_1}\cdots\cdots\alpha_p^{c_p}\,[\varepsilon,\rho]\,\alpha'\,\xi^2,$$

wo $[\varepsilon,\rho]$ ein quadratischer Rest nach $\mathfrak{m}$ bedeutet, welcher dem System (1) angehört. Da nach der Voraussetzung die Zahlen $\alpha_1,\cdots\cdots\alpha_p$, $[\varepsilon,\rho]$, α' von einander unabhängige Vorzeichencombinationen besitzen, so müssen auch alle Exponenten $c_1\cdots\cdots c_p$ verschwinden.

Daher ergibt sich für den Rang von G_0 der Wert

$$\overline{t}=t+N-N'+p,$$

wie zu beweisen war

§ 18.

Existenzbeweis des Classenkörpers vom ungeraden Primzahlgrade.

Wir beschäftigen uns nun mit demjenigen Falle des in § 15 aufgestellten Existenzsatzes, in welchem der Index l der Classengruppe H eine ungerade Primzahl ist, und der Grundkörper k die primitive l^{te} Einheitswurzel ζ enthält. Unter Beibehaltung der in den beiden vorhergehenden Artikeln benutzten Bezeichnungsweise, ist zunächst

$$\delta=1\,;\ ^{1)}$$

sodann, wenn m der Grad des Körpers k ist,

$$m=2(r+1),$$

ferner ist für jedes Primideal $\mathfrak{l}$,

$$e=1,\ ^{2}$$

und

$$s=\sigma(l-1)\ ^{2)}$$

durch $l-1$ teilbar.

Der Modul $\mathfrak{m}$ enthalte d von einander verschiedene zu l prime Primideale: $\mathfrak{p}, \mathfrak{p}', \cdots\cdots \mathfrak{p}^{(d-1)}$ als Factoren, für jedes derselben $\varphi(\mathfrak{p})$ durch l teilbar ist.[3] Von den in l aufgehenden Primidealen seien diejenigen, die in $\mathfrak{m}$ aufgehen, deren Anzahl d' (mit Einschluss des Wertes: $d'=0$) sei, durchweg mit $\mathfrak{l}$, die übrigen mit $\mathfrak{l}'$ bezeichnet.

Einfachheitshalber wollen wir zunächst annehmen, dass jedes Primideal $\mathfrak{l}$, wenn überhaupt, wenigstens zur $\sigma l+1^{ten}$ Potenz in $\mathfrak{m}$ aufgehe, so dass in der Formel (2), § 17 für den Rang der Classengruppe G_0

$$R(g)=sf+1$$

---

1) Vgl. Formel (2) §17.

2) Vgl. Hülfssatz, §16.

3) Dies folgt aus der Tatsache, dass die Norm jedes Primideals in dem durch ζ erzeugten Kreiskörper congruent 1 nach l ist; vgl. Hilbert, Bericht, Satz 119.

zu setzen ist. Dieselbe Formel lautet daher im gegenwärtigen Falle:

$$\bar{t}=d+d'+\Sigma sf+n-(r+1), \tag{1}$$

wo die Summation auf alle in $\mathfrak{m}$ aufgehenden Primideale $\mathfrak{l}$ zu erstrecken ist. Die l^n in dem System

$$\varepsilon_1^{x_1}\cdots\cdots\varepsilon_{r+1}^{x_{r+1}}\rho_1^{y_1}\cdots\cdots\rho_t^{y_t} \quad (0\leqq x, y<l)$$

enthaltenen l^{ten} Potenzreste nach $\mathfrak{m}$ seien mit

$$\alpha^e\alpha'^{e'}\cdots\cdots\alpha^{(n-1)e^{(n-1)}} \quad (0\leqq e<l)$$

bezeichnet. Ich führe dann nach Hilbert n Primideale

$$\mathfrak{q},\ \mathfrak{q}',\cdots\cdots\mathfrak{q}^{(n-1)}$$

ein, die zu $\mathfrak{m}$, $\mathfrak{l}$, und $\mathfrak{r}_1, \mathfrak{r}_2, \cdots\cdots \mathfrak{r}$ prim sind, von der Art, dass

$$\left(\frac{\alpha^{(i)}}{\mathfrak{q}^{(i)}}\right)\neq 1, \quad \left(\frac{\alpha^{(j)}}{\mathfrak{q}^{(i)}}\right)=1, \quad (i\neq j) \tag{2}$$

und setze

$$\bar{\mathfrak{m}}=\mathfrak{m}\mathfrak{q}\mathfrak{q}'\cdots\cdots\mathfrak{q}^{(n-1)}$$

Dann ist in dem Ausdruck (1) für den Rang der entsprechenden Gruppe G_0 für den Modul $\bar{\mathfrak{m}}$, d durch $d+n$, dagegen n durch 0 zu ersetzen, so dass $\bar{t}$ unverändert bleibt. Dies hat zur Folge, dass jede der $l^{\bar{t}}-1 : l-1$ Classengruppen vom Index l nach dem Modul $\bar{\mathfrak{m}}$ auch Classengruppen nach $\mathfrak{m}$ ist, wobei die Primideale $\mathfrak{q}, \mathfrak{q}'\cdots\cdots \mathfrak{q}^{(n-1)}$ als unwesentlicher Excludenten auftreten.[1]

Nunmehr sei

$$\mathfrak{p}\,\mathfrak{r}_1^{a_1}\mathfrak{r}_2^{a_2}\cdots\cdots\mathfrak{r}_t^{a_t}\,\mathfrak{j}^l=(\varpi),$$

$$\mathfrak{l}\,\mathfrak{r}_1^{b_1}\mathfrak{r}_2^{b_2}\cdots\cdots\mathfrak{r}_t^{b_t}\,\mathfrak{j}'^l=(\lambda),$$

$$\mathfrak{q}\,\mathfrak{r}_1^{c_1}\mathfrak{r}_2^{c_2}\cdots\cdots\mathfrak{r}_t^{c_t}\,\mathfrak{j}''^l=(\varkappa),$$

1) Vgl. § 2. S. 13.

wo $\mathfrak{j}, \mathfrak{j}', \mathfrak{j}'' \cdots$ Ideale in k; $\varpi, \lambda, \varkappa, \cdots$ $d+d'+n$ Zahlen in k, die wir prim zu jedem Primideale $\mathfrak{l}'$ annehmen können, und die Exponenten $a, b, c \ldots$ Zahlen aus der Reihe: $0, 1, 2, \ldots l-1$ bedeuten. Wir betrachten dann das System der

$$l^{r+1+t+d+d'+n}$$

Zahlen:

$$\underbrace{\varepsilon_1^{x_1} \cdots}_{r+1} \underbrace{\rho_1^{y_1} \cdots}_{t} \underbrace{\varpi^{u} \cdots}_{d} \underbrace{\lambda^{v} \cdots}_{d'} \underbrace{\varkappa^{w} \cdots}_{n} \qquad (3)$$

$$(0 \leqq x, y, u, v, w < l)$$

Wir unterwerfen diese Zahlen (3) zunächst der Bedingung, dass sie jedes der t Ideale $\mathfrak{r}_1, \mathfrak{r}_2, \cdots \mathfrak{r}_t$ zu einer Potenz mit einem durch l teilbaren Exponenten als Factor enthalten sollen, so dass die Exponenten x, y, u, v, w den t linearen Congruenzen:

$$\left.\begin{aligned} &a_1 u + \cdots + b_1 v + \cdots + c_1 w + \cdots \equiv 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &a_t u \cdots + b_t v + \cdots + c_t w + \cdots \equiv 0. \end{aligned}\right\} (l)$$

zu genügen haben.

Wir verlangen sodann, dass die Zahlen (3) noch *primär* in Bezug auf jedes $\mathfrak{l}'$ d.h. l^{te} *Reste nach der* $\sigma' l^{\text{ten}}$ *Potenz von* $\mathfrak{l}'$ sein sollen. Bezeichnen wir für einen Augenblick mit $\nu = s'f'$ den Rang der Zahlengruppe, mit $\gamma_1, \gamma_2, \cdots \gamma_\nu$ ein System der unabhängigen l^{ten} Nichtreste nach dem Modul $\mathfrak{l}'^{\sigma' l}$, und ist demnach

$$\left.\begin{aligned} \varepsilon_1 &\equiv \gamma_1^{e_1} \cdots \gamma_\nu^{e_\nu} \alpha^l, \cdots \\ \rho_1 &\equiv \gamma_1^{r_1} \cdots \gamma_\nu^{r_\nu} \beta^l, \cdots \\ \varpi &\equiv \gamma_1^{p_1} \cdots \gamma_\nu^{p_\nu} \gamma^l, \cdots \\ \lambda &\equiv \gamma_1^{h_1} \cdots \gamma_\nu^{h_\nu} \delta^l, \cdots \\ \varkappa &\equiv \gamma_1^{k_1} \cdots \gamma_\nu^{k_\nu} \varepsilon^l, \cdots \end{aligned}\right\} (\mathfrak{l}'^{\sigma' l})$$

so ist eine Zahl (3) dann und nur dann ein l^{ter} Rest nach $l^{\sigma l}$, wenn die Exponenten x, y, u, v, w, dem System von ν linearen Congruenzen:

$$\left.\begin{aligned} &e_1x_1+\cdots\quad r_1y_1+\cdots+p_1u\cdots\cdots+l_1v+\cdots+k_1w+\cdots\cdots\equiv 0,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &e_\nu x_1+\cdots\cdots t_\nu y_1+\cdots\cdots p_\nu u+\cdots\cdots l_\nu v+\cdots\cdots k_\nu w+\cdots\cdots\equiv 0, \end{aligned}\right\}(l)$$

genügen.

Unter den Zahlen (3) gebe es nun $l^{t'}$ Zahlen, welche diese $t+\Sigma s'f'$ Bedingungen genügen, die wir dann in der Form

$$\mu_1^{e_1}\mu_2^{e_2}\cdots\cdots\mu_{t'}^{e_{t'}} \qquad (0\leqq e<l) \tag{4}$$

darstellen können, wobei die Zahlen $\mu_1, \mu_2, \cdots\cdots \mu_{t'}$ in dem Sinne von einander unabhängig sind, dass eine Zahl (4) nur dann l^{te} Potenz einer Zahl in k sein kann, wenn die sämtlichen Exponenten $e_1, e_2, \ldots\ldots e_{t'}$ verschwinden; und es ist

$$t'\geqq r+1+t+d+d'+n-(t+\Sigma s'f'), \tag{5}$$

woraus folgt

$$t'\geqq \overline{t}. \tag{6}$$

In der Tat: nach (1) und (5)

$$t'-\overline{t}\geqq 2(r+1)-(\Sigma sf+\Sigma s'f')=2(r+1)-m=0.$$

Adjungirt man nun dem Körper k die l^{te} Wurzel einer der Zahlen (4), die wir durchweg mit μ bezeichnen wollen, so erhalten wir also wenigstens $\overline{t}$ von einander unabhängige relativ cyclische Körper

$$K=k(\sqrt[l]{\mu})$$

vom l^{ten} Grade in Bezug auf k. Die Relativdiscriminante dieser Körper ist durch kein Primideal teilbar, welches nicht in $\mathfrak{m}$

aufgeht, weil jedes der Ideale $\mathfrak{r}_1, \mathfrak{r}_2, \ldots\ldots \mathfrak{r}_t$ genau zu einer Potenz in μ aufgeht, deren Exponent Vielfaches von l ist, und überdies μ l^{er} Potenzrest nach jedem $\mathfrak{l}^{\sigma l}$ ist. Da ferner für jedes wirklich in die Relativdiscriminante aufgehende Primideal $\mathfrak{l}$ die entsprechende Zahl $v \leqq \sigma l$ (Satz 8), und anderseits nach Voraussetzung der Modul $\mathfrak{m}$ dasselbe Ideal $\mathfrak{l}$ wenigstens zur $\sigma l+1^{\text{ten}}$ Potenz als Factor enthält, so ist Satz 13 auf den Körper K anwendbar, demzufolge K Classenkörper für eine der Classengruppen H sein muss.

Da es genau $\bar{l}^{\bar{t}}-1 : l-1$ Classengruppen H, und nach (6) wenigstens ebensoviele Körper K gibt, da ferner nach Satz 6 für jede Classengruppe nicht mehr als ein Classenkörper existiren kann, so folgt, dass jeder Classengruppe H ein Classenkörper K zugeordnet sein muss.

Es bleibt noch übrig, nachzuweisen, dass die Relativdiscriminante des Körpers K durch keines der Primideale $\mathfrak{q}, \mathfrak{q}', \ldots\ldots \mathfrak{q}^{(n-1)}$ teilbar ist. Wäre aber der Gegenteil der Fall, so wähle man ein zweites, vollständig vom ersten verschiedenes System der n Primideale $\bar{\mathfrak{q}}, \bar{\mathfrak{q}}', \ldots\ldots \bar{\mathfrak{q}}^{(n-1)}$, welche den Bedingungen (2) genügen, und bilde darauf die entsprechenden Körper $\overline{\mathrm{K}}$, deren Discriminanten dann sicher nicht durch $\mathfrak{q}, \mathfrak{q}', \ldots\ldots \mathfrak{q}^{(n-1)}$ teilbar sind, und folglich notwendig von K verschieden sein mussten. Da auch diese Körper $\overline{\mathrm{K}}$ Classenkörper für je eine der nämlichen Gruppen H sein müssen, so führt die Annahme zu einem Widerspruch gegen Satz 6.

Hiermit ist im gegenwärtigen Falle unser Existenzsatz bewiesen.

Wir haben zu Beginn dieses Beweises angenommen, dass jedes in l aufgehende Primideal $\mathfrak{l}$ entweder gar nicht oder wenigstens zur $\sigma l+1^{\text{ten}}$ Potenz in $\mathfrak{m}$ als Factor enthalten sein soll. Es ist nun leicht, diese Beschränkung aufzuheben. Es sei nämlich $\mathfrak{m}_0$ ein Teiler vom $\mathfrak{m}$ derart, dass $\mathfrak{m}_0$ genau durch $\mathfrak{l}^g$ teilbar ist, wo $g \leqq \sigma l$, und es sei $\bar{t}_0$ der Rang der entsprechenden Classengruppe $\mathfrak{G}_0$ für den Modul $\mathfrak{m}_0$, so dass offenbar $\bar{t}_0 \leqq \bar{t}$. Fällt nun $\bar{t}_0 < \bar{t}$ aus, so gibt es unter den $\bar{l}^{\bar{t}}-1 : \bar{l}-1$ Classengruppen H nach $\mathfrak{m}$ genau $\bar{l}^{\bar{t}}-1 : l-1$, welche Classengruppen nach $\mathfrak{m}_0$ sind. Den letzteren

müssen nun genau ebensoviele unter den vorhin aufgestellten Körper K als Classenkörper zugeordnet sein. Denn, andernfalls mussten für die übrigbleibenden $l^{\bar{t}-\bar{t}_0}:l-1$ Gruppen $\mathfrak{H}$ insgesamt eine grössere Anzahl der zugeordneten Körper K vorhanden sein, was einen Verstoss gegen Satz 6 nach sich ziehen würde.

Jedoch konnten wir auch ohne die beschränkende Annahme über $\mathfrak{m}$ direct den Nachweis des Existenzsatzes führen, wozu eine sehr geringe Modification der vorhin benutzten Methode hinreichen würde.

Ausser den d' Primidealpotenzen $\mathfrak{p}$, für welche $g>\sigma l$, mögen noch gewisse andere, sie seien durchweg mit $\mathfrak{p}_1^{g_1}$ bezeichnet, wo $g_1 \leqq \sigma_1 l$, in $\mathfrak{m}$ aufgehen; die übrigbleibenden in l aufgehenden Primideale seien, wie vorhin, durchweg mit $\mathfrak{p}'$ bezeichnet. Indem wir die sonstingen Bezeichnungsweise des vorhergehenden Beweises beibehalten, ist nun nach Satz 25

$$\bar{t}=d+d'+\Sigma sf+\Sigma R(g_1)+n-(r+1),$$

wo $R(g_1)$ die in Satz 25 erläuterte Bedeutung hat, und die Summation $\Sigma R(g_1)$ auf alle Primideale $\mathfrak{p}_1$ zu erstrecken ist. Wir unterwerfen dann die Zahlen μ ausser den $t+\Sigma s'f'$ früheren Bedingungen noch den, dass für jedes Primideal $\mathfrak{p}_1$ die Congruenz

$$\xi^l \equiv \mu, \quad (\mathfrak{p}_1^{\sigma_1 l-g_1+1}) \tag{7}$$

in k möglich sein sollen. Da diese offenbar $\Sigma R(\sigma_1 l-g_1+1)$ neue lineare Congruenzbedingungen für die Exponenten x, y, u, v, w involviren, so bleiben nun

$$t' \geqq r+1+d+d'+n-\{t+\Sigma s'f'+\Sigma R(\sigma_1 l-g_1+1)\}$$

unabhängige Zahlen μ, welche ebensoviele unabhängige Körper

$$\mathrm{K}=\mathrm{k}(\sqrt[l]{\mu})$$

hervorbringen werden. Da nach Hülfssatz des § 16

$$R(g_1)+R(\sigma_1 l-g_1+1)=\left\{\left[g_1-\frac{g_1}{l}\right]+\left[\sigma_1 l-g_1+1-\sigma_1+\frac{g_1-1}{l}\right]\right\}f_1$$

$$=\sigma_1(l-1)f_1=s_1 f_1,$$

so ist auch in diesem Falle noch

$$t'-\bar{t}\geqq 2(r+1)-(\Sigma sf+\Sigma s_1 f_1+\Sigma s'f')=2(r+1)-m=0.$$

Enthält nun die Relativdiscriminante eines dieser Körper K den Primfactor $\mathfrak{l}_1$ dann ist wegen (7) die entsprechende Zahl $v_1 \leqq g_1-1$. Daher ist Satz 13 noch anwendbar, und es folgt, genau wie vorhin, die Existenz der $\bar{t}$ unabhängigen Classenkörper für die Gruppen $\mathfrak{H}$, welche alle Forderungen des Existenzsatzes befriedigen.

Das Ergebnis dieser Betrachtungen sprechen wir in den folgenden Satz aus:

Satz 25. *Geht ein in l aufgehendes Primideal $\mathfrak{l}$ zur g^{ten} Potenz in $\mathfrak{m}$ auf, wo $g \leqq \sigma l$, und ist die Relativdiscriminante eines Classenkörpers für eine Classengruppe vom Index l nach dem Modul $\mathfrak{m}$ durch dieses Primideal $\mathfrak{l}$ teilbar, dann ist die entsprechende Zahl v kleiner als g.*[1]

Dasselbe gilt offenbar auch, wenn $g=\sigma l+1$. Ferner ist, wenn $g=1$, die Relativdiscriminante des Classenkörpers prim zu $\mathfrak{l}$. Ein einfacher Factor $\mathfrak{l}$ von $\mathfrak{m}$ macht keinen Beitrag zu der Rangzahl von $\mathfrak{G}_0$

Ferner gilt[1]

Satz 26. *Hat der relativ cyclische Körper* K/k *vom Primzahlgrade l die Relativdiscriminante $\mathfrak{d}=\mathfrak{f}^{l-1}$, dann ist $\mathfrak{f}$ der Führer*[2] *der zugeordneten Classengruppe vom Index l im Grundkörper* k.

Das soll heissen: Um die Relativnormen aller zu $\mathfrak{d}$ primen Ideale von K in eine Classengruppe vom Index l in k einzuschliessen, genügt es nach Satz 13, die Classen von k nach einem durch $\mathfrak{f}$ teilbaren Modul $\mathfrak{m}$ zu definiren. In Satz 26 wird nun umgekehrt behauptet, dass es auch notwendig ist, dass $\mathfrak{m}$ alle Primfactoren von $\mathfrak{f}$, speciell jeden Factor $\mathfrak{l}$ wenigsten zur $v+1^{\text{ten}}$ Potenz, als Factor enthalte.

