JOURNAL OF THE COLLEGE OF SCIENCE, IMPERIAL UNIVERSITY,
TOKYO, JAPAN.
VOL. XIX., ARTICLE 5.

Ueber die im Bereiche der rationalen complexen Zahlen Abel'schen Zahlkörper.

Von

T. Takagi,

a. o. Professor der Mathematik an der Universität zu Tōkyō.

Kronecker hat zuerst den Satz ausgesprochen, dass alle im natürlichen Rationalitätsbereich Abel'schen Zahlkörper durch die Kreiskörper, d.h., die aus den Kreisteilungsgleichungen entspringenden Zahlkörper erschöpft sind. Der erste vollständige Beweis dieses schönen Satzes rührt von H. Weber[1] her, welchem sich in neuester Zeit ein einfacherer und direkterer Beweis von Hilbert[2] zugesellte. Es war auch Kronecker, der der Vermutung Ausdruck gab, dass alle in Bezug auf einem imaginären quadratischen Zahlkörper relativ-Abel'schen Zahlkörper durch diejenigen Körper erschöpft seien, welche aus den Transformationsgleichungen der elliptischen Functionen mit singulären Moduln entstehen. So wahrscheinlich auch diese Vermutung durch die Untersuchungen von H. Weber, Hilbert, u. A. geworden ist, harrt die Frage doch noch der entscheidenden Erledigung. Indessen es gibt specielle Fälle dieser grossen Aufgabe, wo man von vorn herein eines glücklichen Abschlusses sicher sein

1) H. Weber, Acta Mathematica, Bd. 8; Lehrbuch der Algebra, Bd. II.

2) Hilbert, Göttinger Nachrichten, 1896; Jahresbericht der Deutschen Mathematiker-Vereinigung IV.

kann, nämlich die, wo die zu Grunde gelegten quadratischen Körper einclassig sind, also z. B. durch die dritten und die vierten imaginären Einheitswurzeln erzeugt werden; sie bilden in der Tat die unmittelbare Verallgemeinerung des Satzes über die Kreiskörper. Der zuletzt genannte specielle Fall, welcher sich auf die Teilung des Umfangs einer Lemniskate bezieht, und von jeher besonders hohes Interesse beanspruchte, wird nun in den folgenden Zeilen behandelt, und die Bestätigung der Kronecker'schen Vermutung in diesem speciellen Falle wird unter Benutzung der Hilbert'schen Methode[1] bis zu den Einzelheiten ausgeführt.

Diese fast überflüssigen Einleitungworte schliesse ich mit dem Ausdruck herzlichsten Dankes an den Herrn Prof. Hilbert in Göttingen, dessen Anregung diese Erstlingsarbeit ihr Entstehen verdankt.

§. 1.

Für die $\wp$-Function mit dem Periodenverhältnis i ist $g_3=0$; nimmt man $e_1=1$, $e_2=-1$, $e_3=0$, so wird $2\omega=\Omega$ reell, $2\omega'=\Omega i$ rein imaginär; $\wp(u)$ ist reell für reelles u, und nimmt conjugirt complexe Werte an für conjugirt complexe Werte des Arguments Es ist ferner $\wp(iu)=-\wp(u)$. Zwischen dieser $\wp$ Function und der Function $sn\, u$ mit $K=i$ besteht die Beziehung

$$\wp u=(sn\, u)^{-2}$$

mit demselben Argument für die beiden Functionen; ferner

$$2K=\Omega, \qquad 2K'i=(1+i)\,\Omega$$

$$sn\, iu=i\, sn\, u$$

1) Hilbert, *l. c.*

Verstehen wir under μ eine ganze Zahl des Körpers der rationalen complexen Zahlen, welchen wir im folgenden stets mit $k(i)$ bezeichnen wollen, so gelten für diese Functionen die folgenden Multiplicationsgesetze:

I. μ ist eine ungerade ganze rationale primäre Zahl in $k(i)$:

$$sn\ \mu u = x\frac{\psi_\mu(x^4)}{\chi_\mu(x^4)}: \qquad x = sn\ u$$

$$\wp\ \mu u = x\left(\frac{\psi_\mu(x^2)}{\chi_\mu(x^2)}\right)^2: \qquad x = \wp\ u$$