Beweis. Betreffs eines zu l primen Primfactor $\mathfrak{p}$ von $\mathfrak{f}$ ist dies evident; denn wäre $\mathfrak{H}$ eine Classengruppe vom Index l nach einem zu $\mathfrak{p}$ primen Modul $\mathfrak{m}$, dann musste nach dem vorhergehen-

1) Dies zunächst unter der Annahme, dass l ungerade ist, und k die l^{te} primitive Einheitswurzel enthält; diese Beschränkung wird später aufgehoben werden. Vgl. § 19.

2) Vgl. § 2, S 13.

den Beweis ein Classenkörper K′ für $\mathfrak{H}$ existiren, dessen Relativdiscriminante zu $\mathfrak{p}$ prim ist, der folglich gewiss von K verschieden ist. Enthalte aber $\mathfrak{m}$ einen Primfactor $\mathfrak{l}$ zu einer Potenz, deren Exponent kleiner als $v+1$ ist, dann musste nach Satz 25 ein Classenkörper K′ für $\mathfrak{H}$ existiren, für welchen die entsprechende Zahl $v'<v$ ausfällt, oder dessen Relativdiscriminante prim zu $\mathfrak{l}$ ist, welcher also jedenfalls von K verschieden wäre. Beide Annahme führen somit zu einem Widerspruch gegen Satz 6.

§. 19.

Fortsetzung des vorhergehenden Artikels.

In dieser Fortsetzung des vorhergehenden Artikels behandle ich denjenigen Fall des Existenzsatzes, wo der Index der Classengruppe $\mathfrak{H}$ eine ungerade Primzahl l ist, aber der Grundkörper nicht die primitive l^{te} Einheitswurzel ζ enthält. Für den Fall, wo $\mathfrak{m}=1$, also für den absoluten Classenkörper hat Herr Ph. Furtwängler[1] den Existenzbeweis dadurch geführt, dass er zunächst dem Körper k die l^{te} Einheitswurzel ζ adjungirte, dann einen geeigneten Oberkörper zu den so erweiterten Grundkörper k′ construirte; sodann zeigte er, dass dieser Oberkörper den gesuchten Körper als Unterkörper enthalten muss. Diese Beweismethode bewährt sich auf in unserem Falle. Indem ich hier dieselbe Methode anwende, schicke ich einen Hülfssatz voran, welcher eine gewisse Vereinfachung des Beweises bewirken wird.

Hülfssatz. *Es sei* k′ *relativ cyclisch vom Relativgrade* n *in Bezug auf* k, K *relativ cyclisch vom Grade* l *in Bezug auf* k′, *und relativ normal aber nicht relativ Abel'sch in Bezug auf* k; *und es sei* l *eine Primzahl, die nicht in* n *aufgeht. Wenn dann ein Primideal von* k, *welches nicht in die Relativdiscriminante von* K/k *aufgeht, in weniger als* n *Primfactoren in* k′ *zerfällt, dann zerfällt jedes dieser Primideale von* k′ *in* l *Primfactoren in* K.

Beweis. Sei $\mathfrak{G}$ die Galois'sche Gruppe des relativ normalen Körpers K/k, von der Ordnung nl, $\mathfrak{H}$ die invariante Untergruppe

1) Math. Ann. 63.

von $\mathfrak{G}$, welche den Körper k'/k unverändert lässt, so dass nach Voraussetzung $\mathfrak{H}$ cyclisch von der Ordnung l, und die complementäre Gruppe $\mathfrak{G}/\mathfrak{H}$ ebenfalls cyclisch von der Ordnung n ist. Daher gibt es in $\mathfrak{G}$ eine Substitution T, von der Art, dass die Zerlegung gilt:

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}T+\mathfrak{H}T^2+\cdots\cdots+\mathfrak{H}T^{n-1}.$$

Die Ordnung der Substitution T, welche durch n teilbar und in nl aufgeht, muss notwendig gleich n sein, weil die Gruppe $\mathfrak{G}$ nicht cyclisch sein soll. Ist aber H eine beliebige Substitution von $\mathfrak{H}$, dann ist HT auch von der Ordnung n, weil HT in der oben angegebenen Zerlegung von $\mathfrak{G}$ an Stelle von T treten kann. Ebenso folgert man, dass die Ordnung jeder nicht in $\mathfrak{H}$ enthaltenen Substitution ein Teiler von n sein muss.

Sei nun $\mathfrak{p}$ ein Primideal von k, welches die Voraussetzung des Satzes genügt, und es gelte in K die Zerlegung

$$\mathfrak{p}=\mathfrak{P}_1\mathfrak{P}_2\cdots\cdots\mathfrak{P}_\nu,$$

so dass

$$nl=\nu f,$$

wenn f der Relativgrad der Primideale $\mathfrak{P}_1, \mathfrak{P}_2, \cdots\cdots$ in Bezug auf k ist. Nach Voraussetzung ist also $f>1$. Die Zerlegungsgruppe des Primideals $\mathfrak{P}_1$, welche von der Ordnung f ist, muss hier eine cyclische Gruppe sein, weil die Trägheitsgruppe die identische ist. Nach dem vorhin bewiesenen, muss daher f ein Teiler von n, oder gleich l sein. Die letzte Eventualität ist aber ausgeschlossen, weil alsdann $\mathfrak{H}$ die Zerlegungsgruppe ist und folglich $\mathfrak{p}$ in n Factoren in k' zerlegt werden muss. Da also f ein Teiler von n ist, so muss ν durch l teilbar sein, womit der Satz bewiesen ist.

Wir gehen nunmehr zum Beweis des Existenzsatzes über, unter der Voraussetzung, dass der Grundkörper k nicht die primitive l^{te} Einheitswurzel enthält. Durch Adjunction derselben erweitern wir k zum Körper k', welcher relativ cyclisch über k von einer Ordnung n ist, wo n ein Teiler von $l-1$, folglich prim zu l ist. Die Idealclassen von k seien nach der Zahlengruppe $\mathfrak{o}$

der Zahlen $\equiv 1$ $(\mathfrak{m})$ definirt, wo der Modul $\mathfrak{m}$ ein jedes in l aufgehendes Primideal $\mathfrak{l}$ mindestens zur ersten Potenz als Factor enthalten soll, eine Annahme, die ohne Schaden der Allgemeinheit geschieht, weil die Hinzunahme eines einfachen Factors $\mathfrak{l}$ zu $\mathfrak{m}$, falls $\mathfrak{m}$ nicht durch $\mathfrak{l}$ teilbar sein sollte, offenbar den Rang $\bar{t}$ der vollständigen Classengruppe G_0 von k nicht beeinflussen wird.[1] Legt man dann der Classeneinteilung in k′ die Zahlengruppe o′ der Zahlen $\equiv 1$ $(\mathfrak{m})$ zu Grunde, dann fallen die Relativnormen der Ideale einer Classe nach o′ in eine und dieselbe Classe nach o in k hinein, so dass wir berechtigt sind, von den Relativnormen der Classen von k′ zu sprechen. Dasselbe gilt offenbar auch für jedem in k′ enthaltenen Oberkörper von k.

Sei nun in leicht verständlicher Bezeichnungsweise

$$G = \{C_1, C_2, \cdots\cdots C_{\bar{t}}; D\} \qquad (1)$$

die vollständige Classengruppe von k, wo D wie in § 17 die Gruppe der Classen, deren Ordnung zu l prim sind, und C_1, C_2,.....ein System der Basisclassen der Gruppe G_0 bedeuten, die so gewählt sind, dass eine gegebene Untergruppe H von G vom Index l in der Form dargestellt werden kann:

$$H = \{C_1^l, C_2, \cdots\cdots C_{\bar{t}}; D\}. \qquad (2)$$

Anderseits bezeichnen wir mit D_0 diejenige Untergruppe von D, welche aus allen Relativnormen der Classen von k′ besteht. Obgleich es sich später herausstellen wird, dass der Gruppenindex $(D: D_0)$ gleich n ist, sind wir in dem gegenwärtigen Stadium nicht berechtfertigt, dies vorauszusetzen, weil Satz 13 nur für einen Oberkörper vom Primzahlgrade bewiesen worden ist. Wir wissen aber, dass gewiss $(D: D_0) > 1$, also D_0 nicht mit D zusammenfällt, eben zufolge jenes Satzes, weil derselbe auf jeden Unterkorper k_0' von k′ angewandt werden kann, welcher von einem Primzahlgrade im Bezug auf k ist, da $\mathfrak{m}$ jedes in l aufgehendes Primideal als Factor enthält.

1) Vgl. Hülfssatz in § 16 und Satz 24.

Bezeichnen wir ferner mit $\mathfrak{D}'$ die Gruppe derjenigen Classen von k', deren Relativnormen in $\mathfrak{D}_0$ hineinfallen, dann lässt sich die vollständige Classengruppe $\mathfrak{G}'$ von k' in der Form darstellen:

$$\mathfrak{G}' = \{\mathfrak{C}_1, \mathfrak{C}_2, \cdots\cdots \mathfrak{D}'\}. \tag{3}$$

Denn, ist $\mathfrak{c}'$ eine beliebige Classe in k' und

$$\mathfrak{n}(\mathfrak{c}') = \mathfrak{C}_1^{e_1}\, \mathfrak{C}_2^{e_2} \cdots\cdots [\mathfrak{D}_0],$$

wo $\mathfrak{n}$ die im Relativkörper k'/k genommene Relativnorm bezeichnet, und $[\mathfrak{D}_0]$ eine Classe in der Classengruppe $\mathfrak{D}_0$ bedeutet. Setzt man dann

$$\mathfrak{c}' = \mathfrak{C}_1^{x_1}\, \mathfrak{C}_2^{x_2} \cdots\cdots \mathfrak{U}, \tag{4}$$

so dass

$$\mathfrak{n}(\mathfrak{c}') = \mathfrak{C}_1^{nx_1}\, \mathfrak{C}_2^{nx_2} \cdots\cdots \mathfrak{n}(\mathfrak{U}).$$

Bestimmt man dann $x_1, x_2, \ldots\ldots$ so, dass

$$\mathfrak{C}_1^{nx_1} = \mathfrak{C}_1^{e_1}, \quad \mathfrak{C}_2^{nx_2} = \mathfrak{C}_2^{e_2}, \cdots\cdots,$$

was ja möglich ist, weil n prim zu l ist, dann folgt

$$\mathfrak{n}(\mathfrak{U}) = [\mathfrak{D}_0],$$

also, dass in (4) $\mathfrak{U}$ der Gruppe $\mathfrak{D}'$ angehört.

Zugleich sieht man ein, dass die Classen $\mathfrak{C}_1, \mathfrak{C}_2, \ldots\ldots$ in k' unabhängig in Bezug auf der Gruppe $\mathfrak{D}'$ sind. Denn die Annahme

$$\mathfrak{C}_1^{x_1}\, \mathfrak{C}_2^{x_2} \cdots\cdots [\mathfrak{D}'] = 1,$$

wo mit $[\mathfrak{D}']$ eine Classe der Classengruppe $\mathfrak{D}'$ bezeichnet wird, bedingt, dass

$$\mathfrak{C}_1^{nx_1}\, \mathfrak{C}_2^{nx_2} \cdots\cdots [\mathfrak{D}_0] = 1,$$

was nur dann der Fall ist, wenn

$$\mathfrak{C}_1^{nx_1} = 1, \quad \mathfrak{C}_2^{nx_2} = 1, \cdots\cdots; \; [\mathfrak{D}_0] = 1$$

in k; also, weil n prim zu l ist, wenn

$$\mathfrak{C}_1^{x_1} = 1, \quad \mathfrak{C}_2^{x_2} = 1, \cdots\cdots$$

Die Classen c_1, c_2,.....erleiden also in k′ weder die Verlust der Unabhängigkeit noch die Erniederung der Ordnungen.

Demnach wird durch

$$H' = \{c_1^l, c_2, \cdots\cdots D'\} \tag{5}$$

eine Classengruppe vom Index l in k′ definirt.

Für diese Classengruppe H' existirt nun nach dem vorhergehenden Artikel ein zugeordneter Classenkörper K vom Relativgrade l in Bezug auf k′, weil k′ die primitive l^{te} Einheitswurzel enthält.

Weil aber die Classengruppe H' gegenüber der Substitutionen des Relativkörpers k′/k invariant ist, so fallen die in Bezug auf k mit K relativ conjugirten Körper als Classenkörper von H' nach Satz 6 mit K zusammen; also ist K relativ normal in Bezug auf k. Aus der Tatsache, dass die Relativnormen der Idealen von K in Bezug auf k in die Classengruppe

$$\{c_1^l, c_2, \cdots\cdots ; D_0\} \tag{6}$$

hineinfallen, ist aber zu schliessen, dass K relativ Abel'sch in Bezug auf k sein muss.

In der Tat, sei $\mathfrak{p}$ ein Primideal von k, welches nicht in die Primideale des ersten Relativgrades in k′ zerfällt, und zugleich in einer Classencomplex

$$c_1^{e_1} c_2^{e_2} \cdots\cdots D \quad \text{mit} \quad e_1 \not\equiv 0, \quad (l) \tag{7}$$

enthalten ist; die Existenz solcher Primideale folgt aus dem Hülfssatze des § 4. Wäre nun K nicht relativ Abel'sch in Bezug auf k, dann musste jedes in $\mathfrak{p}$ aufgehende Primideal $\mathfrak{p}'$ von k′, nach dem vorhin bewiesenen Hülfssatze in l von einander verschiedene Primfactoren in K zerfallen. Folglich musste $\mathfrak{p}'$ einer Classe der Gruppe (5) angehören, und infolgedessen $n(\mathfrak{p}') = \mathfrak{p}^f$ in eine Classe der Gruppe (6) in k hineinfallen. Da aber $\mathfrak{p}$ der Classe (7) angehört, und da f als Teiler von n prim zu l ist, so ist dies unmöglich.

Da also K relativ Abel'sch vom Grade nl in Bezug auf k ist, so enthält K einen Unterkörper K_0, welcher relativ cyclisch vom Grade l in Bezug auf k ist. Dieser Körper K_0 muss nach Satz 13 (vgl. weiter unten) einer Classengruppe in k vom Index l als Classenkörper zugeordnet sein. Diese Classengruppe muss aber, da K_0 in K enthalten ist, offenbar die Classengruppe (6) enthalten, kann also keine andere sein als die vorgelegte Gruppe H.

Die Relativdiscriminante des Körpers K_0/k enthält offenbar kein Primideal als Factor, welches nicht in $\mathfrak{m}$ aufgeht. Geht insbesondere ein Primideal $\mathfrak{l}$ genau zur g^{ten} Potenz in $\mathfrak{m}$ auf, wo $1<g\leqq\sigma l$, dann ist in k' der Modul $\mathfrak{m}$ genau durch die gn^{ten} Potenz von dem entsprechenden Primideal $\mathfrak{l}'$ ($\mathfrak{l}=\mathfrak{l}'^n$) teilbar. Geht daher dieses Primideal $\mathfrak{l}'$ in die Relativdiscriminante des Körpers K/k' auf, dann ist nach Satz 26 die entsprechende Zahl $v'<gn$. Hieraus ist aber zu schliessen, dass $\mathfrak{l}$ in die Relativdiscriminante von K_0/k aufgehen muss (ausser wenn $g=1$), und zwar ist die entsprechende Zahl $v<g$. Denn setzt man $\mathfrak{l}=\mathfrak{L}^{nl}$, wo $\mathfrak{L}$ Primideal in K bedeutet, dann folgt, wenn man die Relativdifferente des Körpers K/k einmal als Product der Relativdifferenten von K/K_0 und von K_0/k, das andere Mal als Product der Relativdifferenten von K/k' und von k'/k darstellt,

$$\mathfrak{L}^{n-1}\cdot\mathfrak{L}^{n(v+1)(l-1)}=\mathfrak{L}^{(v'+1)(l-1)}\mathfrak{L}^{l(n-1)},$$

folglich

$$v=\frac{v'}{n},$$

woraus das Gesagte folgt. Wenn aber $g\geqq\sigma l+1$, dann ist die Beziehung $v<g$ selbstverständlich.[1]

Ist dagegen $\mathfrak{m}$ nur durch die erste Potenz von $\mathfrak{l}$ teilbar ($g=1$), dann ist die Relativdiscriminante von K_0/k prim zu $\mathfrak{l}$. Denn andernfalls würde, wie oben, aus $v'<n$ die unmögliche Beziehung $v<1$ folgen.

1) Die Beziehung $v<g$ rechtfertigt die Anwendung von Satz 13 auf den Körper K_0/k (vgl. oben).

§ 20.

Relativ quadratische Classenkörper.

Um den Beweis unseres Existenzsatzes für den Fall durchzuführen, wo der Index der vorgelegten Classengruppe gleich 2 ist, sprechen wir ihn in precisirter Fassung wie folgt aus.

Satz 27. *In einem algebraischen Körper* k *vom Grade m sei die Idealclassen nach der Zahlengruppe* o *derjenigen Zahlen* α *definirt, welche die Bedingung:* $\alpha \equiv 1\ (\mathfrak{m})$ *befriedigen, jedoch ohne irgendwelcher Vorzeichenbeschränkung unterworfen zu sein. Dann existirt für jede vorgelegte Classengruppe vom Index 2 ein relativ quadratischer Oberkörper* K *von* k, *welcher derselben als Classenkörper zugeordnet ist und von der Art, dass unter den mit* K *conjugirten* $2m$ *Körpern doppelt so viel reelle Körper als unter den mit* k *conjugirten* m *Körpern vorhanden sind.*

Oder allgemeiner:

Wenn von den r_1 *reellen mit* k *conjugirten Körpern eine beliebige Anzahl* ν*: es seien diese* $k_1, k_2, \ldots\ldots k_\nu$ *ausgewählt wird, und wenn in die Zahlengruppe* o^+ *nur diejenigen Zahlen von* o *aufgenommen werden, welche positiv in* $k_1, k_2, \ldots\ldots k_\nu$ *ausfallen, dann existirt für jede Classengruppe vom Index 2 nach* o^+, *ein Classenkörper* K, *welcher unter den* $2m$ *conjugirten Körpern wenigstens* $2(r_1-\nu)$ *reelle aufweist.*

Natürlich soll K die in Satz 23 und Satz 25 ausgesprochenen Bedingungen in Bezug auf die Relativdiscriminante befriedigen.

Beweis. Es genügt, den Satz in der im zweiten Teil ausgesprochenen allgemeineren Form zu beweisen; dies geschieht auf derselben Weise wie in § 18. Nur soll im gegenwärtigen Falle für die Zahl $\bar{t}$ der Wert[1]

$$\bar{t}=d+d'+\Sigma sf+\Sigma R(g_1)+\nu+n-(r+1) \qquad (a)$$

angenommen werden, wo 2^n die Anzahl der quadratischen Reste nach $\mathfrak{m}$ ist, welche in dem System der Zahlen

$$(-1)^{u_0}\varepsilon_1^{u_1}\ldots\ldots\varepsilon_r^{u_r}\rho_1^{v_1}\ldots\ldots\rho_t^{v_t} \qquad (0 \leqq u, v < 2)$$

1) Vgl. Formel (8) in § 17, wo jetzt an Stelle von $\Sigma R(g)$ und r_1-r_0 bez. $\Sigma(sf+1)+\Sigma R(g_1)$ und ν gesetzt werden müssen.

enthalten sind, und in $k_1, k_2, \ldots k_\nu$ positiv ausfallen. Ferner sollen die Zahlen des Systems (3) in § 18, ausser den dort erklärten $t+\Sigma s'f'+\Sigma R(2s_1-g_1+1)$ Bedingungen (vgl. S. 76), noch $r_1-\nu$ weiteren unterworfen sein, in den von $k_1, k_2, \ldots k_\nu$ verschiedenen $r_1-\nu$ reellen mit k conjugirten Körpern positiv zu sein. Da diese letzteren Bedingungen $r_1-\nu$ lineare Congruenzen mod. 2 involviren, welche die Exponenten $x, y, u, v, w, \ldots$ der Zahlen (3) in § 18 zu befriedigen haben, so haben wir jetzt an Stelle von (5) in § 18,

$$t' \geqq r+1+t+d+d'+n-\{t+\Sigma s'f'+\Sigma R(2s_1-g_1+1)+r_1-\nu\}. \quad (b)$$

Man erhält aus (a) und (b)

$$t'-\bar{t} \geqq 2(r+1)-r_1-m,$$

woraus, weil bekanntlich

$$r+1=\frac{m+r_1}{2},$$

noch immer

$$t' \geqq \bar{t}.$$

Da die Zahl μ (vgl. (4), § 18) nun höchstens in den ν Körpern $k_1, k_2, \ldots k_\nu$ negativ ausfallen kann, so ist die Anwendbarkeit von Satz 13 gesichert, und man überzeugt sich wie in § 18 von der Richtigkeit des zu beweisenden Satzes.