Hierbei bedeuten ψ_μ, χ_μ die zu einander primen ganzen rationalen Functionen von der Form:

$$\psi_\mu(y) = y^M + a_1 y^{M-1} + \ldots\ldots + a_{M-1}y + \mu,$$

$$\chi_\mu(y) = \mu y^M + a_{M-1}y^{M-1} + \ldots\ldots + a_1 y + 1,$$

worin $a_1, a_2, \ldots a_{M-1}$ ganze Zahlen des Körpers $k(i)$ sind, welche im Falle, wo μ eine Primzahl ist, alle durch μ teilbar sind, und ferner

$$M = \tfrac{1}{4}(m-1), \qquad m = n(\mu). \quad ^{1)}$$

Ferner sind

$$\frac{cn\ \mu u}{cn\ u} \qquad \frac{dn\ \mu u}{dn\ u}$$

rationale Functionen von $(sn\ u)^2$ in $k(i)$

II. μ ist gerade, d.h. teilbar durch $1 + i$:

$$sn\ \mu u = sn\ u.\ cn\ u.\ dn\ u\frac{f_\mu(x)}{g_\mu(x)} \qquad x = sn\ u$$

worin $f_\mu(x)$, $g_\mu(x)$ ganze rationale, zu einander prime Functionen in $k(i)$ sind, und zwar $g_\mu(x)$ vom Grade m, $f_\mu(x)$ vom Grade $m-3$

1) Eisenstein, Beiträge zur Theorie der Elliptischen Functionen, (Mathematische Abh. S. 129.)

oder $m-4$ jenachdem μ durch 2 teilbar ist oder nicht. Eine Ausnahme hievon bildet der Fall, wo

III. $\mu=1+i$:

$$\left.\begin{aligned} sn\,(1+i)\,u &= \frac{(1+i)\,sn\,u}{cn\,u.\,dn\,u} \\ \wp\,(1+i)\,u &= \frac{\wp\,u^2-1}{2i\,\wp\,u} \end{aligned}\right\} \qquad (3)$$

§. 2.

Teilung der Periode durch eine ungerade Primzahl in $k(i)$.—Es bedeute μ eine ungerade Primzahl des Körpers $k(i)$, m die Norm derselben. Die Gleichung $m-1^{\text{ten}}$ Grades in x

$$\psi_\mu\,(x^4)=0 \qquad (4)$$

ist nach einem wohlbekannten Satze Eisensteins in $k(i)$ irreducibel. Die Wurzeln derselben sind die Grössen

$$x_\lambda = sn\,\gamma^\lambda \frac{\Omega}{\mu} \qquad \lambda=0,\,1,\ldots\ldots m-2 \qquad (5)$$

wenn mit γ eine Primitivzahl nach μ bezeichnet wird. Die Gleichung (4) ist cyclisch in dem Rationalitätsbereich $k(i)$; sie definirt einen relativ-cyclischen Körper C_μ vom Relativgrade $m-1$ in Bezug auf $k(i)$.

Um die Discriminante D der Gleichung (4) zu finden, bedienen wir uns der Identität:

$$\begin{aligned} &(sn\,u-sn\,v)\,(sn\,u+su\,v)\{sn\,(u+v)-sn(u-v)\} \\ &\qquad =2\,sn\,u.\,cn\,u.\,dn\,u.\,sn\,(u+v)\,sn\,(u-v) \qquad (6) \end{aligned}$$

worin wir $sn\,u$, $sn\,v$ der Reihe nach durch alle möglichen Combinationen x_λ, $x_{\lambda'}$ aus den Grössen (5) ersetzen, mit Ausnahme derjenigen für die $\lambda=\lambda'$ oder $\lambda\equiv\lambda'$ mod. $\frac{m-1}{2}$ wird; dann nehmen $sn\,(u+v)$,

$sn\,(u-v)$ bis auf die Anordnung dieselben Werte. Zusammenmultiplicirt und noch vervollständigt mit dem Factor:

$$(\overset{\lambda}{\Pi}\, 2\, x_\lambda)^3 = 2^{3(m-1)}\mu^3 \qquad \lambda=0,\,1,\,\ldots\ldots m-2$$

ergeben diese Gleichungen:

$$D^3 = 2^{m(m-1)}\mu^{3(m-2)}\left(\overset{\lambda}{\Pi}\, cn\, \gamma^\lambda \frac{\Omega}{\mu} dn\, \gamma^\lambda \frac{\Omega}{\mu}\right)^{m-3}$$

Lassen wir in der ersten Formel (3) u die Werte $\gamma^\lambda \frac{\Omega}{\mu} (\lambda=0,\,1,\ldots m-2)$ durchlaufen, so durchläuft $sn\, u$ und $sn\,(1+i)\,u$ die Grössenreihe (5), woraus sich ergibt

$$\overset{\lambda}{\Pi}\, cos\, \gamma^\lambda \frac{\Omega}{\mu} du\, \gamma^\lambda \frac{\Omega}{\mu} = (1+i)^{m-1}$$

sodass endlich

$$D = 2^{\frac{(m-1)^2}{2}} \mu^{m-2} \tag{7}$$

§ 3.

Bestimmung der Discriminante des Körpers C_μ.—Es sei nun

$$m-1 = 2^{h_0} p_1^{h_1} p_2^{h_2} \cdots\cdots$$

die Primzahlzerlegung der rationalen Zahl $m-1$ im natürlichen Rationalitätsbereich, so besizt der zu $k(i)$ relativ-cyklische Körper C_μ je einen Unterkörper vom Relativgrade $2^{h_0}, p_1^{h_1}, p_2^{h_2}, \ldots$ in Bezug auf $k(i)$, welche durch Zusammensetzung den Körper C_μ erzeugen. Da ein relativcyklischer Körper von einem ungeraden Relativgrade über $k(i)$ nicht den Factor $1+i$ in ihrer Relativdiscriminante enthalten kann (§. 11.) so sind nach (7) die Relativdiscriminanten der obenerwähnten Relativkörper vom Relativgrade $p_1^{h_1}, p_2^{h_2}, \ldots$ eine Potenz von μ. Weil es aber keinen Relativkörper

über $k(i)$ gibt, dessen Relativdiscriminante eine Einheit ist, so muss die Zahl μ in jedem dieser Unterkörper in so viele identische Primideale zerfallen, wie der Relativgrad des betreffenden Körpers beträgt.

Was den Unterkörper vom Relativgrade 2^{h_0} betrifft, so muss seine Relativdiscriminante gewiss den Factor μ enthalten; denn da die Wurzeln der Gleichung (4) aus Paaren entgegengesetzter Zahlen bestehen, und da die Anzahl der Wurzeln $m-1$ Vielfaches von 4 ist, so sieht man aus

$$x_0\, x_1 \ldots\ldots x_{m-2} = \mu$$

dass die Zahl $\sqrt{\mu}$ im Körper C_μ enthalten sein muss. Diese Zahl $\sqrt{\mu}$ bestimmt aber einen relativquadratischen Körper über $k(i)$, welcher als Teiler in unserem Körper vom Relativgrade 2^{h_0} enthalten ist. Die Relativdiscriminante dieses relativquadratischen Körpers enthält aber gewiss den Factor μ, und infolgedessen auch die Relativdiscriminante des Körpers vom Relativgrade 2^{h_0}. Da dieser Körper als ein relativ-cyklischer über $k(i)$ keinen anderen relativquadratischen Unterkörper ausser $k(\sqrt{\mu})$ enthalten kann, so folgt aus der Betrachtung des Trägheitskörpers von μ, dass μ auch in unserem Körper vom Relativgrade 2^{h_0} in 2^{h_0} identischen Primideale zerfallen muss.

Die Zahl μ muss hiernach im Körper C_μ in $m-1$ identische Primideale zerfallen; die Relativdiscriminante von C_μ enthält μ zur $m-2$ ten Potenz. Dieses Primideal ist ein Hauptideal in C_μ und wird durch jede der Wurzeln (5) erzeugt, welche folglich associrte Zahlen sind.

Es handelt sich nun darum, zu entscheiden, ob und inwiefern die Zahl $1+i$ in der Relativdiscriminante des Körpers C_μ enthalten ist.

Ist $sn\, u$ eine beliebige Wurzel der Gleichung (4), so ist $sn\,(1+i)\,u$ auch Wurzel der Gleichung (4) und als solche associrt mit $sn\, u$. Es folgt daher aus der Formel (3), dass

$$cn\ u.\ dn\ u \text{ associrt mit } 1+i$$

ist.