Der obige Beweis bleibt gültig, wenn $\nu=0$, was den ersten Teil unseres Satzes bestätigt.

Man erhält alle für ein gegebenes $\mathfrak{m}$ überhaupt möglichen relativ quadratischen Classenkörper, wenn man in o^+ nur die total positiven Zahlen von o zulässt, und für jede Classengruppe vom Index 2 nach o^+ den entsprechenden Classenkörper construirt.

§ 21.

Relativ cyclische Classenkörper vom Primzahlpotenzgrade.

Wir wollen nunmehr den Existenzsatz in dem Falle beweisen, wo $\mathfrak{H}$ eine Classengruppe nach dem Modul $\mathfrak{m}$ von einem geraden

oder ungeraden Primzahlpotenzindex l^n und die complementäre Gruppe G/H cyclisch ist.

Es sei also c eine solche Classe in k, dass erst die l^n te Potenz von c in H enthalten ist; ferner sei G_0 die Classengruppe vom Index l, welche H in sich enthält, so dass in einer wiederholt angewandten Bezeichnungsweise

$$G=\{c, H\}, \quad G_0=\{c^l, H\}.$$

Es existirt alsdann ein relativ cyclischer Körper k'/k vom Grade l, welcher Classenkörper für G_0 ist. Nach Satz 22 ist es nun möglich, ein in $\mathfrak{m}$ aufgehendes invariantes Ideal $\mathfrak{m}'$ so zu wählen, dass die Relativnormen aller Ideale einer Classe nach $\mathfrak{m}'$ in k' einer und derselben Classe nach $\mathfrak{m}$ in k angehören werden. Demnach ist die Gruppe der sämtlichen Classen von k' in der Form darstellbar:

$$\{c, H'\},$$

wo H' die Gruppe derjenigen Classen von k' bedeutet, deren Relativnormen in die Classengruppe H von k hineinfallen, und c diejenige Classe von k', welche die Ideale von c in k enthält. Von den Potenzen dieser Classe c von k' ist erst die l^{h-1} te in H' enthalten.

Wir nehmen nun an: der Existenzsatz sei bewiesen für den Index l^{h-1}. Demnach existirt ein relativ cyclischer Körper K vom Relativgrade l^{h-1} in Bezug auf k', welcher Classenkörper für die Classengruppe H' von k' ist. Da H' offenbar gegenüber der erzeugenden Substitution s der Galois'schen Gruppe des Relativkörpers k'/k invariant ist, so folgt nach Satz 6, dass K relativ normal in Bezug auf k ist. Weil aber K der Classengruppe H von k zugeordnet ist, so folgt, dass K keinen Unterkörper ausser k' enthält, welcher relativ cyclisch vom Relativgrade l in Bezug auf k ist. Denn ein solcher musste als Classenkörper einer Classengruppe vom Index l in k zugehören, welche notwendig H in sich enthalte. Ausser G_0, welcher der Classenkörper k' zugeordnet ist, gibt es aber keine solche Classengruppe in k.

Bedeutet daher $\mathfrak{G}$ die Galois'sche Gruppe des relativ normalen Körpers K/k, dann ist $\mathfrak{G}$ von der Ordnung l^h, und es enthält $\mathfrak{G}$ eine einzige Untergruppe $\mathfrak{G}_0$ vom Index l (welche die Zahlen von k′ unverändert lässt), und es ist

$$\mathfrak{G}=\mathfrak{G}_0+\mathfrak{G}_0 s+\cdots\cdots+\mathfrak{G}_0 s^{l-1}$$

Hieraus ist aber zu schliessen, dass $\mathfrak{G}$ cyclisch, also s von der Ordnung l^h sein muss. Denn widrigenfalls musste es bekanntlich[1] in $\mathfrak{G}$ eine Untergruppe der Ordnung l^{h-1} geben, welche s enthält und folglich von $\mathfrak{G}_0$ verschieden wäre. Daher ist K relativ cyclisch in Bezug auf k.

Wenn die Relativdiscriminanten der Relativkörper k′/k und K/k′ bez. mit $\mathfrak{d}$ und $\mathfrak{d}'$ bezeichnet werden, dann ist die Relativdiscriminante von K/k gleich $\mathfrak{d}\mathfrak{d}'^{l}$. Da nach Annahme jeder Primfactor von $\mathfrak{d}'$ in $\mathfrak{m}'$ also auch in $\mathfrak{m}$ aufgeht, und da dasselbe ebenfalls von $\mathfrak{d}$ gilt, so ist die Relativdiscriminante von K/k durch kein Primideal teilbar, welches nicht in $\mathfrak{m}$ aufgeht.

Oben haben wir die Vorzeichenbedingung für die Classengruppe H ausser Betracht gelassen. Um unseren Existenzbeweis für $l=2$ allgemein zu führen, haben wir die Classen von k nach total positiver Zahlengruppe zu definiren, und demgemäss nach Satz 22 die Classen von k′ einer entsprechenden Vorzeichenbedingung zu unterwerfen. Tatsächlich ist aber, wenn der Index von H grösser als 2 ist, und G/H cyclisch, jede Vorzeichenbedingung für die Gruppe $G_0=\{C^2, H\}$ ohne Belang, so dass k′ ein relativ quadratischer Körper von der im ersten Teil des Satzes 27 erläuterten Art ist. Es musste dies so sein, wenn überhaupt ein relativ cyclischer Körper vom 2^hten Grade existiren soll, welcher den Körper k′ als Unterkörper enthält. Denn für einen reellen Grundkörper muss jeder relativ cyclische Körper vom Grade 2^h notwendig den reellen Unterkörper vom Relativgrade 2^{h-1} enthalten.

---

1) Vgl. z.B. H. Weber, Lehrbuch der Algebra, II (2te Aufl., Braunschweig, 1899) S. 140. Der hier benutzte Gruppensatz ist ein specieller Fall eines allgemeinen Satzes von W. Burnside: vgl. dessen Theory of finite groups (2. ed. Cambridge, 1911.) p. 131–132.

§ 22.

Existenzbeweis im allgemeinen Falle.

Nachdem im Vorhergehenden unser Existenzsatz in allen denjenigen Fällen bewiesen worden ist, wo die complementäre Gruppe der gegebenen Classengruppe cyclisch von einer Primzahlkotenzordnung ist, können wir nun den allgemeinen Fall rasch erledigen. Sei also $\mathfrak{H}$ eine Classengruppe von einem beliebigen Index n nach dem Modul $\mathfrak{m}$ mit oder ohne Vorzeichenbeschränkung. Es seien ferner $\mathfrak{C}_1, \mathfrak{C}_2, \ldots \mathfrak{C}_r$ ein System der Basisclassen von den Primzahlpotenzordnungen $l_1^{h_1}, l_2^{h_2}, \ldots l_r^{h_r}$ der vollständigen Classengruppe $\mathfrak{G}$ in Bezug auf $\mathfrak{H}$, derart dass

$$\mathfrak{G}=\{\mathfrak{C}_1, \mathfrak{C}_2, \cdots\cdots \mathfrak{C}_r, \mathfrak{H}\},$$

$$n=l_1^{h_1} l_2^{h_2} \cdots\cdots l_r^{h_r}.$$

Diejenige Untergruppe von $\mathfrak{G}$, welche ausser $\mathfrak{H}$ noch die sämtlichen Basisclassen mit alleiniger Ausnahme von $\mathfrak{C}_\rho$ enthält, sei mit $\mathfrak{H}_\rho$ bezeichnet, so dass $\mathfrak{G}/\mathfrak{H}_\rho$ cyclisch von der Ordnung $l_\rho^{h_\rho}$ ist. Ist dann K_ρ der Classenkörper für $\mathfrak{H}_\rho$, deren Existenz in den vorhergenden Artikeln bewiesen worden ist, dann entsteht durch Zusammensetzung der r Körper $K_1, K_2, \ldots K_r$ ein relativ Abel'scher Körper K, welcher der gesuchte Classenkörper für die Classengruppe $\mathfrak{H}$ sein wird.

Denn da die Relativnormen der Ideale des zusammengesetzten Körpers $K_1 K_2$ offenbar sowohl der Classengruppe $\mathfrak{H}_1$ als auch $\mathfrak{H}_2$, folglich der Classengruppe $\{\mathfrak{C}_3, \ldots \mathfrak{H}\}$ vom Index $l_1^{h_1} l_2^{h_2}$ angehören, so folgt nach Satz 4, dass der Relativgrad von $K_1 K_2$ wenigstens gleich $l_1^{h_1} l_2^{h_2}$ sein muss. Anderseits kann aber dieser Relativgrad höchstens gleich dem Product der Relativgrade der beiden Körper K_1 und K_2 sein; also ist er genau gleich $l_1^{h_1} l_2^{h_2}$. Mit andern Worten: $K_1 K_2$ ist der Classenkörper für die Classengruppe $\{\mathfrak{C}_3, \ldots \mathfrak{H}\}$. So fortfahrend überzeugt man sich davon, dass der Körper $K=K_1 K_2 \ldots K_r$ in der Tat der Classenkörper für die Classengruppe $\mathfrak{H}$ ist.

Hieraus folgt aber weiter, dass K vom Relativgrade n ist und dass die Galois'sche Gruppe des Relativkörpers K/k mit der complementären Gruppe $\mathfrak{G}/\mathfrak{H}$ holoedrisch isomorph ist.

Da endlich die Relativdiscriminante jedes der Körper $K_1, K_2, \ldots K_r$ kein Primideal als Factor enthält, welches nicht in den Modul $\mathfrak{m}$ aufgeht, so gilt dassalbe auch von der Relativdiscriminante von K.

Wie man sieht, erfüllt der Körper K alle Forderungen des zu Beginn dieses Capitels aufgestellten Satzes 23, welcher nunmehr in allen seinen Teilen vollständig bewiesen worden ist.

CAPITEL IV.

Weitere allgemeine Sätze.

§ 23.

Der Vollständigkeitssatz.

Ist $\mathfrak{m}$ ein beliebiges Ideal im Grundkörper k, o^+ die Zahlengruppe der *total positiven* Zahlen α, welche die Bedingung: $\alpha \equiv 1, (\mathfrak{m})$ erfüllen, dann ist die Classenzahl nach o^+ durch die Formel gegeben;

$$h(\mathfrak{m}) = h_0 \frac{\varphi(\mathfrak{m})}{e},$$

wo $h_0 = h(1)$ die Classenzahl im absoluten Sinne, φ die Euler'sche Function, und

$$e = (\mathfrak{E} : \mathfrak{E}_0)$$

der Gruppenindex ist, wobei $\mathfrak{E}$ die Gruppe der sämtlichen Einheiten in k, die Einheitswurzeln mitgerechnet, und $\mathfrak{E}_0$ die Gruppe der Einheiten in o^+ bedeutet.

Dann existirt nach Satz 23 ein relativ Abel'scher Körper vom Grade $h(\mathfrak{m})$ in Bezug auf k, welcher Classenkörper für die durch o^+ erzeugte Idealengruppe in k ist. Derselbe sei mit $K(\mathfrak{m})$ bezeichnet.

Dieser Körper $K(\mathfrak{m})$ soll der **vollständige Classenkörper nach dem Modul** $\mathfrak{m}$ genannt werden. Für $\mathfrak{m} = (1)$ ist der Körper $K(1)$

der zuerst von D. Hilbert eingeführte Classenkörper von k, den wir als den *absoluten Classenkörper* bezeichnen wollen. Ist ferner $\mathfrak{m}$ der Führer eines Ringes in k, dann ist derjenige Körper, welcher Hilbert gelegentlich[1] als einen Ringclassenkörper bezeichnet hat, als einen Unterkörper in $K(\mathfrak{m})$ enthalten, wie überhaupt jeder Classenkörper für irgend eine Classengruppe nach dem Modul $\mathfrak{m}$.

Eine wichtige Frage ist nun, ob auch umgekehrt jeder relativ Abel'sche Körper in Bezug auf k als Classenkörper einer Classengruppe nach einem geeignet gewählten Modul $\mathfrak{m}$ in k zugeordnet ist? Diese Frage ist im bejahenden Sinne zu beantworten:

Satz 28. *Alle relativ Abel'schen Körper in Bezug auf einen beliebigen algebraischen Körper werden durch die Classenkörper nach den Idealmoduln in demselben erschöpft.*

Es genügt, diesen Satz für die relativ cyclischen Oberkörper vom Primzahlpotenzgrade zu beweisen.

Denn aus solchen lässt sich jeder relativ Abel'sche Körper zusammensetzen. Anderseits seien K, K′ relativ Abel'sch von den Relativgraden n, n' in Bezug auf k und bez. den Classengruppen $\mathfrak{H}$, $\mathfrak{H}'$ nach den Moduln $\mathfrak{m}$, $\mathfrak{m}'$ als Classenkörper zugeordnet. Ist $\mathfrak{m}_0$ das kleinste gemeinsame Vielfaches von $\mathfrak{m}$ und $\mathfrak{m}'$, dann sind $\mathfrak{H}$, $\mathfrak{H}'$ als Classengruppen nach dem Modul $\mathfrak{m}_0$ aufzufassen. Unter der Voraussetzung, dass K, K′ keinen gemeinsamen Unterkörper über k enthalten, folgt, dass die Gruppe $\{\mathfrak{H}, \mathfrak{H}'\}$ mit der vollständigen Classengrappe $\mathfrak{G}$ von k zusammenfällt, weil sonst der zu der Classengruppe $\{\mathfrak{H}, \mathfrak{H}'\}$ gehörige Classenkörper nach Satz 6 notwendig sowohl in K als auch in K′ enthalten sein musste. Da nun $\mathfrak{H}$, $\mathfrak{H}'$ bez. vom Index n, n' sind, und $\{\mathfrak{H}, \mathfrak{H}'\}=\mathfrak{G}$, so muss die grösste gemeinsame Untergruppe $\mathfrak{H}_0$ von $\mathfrak{H}$ und $\mathfrak{H}'$ notwendig vom Index nn' sein. Weil aber die Relativnormen der Ideale von dem zusammengesetzten Körper KK′ vom Relativgrade nn' sämtlich in $\mathfrak{H}_0$ enthalten sind, so folgt, dass KK′ der Classenkörper für die Classengruppe $\mathfrak{H}_0$ ist. Da dasselbe auch von mehreren relativ Abel'schen Körpern K, K,′ K″...gilt, so folgt das Gesagte.

1) D. Hilbert, über die Theorie der relativ Abel'schen Körper. Göttinger Nachr. 1898.

Da Satz 28 schon für die relativ cyclischen Körper vom Primzahlgrade in Satz 13 bewiesen worden ist, so handelt es sich jetzt darum, den letzteren auf die relativ cyclischen Körper vom Primzahlpotenzgrade zu verallgemeinern.

§. 24.

Ueber die Geschlechter im relativ cyclischen Körper eines Primzahlpotenzgrades.

Um am Ende des vorigen Artikels angezeigten Beweis durchzuführen, stellen wir den folgenden Satz auf:

Satz 29. *Es sei* K/k *ein relativ cyclischer Körper vom Primzahlpotenzgrade* l^h. *Dann gibt es stets ein Ideal* $\mathfrak{m}$ *in* k, *welches jedes in die Relativdiscriminante von* K *aufgehende Primideal von* k *als Factor, und zwar solches, welches zu* l *prim ist, zur ersten, dagegen solches, welches in* l *aufgeht, zu einer hinreichend hohen Potenz, enthält, von der Art, dass* K *Classenkörper für eine Classengruppe vom Index* l^h *nach dem Modul* $\mathfrak{m}$ *ist.*

Ferner lässt sich im Oberkörper K *ein in* $\mathfrak{m}$ *aufgehendes Ideal* $\mathfrak{M}$ *auffinden, derart, dass, wenn die Classen in* K *und* k *nach den Zahlengruppen definirt werden, die aus den Zahlen dieser Körper bestehen, welche bez. nach den Moduln* $\mathfrak{M}$, $\mathfrak{m}$ *mit* 1 *congruent sind, jede Classe von* K, *deren Relativnorm die Hauptclasse von* k *ist, die symbolische* $1-s^{te}$ *Potenz einer Classe von* K *wird, wenn* s *eine erzeugende Substitution der Galois'schen Gruppe des Relativkörpers* K/k *bedeutet.*

Beweis. Zunächst sei das Folgende bemerkt: Wenn es nachgewiesen wird, dass der Körper K einer Classengruppe $\mathfrak{H}$ vom Index l^h als Classenkörper zugeordnet ist, dann ist klar, dass die complementäre Gruppe $\mathfrak{G}/\mathfrak{H}$ notwendig cyclisch sein muss, wo $\mathfrak{G}$, wie immer, die vollständige Classengruppe von k bedeutet. Denn andernfalls musste es mehr als eine Classengruppe vom Index l geben, welche $\mathfrak{H}$ enthält, und jeder derselben nach Satz 23 ein relativ cyclischer Körper vom Relativgrade l als Classenkörper zugeordnet sein muss. Diese Körper mussten aber nach Satz 6 sämtlich in K enthalten sein, was unmöglich ist, weil K relativ cyclisch sein sollte.

Um nun unseren Satz durch vollständige Induction zu beweisen, werde angenommen: der Satz sei für den in K enthaltenen relativ cyclischen Körper K′/k vom Grade l^{h-1} richtig. Hierunter ist genauer folgendes zu verstehen: Die in die Relativdiscriminante von K aufgehenden, zu l primen, und in l aufgehenden Primideale von k seien bez. durchweg mit $\mathfrak{p}$ und $\mathfrak{l}$, die in sie aufgenden Primideale von K bez. K′ durchweg mit $\mathfrak{P}$ und $\mathfrak{L}$, bez. $\mathfrak{P}'$ und $\mathfrak{L}'$ bezeichnet, so dass

$$\mathfrak{P}'=\mathfrak{P}^l, \quad \mathfrak{L}'=\mathfrak{L}^l.^{1)}$$

Man setze

$$\mathfrak{m}=\Pi\mathfrak{p}\Pi\mathfrak{l}^u, \quad \mathfrak{M}=\Pi\mathfrak{P}.\ \Pi\mathfrak{L}^U, \quad \mathfrak{M}'=\Pi\mathfrak{P}'.\ \Pi\mathfrak{L}'.^{U'} \tag{1}$$

Es soll dann angenommen werden, dass sobald U und U' bez. grösser als gewisse näherzubestimmende feste Grössen sind, die Relativnormen der Classen (nach $\mathfrak{M}'$) von K′ eine Classengruppe $\mathfrak{H}'$ vom Index l^{h-1} in k (nach $\mathfrak{m}$) ausmachen, dass ferner die Classen von K,′ deren Relativnormen Hauptclasse von k sind, durch die symbolischen $1-s^{\text{ten}}$ Potenzen in K′ erschöpft werden.