Bedeuten nun $x_1 = sn\ u$, $x_1' = sn\ v$ zwei beliebige Grösse der Reihe (5), welche jedoch nicht der Gleichung $x_1 = \pm x_1'$ genügen, so sind $x_2 = sn(u+v)$, $x'_2 = sn(u-v)$ auch Wurzeln der Gleichung (4) und $x_2 \neq \pm x_2'$. Es folgt daher aus der Identität (6) dass

$$(x_1 - x_1')(x_1 + x_1')(x_2 - x_2') \text{ associrt mit } (1+i)^3 x_1^3$$

ist; vertauscht man v mit $-v$, was offenbar erlaubt ist, so folgt hieraus dass

$$(x_1 + x_1')(x_1 - x_1')(x_2 + x_2') \text{ associrt mit } (1+i)^3 x_1^3$$

ist, woraus dann folgt:

$$x_2 + x_2' \text{ associrt mit } x_2 - x_2'.$$

Dies gilt aber offenbar für jede zwei Wurzeln x, x', die der Gleichung $x = \pm x'$ nicht genügen.

Es ist daher

$$(x_1 - x_1')^2 (x_2 - x_2') \text{ ass. mit } (1+i)^3 x_1^3;$$

ersetzt man hierin u, v resp. durch $u+v$, $u-v$, so erhält man

$$(x_2 - x_2')^2 (x_3 - x_3') \text{ ass. mit } (1+i)^3 x_1^3$$

Fährt man aber in dieser Weise fort, so gelangt man schliesslich zu:

$$(x_h - x_h')^2 (x_1 - x_1') \text{ ass. mit } (1+i)^3 x_1^3$$

Aus dieser Kette von Beziehungen schliesst man, dass

$$x_1 - x_1' \text{ ass. mit } (1+i)\, x_1$$

ist.

Mit Hülfe der Gleichungen

$$sn\ 2\ u = \frac{2\ sn\ u.\ cn\ u.\ dn\ u}{1 + (sn\ u)^4}$$

$$sn\,(-1+2i)u = sn\,u.\frac{(sn\,u)^4+(-1+2i)}{(-1+2i)\,(sn\,u)^4+1}$$

oder

$$\frac{sn\,u - sn\,(-1+2i)\,u}{sn\,(-1+2i)\,u} = \frac{2i\,(sn\,u^4+1)}{sn\,u^4+(-1+2i)}$$

schliesst man sodann für $\mu \neq -1+2i$, d.h. $m>5$, dass

$$\frac{x^4-1+2i}{4}$$

eine Einheit ist, wenn x eine beliebige der Wurzeln der Gleichung (4) bedeutet.

Die Discriminante der Gleichung für x^4, $\psi_\mu(x^4)=0$ ist aber, wie unmittelbar aus (7) folgt,

$$\pm 4^{M(M-1)}\mu^{M-1}, \qquad M=\frac{m-1}{4}.$$

Die Discriminante der Zahl $\frac{x^4-1+2i}{4}$ in dem durch x^4 definirten Körper ist daher

$$\pm\mu^{M-1}.$$

Hieraus folgt, dass die Relativdiscriminante des Körpers $k(x^4)$ in Bezug auf $k(i)=\mu^{M-1}$ also relativ prim zu $1+i$ ist.

Um die Relativdiscriminante des Körpers $k(x^2)$ in Bezug auf $k(x^4)$ zu bestimmen, betrachten wir die Zahl

$$\omega = \frac{i+(sn\,u)^2}{cn\,u.\,dn\,u}$$

indem wir mit $sn\,u$ eine Wurzel der Teilungsgleichung (4) bezeichnen. Dann ist ω eine Zahl des Körpers $k(x^2)$, ihre Conjugirte in Bezug auf $k(x^4)$ ist

$$\omega' = \frac{i-(sn\,u)^2}{cn\,u.\,dn\,u}$$

Ferner

$$\omega+\omega'=\frac{2i}{cn\,u.\,dn\,u},\qquad \omega\omega'=\frac{1+(sn\,u)^4}{(cn\,u\,dn\,u)^2}$$

$$\frac{\omega}{\omega'}+\frac{\omega'}{\omega}=\frac{2\,(1-sn\,u^4)}{1+sn\,u^4}$$