Um nun auf Grund dieser Annahme die entsprechende Tatsache für den Körper K nachzuweisen, machen wir die erlaubte Annahme, dass

$$U' > v, \tag{2}$$

und setzen

$$U=(U'-v)l+v, \tag{3}$$

wo v die mehrmals erklärte Bedeutung in Bezug auf das Primideal $\mathfrak{L}$ und den Relativkörper K/K′ besitzt: es ist die Relativdifferente von K/K′ genau durch die $(v+1)(l-1)^{\text{te}}$ Potenz von $\mathfrak{L}$ teilbar. (Ist also $U'=v+n$, dann ist $U=v+nl$, wo $n>0$).

Wir setzen diesen Wert von U in den Ausdruck von $\mathfrak{M}$ in (1) ein, und definiren die Classen von K nach diesem Modul $\mathfrak{M}$. Dann kommt Satz 22 in Anwendung, demzufolge die Relativnormen

1) Hiermit ist nicht gesagt, dass jedes $\mathfrak{p}$ und jedes $\mathfrak{l}$ schon in die Relativdiscriminante von K′ aufgeht. Auch sollen, wenn mehrere von einander verschiedene $\mathfrak{P}'$ in ein $\mathfrak{p}$ aufgehen, das Product $\Pi\mathfrak{P}'$ und $\Pi\mathfrak{P}$ in (1) auf alle diese Primfactoren von $\mathfrak{p}$ erstreckt werden; gleiches gilt für die Primideale $\mathfrak{l}$.

der Classen von K in Bezug auf K′ eine Classengruppe H′ vom Index l nach $\mathfrak{M}'$ ausmachen, und speciell die Classen von K, deren Relativnormen die Hauptclasse nach $\mathfrak{M}'$ sind, symbolische $1-s^{l^{h-1}}$ te Potenzen der Classen von K sein müssen.

Da nun die Classengruppe H′ ihrer Bedeutung nach offenbar gegenüber s invariant ist, so ist zu schliessen, dass die (1−s) te Potenz jeder Classe von K′ notwendig in H′ enthalten sein muss. In der Tat: sei C eine nicht in H′ enthaltene Classe von K′, so dass auch C^s nicht in H′, folglich in einem Classencomplex $H'C^a$ enthalten sein muss, wo a eine Zahl aus der Reihe: $1, 2, \ldots l-1$ bedeutet. Da dann C^{s^n} in $H'C^{a^n}$ enthalten ist, so folgt, wenn man $n=l^{h-1}$ macht, dass die $(1-a^n)^{te}$ Potenz von C in H′ enthalten ist, d. h. es ist

$$a^{l^{h-1}} \equiv 1, \quad (l),$$

woraus folgt, dass $a \equiv 1$, (l), also $a=1$ sein muss. Es ist daher C^{1-s} in H′ enthalten, wie behauptet wird.

Demnach folgt, nach Annahme, dass alle Classen von K′, deren Relativnormen in Bezug auf k die Hauptclasse nach m in k sind, in H′ enthalten, folglich, da H′ nur den l^{ten} Teil der sämtlichen Classen von K′ ausmacht, dass die Relativnormen aller Classen von K in Bezug auf k eine Classengruppe H vom Index l^h in k ausmachen, welche in der Classengruppe H′ enthalten ist.

Nunmehr ist noch zu zeigen, dass die Classen von K, deren Relativnormen in Bezug auf k die Hauptclasse in k sind, notwendig die symbolischen $1-s^{ten}$ Potenzen in K sein müssen. Da, wie vorhin bemerkt, die complementäre Gruppe G/H cyclisch ist, so kann man in k eine Basisclasse c angeben, deren Ordnung eine Potenz von l, und von der erst die l^h te Potenz in H enthalten ist. Demnach hat man, in einer leicht verständlichen Bezeichnungsweise

$$G=\{c, D\}, \quad H=\{c^{l^h}, D\}, \quad H'=\{c^{l^{h-1}}, D\};$$

dementsprechend lässt sich die vollständige Classengruppe von K′ in der Form darstellen:

$$\{c, D'\}, \qquad (4)$$

wo D′ den Inbegriff der Classen von K′ bedeutet, deren Relativnormen in k in D hineinfallen; so dass jede Classe in D′ Relativnorm einer Classe von K in Bezug auf K′ ist.

Sei nun C eine Classe von K, deren Relativnorm die Hauptclasse in k ist. Dann ist, nach Annahme

$$\mathfrak{N}(C)=C'^{1-s}, \tag{5}$$

wo $\mathfrak{N}$ die in K genommene Relativnorm in Bezug auf K′, und C′ eine Classe von K′ bedeutet. Da aber nach (4)

$$C'=c^{\alpha}\,[D'] \tag{6}$$

wo mit [D′] eine Classe von K′ bezeichnet wird, welche der Gruppe D′ angehört, folglich Relativnorm einer Classe D von K ist:

$$D'=\mathfrak{N}(D). \tag{7}$$

Aus (5), (6), (7) folgt

$$\mathfrak{N}(C)=\mathfrak{N}(D^{1-s}).$$

Setzt man daher

$$C=D^{1-s}A, \tag{8}$$

so ist A eine solche Classe von K, dass $\mathfrak{N}$ (A) die Hauptclasse von K′ ist. Folglich ist A eine $1-s^{l^{h-1}}$ te Potenz, also auch eine $1-s^{te}$ Potenz einer Classe von K. Dasselbe gilt daher nach (8) auch von C selbst, wie zu beweisen war.

Um eine untere Grenze für den Exponenten u zu bestimmen, sei angenommen, dass das Primideal $\mathfrak{P}$ von K genau zur l^g ten Potenz in $\mathfrak{l}$ aufgeht, sodass die Verzweigung von $\mathfrak{l}$ erst in dem Unterkörper von K vom Relativgrade l^{h-g+1} über k beginnt. Indem wir allgemein mit K_γ den in K enthaltenen relativ cyclischen Oberkörper vom Grade l^r über k bezeichnen, seien $v_1, v_2, \ldots v_g$ die Zahlen, die mehrmals erklärte Bedeutung[1] in Bezug auf die Relativkörper K_{h-g+1}/K_{h-g}, $K_{h-g+2}/K_{h-g+1}, \ldots\ldots K_h/K_{h-1}$ haben, so dass bekanntlich

$$1\leqq v_1<v_2<\cdots\cdots<v_g \tag{9}$$

1) Es ist v_g die oben (S. 92) mit v bezeichnete Zahl.

Für den Modul $\mathfrak{M}_\tau$ in K_τ genügt es, den entsprechenden Exponenten U_τ so zu bestimmen, dass

$$u=U_1=U_2=\cdots\cdots=U_{h-g},$$

und, gemäss (2) und (3), für $\tau=h-g, h-g+1, \ldots\ldots h,$

$$U_\tau > v_{\tau-(h-g)+1},$$
$$U_{\tau+1}=lU_\tau-(l-1)v_{\tau-(h-g)+1}.$$

Diese Bedingungen werden erfüllt, wie man leicht mit Hülfe von (9) bestätigt, wenn u so gross genommen wird, dass

$$U=U_h=ul^g-(l-1)\{v_g+v_{g-1}l+\cdots\cdots+v_1 l^{g-1}\}>v_g. \qquad (10)$$

In die Relativdiscriminante von K/k geht $\mathfrak{l}$ genau zur $\delta(l-1)$ ten Potenz auf, wo[1])

$$\delta=\{(v_g+1)+(v_{g-1}+1)l+\cdots\cdots(v_1+1)l^{g-1}\}l^{h-g}$$
$$=\left\{v_g+v_{g-1}l+\cdots\cdots+v_1l^{g-1}+\frac{l^g-1}{l-1}\right\}l^{h-g}.$$

Nach (10) kann man daher einen Wert von u finden, derart, dass

$$\delta>u,$$

ausser wenn $h=g=1$, wo notwendig $\delta=u=v_1+1$.

Ohne nähere Kenntnis über die Zahlen $v_1, v_2, \ldots\ldots v_g$, kann man eine untere Grenze für u angeben, welche sich für alle Fälle bewähren wird: nämlich

$$u>gs+\frac{s}{l-1}, \qquad (11)$$

wo s der Exponent der höchsten in l aufgehenden Potenz von $\mathfrak{l}$ bedeutet. Denn es ist nach Satz 8

$$\frac{sl}{l-1}\geqq v_1, \quad \frac{sl^2}{l-1}\geqq v_2, \ldots\ldots \frac{sl^g}{l-1}\geqq v_g,$$

so dass aus (11) folgt

$$ul^g>gsl^g+\frac{sl^g}{l-1}\geqq(l-1)\{v_g+v_{g-1}l+\cdots\cdots+v_1l^{g-1}\}+v_g,$$

wodurch (10) befriedigt wird.

Wir haben bisher den Fall ausser Betracht gelassen, wo $l=2$ und unter den mit k conjugirten Körpern reelle vorhanden sind,

1) Vgl. Hilbert, Bericht, Satz 79.

wo also unter Umständen eine Vorzeichenbedingung für die Classeneinteilung in k unentbehrlich werden kann. Gebe es nun in diesem Falle einen mit k conjugirten reellen Körper k^*, für welchen der entsprechende mit K conjugirte Körper K^* imaginär ausfällt, dann ist notwendig der in K^* enthaltene mit K′ conjugirte Körper K'^* vom Relativgrade 2^{h-1} reell. Es ist daher leicht, in Bezugnahme auf Satz 22 einzusehen, dass unser Beweis seine Gültigkeit beibehält, wenn in der Zahlengruppe, welche der Classeneinteilung in k zu Grunde gelegt wird, nur diejenigen Zahlen, die in allen vorhandenen Körpern k^* positiv ausfallen, umsomehr also, wenn nur die total positiven Zahlen zugelassen werden.

Durch das Vorhergende ist, nach der Bemerkung am Ende des § 23, Satz 28 allgemein bewiesen worden. Es ist jeder relativ Abel'sche Körper K/k Classenkörper für eine Classengruppe H in k, deren Führer jedenfalls ein Teiler der Relativdiscriminante von K/k ist, wie man sich auf Grund des vorhergehenden Beweises leicht überzeugt. Nach Satz 23 ist die Galois'sche Gruppe des Relativkörpers K/k holoedrisch isomorph mit der complementären Gruppe G/H. Allgemeiner ist *jeder Unterkörper* K′/k *von* K/k *als Classenkörper einer Classengruppe* H′ *zugeordnet, welche* H′ *in sich enthält und ungekehrt; es ist dabei die Galois'sche Gruppe des relativ Abel'schen Körpers* K/K′ *holoedrisch isomorph mit der complementären Gruppe* H′/H.

§ 25.

Der Zerlegungssatz.

Wenn K der Classenkörper für die Classengruppe H des Grundkörpers k ist, dann ist jedes zum Führer der Classengruppe relativ prime Primideal von k, welches in K in die Primideale des ersten Relativgrades zerfällt, in einer Classe von H enthalten. Umgekehrt gilt der folgende sehr wichtige Satz.

Satz 30. (*Der Zerlegungssatz*). *Jedes in einer Classengruppe eines beliebigen Körpers enthaltene Primideal zerfällt in die von*

einander verschiedenen Primideale des ersten Relativgrades in dem Classenkörper für diese Classengruppe.

Beweis. Es genügt, diesen Satz für den Fall zu beweisen, wo der Oberkörper relativ cyclisch von einem Primzahlpotenzgrade ist. Denn die dem Oberkörper K zugehörige Classengruppe H ist die grösste gemeinsame Untergruppe der Classengruppen, welche den relativ cyclischen Körpern von den Primzahlpotenzgraden zugeordnet sind, aus welchen K zusammengesetzt wird. Zerfällt anderseits ein Primideal des Grundkörpers in allen jenen Körpern in die von einander verschiedenen Primideale des ersten Relativgrades, so muss dasselbe auch in dem zusammengesetzten Körper K gelten, wie leicht einzusehen ist.

Sei also K relativ cyclisch vom Relativgrade l^n in Bezug auf k, H die zugehörige und G die vollständige Classengruppe von k, so dass die complementäre Gruppe G/H cyclisch von der Ordnung l^n ist. Wir setzen

$$G = \sum^{\alpha} HA^{\alpha}, \qquad (0 \leqq \alpha < l^n)$$

wo A eine Classe bedeutet, von welcher erst die l^nte Potenz in H enthalten ist. Sei ferner C eine Classe in H, und $\mathfrak{p}$ ein Primideal der Classe C. Wir nehmen zunächst an, es sei C nicht l^{te} Potenz einer Classe von k. Dann gibt es offenbar eine Classengruppe H′ vom Index l, welche nicht die Classe C enthält, und es ist

$$G = \Sigma H' C^{\beta}. \qquad (0 \leqq \beta < l).$$

Ist dann H_0 die Durchschnitt der beiden Gruppen H und H′, dann ist H_0 vom Index l^{n+1}, und man hat

$$\begin{aligned} H &= \Sigma H_0 C^{\beta}, \qquad (0 \leqq \beta < l) \\ H' &= \Sigma H_0 A^{\alpha}, \qquad (0 \leqq \alpha < l^n) \\ G &= \Sigma H_0 A^{\alpha} C^{\beta}. \end{aligned}$$

Der relativ cyclische Körper l^{ten} Grades über k, welcher der Classengruppe H′ zugeordnet ist, sei mit K′ bezeichnet. Dann ist der zusammengesetzte Körper KK′ vom Relativgrade l^{n+1} der Classenkörper für H_0.

Angenommen nun, das Primideal $\mathfrak{p}$ zerfalle in K in ein Product von e von einander verschiedenen Primidealen, und $e < l^n$. Da $\mathfrak{p}$ nicht in H' enthalten ist, so bleibt $\mathfrak{p}$ prim in K'. Wir betrachten nun den Zerlegungskörper K_z für $\mathfrak{p}$ in dem Körper KK'. Da $\mathfrak{p}$ nicht in die Relativdiscriminante von KK' aufgeht, muss KK' relativ cyclisch in Bezug auf K_z sein. Weil aber K_z nach Annahme nicht K und auch nicht K' enthält, ist dies nur so möglich, dass $K_z K$ mit KK' zusammenfällt. Daher ist K_z nicht in K enthalten. Diesem Körper K_z muss daher eine Classengruppe zugeordnet sein, welche H_0, aber nicht H enthält, folglich gewiss nicht die Classe c enthalten kann. Dann könnte aber das in c enthaltene Primideal $\mathfrak{p}$ nicht in die Primideale vom ersten Relativgrade in K_z zerfallen, was ein Widerspruch ist. Es ist daher unsere Annahme zu verwerfen: $\mathfrak{p}$ muss notwendig in l^n von einander verschiedene Primideale in K zerfallen. Somit ist der Satz im gegenwärtigen Falle bewiesen.

Wir gehen nun zu dem Falle über, wo c l^{te} Potenz einer Classe in k ist. Dann muss es eine Zahl ϖ in der Zahlengruppe o geben, die der Classeneinteilung in k zu Grunde gelegt ist, von der Art, dass

$$\mathfrak{p}\mathfrak{j}^l = (\varpi),$$

wo $\mathfrak{j}$ ein gewisses Ideal von k bedeutet. Zum Modul $\mathfrak{m}$ der Zahlengruppe o sei alsdann ein Primfactor $\mathfrak{q}$ hinzugefügt, von der Beschaffenheit, dass jede Einheit ε und jede Zahl ρ, welche l^{te} Potenz eines Ideals von k ist, l^{ter} Potenzrest nach $\mathfrak{q}$, dagegen die Zahl ϖ ein l^{ter} Nichtrest nach $\mathfrak{q}$ ist. Definirt man dann die Classen von k nach dem Modul $\overline{\mathfrak{m}} = \mathfrak{m}\mathfrak{q}$, dann wird das Primideal $\mathfrak{p}$ gewiss in einer Classe enthalten sein, welche nicht die l^{te} Potenz einer Classe ist, und wir können den Beweis des Satzes genau wie oben durchführen.

Es kommt also darauf an, die Existenz des Primideals $\mathfrak{q}$ nachzuweisen. Enthält k die primitive l^{te} Einheitswurzel, dann ist dies evident, weil eine Gleichung von der Gestalt

$$\varpi = \varepsilon^u \cdots \rho^v \cdots \xi^l \qquad (0 \leqq u, v < l) \qquad (1)$$

offenbar nicht durch eine Zahl ξ von k zu befriedigen ist.[1] Enthält aber k nicht die primitive l^{te} Einheitswurzel, dann adjungire man dieselbe dem Körper k, und erweitre ihn zu k'. Da der Relativgrad von k'/k prim zu l ist, so kann eine Relation von der Form (1) auch nicht in k' bestehen. Daher gibt es in k' ein Primideal ersten Grades $\mathfrak{q}'$, für welches

$$\left(\frac{\varpi}{\mathfrak{q}'}\right)\neq 1, \qquad \left(\frac{\varepsilon}{\mathfrak{q}'}\right)=1,\cdots\cdots\left(\frac{\rho}{\mathfrak{q}'}\right)=1,\cdots\cdots$$

Ist dann $\mathfrak{q}$ das durch $\mathfrak{q}'$ teilbare Primideal von k, dann ist offenbar $\mathfrak{q}$ ein Primideal von der geforderten Beschaffenheit.

Nur scheinbar allgemeiner als der vorhergehende ist

Satz 31. *Ist* K *der Classenkörper für die Classengruppe* H *von* k, *dann werden die Primideale von* k, *welche einem und demselben Classencomplex* HC *angehören, in* K *auf derselben Weise zerlegt, d. h. sie erfahren in* K *eine Zerlegung in dieselbe Anzahl von Primidealen derselben Relativgrade.*

Beweis. Ist $\mathfrak{p}$ ein Primideal, welches der Classe C oder einer Classe des Complexes HC angehört, dann ist der Zerlegungskörper für $\mathfrak{p}$ in K der umfassendste in K enthaltene Oberkörper von k, in welchem $\mathfrak{p}$ in die Primideale des ersten Relativgrades zerfällt. Dieser Körper ist daher der kleinsten Classengruppe in k zugeordnet, welche H und C enthält, d. h. der Classengruppe $\{H, C\}$. Ist daher n der Relativgrad des Körpers K/k, also der Index der Classengruppe H, und ist f der kleinste positive Exponent, für welchen C^f in H enthalten ist, dann ist der Index der Classengruppe $\{H, C\}$, und demnach auch der Relativgrad des Zerlegungskörpers für $\mathfrak{p}$ gleich $e=\frac{n}{f}$; und das Primideal $\mathfrak{p}$ zerfällt in K in e von einander verschiedene Primideale vom f^{ten} Relativgrade.

Wir erläutern noch kurz das Zerlegungsgesetz für das in die Relativdiscriminante aufgehende Primideal. Das Gesetz ist besonders einfach für den vollständigen Classenkörper $K(\mathfrak{m})$ nach dem Modul $\mathfrak{m}$. Sei $\mathfrak{l}$ ein genau zur n^{ten}-Potenz in $\mathfrak{m}$ aufgehendes Primideal, so dass

1) Vgl. § 4. S. 16.

$$\mathfrak{m}=\mathfrak{l}^n\mathfrak{m}_0,$$

wo $\mathfrak{m}_0$ prim zu $\mathfrak{l}$ ist. Der Körper $K(\mathfrak{m})$ enthält eine Reihe von Unterkörpern, von welcher der erste der absolute Classenkörper und der letzte der Körper $K(\mathfrak{m})$ selbst ist:

$$K(1),\quad K(\mathfrak{m}_0),\quad K(\mathfrak{l}\mathfrak{m}_0),\quad K(\mathfrak{l}^2\mathfrak{m}_0),\cdots\cdots K(\mathfrak{l}^n\mathfrak{m}_0).$$

Die Relativgrade dieser Körper werden durch die entsprechende Zerlegung des Relativgrades von $K(\mathfrak{m})$ klargestellt:

$$h\times\frac{\varphi(m_0)}{(E:E_0)}\times\frac{l^f-1}{(E_0:E_1)}\times\frac{l^f}{(E_1:E_2)}\times\cdots\cdots\frac{l^f}{(E_{n-1}:E_n)};$$

hierbei bedeutet h die Classenzahl des Grundkörpers k im absoluten (sogenannten engeren) Sinne; f der absolute Grad des Primideals $\mathfrak{l}$ in k, E die Gruppe der sämtlichen total positiven Einheiten in k, E_e für $e\geqq 0$ die Gruppe derjenigen, welche nach dem Modul $\mathfrak{l}^e\mathfrak{m}_0$ mit 1 congruent sind, und das Zeichen $(A:B)$ wie bisher den Gruppenindex.