woraus unmittelbar folgt, dass diese drei Zahlen mit $1+i$ associrt sind. Hieraus ergibt sich dass ω, ω' ganze und zwar associrte Zahlen sind; da ferner $\omega\omega'$ mit $1+i$ associrt ist, so folgt, dass jedes Primideal des Körpers $k(x^4)$ welches in $1+i$ aufgeht, in $k(x^2)$ in zwei identische Primideale zerfällt. Wir setzen demnach

$$(1+i)=\mathfrak{z}^2\mathfrak{z}'^2\ldots\ldots$$

dann wird

$$(\omega)=\mathfrak{z}\mathfrak{z}'\ldots\ldots$$

Hieraus ergibt sich, dass die Relativdifferente des Körpers $k(x^2)$ in Bezug auf $k(x^4)$ dieselbe Potenz der Primideale $\mathfrak{z}$, $\mathfrak{z}'$...enthält, wie die Relativdifferente der Zahl ω in Bezug auf $k(x^4)$[1]. Es ist aber

$$\omega-\omega'=\frac{2\,sn\,u^2}{cn\,u.\,du\,u}$$

Die Relativdifferente des Körpers $k(x^2)$ in Bezug auf $k(x^4)$ enthält den Factor $1+i$ zur ersten Potenz.

Es bleibt nur noch übrig, zu bestimmen, welche Potenzen von $\mathfrak{z}$, $\mathfrak{z}'$...in die Relativdiscriminante des Körpers $C_\mu=k(x)$ in Bezug auf $k(x^2)$ aufgehen.

Es bedeute wie vorher $x=sn\,u$ eine beliebige der Wurzeln der Gleichung (4); jede ganze Zahl des Körpers C_μ lässt sich dann in der Form darstellen

1) Vgl. Hilbert, Die Theorie der alg. Zahlkörper, Bericht, erstattet der Deutschen Mathematiker-Vereinigung, S. 392.

$$\gamma=\frac{\alpha+\beta x}{2}$$

wenn α, β ganze Zahlen des Körpers $k(x^2)$ bedeuten, die der Bedingung

$$\alpha^2-\beta^2x^2\equiv 0 \quad mod.\ 4 \tag{8}$$

Genüge leisten. Nun ist die Zahl

$$\xi=1+i\ cn\ u$$

gewiss eine ganze Zahl des Körpers $k(x^2)$ und

$$\xi^2-x^2=2i\ cn\ u\equiv 0 \quad mod.\ \mathfrak{z}^5\mathfrak{z}'^5\ldots\ldots$$

nicht aber für eine höhere Potenz irgend eines $\mathfrak{z}$ als Modul. Es ist nun zu beweisen, dass eine Congruenz der Form

$$\zeta^2-x^2\equiv 0 \quad (mod.\ \mathfrak{z}^6)$$

überhaupt für eine Zahl ζ des Körpers $k(x^2)$ unmöglich ist. In der Tat: wäre $\zeta^2\equiv x^2$ (mod $\mathfrak{z}^6$) so müsste erstens $\zeta^2\equiv\xi^2$ (mod $\mathfrak{z}^5$), d.h. $\zeta^2-\xi^2=(\zeta-\xi)\ (\zeta+\xi)$ teilbar durch $\mathfrak{z}^5$. Dies hätte aber zur Folge, dass $\zeta^2\equiv\xi^2$ (mod. $\mathfrak{z}^6$) und daher müsste $\xi^2-x^2=(\zeta^2-x^2)-(\zeta^2-\xi^2)$ auch durch $\mathfrak{z}^6$ teilbar sein, was aber nicht der Fall sein kann.

Wir können nun zeigen, dass die Congruenz (8) dann und nur dann möglich ist, wenn β durch $1+i$ teilbar ist. Wäre nämlich β nicht durch $\mathfrak{z}^2$ teilbar, so könnte man, da jedenfalls α und β durch dieselbe Potenz von $\mathfrak{z}$ teilbar sein müssen, eine Zahl ζ aus der Congruenz

$$\alpha\equiv\beta\zeta \quad (mod.\ \mathfrak{z}^8)$$

bestimmen; es muss dann $\beta^2\ (\zeta^2-x^2)$ durch $\mathfrak{z}^8$ teilbar sein, uud da β nicht durch $\mathfrak{z}^2$ teilbar sein sollte, so musste ζ^2-x^2 wenigstens durch $\mathfrak{z}^6$ teilbar sein, was aber nicht möglich ist. Es muss daher β durch $\mathfrak{z}^2$ und ähnlicherweise durch $\mathfrak{z}'^2,\ldots$also durch $1+i$ teilbar sein.