Bezeichnen wir ferner mit G die vollständige Classengruppe von k, mit G_{-1} die durch die sämtlichen total positiven Zahlen von k definirte Idealgruppe, und allgemein mit G_e $(e\geqq 0)$ die Idealgruppe, welche durch die total positiven Zahlen α erzeugt wird, die der Congruenz

$$\alpha\equiv 1,\quad (\mathfrak{l}^e\mathfrak{m}_0)$$

genügen, dann sind die oben angegebenen Körper der Reihe nach den Classengruppen zugeordnet:

$$G_{-1},\quad G_0,\quad G_1,\quad G_2,\cdots\cdots G_n.$$

Es ist die complementäre Gruppe G_1/G_0 und dementsprechend der Relativkörper $K(\mathfrak{l}\mathfrak{m}_0)/K(\mathfrak{m}_0)$ cyclisch, dagegen $G_2/G_1,\ldots\ldots$ G_{n-1}/G_n und entsprechend $K(\mathfrak{l}^2\mathfrak{m}_0)/K(\mathfrak{l}\mathfrak{m}_0),\ldots\ldots K(\mathfrak{m})/K(\mathfrak{l}^{n-1}\mathfrak{m}_0)$ Abel'sch vom Typus $(l, l,\ldots\ldots l)$, wo der Rang nicht grösser als f ist. Es ist $K(\mathfrak{m}_0)$ der Trägheitskörper, $K(\mathfrak{l}\mathfrak{m}_0)$ der Verzweigungskörper, $K(\mathfrak{l}^2\mathfrak{m}_0),\ldots\ldots K(\mathfrak{m})$ die Verzweigungskörper höheren Grades für $\mathfrak{l}$ in $K(\mathfrak{m})$. Das Primideal $\mathfrak{l}$ wird in $K(\mathfrak{m})$ die Potenz mit dem Exponenten:

$$\frac{\varphi(\mathfrak{l}^n)}{(\mathrm{E}_0 : \mathrm{E}_n)} = \frac{l^f-1}{(\mathrm{E}_0 : \mathrm{E}_1)} \cdot \frac{l^f}{(\mathrm{E}_1 : \mathrm{E}_2)} \cdots\cdots \frac{l^f}{(\mathrm{E}_{n-1} : \mathrm{E}_n)}$$

eines Ideals, welches ein Product von einer gewissen Anzahl von einander verschiedener Primideale in $\mathrm{K}(\mathfrak{m})$ ist. Diese Anzahl und der Relativgrad dieser Primideale werden gefunden, indem man die Zerlegung von $\mathfrak{l}$ in dem Trägheitskörper $\mathrm{K}(\mathfrak{m}_0)$ nach Satz 31 bestimmt.

Wenn allgemein K der Classenkörper für die Classengruppe H nach dem Modul $\mathfrak{m}$ ist, dann ist der Trägheitskörper $\mathrm{K}_\mathfrak{l}$ für $\mathfrak{l}$ in K der grösste gemeinsame Unterkörper von K und $\mathrm{K}(\mathfrak{m}_0)$, also der Classengruppe

$$\{\mathrm{H}, \mathrm{G}_0\} = \mathrm{HG}_0$$

zugeordnet; sie ist eine Classengruppe nach dem Modul $\mathfrak{m}_0$. Ist

$$\mathfrak{l} = (\mathfrak{L}_1 \cdots\cdots \mathfrak{L}_v)^g$$

die Zerlegung von $\mathfrak{l}$ in K, dann ist g gleich dem Relativgrade von $\mathrm{K}/\mathrm{K}_\mathfrak{l}$ also gleich dem Gruppenindex $(\mathrm{HG}_0 : \mathrm{H}) = (\mathrm{G}_0 : \mathrm{H}_0)$, wenn H_0 die Durchschnitt von G_0 und H bedeutet.

Das in diesem Artikel auseinandergesetzte Zerlegungssatz ist die naturgemässe Verallgemeinerung des Gesetzes, welches die Zerlegung der natürlichen Primzahlen in dem Kreisteilungskörper regeln. Der durch die primitiven m^{ten} Einheitswurzeln definirte Kreisteilungskörper $\varphi(m)^{\text{ten}}$ Grades ist der vollständige Classenkörper $\mathrm{K}(m)$, wenn der Grundkörper k der natürliche ist. Ist p eine nicht in m aufgehende rationale Primzahl, dann ist die in Satz 31 mit f bezeichnete Zahl der kleinste positive Exponent, für welchen $p^f \equiv 1$, (m) ausfällt; p zerfällt daher in $\mathrm{K}(m)$ in $e = \varphi(m) : f$ von einander verschiedene Primideale. Ist ferner l eine genau zur n^{ten} Potenz in $m = l^n m_0$ aufgehende natürliche Primzahl, dann ist der Trägheitskörper für l in $\mathrm{K}(m)$ der Körper $\mathrm{K}(m_0)$, d. h. der durch die m_0^{te} primitiven Einheitswurzeln definirte Körper. In $\mathrm{K}(m)$ zerfällt l in ein Product von $\varphi(l^n)$ ten Potenzen der e von einander verschiedenen Primideale, wo e genau wie oben zu bestimmen ist, indem man m_0 an Stelle von m setzt.[1]

1) Vgl. Hilbert, Bericht, Satz 125.

Als ein weiteres Beispiel sei der Teilungskörper der lemniskatischen Function sn $(u; i)$ angeführt. Der Grundkörper k ist der Gauss'sche; sei $\mathfrak{l}=(1+i)$, und $\mathfrak{m}=(\mu)$ ein ungerades Primideal in k. Der Teilungskörper zum Divisor $\mathfrak{m}$[1] ist dann der Classenkörper $K(\mathfrak{l}^3\mathfrak{m})$ vom Relativgrade $\varphi(\mathfrak{m})=N(\mathfrak{m})-1$. Der Trägheitskörper für $\mathfrak{l}$ ist $K(\mathfrak{m})$ vom Relativgrade $\varphi(\mathfrak{m}):4$. Ist also f der kleinste positive Exponent, für welchen

$$(1+i)^f \equiv i^\alpha \pmod{\mathfrak{m}}$$

ausfällt, wo i^α die Einheiten von k bedeutet, und setzt man

$$\frac{\varphi(\mathfrak{m})}{4}=ef,$$

dann zerfällt $\mathfrak{l}$ in $K(\mathfrak{l}^3\mathfrak{m})$ in ein Product von 4^{ten} Potenzen der e von einander verschiedenen Primideale.[2]

§ 26.

Ein Criterium für den relativ Abel'schen Zahlkörper.

H. Weber[3] hat den Classenkörper durch die folgende Definition eingeführt, welche, offenbar auf der Analogie mit gewissen in der Theorie der complexen Multiplication der elliptischen Functionen vorkommenden Körpern beruhend, von der unsrigen gründlich verschieden ist.

Es sei im Grundkörper k eine Zahlengruppe $\mathfrak{H}$ nach dem Modul $\mathfrak{m}$ vorgelegt, welche eine Idealengruppe vom Index h erzeugen möge; ferner sei $\mathfrak{K}$ ein Oberkörper von k vom Relativgrade n, welcher aber nicht als relativ normal vorausgesetzt wird. Dann heisst $\mathfrak{K}$ nach Weber Classenkörper für die Zahlengruppe $\mathfrak{H}$, wenn die folgenden Bedingungen erfüllt sind:

---

1) Vgl. weiter unten, § 32.

2) Dieses Ergebnis ist durch direkte Rechnung hergeleitet in der Abhandlung: T. Takagi, Über die im Bereiche der rationalen complexen Zahlen Abel'schen Zahlkörper, diese Journal, vol. 19. (1903) Vgl. daselbst S. 25, wo jedoch ein Fehler zu corrigiren ist: es soll statt $(1+i)^f\equiv 1$, die richtige: $(1+i)^f\equiv i^\alpha$ zu setzen.

3) Lehrbuch der Algebra, III. S. 607; Vgl. auch Über Zahlengruppen usw. Math. Ann. Bd. 49, S. 87.

1) *Alle Primideale ersten Grades von* k, *die in* H *enthalten sind, zerfallen in* $\mathfrak{K}$ *in ein Produkt von lauter Primidealen ersten Grades.*

2) *Kein Primideal ersten Grades von* $\mathfrak{K}$ *geht in ein Primideal von* k *auf, welches nicht in* H *enthalten ist.*

In den beiden Forderungen 1) und 2) wird eine endliche Anzahl Ausnahme zugelassen, die dann als Factor in den Modul $\mathfrak{m}$ hingenommen werden, weil von den in den Modul aufgehenden Primidealen von k überhaupt abgesehen werden.

Auf dieser Definition gestützt, beweist Weber[1] die folgenden Tatsachen:

3) Es ist $n \geqq h$.

4) Für ein gegebenes H, kann es nicht mehr als einen Classenkörper $\mathfrak{K}$ geben.

5) $\mathfrak{K}$ ist relativ normal in Bezug auf k.

Ferner spricht er die Vermutung aus:

6) Für jeden Classenkörper $\mathfrak{K}$ ist $n=h$.[2]

Es sei nun K der Classenkörper (in unserem Sinne) für die Classengruppe H. Da die Forderung 2) in unserer Definition des Classenkörpers enthalten ist, und da nach Satz 30 auch 1) erfüllt ist, so ist die Existenzfrage[3] für den Körper $\mathfrak{K}$ nach Satz 23 gelöst, und zwar wie aus 4) folgt, mit der Eindeutigkeit der Lösung. Ferner ist die Vermutung 6) bestätigt, und das Prädicat in 5) zu „*relativ Abelsch*" precisirt. Nachträglich folgt noch aus Satz 30, dass für alle nicht in dem Führer der Classengruppe H aufgehenden Primideale von k ohne Ausnahme die Bedingung 1) erfüllt sind.

In der Weber'schen Definition des Classenkörpers $\mathfrak{K}$ ist die Forderung versteckt, dass $\mathfrak{K}$ relativ normal in Bezug auf k ist, eine Forderung, die von der Classeneinteilung in k unabhängig ist. In der Tat, besagen 1) und 2), dass überhaupt jedes Primideal ersten Grades von k, welches bei der Zerlegung in $\mathfrak{K}$ ein

1) Lehrbuch, III. S. 607-611.

2) In der S. 102 citirten Abhandlung, nimmt Weber diese Beziehung als eine Forderung in der Definition des Classenkörpers auf.

3) Eine Frage, in die Weber nicht eingeht, indem er sich nur mit den von der Theorie der elliptischen Functionen gelieferten actuell vorhandenen Körpern beschäftigt.

Primideal ersten Grades von $\mathfrak{K}$ unter den Factoren aufweist, notwendig in lauter Primideale ersten Grades von $\mathfrak{K}$ zerfallen muss; dies ist aber ein Criterium dafür, dass $\mathfrak{K}$ relativ normal in Bezug auf k ist. Denn aus dieser Voraussetzung folgt

$$\prod^{\mathfrak{P}} \frac{1}{1-N(\mathfrak{P})^{-s}} = \left(\prod^{\mathfrak{p}_0} \frac{1}{1-N(\mathfrak{p}_0)^{-s}} \right)^n,$$

wo das Product links auf alle Primideale ersten Grades von $\mathfrak{K}$, und das Product rechts auf alle Primideale ersten Grades von k, welche in n Primideale ersten Grades von $\mathfrak{K}$ zerfallen, erstreckt wird, und wo N das Zeichen für die in dem bezüglichen Körper genommene absolute Norm ist. Daher ist, wenn

$$P_0(s) = \prod^{\mathfrak{p}_0} \frac{1}{1-N(\mathfrak{p}_0)^{-s}}$$

gesetzt wird,

$$\text{Lim}\ (s-1)^{\frac{1}{n}}\ P_0(s) = a \qquad (1)$$

endlich und von Null verschieden, wenn sich der reelle Veränderliche s abnehmend der Grenze 1 zustrebt.

Ist nun $\mathfrak{K}'$ ein beliebiger mit $\mathfrak{K}$ relativ conjugirter Körper, dann zerfallen alle Primideale $\mathfrak{p}_0$ in lauter Primideale ersten Grades in $\mathfrak{K}'$, welche letztere mit einer endlichen Anzahl Ausnahmen alle Primideale ersten Grades von $\mathfrak{K}'$ erschöpfen. Gleiches gilt daher von dem zusammengesetzten Körper $\mathfrak{K}\mathfrak{K}'$, für welchen also die entsprechende Relation (1) bestehen muss, demzufolge der Relativgrad von $\mathfrak{K}\mathfrak{K}'$ notwendig gleich n ist. Daher fällt $\mathfrak{K}$ mit $\mathfrak{K}'$ zusammen, ist folglich relativ normal in Bezug auf k.

Unter Hervorhebung dieser Forderung kommt die Weber'sche Definition des Körpers $\mathfrak{K}$ auf das folgende hinaus: Ein relativ normaler Körper $\mathfrak{K}/k$ soll in dem zu Beginn des § 4. erläuterten Sinne der Classengruppe H zugeordnet sein (Weber'sche Bedingung 2); in Bezug auf diesen Körper $\mathfrak{K}$ und diese Classengruppe H soll das in Satz 30 ausgesprochene Zerlegungsgesetz gelten (Weber'sche Bedingung 1). Wie oben bemerkt, folgt aus diesen Bedingungen die Uebereinstimmung des Körpers $\mathfrak{K}$ mit unseren Classenkörper

für H. Wir sind aber umgekehrt aus dem Zusammenfallen des Körpergrades und des Gruppenindex als Definition des Classenkörpers ausgegangen und durch eine Reihe von Schlüssen an den Zerlegungssatz gelangt. Für den Existenzbeweis hat dieser Weg als eine grosse Erleichterung erwiesen. Immerhin gibt die Weber'sche Definition ein Criterium für den relativ Abel'schen Körper, welches sich für die Anwendung auf die Theorie der complexen Multiplication besonders eignet. Wir wollen dieses Criterium noch als einen Satz aussprechen.

Satz 32. *Wenn* K *relativ normal in Bezug auf* k *ist, und wenn alle in einer Classengrupe* H *von* k *enthaltenen Primideale ersten Grades, und nur diese, wieder in die Primideale ersten Grades in* K *zerfallen, dann ist* K *relativ Abel'sch in Bezug auf* k, *und der Relativgrad von* K *stimmt mit dem Index der Classengruppe* H *überein.*

Zum Schluss sei noch das folgende bemerkt. Sei immer K/k relativ normal vom Relativgrade n, und die Classen von k nach einem Modul $\mathfrak{m}$ definirt. Der Inbegriff aller Classe von k, die ein Primideal enthält, welches in die Primideale ersten Grades in K zerfällt, bildet eine Classengruppe H. Denn sind c und c′ zwei beliebige dieser Classen, dann enthält die Classe cc′ gewiss ein Ideal $\mathfrak{j}$, welches Relativnorm eines Ideals $\mathfrak{J}$ von K ist. Denkt man sich nun die Classen von K auch nach dem Modul $\mathfrak{m}$ definirt, so enthält die Classe von K, welche eben das Ideal $\mathfrak{J}$ enthält, nach Satz 5, ein Primideal ersten Grades $\mathfrak{P}$, derart, dass $\mathfrak{P}=A\mathfrak{J}$, wo $A\equiv 1, (\mathfrak{m})$. Hieraus folgt: $\mathfrak{j}=\mathfrak{N}(A\mathfrak{P})=a\mathfrak{p}$, wo $a=\mathfrak{N}(A)\equiv 1, (\mathfrak{m})$, $\mathfrak{p}=\mathfrak{N}(\mathfrak{P})$, wenn $\mathfrak{N}$ die Relativnorm in Bezug auf k bedeutet. Daher enthält die Classe cc′ auch ein Primideal ersten Grades von k.

Der Index h dieser Classengruppe H hängt von der Wahl des Moduls $\mathfrak{m}$; nur bleibt stets $h \leqq n$ (Satz 4). Erreicht nun h für einen gewissen Modul $\mathfrak{m}$ die obere Grenze n, dann ist K relativ Abel'sch, er ist der Classenkörper für H. Wird dagegen die obere Grenze n nie erreicht, dann sei H diejenige offenbar eindeutig bestimmte Classengruppe, bei der der Index h den möglichst grossen Wert hat. Dann ist der Classenkörper für H der grösste relativ Abel'sche Körper, welcher in K enthalten ist; K selbst ist

folglich nicht relativ Abel'sch. In diesem Falle müssen also in H unendlichviele Primideale enthalten sein, welche in K nicht in die Primideale ersten Grades zerfallen. Mit andern Worten, *die Primideale von* k, *welche in einem relativ normalen aber nicht relativ Abel'schen Oberkörper in die Primideale des ersten Grades zerfallen, lassen sich nicht durch eine Congruenzbedingung characterisiren, wie sie in unseren bisherigen Betrachtungen zu Grunde gelegt worden ist.*

CAPITEL V.

Anwendung auf die Theorie der complexen Multiplication der elliptischen Functionen.

§. 27.

Absolut Abel'scher Zahlkörper.

Wenn der Grundkörper k der natürliche ist, dann ist der vollständige Classenkörper $K(m)$ derjenige Zahlengruppe $o(m)$ zugeordnet, welche aus den positiven Zahlen a besteht, die der Congruenz

$$a \equiv 1, \ (m)$$

genügen. Er ist also von der Ordnung $\varphi(m)$. Der Führer für den Körper $K(m)$ ist m, ausgenommen der Fall, wo $m=2m'$, und m' ungerade ist, wo $K(m)=K(m')$, und der Führer für denselben gleich m' ist.

Der Körper $K(m)$ ist der Kreisteilungskörper, welcher durch die primitive m^{te} Einheitswurzel erzeugt wird. Denn sei ζ eine solche, und $\mathfrak{P}$ ein Primideal erstens Grades des Kreisteilungskörpers, welches in die rationale Primzahl p aufgehen mag. Dann ist notwendig

$$\zeta^p \equiv \zeta, \ (\mathfrak{P}),$$

also, von einer endlichen Anzahl der in die Zahlen der Form $1-\zeta^a$ aufgehenden $\mathfrak{P}$ abgesehen,

$$p \equiv 1, \ (m).$$

Der Kreisteilungskörper ist daher der durch die Zahlengruppe $o(m)$ definirten Idealengruppe von k zugeordnet. Berücksichtigt man daher nur die Tatsache, dass der Kreisteilungskörper höchstens von der Ordnung $\varphi(m)$ sein kann, so folgt hieraus nach § 26. die Übereinstimmung desselben mit $K(m)$ und somit auch die Irreducibilität der Kreisteilungsgleichung $\varphi(m)^{ten}$ Grades für ζ.[1]

Wenn a, b relativ prime ganze rationale Zahlen sind, dann ist $K(ab)$ aus $K(a)$ und $K(b)$ zusammengesetzt:

$$K(ab)=K(a).K(b), \qquad (1)$$

weil die Gruppe $o(ab)$ die Durchschnitt der Gruppen $o(a)$, $o(b)$ ist. Daher lassen sich alle Abel'sche Körper auf die Körper

$$K(p^n)$$

zurückführen, wenn p natürliche Primzahlen, und n positive ganzzahlige Exponenten bedeutet.

Wenn von den Zahlengruppen $o(m)$ die Vorzeichenbedingung aufgehoben wird, dann erhält man eine Idealengruppe vom Index $\frac{1}{2}\varphi(m)$. Daher ist $K(m)$ imaginär, enthält aber einen reellen Körper vom halben Grade, welcher durch $\cos\frac{2\pi}{m}$ erzeugt wird. Bezeichnen wir denselben mit $K_o(m)$, dann gelten für diesen das Compositionsgesetz (1) nicht mehr. Denn der zusammengesetzte Körper $K_o(a).K_o(b)$ ist der Zahlengruppe zugeordnet, deren Zahlen den Congruenzen genügen:

$$x\equiv 1, \quad (a), \quad \equiv\pm 1, \ (b),$$

oder

$$x\equiv -1, \ (a), \quad \equiv\pm 1, \ (b).$$

Diese Gruppe ist daher als eine Untergruppe vom Index 2 in der Zahlengruppe für $K_o(ab)$ enthalten, welcher folglich relativ quad-

1) Vgl. H. Weber, Lehrbuch, II. (2. Aufl.) S. 723.

ratisch in Bezug auf $K_0(a).K_0(b)$ ist.[1] Sind aber a, b ungerade und relativ prim, dann ist, wie man leicht einsieht,

$$K_0(4ab)=K_0(4a).K_0(4b).$$

Alle reelle Abel'sche Körper lassen sich daher auf die Körper

$$K_0(2^n), \qquad K_0(4p^n)$$

zurückführen. Diese sind cyclisch vom Grade 2^{n-2}, $\varphi(p^n)$, und bez. durch $\sin\frac{2\pi}{2^n}$, und $\sin\frac{2\pi}{p^n}$ erzeugt.

Ich habe diese an sich triviale Tatsache erwähnt, weil sie ein gewisses Analogon in der Theorie der complexen Multiplication der elliptischen Function hat, welches dort eine bedeutende Rolle spielen wird.

§. 28.

Relativ Abel'sche Oberkörper eines imaginären quadratischen Körpers.

Nebst dem Körper der rationalen Zahlen zeichnen sich die imaginären quadratischen dadurch aus, dass sich die relativ Abel'schen Oberkörper derselben auf gewisse von den Primidealpotenzen im Grundkörper abhängende elementare Körper zurückführen lassen.

Es sei k ein imaginärer quadratischer Körper von der Discriminante Δ, $\mathfrak{m}$ ein beliebiges Ideal in k, dann ist der vollständige Classenkörper $K(\mathfrak{m})$ zum Modul $\mathfrak{m}$ vom Relativgrade

$$\frac{\Phi(\mathfrak{m})h}{w},$$

wo h die Classenzahl von k im absoluten Sinne, Φ die Euler'sche Function in k, und w die in § 23 mit $(E:E_0)$ bezeichnete Zahl, hier also die Anzahl der nach $\mathfrak{m}$ incongruenten Einheiten von k bedeutet; es ist demnach,

1) Ausgenommen der Fall, wo a oder $b=2$ ist.

wenn $\Delta < -4$,

$w=2$, im allgemeinen,
$w=1$, wenn $\mathfrak{m}$ in 2 aufgeht;

wenn $\Delta = -4$,

$w=4$, im allgemeinen,
$=2$, wenn $\mathfrak{m}=(2)$,
$=1$, ween $\mathfrak{m}=(1+i)$ oder $\mathfrak{m}=(1)$;

wenn $\Delta = -3$,

$w=6$, im allgemeinen,
$=3$, wenn $\mathfrak{m}=(2)$,
$=2$, wenn $\mathfrak{m}=(\sqrt{-3})$,
$=1$, wenn $\mathfrak{m}=(1)$.

Das Ideal $\mathfrak{m}$ ist nicht notwendigerweise der Führer für die Classengruppe, welche dem Körper $K(\mathfrak{m})$ zugeordnet ist. Ist aber $\mathfrak{f}$ der Führer, so muss, weil $\mathfrak{f}$ Teiler von $\mathfrak{m}$ ist, $K(\mathfrak{f})$ in $K(\mathfrak{m})$ enthalten sein, und da $K(\mathfrak{f})$ der umfassendste Classenkörper für den Modul $\mathfrak{f}$ ist, so ist notwendig $K(\mathfrak{f})=K(\mathfrak{m})$; also

$$\frac{\Phi(\mathfrak{m})}{\Phi(\mathfrak{f})} = \frac{w_{\mathfrak{m}}}{w_{\mathfrak{f}}},$$

wo $w_{\mathfrak{m}}$ die oben angegebene Bedeutung hat. Im folgenden geben wir die Tabelle für sämtliche Fälle, wo $\mathfrak{m}$ nicht mit $\mathfrak{f}$ zusammenfällt. Darin werden mit $\mathfrak{p}, \mathfrak{p}'$ und $\mathfrak{q}, \mathfrak{q}'$ die Primideale ersten Grades von k bezeichnet, welche bez. in 2 und 3 aufgehen, so dass

$$(2)=\mathfrak{p}^2 \text{ oder} = \mathfrak{p}\mathfrak{p}'; \quad (3)=\mathfrak{q}^2 \text{ oder} = \mathfrak{q}\mathfrak{q}'.$$

$\Delta \equiv 0$, (4): $(2)=\mathfrak{p}^2$.

$K(\mathfrak{m})=K(\mathfrak{p}\mathfrak{m})$, wenn $\mathfrak{m}$ ungerade ist.

$k=K(1)=K(\mathfrak{p})=K(\mathfrak{q})=K(\mathfrak{p}\mathfrak{q})$

$K(2)=K(2\mathfrak{p})=K(2\mathfrak{q})$.

$\Delta \equiv 1$, (8): $(2)=\mathfrak{p}\mathfrak{p}'$.

$K(\mathfrak{m})=K(\mathfrak{p}\mathfrak{m}),=K(\mathfrak{p}'\mathfrak{m}),=K(2\mathfrak{m})$,

wo $\mathfrak{m}$ prim bez. zu $\mathfrak{p}$, $\mathfrak{p}'$, 2 ist.

$k=K(1)=K(P)=K(\mathfrak{q})=K(\mathfrak{p}\mathfrak{q})=K(\mathfrak{p}'\mathfrak{q})=K(2\mathfrak{q})$,

wo P die 7 eigentlichen Teiler von 4 bedeutet.

$\Delta \equiv 5, (8)$:

$$\mathfrak{k} = K(1) = K(\mathfrak{q}).$$
$$K(2) = K(2\mathfrak{q}).$$

$\Delta = -4$: $\mathfrak{p} = (1+i)$

$$K(\mathfrak{m}) = K(\mathfrak{p}\mathfrak{m}), \qquad \mathfrak{m}, \text{ ungerade}$$
$$\mathfrak{k} = K(1) = K(\mathfrak{p}^n) = K(1 \pm 2i), \qquad 0 \leqq n \leqq 3.$$

$\Delta = -3$: $\mathfrak{q} = (\sqrt{-3})$

$$\mathfrak{k} = K(1) = K(\mathfrak{q}) = K(\mathfrak{q}^2) = K(2) = K(2\mathfrak{q}) = K(2 \pm \sqrt{-3})$$

Sind nun $\mathfrak{a}, \mathfrak{b}$ relativ prim, dann ist der aus $K(\mathfrak{a})$ und $K(\mathfrak{b})$ zusammengesetzte Körper der Classengruppe in $\mathfrak{k}$ zugeordnet, welche aus den monomischen Idealen (α) besteht, wo für α eine Zahl gesetzt werden kann, die den Bedingungen

$$\left.\begin{matrix} \alpha \equiv \varepsilon_1, (\mathfrak{a}), \\ \equiv \varepsilon_2, (\mathfrak{b}), \end{matrix}\right\} \quad \text{oder} \quad \left\{\begin{matrix} \alpha \equiv 1, (\mathfrak{a}), \\ \equiv \varepsilon, (\mathfrak{b}) \end{matrix}\right.$$

genügen, wenn mit $\varepsilon, \varepsilon_1, \varepsilon_2$ beliebige Einheiten von $\mathfrak{k}$ bezeichnet werden. Für den Körper $K(\mathfrak{a}\mathfrak{b})$ dagegen müssen $\varepsilon_1 \equiv \varepsilon_2$ oder $1 \equiv \varepsilon$ sein. Es gilt demnach

Satz 33. *Wenn* $\mathfrak{a}, \mathfrak{b}$ *relativ prime Ideale in einem imaginären quadratischen Körper sind, dann ist, abgesehen von gewissen trivialen speciellen Fällen, der aus* $K(\mathfrak{a})$ *und* $K(\mathfrak{b})$ *zusammengesetzte Körper als echter Unterkörper in* $K(\mathfrak{a}\mathfrak{b})$ *enthalten. Der Relativgrad von* $K(\mathfrak{a}\mathfrak{b})$ *in Bezug auf* $K(\mathfrak{a})K(\mathfrak{b})$ *ist* $\frac{w_{\mathfrak{a}} w_{\mathfrak{b}}}{w_{\mathfrak{a}\mathfrak{b}}}$, *wo* $w_{\mathfrak{m}}$ *die in S* 109 *erläuterte Bedeutung hat.* (Wenn von den speciellen Fällen: $\Delta = -4$ und $\Delta = -3$ abgesehen wird, ist dieser Relativgrad gleich 2, ausser wenn $\mathfrak{a}$ oder $\mathfrak{b}$ in 2 aufgeht).

Dagegen ist, wenn $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ relativ prim sind und $\mathfrak{a}$ nicht in 2 aufgeht (für $\Delta = -3$, auch noch nicht gleich $(\sqrt{-3})$ ist)

$$K(\mathfrak{a}\mathfrak{b}\mathfrak{c}) = K(\mathfrak{a}\mathfrak{b})\ K(\mathfrak{a}\mathfrak{c}).$$

Denn der zusammengesetzte Körper $K(\mathfrak{a}\mathfrak{b})$. $K(\mathfrak{a}\mathfrak{c})$ ist der Zahlengruppe zugeordnet, welche durch das Congruenzensystem

$$\alpha \equiv 1, (\mathfrak{a}\mathfrak{b}), \qquad \equiv \varepsilon, (\mathfrak{a}\mathfrak{c})$$

definirt wird, wo ε eine Einheit von k bedeutet. Es muss daher

$$1 \equiv \varepsilon, \pmod{\mathfrak{a}},$$

und wegen der dem Ideale $\mathfrak{a}$ auferlegten Beschränkung

$$\varepsilon = 1,$$

folglich

$$a \equiv 1, \pmod{abc}.$$

Um mich bestimmt auszudrücken und in Hinsicht auf die Beziehung auf die Theorie der complexen Multiplication der elliptischen Functionen, setze ich $\mathfrak{a} = \mathfrak{l}$, wo $\mathfrak{l}$ ein *in* 2 *aufgehendes Primideal von* k bedeutet, und

$$e = 3 \quad \text{oder} \quad 2,$$

jenachdem

$$\Delta \equiv 0 \quad \text{oder} \quad 1, \pmod{4},$$

so dass $\mathfrak{l}^e$ nicht in 2 aufgeht. Dann ist, wenn $\mathfrak{l}, \mathfrak{m}, \mathfrak{m}_1, \mathfrak{m}_2, \ldots\ldots$ zu je zweien relativ prim sind

$$K(\mathfrak{m}_1 \mathfrak{m}_2 \cdots) < K(\mathfrak{l}^e \mathfrak{m}_1).\ K(\mathfrak{l}^e \mathfrak{m}_2) \cdots\cdots = K(\mathfrak{l}^e \mathfrak{m}_1 \mathfrak{m}_2 \cdots),$$

$$K(\mathfrak{l}^n \mathfrak{m}) = K(\mathfrak{l}^n)\ K(\mathfrak{l}^e \mathfrak{m}), \qquad (n \geqq e)$$

wo zur Abkürzung mit $K < K'$ das „Enthaltensein von K als echtem Teil in K'" angedeutet wird. Daher folgt

Satz 34. *Jeder relativ Abel'sche Oberkörper von* k *lässt sich zurückführen auf die Classenkörper* $K(\mathfrak{l}^n)$, $K(\mathfrak{l}^e \mathfrak{m})$, *wo* $\mathfrak{m}$ *Potenz eines von* $\mathfrak{l}$ *verschiedenen Primideals bedeutet.*

Bedeutet p eine ungerade rationale Primzahl, dann kann man auch mit den Classenkörpern der folgenden Typen auskommen:

$$K(2^n), \quad K(p^n), \quad K(4p),$$

wie man leicht einsehen wird, wenn man sich erwägt, dass

$$K(4p^n) = K(p^n).K(4p).$$

§. 29.

Der durch den singulären Wert der elliptischen Modulfunction erzeugte Ordnungskörper.

Ist ω eine quadratische Irrationalzahl von k, welche der primitiven quadratischen Gleichung von der Discriminante $D=\Delta m^2$:

$$A\omega^2+B\omega+C=0,$$

$$(D=\Delta m^2=B^2-4AC)$$

genügt, also eine ganze oder gebrochene Zahl des Ringes mit dem Führer m, dann entsteht, wenn dem Grundkörper k ein singulärer Wert der Modulfunction: $J(\omega)$ adjungirt wird, ein relativ Abel'scher Körper in Bezug auf k, welcher nach H. Weber der *Ordnungskörper für den Führer m* genannt wird. Wir wollen ihn mit $M(m)$ bezeichnen. Derselbe ist der Classenkörper für die Idealengruppe, welche durch die Zahlen α erzeugt wird, die nach dem Modul m mit rationalen Zahlen r congruent sind:[1]

$$\alpha\equiv r, \quad (m).$$

Daher ist M(1) der Classenkörper im absoluten Sinne; allgemein ist $M(m)$ der Ringclassenkörper für den Ring mit dem Führer m.

Der Körper $M(m)$ ist vom Relativgrade

$$\frac{\psi(m)}{w_0}h,$$

wo

h die Classenzahl von k im absoluten Sinne,

$\psi(m)=\frac{\Phi(m)}{\varphi(m)}=m\overset{p}{\Pi}\left(1-\frac{\left(\frac{\Delta}{p}\right)}{p}\right)$, wenn mit Φ, φ die Euler'schen Functionen bez. in k und im Körper der rationalen Zahlen bezeichnet werden, und das Product $\overset{p}{\Pi}$ auf alle in m aufgehenden natürlichen Primzahlen erstreckt wird,

1) H. Weber, Lehrbuch, III. §. 122.

$$w_0=1, \text{ im allgemeien,}$$
$$=2, \text{ wenn } \Delta=-4,$$
$$=3, \text{ wenn } \Delta=-3.$$ [1]

Der Führer m des Ringes ist begrifflich verschieden von dem Führer der Classengruppe, welcher der Körper $K(m)$ zugeordnet ist, wie wir ihn in § 2 definirt haben. Diesen letzteren bezeichnen wir mit $\mathfrak{f}$. Es ist wichtig, denselben für $M(m)$ zu bestimmen.

Da $M(m)$ jedenfalls Classenkörper nach dem Modul m ist, so ist $\mathfrak{f}$ ein Teiler von m, und wie aus der Natur der zugehörigen Classengruppe ersichtlich, ein invariantes Ideal von k. Wir setzen

$$m=\mathfrak{f}\mathfrak{a}=f\mathfrak{a}, \tag{1}$$

wo f die kleinste durch $\mathfrak{f}$ teilbare natürliche Zahl bedeutet. Dann muss durch jede Zahl γ von k, die der Congruenz

$$\gamma\equiv 1, \quad (\mathfrak{f}) \tag{2}$$

genügt, auch die andere:

$$\gamma\equiv r\varepsilon, \quad (m) \tag{3}$$

befriedigt werden, wenn r eine rationale Zahl und ε eine Einheit von k ist. Da im allgemeinen $\varepsilon=\pm 1$, so ersetzen wir (3) durch

$$\gamma\equiv r, \quad (m). \tag{4}$$

Vergleicht man die Anzahlen der nach m incongruenten Lösungen von (2) und (4) mit einander, so erhält man

$$N(\mathfrak{a})=a.$$

Da aber nach (1) $\mathfrak{a}$ durch a teilbar ist, so folgt hieraus $\mathfrak{a}=1$, also ist im allgemeinen $\mathfrak{f}=m$.

In dem speciellen Falle: $\Delta=-4$, sind noch in (3) die Werte $\varepsilon=\pm i$ zu berücksichtigen; weil aber nach (2), (3) $1\equiv r\varepsilon$ $(\mathfrak{f})$ so kommen nur die Möglichkeiten: $\mathfrak{f}=(1)$ und $\mathfrak{f}=(1+i)$ in Betracht.

1) H. Weber, Lehrbuch, III. S. 366. Für $m=1$ ist der Relativgrad immer gleich h, also ist $w_0=1$ zu setzen.

Da $K(1+i)=K(1)$, so kann $(1+i)$ überhaupt nicht als ein Führer der Classengruppe auftreten. Daher bleibt nur noch ein Fall: $\mathfrak{f}=(1)$ zu untersuchen übrig. In diesem Falle, muss offenbar $M(m)=K(1)=k$, also

$$\psi(m)=2,$$

woraus als der einzig mögliche Fall, $m=2$ sich ergibt.

In dem zweiten speciellen Falle: $\Delta=-3$, erhält man durch genau dieselbe Überlegung die Bedingung: $\mathfrak{f}=1$, $M(m)=k$. woraus

$$\psi(m)=3,$$

so dass man erhält: $m=2$ oder $m=3$.

Daher haben wir nach § 24

Satz 35. *In die Relativdiscriminante von* $M(m)$ *gehen alle und nur die Primideale von* k *auf, welche in* m *aufgehen; ausgenommen sind nur die drei Fälle, wo* $M(m)$ *mit dem Grundkörper* k *zusammenfällt:*

$$\Delta=-4, \quad m=2;$$

$$\Delta=-3, \quad m=2 \text{ oder } 3.$$

Als ein Beispiel für die am Ende des § 26 gemachten Bemerkung behandeln wir noch kurz eine von H. Weber gelöste Aufgabe:

Alle in $M(f)$ *enthaltenen absolut Abel'schen Körper zu finden.*

Es handelt sich darum, den grössten Abel'schen Körper zu bestimmen, welcher in dem (absolut) normalen Körper $M(f)$ enthalten ist, der daher nach § 26 Classenkörper für die dort mit $\mathfrak{H}$ bezeichnete Gruppe in dem absoluten Rationalitätsbereich ist. Diese Classengruppe $\mathfrak{H}$ ist aber offenbar durch die rationalen Zahlen a definirt, welche Normen der Zahlen α von k sind, die nach f mit rationalen Zahlen r congruent ausfallen: also

$$\begin{cases} a>0, \\ a\equiv r^2, \quad (f) \\ a=\text{Normenrest nach } \Delta. \end{cases}$$ [1]

1) Vgl. § 7.

Ist daher f_0 das kleinste gemeinsame Vielfache von f und Δ, dann soll a zunächst quadratischer Rest nach jeder in f_0 aufgehenden ungeraden Primzahl sein, und ausserdem noch in Bezug auf die in f_0 aufgehende Potenz von 2 die folgenden Bedingungen befriedigen:

1) wenn, $f_0 \equiv 4$, (8), $a \equiv 1$, (4);

2) wenn, $f_0 \equiv 0$, (8), aber $f \not\equiv 0$, (4), folglich $\Delta \equiv 0$, (8),

a = Normenrest nach 8,

$\equiv \pm 1$, (8), wenn $\frac{\Delta}{4} \equiv 2$, (8),

$\equiv 1, 3$, (8), wenn $\frac{\Delta}{4} \equiv -2$, (8);

3) wenn $f_0 \equiv 0$, (8), und f wenigstens durch 4 teilbar,[1]

$a \equiv 1$, (8).

4) wenn f_0 nur durch 2 teilbar ist, so ist a nur der irrelevanten Beschränkung unterworfen, ungerade zu sein.

Der gesuchte Abel'sche Körper ist demnach zusammengesetzt aus den unabhängigen quadratischen Körpern, die durch die folgenden Zahlen erzeugt werden können:[2]

$\sqrt{(-1)^{\frac{p-1}{2}} p}$, wo p die in f_0 aufgehenden ungeraden Primzahlen sind; und

1) $\sqrt{-1}$, wenn $f_0 \equiv 4$, (8);

2) $\sqrt{\pm 2}$, wenn $f \not\equiv 0$, (4) und $\Delta \equiv 0$, (8), jenachdem $\frac{\Delta}{4} \equiv \pm 2$, (8);

3) $\sqrt{-1}$ und $\sqrt{2}$, wenn $f \equiv 0$, (8), oder $f \equiv 4$, (8) und $\Delta \equiv 0$, (8).

---

1) Wenn f nur durch 4 teilbar ist, dann soll $a \equiv 1$ (4), und Normenrest nach 8 sein, sodass $a \equiv 5$ (8) ausgeschlossen ist.

2) Vgl. H. Weber, Lehrbuch, III. S. 619. R. Fueter, Math. Ann. 75. S. 183.

Endlich seien die folgenden den Modul der Jacobi'schen Functionen betreffenden Tatsachen angeführt, weil wir sie später einmal benutzen müssen.

Es sei ω eine quadratische Irrationalzahl des Körpers k, mit der zugehörigen Discriminante D, d.h. ω genüge einer primitiven quadratischen Gleichung mit ganzen rationalen Coefficienten

$$A\omega^2+B\omega+C=0, \tag{5}$$

wo

$$D=B^2-4AC=f^2\Delta,$$

wenn Δ die Discriminante des Körpers k bedeutet. (Demnach ist ω ein Quotient zweier Zahlen des Ringes mit dem Führer f, speciell ist $A\omega$ eine Zahl, die mit 1 eine Basis des Ringes bildet). Wir wollen die Wurzel der Gleichung (5) mit dem positiven imaginären Teil mit

$$\omega=\{A, B, C\}$$

bezeichnen; dann ist

$$\frac{\omega}{2}=\left\{4A,\ 2B,\ C\right\},\ \left\{2A,\ B,\ \frac{C}{2}\right\},\ \text{oder}\ \left\{A,\ \frac{B}{2},\ \frac{C}{4}\right\}$$

also der Discriminante, $4D$, D, oder $\frac{D}{4}$ zugehörig, jenachdem $C\equiv 1$, (2), $C\equiv 2$, (4), oder $D\equiv 0$, $C\equiv 0$, (4).

Ist dann $\varkappa(\omega)$ der Modul der Jacobi'schen Function, und adjungirt man dem Körper k $\varkappa^2(\omega)$ oder $\varkappa(\omega)$, so ist nach Weber[1]

$$\mathrm{k}[\varkappa^2(\omega)]=\mathrm{M}(2f), \tag{6}$$

ferner ist

$$\mathrm{k}[\varkappa(\omega)]=\mathrm{M}(2f)\quad\text{oder}\quad\mathrm{M}(4f) \tag{7}$$

jenachdem C gerade oder ungerade ist.

Wendet man dieses Resultat auf $\varkappa\left(\frac{\omega}{2}\right)$, dann folgt mit Hülfe der Formel (der Gauss'schen Transformation)

$$\varkappa\left(\frac{\omega}{2}\right)=\frac{2\sqrt{\varkappa(\omega)}}{1+\varkappa(\omega)}$$

1) H. Weber, Lehrbuch, III. S. 505-507.

$$k[\sqrt{\varkappa(\omega)}]=M(2f), \quad M(4f), \quad M(8f), \tag{8}$$

jenachdem

$$C\equiv 0, (4), \quad C\equiv 2, (4), \quad C\equiv 1, (2).$$

Nun sind, wenn $D\equiv 5$, (8), A, C notwendig ungerade, in anderen Fällen kann man stets ein ω so bestimmen, das A ungerade und C gerade und zwar $C\equiv 0$, (4) wird, ausgenommen der Fall: $\Delta\equiv 0$, (4) und $f\equiv 1$, (2), wo notwendig $C\equiv 2$, (4) ausfällt. Unter dieser Voraussetzung folgt aus (6), (7), (8):

wenn $f\equiv 1$, (2), $\Delta\equiv 0$, (4),

$$k[\varkappa^2(\omega)]=k[\varkappa(\omega)]=M(2f); \quad k[\sqrt{\varkappa}]=M(4f); \tag{9}$$

wenn $f\equiv 1$, (2), $\Delta\equiv 5$, (8),

$$k[\varkappa^2]=M(2f), \quad k[\varkappa]=M(4f); \quad k[\sqrt{\varkappa}]=M(8f); \tag{10}$$

wenn $f\equiv 0$, (2), $\Delta\equiv 0$, (4) oder $\Delta\equiv 5$, (8),

oder wenn $\Delta\equiv 1$, (8), für beliebiges f,

$$k[\varkappa^2]=k[\varkappa]=k[\sqrt{\varkappa}]=M(2f). \tag{11}$$

§ 30.

Gleichzeitige Adjunction der singulären Moduln und der Einheitswurzeln.

Wenn der Ordnungskörper $M(m)$ durch die Adjunction der primitiven m^{ten} Einheitswurzeln erweitert wird, so entsteht ein relativ Abel'scher Körper über k, den wir mit

$$\mathfrak{M}(m)$$

bezeichnen wollen. Da $M(m')$ in $M(m)$ enthalten ist, wenn m' in m aufgeht, und ähnliches für die Kreisteilungskörper gilt, so ist das Gleichsetzen von dem Führer des Ordnungskörpers und dem Grad der zu adjungirenden Einheitswurzel offenbar keine wesentliche Beschränkung.

Der Körper $\mathfrak{M}(m)$ ist der Classenkörper für die Idealengruppe, welche durch die Zahlen α definirt wird, die der Congruenz

$$\alpha\equiv r_0, \quad (m) \tag{1}$$

genügen, wo r_0 eine rationale Zahl bedeutet, derart, dass

$$r_0^2 \equiv 1, \quad (m). \tag{2}$$

Wenn von den in Satz 35 angegebenen drei trivialen Fällen abgesehen wird, ist m der Führer für den Classenkörper $\mathbf{M}(m)$.[1]

Der Relativgrad von $\mathbf{M}(m)$ ist, in der Bezeichnungsweise des § 29,

$$\frac{\Phi(m).h}{w.2^\rho}, \tag{3}$$

wo 2^ρ die Anzahl der nach m incongruenten Lösungen der Congruenz (2) bedeutet.

Wenn $m=p^n$ eine ungerade Primzahlpotenz ist, dann ist in (1) $r_0 = \pm 1$ zu setzen, so dass

$$\mathbf{M}(p^n)=\mathrm{K}(p^n). \tag{4}$$

Ebenso ist

$$\mathbf{M}(4)=\mathrm{K}(4); \tag{5}$$

dagegen ist, wenn $n \geqq 3$

$$\mathbf{M}(2^n)<\mathrm{K}(2^n)<\mathbf{M}(2^{n+1}), \tag{6}$$

da dann noch die Werte $r_0=\pm 1+2^{n-1}$ auftreten.

Wenn ferner a, b zwei beliebige relativ prime ganze rationale Zahlen sind, abgesehen von den Specialfällen $\Delta=-4$, $\Delta=-3$,

$$\mathbf{M}(ab)=\mathbf{M}(a).\ \mathbf{M}(b),$$

also insbesondere, wenn p eine ungerade Primzahl ist, nach (4) und (5)

$$\mathbf{M}(4p)=\mathbf{M}(4).\mathbf{M}(p)=\mathrm{K}(4)\mathrm{K}(p)<\mathrm{K}(4p),$$

und zwar gelangt man von $\mathbf{M}(4p)$ aus erst durch die Adjunction einer Quadratwurzel an $\mathrm{K}(4p)$, eine Tatsache, welche auch in den Speialfällen: $\Delta=-4$, $\Delta=-3$, ihre Geltung beibehält; in der Tat,

1) In Nichtübereinstimmung mit R. Fueter, vgl. Math. Ann, 75, S. 239. Vgl. auch T. Takenouchi, On the relatively Abelian corpus with respect to the corpus defined by a primitive cube root of unity, diese Journal, vol. 37. Art. 5 (S. 70), 1916.

$\mathbf{M}(4p)$ ist allgemein der Classengruppe zugeordnet, die durch die Zahlen a definirt ist, welche der Congruenz

$$a \equiv 1,\ 1+2p,\quad (4p)$$

genügen.

Da anderseits $\mathbf{M}(m)$ nur dann $4p$ zum Führer hat, wenn $m=4p$, so ist $\mathrm{K}(4p)$ niemals in einem Körper $\mathbf{M}(m)$ enthalten.

Man sieht hieraus, dass, von den in Satz 34 angegebenen elementaren Körpern, die beiden ersten Typen $\mathrm{K}(2^n)$ und $\mathrm{K}(p^n)$, nicht aber der letzte $\mathrm{K}(4p)$ durch die singulären Moduln und die Einheitswurzeln zu erzeugen sind, dass um $\mathrm{K}(4p)$ zu erhalten, weitere Ausziehung einer Quadratwurzel unumwendbar notwendig ist.[1]

Allgemeiner ist, wenn m (>2) eine ganze rationale Zahl ist, $\mathrm{K}(m)$ Oberkörper von $\mathbf{M}(m)$ vom Relativgrade $2^{\rho-1}$, welche aus $\rho-1$ unabhängigen relativ quadratischen Körpern über $\mathbf{M}(m)$ zusammengesetzt werden kann; hierbei hat die Zahl ρ dieselbe Bedeutung wie oben in (3).

Das Ergebnis dieser Betrachtungen formuliren wir als

Satz 36. *Jeder in Bezug auf einen imaginären quadratischen relativ Abel'sche Zahlkörper vom ungeraden Relativgrade lässt sich durch Einheitswurzeln und singuläre Werte der Modulfunction $J(\tau)$ erzeugen. Gleiches gilt auch im Falle eines geraden Relativgrades, wenn die Relativdiscriminante keine anderen Primfactoren enthält, als solche, die in eine und dieselbe natürliche Primzahl aufgehen; im gegenteiligen Falle aber kann noch die Adjunction gewisser Quadratwurzeln notwendig werden, deren Anzahl im äussersten Falle bis zu der Anzahl der von einander verschiedenen, durch die Primfactoren der Relativdiscriminante teilbaren, rationalen Primzahlen ansteigt.*

Wie in den folgenden Paragraphen nachgewiesen werden soll, können alle relativ Abel'sche Oberkörper erzeugt werden, wenn man noch die Teilwerte der Perioden der Jacobi'schen Function $\mathrm{sn}(u)$ zu Hülfe nimmt.

---

1) Eine zuerst von R. Fueter entdeckte Tatsache; vgl. Math. Ann. 75.

§ 31.

Ueber die complexe Multiplication der Jacobi'schen Function.

Um die zuletzt erwähnte Frage zu erledigen, betrachten wir die Teilungsgleichung der Jacobi'schen Function $\mathrm{sn}(u)$ mit einem singulären Modul $\varkappa(\omega)$ durch ein ungerades Ideal. Da es aber nicht in unserer Absicht liegt, die Theorie des Teilungskörpers für sich ausführlich zu entwickeln, so begnügen wir uns damit, nachzuweisen, dass der Elementarkörper $K(4p)$ oder $K(\mathfrak{f}_\mathfrak{m})$ (vgl. §28) durch die Teilwerte von $\mathrm{sn}(u)$ erzeugt wird, indem wir das hierzu nötige Material aus dem Weber'schen Buche[1] entnehmen.

Sei

$$\omega=\{A,\ B,\ C\} \tag{1}$$

eine zur Stammdiscriminante Δ gehörige Irrationalzahl von k, so dass

$$\Delta=B^2-4AC,$$

und $[1, A\omega]$ eine Basis des Körpers k bildet.

Für die Function

$$S(v)=\sqrt{\varkappa}\,\mathrm{sn}(2Kv,\ \varkappa)=\frac{\vartheta_1(v\,|\,\omega)}{\vartheta_0(v\,|\,\omega)}$$

und einen ungeraden complexen Multiplicator μ, welcher dem Ringe mit dem Führer 2 angehört, also

$$\mu=a+b\omega, \tag{2}$$

wo a eine ungerade und b eine durch $2A$ teilbare ganze rationale Zahl bedeutet, besteht die folgende Multiplicationsformel:

$$\varepsilon S(\mu v)=\frac{\mathrm{A}(S)}{\mathrm{D}(S)}, \tag{3}$$

wo

$$S=S(v),$$

1) H. Weber, III, 23. Abschnitt, vgl. insbesondere S. 576-596.

und

$$\left.\begin{aligned} A(S)&=A_1S+A_3S^3+\cdots\cdots+A_{m-2}+S^{m-2}+S^m,\\ D(S)&=A_1S^{m-1}+A_3S^{m-3}+\cdots\cdots+A_{m-2}S+1 \end{aligned}\right\} \quad (4)$$

ganze ganzzahlige Functionen im Körper $k'=k(\varkappa)$ sind, und

$$m=N(\mu)=\mu\overline{\mu},$$

ferner

$$\varepsilon=\pm 1 \text{ oder } \pm i,$$

je nach der Beschaffenheit von μ nach dem Modul 4.

Es ist

$$A(x)=\prod_{\rho}\left\{x-S\left(\frac{2\rho}{\mu}\right)\right\}=0$$

die *Teilungsgleichung zum Divisor* μ, deren Wurzeln die m Teilwerte

$$S\left(\frac{2\rho}{\mu}\right) \quad (5)$$

sind, wo ρ ein vollständiges Restsystem nach μ durchläuft, allerdings unter der Voraussetzung, dass der Coefficient A in (1) ungerade und prim zu μ ist.[1]

Es ist nun für unseren Zweck unerlässlich, den Coefficienten ε in der Weber'schen Formel (3) genau zu bestimmen, was wir dadurch erreichen, dass die Function $A(S)$ durch die Thetafunction dargestellt wird.

Ist μ eine beliebige ganze Zahl von k, dann kann man setzen

$$\left.\begin{aligned} \mu&=a+b\omega,\\ \mu\omega&=c+d\omega, \end{aligned}\right\} \quad (6)$$

wo a, b, c, d ganze rationale Zahlen sind, so dass

1) Für unseren Zweck genügt es schon, wenn wir ein für allemal annehmen: $A=1$.

$$\begin{vmatrix} a-\mu & b \\ c & d-\mu \end{vmatrix} = \mu^2-(a+d)\mu+ad-bc=0,$$

$$m=\mathrm{N}(\mu)=\mu\bar{\mu}=ad-bc. \tag{7}$$

Für die conjugirte Zahl $\bar{\mu}$ ergibt dann

$$\left.\begin{aligned} \bar{\mu}&=d-b\omega, \\ \bar{\mu}\omega&=-c+a\omega. \end{aligned}\right\} \tag{8}$$

Ich setze nun

$$\Phi(v)=ae^{\pi i l\mu v^2}\frac{\vartheta_1(\mu v)}{\vartheta_0(v)^m} \tag{9}$$

wo für den constanten Coefficienten a noch zu verfügen ist. Für diese Function ergibt sich

$$\frac{\Phi(v+1)}{\Phi(v)}=(-1)^{a+b}e^{\pi i b(\mu-b\omega)}=(-1)^{a+b+ab},$$

$$\frac{\Phi(v+\omega)}{\Phi(v)}=e^{2\pi i v(l\mu\omega-d\mu+m)}\times(-1)^{c+d+m}e^{\pi i\omega(b\mu\omega-d^2+m)}$$

Nun ist nach (6), (7), (8)

$$b\mu\omega-d\mu+m=\mu(b\omega-d+\bar{\mu})=0,$$

$$\omega(b\mu\omega-d^2+m)=\omega(d\mu-d^2)=d(\mu\omega-d\omega)=cd,$$

so dass

$$\frac{\Phi(v+\omega)}{\Phi(v)}=(-1)^{c+d+cl+m}$$

So weit gilt unsere Formel für jede ganze Zahl μ von k. Ist nun μ wie in (2) eine ungerade Zahl aus dem Ringe mit dem Führer 2, dann ist

$$\left.\begin{aligned} a\equiv d\equiv 1,\quad b\equiv c\equiv 0,\quad (2), \\ m\equiv ad\quad (4), \end{aligned}\right\} \tag{10}$$

und

$$\Phi(v+1)=-\Phi(v), \quad \Phi(v+\omega)=\Phi(v).$$

Demnach ist $\Phi(v)$ eine ganze Function von $S(v)$, und da sie dieselben Nullstellen (5) hat wie $S(\mu v)$, so kann man den constanten Factor a in (9) so bestimmen, dass

$$A(S)=\Phi(v)$$

wird: Setzen wir $v=0$ und $v=\frac{\omega}{2}$, so erhalten wir nacheinander

$$A_1=\frac{a\mu}{\vartheta_0^{m-1}},$$

$$1=ae^{\frac{\pi i b\mu\omega^2}{4}}\left(\frac{\vartheta_1(\mu v)}{\vartheta_1'(v)^m}\right)_{v=\frac{\omega}{2}}=\frac{a}{\vartheta_0^{m-1}}\times i^{c+d-m}\,e^{\frac{\pi i\omega}{4}(b\mu\omega-d^2+m)}$$

$$=\frac{a}{\vartheta_0^{m-1}}i^{c+d-m+\frac{cd}{2}}$$

Daher ist

$$A_1=\mu i^{m-c-d-\frac{cd}{2}}$$

und für ε in (3) erhalten wir, indem wir $v=0$ setzen,

$$\varepsilon=i^{m-c-d-\frac{cd}{2}},$$

oder nach (10)

$$\varepsilon=(-1)^{\frac{a-1}{2}}i^{-\frac{c}{2}(d+2)}, \qquad (11)$$

und speciell,

$$\text{wenn} \quad c\equiv 0, \ (4), \qquad \varepsilon=(-1)^{\frac{a-1}{2}+\frac{c}{4}}. \qquad (12)$$

Da nach (6)

$$b\omega^2+(a-d)\omega-c=0,$$

so folgt aus (1)

$$\frac{b}{A}=\frac{a-d}{B}=\frac{-c}{C}=2b',$$

wo b' eine ganze Zahl ist, weil nach (2) b durch $2A$ teilbar ist.

Der in (12) angegebene Fall tritt daher ein, wenn für $\Delta\equiv 0, (4)$ und $\Delta\equiv 1, (8)$, ω so angenommen wird, dass C gerade ausfällt, was stets angeht, oder wenn für $\Delta\equiv 5, (8)$ die Zahl μ dem Ringe mit dem Führer 4 angehört, so dass b' gerade wird; in beiden Fällen ist

$$\varepsilon=(-1)^{\frac{a-1}{2}+\frac{b'c}{2}} \tag{13}$$

§ 32.

Ueber die arithmetische Natur des Teilungskörpers.

Es sei

$$\omega=\{A,\ B,\ C\} \tag{1}$$

eine zur Stammdiscriminante Δ gehörige Irrationalzahl von k, von der wir annehmen, dass A ungerade ist und C gerade, wenn $\Delta\equiv 0, (4)$ oder $\Delta\equiv 1, (8)$, so dass, wenn $\varkappa=\varkappa(\omega)$, $\mathrm{k}'=\mathrm{k}[\varkappa]$ gesetzt wird, nach § 29

$$\left.\begin{array}{lll} \text{(I)} & \mathrm{k}'=\mathrm{M}(2)=\mathrm{K}(2), & \text{wenn } \Delta\equiv 0, (4), \\ \text{(II)} & \mathrm{k}'=\mathrm{M}(2)=\mathrm{K}(1), & \text{,, } \Delta\equiv 1, (8), \\ \text{(III)} & \mathrm{k}'=\mathrm{M}(4)=\mathrm{K}(4), & \text{,, } \Delta\equiv 5, (8) \end{array}\right\} \tag{2}$$

und folglich k' der Ringclassenkörper für den Ring

$$\mathfrak{R} \text{ mit dem Führer 2, 1, 4 im Falle (I), (II), (III)} \tag{3}$$

ist.

Ferner sei $\mathfrak{m}$ ein beliebiges ungerades Ideal von k, $\mathrm{T}'(\mathfrak{m})$ der Teilungskörper, welcher entsteht, wenn dem Ordnungskörper k' ein eigentlicher $\mathfrak{m}^{\text{ter}}$ Teilwert von $S(v)=\sqrt{\varkappa}\,\mathrm{sn}(u,\varkappa)$ adjungirt wird, und welcher relativ Abel'sch in Bezug auf k' ist, von einem

Relativgrade, welcher höchstens gleich $\Phi(\mathfrak{m})$ ist. Es handelt sich darum, nachzuweisen, dass $T'(\mathfrak{m})$ auch relativ Abel'sch in Bezug auf k selbst ist, und vor allem die Classengruppe in k zu bestimmen, welcher $T'(\mathfrak{m})$ zugeordnet ist.

Wir bezeichnen durchweg mit ϖ eine ungerade Zahl vom Ringe $\mathfrak{r}$ in (3), welche ein Primideal ersten Grades von k erzeugt, mit Ausschluss einer endlichen Anzahl, die in $\mathfrak{m}$ oder in die Discriminante der $\mathfrak{m}$-teilungsgleichung von $S(v)$ in k' aufgehen, und wir setzen

$$p=\mathrm{N}(\varpi).$$

Dann ist nach (3), (4), § 31

$$\varepsilon S(\varpi v)=\frac{A_1S+A_3S^3+\cdots\cdots+A_{p-2}S^{p-2}+S^p}{A_1S^{p-1}+A_3S^{p-3}+\cdots\cdots+A_{p-2}S^2+1}, \qquad (4)$$

wo ε die in (13), § 31 angegebene Bedeutung für $\mu=\varpi$ hat, und die Coefficienten $A_1, A_3, \ldots\ldots A_{p-2}$ durch ϖ teilbar sind.[1] Versteht man daher unter v in (4) einen eigentlichen $\mathfrak{m}^{\text{ten}}$ Teil der Periode von $S(v)$, so sind $S(v)$ und $S(\varpi v)$ Wurzel der $\mathfrak{m}$-teilungsgleichung, wenn, wie vorausgesetzt, ϖ nicht in $\mathfrak{m}$ aufgeht, und es folgt

$$\varepsilon S(\varpi v)\equiv S(v)^p, \quad (\varpi). \qquad (5)$$

Wenn nun $\mathfrak{P}$ ein Primideal ersten Grades in $T'(\mathfrak{m})$ ist, welches mit einer endlichen Anzahl Ausnahme in ein ϖ aufgeht, so muss

$$S(v)^p\equiv S(v), \quad (\mathfrak{P}), \qquad (6)$$

so dass nach (5)

$$\varepsilon S(\varpi v)\equiv S(v), \quad (\mathfrak{P}). \qquad (7)$$

Da nach Voraussetzung $\mathfrak{P}$ nicht in die Discriminante der Teilungsgleichung aufgeht, so ist dies nur dann möglich, wenn

---

1) H. Weber, l. c. S. 594; vgl. auch T. Takagi, On a fundamental property of the equation of division etc. Proceedings of the Tōkyō Math. Physical Soc., Ser. 2, vol. 7. S. 414.

$$\varepsilon S(\varpi v)=S(v) \tag{8}$$

d.h., wenn

$$\left.\begin{array}{ll} \varpi\equiv 1, & (\mathfrak{m}),\quad \varepsilon=1, \\ \text{oder} \quad \varpi\equiv -1, & (\mathfrak{m}),\quad \varepsilon=-1. \end{array}\right\} \tag{9}$$

Umgekehrt, wenn eine Zahl ϖ die Bedingung (9) erfüllt, und ist $\mathfrak{P}$ ein Primideal von $\mathrm{T}'(\mathfrak{m})$, welches in ϖ aufgeht, dann folgt nach (5), da (8) und somit (7) besteht, die Relation (6). Weil aber $S(v)$ den Relativkörper $\mathrm{T}'(\mathfrak{m})/\mathrm{k}'$ erzeugt, und für jede Zahl α in k'

$$\alpha^p\equiv\alpha, \quad (\varpi),$$

so ist für jede Zahl A von $\mathrm{T}'(\mathfrak{m})$

$$A^p\equiv A, \quad (\mathfrak{P}),$$

demnach ist $\mathfrak{P}$ ein Primideal ersten Grades in $\mathrm{T}'(\mathfrak{m})$.

Da $\varepsilon=\pm 1$ eine Congruenzbedingung für die Zahl ϖ nach einer Potenz von 2 als Modul bedeutet, so ist hiermit nach § 26 dargetan, dass der Körper $\mathrm{T}'(\mathfrak{m})$ relativ Abel'sch in Bezug auf k, und zwar derjenige Idealengruppe zugeordnet ist, welche durch die Zahlen α des Ringes $\mathfrak{k}$ erzeugt wird, die der Congruenzbedingung (9) genügen:

$$\left.\begin{array}{ll} \alpha\equiv\pm 1, & (\mathfrak{m}) \\ \varepsilon=\pm 1, & \end{array}\right\} \tag{10}$$

Es ist nunmehr unser Ziel, diese Idealengruppe näher zu untersuchen; wie es sich herausstellen wird, ist der Index derselben gleich $\Phi(\mathfrak{m})h'$, wenn h' der Relativgrad von k'/k bedeutet, so dass sich nebenbei ergibt, dass die $\mathfrak{m}$-teilungsgleichung in k' irreducibel ist. Wir müssen aber fernerhin die zu Beginn des Artikels unterschiedenen drei Fälle einzeln in Betracht ziehen.

(I) $\Delta\equiv 0, (4)$.

In diesem Falle, ist in (1) A ungerade, C gerade, folglich

$$C\equiv 2,\ (4).$$

Setzt man

$$\theta=A\omega,$$

so ist in k

$$(2)=\mathfrak{l}^2,\ \text{wo}\ \mathfrak{l}=[2,\ \theta].$$

Für eine ungerade Zahl a im Ringe $\mathfrak{r}$ mit dem Führer 2:

$$a=a+b\omega=a+2b'\theta$$

wird nach (13), § 31, da $\frac{C}{2}$ ungerade ist

$$\varepsilon=(-1)^{\frac{a-1}{2}+b'}, \tag{11}$$

also $\varepsilon=1$, dann und nur dann, wenn

$$a\equiv 1,\ (4),\quad b'\equiv 0,\ (2),$$

oder

$$a\equiv -1,\ (4),\quad b'\equiv 1,\ (2),$$

Nach (10) kommt daher die Zahlengruppe

$$\left.\begin{array}{l} a\equiv 1,\ (\mathfrak{m}),\\ a\equiv 1 \text{ oder } -1+2\theta,\ (\mathfrak{l}^4)\end{array}\right\} \tag{12}$$

in Betracht. Man sieht daher ein, dass

$$K(\mathfrak{l}^2\mathfrak{m})<T'(\mathfrak{m})<K(\mathfrak{l}^4\mathfrak{m}), \tag{13}$$

ohne dass $T'(\mathfrak{m})$ mit $K(\mathfrak{l}^3\mathfrak{m})$ zusammenfällt, welcher letztere der Zahlengruppe

$$a\equiv 1,\ (\mathfrak{m}),\quad a\equiv 1,\ 1+2\theta,\ (\mathfrak{l}^4)$$

zugeordnet ist.

Bezeichnet man nun mit $T_0(\mathfrak{m})$ denjenigen Körper, welcher aus k' entsteht durch Adjunction der Quadrat $S(v)^2$ des $\mathfrak{m}$ten Teilwertes von $S(v)$, oder, was auf dasselbe hinauskommt, von der Quadrat $\mathrm{sn}^2(u)$ des $\mathfrak{m}^{\text{ten}}$ Teilwertes von der Function $\mathrm{sn}(u)$ selbst, dann ist

$$T_0(\mathfrak{m})=K(\mathfrak{f}^2\mathfrak{m}), \tag{14}$$

weil für diesen die Bedingung $\varepsilon=1$ wegfällt.[1]

Um aber den Körper $K(4\mathfrak{m})=K(\mathfrak{f}^4\mathfrak{m})$ zu erhalten, hat man dem Körper $T'(\mathfrak{m})$ noch $\sqrt{\varkappa}$ zu adjungiren, weil nach § 29, $k[\sqrt{\varkappa}]=M(4)$ der Zahlengruppe: $\alpha\equiv\pm1$, (4) zugeordnet ist.

Der Körper $K(4\mathfrak{m})$ ist relativ biquadratisch in Bezug auf $K(2\mathfrak{m})$; er lässt sich zusammensetzen aus zwei relativ quadratischen Körpern über $K(2\mathfrak{m})$, enthält folglich drei von einander verschiedenen relativ quadratischen Körper über $K(2\mathfrak{m})$, welche bez. den Zahlengruppen

$$\begin{aligned}
&\alpha\equiv1,\ (\mathfrak{m}),\quad \alpha\equiv1,\quad -1+2\theta,\quad (\mathfrak{f}^4),\\
&\alpha\equiv1,\ (\mathfrak{m}),\quad \alpha\equiv1,\quad -1,\qquad (\mathfrak{f}^4),\\
&\alpha\equiv1,\ (\mathfrak{m}),\quad \alpha\equiv1,\quad 1+2\theta,\quad (\mathfrak{f}^4)
\end{aligned}$$

zugeordnet sind. Der erste ist $T'(\mathfrak{m})$, der zweite entsteht aus $T_0(\mathfrak{m})$ durch Adjunction von $\sqrt{\varkappa}$; der dritte, welcher $K(\mathfrak{f}^2\mathfrak{m})$ ist, muss daher notwendig derjenige Körper $T(\mathfrak{m})$ sein, welcher durch die Adjunction von dem *Teilwerte von* sn (u) *selbst*, (d.h $S(v)/\sqrt{\varkappa}$) entsteht:

$$T(\mathfrak{m})=K(\mathfrak{f}^2\mathfrak{m}). \tag{15}$$

Dieses merwürdige Ergebnis wollen wir noch auf einem directeren Weg herleiten. Da nach § 29

$$k[\sqrt{\varkappa}]=M(4),$$

so zerfällt ein Primideal (ϖ) von k, wo

$$\varpi=a+2b'\theta,$$

dann und nur dann in die Primideale ersten Grades in $k(\sqrt{\varkappa})$, wenn

$$b'\equiv0,\ (2).$$

Hieraus ist aber zu schliessen, dass[2]

1) Vgl. Weber, l. c. S. 596.

2) Da sowohl $4\varkappa$ als auch $\frac{4}{\varkappa}$ ganze Zahlen sind, so enthält $\varkappa$ im Zähler und Nenner keinen ungeraden Idealfactor, vgl. Weber, l. c. S. 581.

$$\varkappa^{\frac{p-1}{2}} \equiv (-1)^{\nu}, \quad (\varpi).$$

Daher folgt aus (5) und (11)

$$(-1)^{\frac{a-1}{2}} \operatorname{sn}(\varpi u) \equiv \operatorname{sn}(u)^{p}, \quad (\mathfrak{P}),$$

sodass nun für ϖ die Bedingung erhalten wird:

$$\left.\begin{array}{ll} \varpi = a + 2b'\theta \equiv 1 & (\mathfrak{m}) \\ a \equiv 1 & (4) \end{array}\right\}.$$

Da b' beliebig ist, so wird für die zugeordnete Zahlengruppe

$$\left.\begin{array}{l} a \equiv 1, \quad (\mathfrak{m}), \\ a \equiv 1, \quad (\mathfrak{l}^{\mathfrak{d}}), \end{array}\right\}$$

wie zu beweisen war.

(II) $A \equiv 1, \quad (8).$

Es empfiehlt sich in diesem Falle A ungerade und

$$C \equiv 0, \quad (4)$$

anzunehmen, was erreicht wird, wenn man nötigenfalls ω durch $\omega + 2$ ersetzt. Dann ist in k

$$(2) = \mathfrak{l}\mathfrak{l}', \text{ wo } \mathfrak{l} = [2, \theta], \quad \mathfrak{l}^2 = [4, \theta], \quad \mathfrak{l}' = [2, 1+\theta].$$

Es ist hier $k' = K(1)$, aber wenn verlangt wird, dass a ungerade, also prim zu $\mathfrak{l}$ und $\mathfrak{l}'$ sein soll, so ist

$$a = a + b\omega = a + 2b'\theta,$$

demnach kommt nach (13) § 31, da $C \equiv 0$, (4),

$$\varepsilon = (-1)^{\frac{a-1}{2}}.$$

Daher ist $\varepsilon = 1$, dann und nur dann, wenn $a \equiv 1$, (4), d. h. aber, wenn

$$a \equiv 1 \quad (\mathfrak{l}^2 \mathfrak{l}').$$

Man erhält somit

$$T'(\mathfrak{m}) = K(\mathfrak{l}^2 \mathfrak{l}' \mathfrak{m}) = K(\mathfrak{l}^2 \mathfrak{m}),^{(1)}$$

(1) Vgl. § 28.

und weil nach § 29 $k[\sqrt{\varkappa}]=k[\chi]$, so ist hier

$$T(\mathfrak{m})=T'(\mathfrak{m})=K(\mathfrak{l}^2\mathfrak{m}). \tag{16}$$

Für $T_0(\mathfrak{m})$ fällt die Bedingung: $\varepsilon=1$ weg, sodass $T_0(\mathfrak{m})$ gleich $K(2\mathfrak{m})$, folglich[1]

$$T_0(\mathfrak{m})=K(\mathfrak{m}). \tag{17}$$

(III) $\Delta\equiv 5$, (8).

In diesem Falle sind die Coefficienten A, B, C ungerade, und 2 bleibt prim in k. Für die Zahl α im Ringe $\mathfrak{r}$ mit dem Führer 4

$$\alpha=a+b\omega=a+4b'\theta$$

erhält man nach (13) § 31, da C ungerade ist,

$$\varepsilon=(-1)^{\frac{a-1}{2}+b'}, \tag{18}$$

also $\varepsilon=1$, dann und nur dann, wenn

$$a\equiv 1 \quad (4), \quad b'\equiv 0 \ (2),$$

oder

$$a\equiv -1 \ (4), \quad b'\equiv 1 \ (2).$$

Die Zahlengruppe wird folglich durch die folgenden Congruenzen definirt:

$$\left.\begin{aligned} &a\equiv 1, \ (\mathfrak{m}),\\ &a\equiv 1, \ 5, \ -1+4\theta, \ -5+4\theta, \ (8), \end{aligned}\right\}$$

woraus einzusehen ist, dass $T'(\mathfrak{m})$ in $K(8\mathfrak{m})$ enthalten ist, ohne aber mit $K(4\mathfrak{m})$ zusammenzufallen.

Nun ist im gegenwärtigen Falle $k[\sqrt{\varkappa}]=M(8)$, sodass

$$\sqrt{\varkappa}^{p-1}=\varkappa^{\frac{p-1}{2}}\equiv 1, \quad (\varpi),$$

dann und nur dann, wenn $\varpi=\chi+4b'\theta$, und $b'\equiv 0$ (2); also

$$\varkappa^{\frac{p-1}{2}}\equiv(-1)^{b'} \quad (\varpi).$$

(1) Vgl. § 28.

Nach (5) und (18) erhält man daher

$$(-1)^{\frac{a-1}{2}}\,\mathrm{sn}\,(\varpi u)\equiv \mathrm{sn}\,(u)^{p}, \quad (\mathfrak{P}),$$

sodass für den Teilungskörper der Function sn, die Zahlengruppe:

$$\left.\begin{aligned} a&\equiv 1, \quad (\mathfrak{m}),\\ a&\equiv 1, \quad (4)\end{aligned}\right\}$$

auftritt, d.h. es ist

$$\mathrm{T}(\mathfrak{m})=\mathrm{K}(4\mathfrak{m}). \qquad (19)$$

Für den Körper $\mathrm{T}_0(\mathfrak{m})$ erhält man, da die Bedingung $\varepsilon=1$ wegfällt, die Zahlengruppe:

$$\left.\begin{aligned} a&\equiv 1, \quad (\mathfrak{m}),\\ a&\equiv \pm 1, \quad (4).\end{aligned}\right\}$$

Abgesehen von dem Falle $\Delta=-3$, kann man daher setzen

$$\mathrm{T}_0(\mathfrak{m})=\mathrm{K}(4)\mathrm{K}(\mathfrak{m}). \qquad (20)$$

In allen Fällen hat sich somit ergeben, dass bei der geeigneten Wahl von ω im imaginären quadratischen Körper k, der Teilungskörper $\mathrm{T}(\mathfrak{m})$. der Jacobi'schen Function $\mathrm{sn}(u, \omega)$ für einen ungeraden Divisor $\mathfrak{m}$ mit dem Elementarkörper $\mathrm{K}(\mathfrak{f}\mathfrak{m})$ des § 28 übereinstimmt. Mit Rücksicht auf Satz 36 erhalten wir daher in

Bestätigung der Kronecker'schen Vermutung

Satz 37. *Alle relativ Abel'sche Oberkörper eines imaginären quadratischen Körper werden durch die Einheitswurzeln, die singulären Moduln und die Teilwerte der Jacobi'schen Function erzeugt.*

Abgeschlossen im Februar, 1920.

Inhaltsverzeichnis.

CAPITEL I.

Der allgemeine Classenkörper.

CAPITEL II.

Die Geschlechter im relativ cyclischen Körper vom Primzahlgrade.

CAPITEL III.

Existenzbeweis für den allgemeinen Classenkörper.

CAPITEL IV.

Weitere allgemeine Sätze.

CAPITEL V.

Anwendung auf die Theorie der complexen Multiplication der elliptischen Functionen.

Published July 31st, 1920.

Berichtigung

zu meiner Arbeit: Ueber eine Theorie des relativ Abel'schen Zahlkörpers,

dieses Journal, Vol. XLI, Art. 9.

S. 16, Z. 7 v. u. lies ξ_1^e statt ξ.

S. 33, Z. 4 v. o. „ $\mathfrak{Q}^{\nu+1}$ „ $\mathfrak{l}^{\nu+1}$.

S. 34, Z. 11 v. o. „ $\mathfrak{Q}^{\nu+1}$ „ $\mathfrak{l}^{\nu+1}$.

S. 45, Z. 15 v. o. „ l^{ν_0} „ ν_0.

S. 47, Z. 5 v. u. (auf der rechten Seite der Gleichung)
lies 2 statt l.

S. 74, Z. 6 v. o. „ r_ν „ t_ν.

S. 100, Z. 8 v. o. „ $\mathfrak{m}_0$ „ m_0.

S. 114, Satz 35, den aufgezählten Ausnahmefällen hinzuzufügen:

$$\Delta \equiv 1 \pmod 8, \quad m = 2m', \quad m' \text{ ungerade};$$

in diesem Falle ist der Führer m', die Relativdiscriminante somit prim zu 2.

S. 118, Z. 3 v. o. lies *vier* statt *drei*, entsprechened der Berichtigung zu S. 114, Satz 35. Die Fussnote bezieht sich auf den von Herrn Fueter a. a. O. übersehenen Fall:

$$\Delta = -3, \quad m = 2.$$

T. TAKAGI.