Ist aber β durch $1+i$ teilbar, so nehmen wir einfach

$$\alpha=\beta\,\xi=\beta\,(1+i\;cn\;u)$$

sodass

$$\alpha^2-\beta^2\,x^2=\beta^2\,(\xi^2-x^2)\equiv 0 \quad (mod.\ 4)$$

um in

$$\gamma=\frac{\alpha+\beta x}{2}$$

wirklich eine ganze Zahl des Körpers C_μ zu erhalten.
Jede ganze Zahl des Körpers $C_\mu=k(x)$ lässt sich demnach in der Form darstellen

$$\gamma=\frac{\alpha+\beta\,x}{1+i}$$

worin α, β ganze Zahlen des Körpers $k(x^2)$ bedeuten, und es existirt wirklich ganze Zahlen in $k(x)$ bei denen β relativ prim zu $1+i$ ist.

Wir schliessen daher aus

$$\gamma-\gamma'=(1-i)\,\beta x$$

dass die Relativdifferente des Körpers C_μ in Bezug auf $k(x^2)$ den Factor $1+i$ zur ersten Potenz enthält.

Hiermit haben wir den Satz bewiesen:

Ist μ eine ungerade Primzahl des Körpers $k(i)$ so ist der Teilungskörper C_μ relativ cyclisch vom Relativgrade $m-1$ in Bezug auf $k(i)$. Seine Relativdiscriminante ist $2^{m-1}\,\mu^{m-2}$

Ist

$$m-1=2^{h+2}\,p_1^{h1}\,p_2^{h2}\ldots\ldots$$

die Primzahlzerlegung der Zahl $m-1$, so ist in C_μ als Teiler enthalten je ein relativ cyclischer Körper

vom Relativgrade	*mit der Relativdiscriminante*	
$p_1^{\lambda_1}$	$\mu^{p_1^{\lambda_1}-1}$	$(\lambda_1=1, 2, \ldots\ldots h_1)$
$p_2^{\lambda_2}$	$\mu^{p_2^{\lambda_2}-1}$	$(\lambda_2=1, 2, \ldots\ldots h_2)$
.....	.....	
2^{λ}	$\mu^{2^{\lambda}-1}$	$(\lambda=1, 2, \ldots\ldots h)$
2^{h+1}	$(1+i)^{2^{h+1}}\ \mu^{2^{h+1}-1}$	
2^{h+2}	$(1+i)^{2^{h+3}}\ \mu^{2^{h+2}-1}$	

§. 4.

Teilung durch eine ungerade Primzahlpotenz.—Es bedeute wiederum μ eine ungerade complexe Primzahl, m ihre Norm. Die Multiplicationsformel der Function $sn\ u$ mit dem Factor μ^h erhält man durch Iteration aus der Formel

$$sn\ \mu u = x\frac{\psi_1(x^4)}{\chi_1(x_4)} \qquad x = sn\ u.$$

Ersetzt man hierin x durch $x\,\dfrac{\psi_1(x^4)}{\chi_1(x^4)}$, so kommt nachdem man die Brüche in Nenner und Zähler beseitigt hat

$$sn\ \mu^2 u = x\frac{\Psi_2}{X_2}$$

Ψ_2 enthält ψ_1 als Factor; setzt man

$$\Psi_2 = \psi_1\psi_2$$

so ist ψ_2 vom Grade $\varphi(\mu^2)=m(m-1)$ in x; die Coefficient der höchsten Potenz von x in ψ_2 ist 1, das constante Glied μ, die anderen Coefficienten sind alle durch μ teilbar.

Durch den Schluss von n auf $n+1$ erhält man das allgemeine Resultat:

$$sn\ \mu^h u = x.\frac{\Psi_h(x^4)}{X_h(x^4)} \qquad x = sn\ u$$

$$\Psi_h = \psi_1\psi_2 \ldots\ldots \psi_h$$

ψ_h ist vom Grade $\varphi(\mu^h) = m^{h-1}(m-1)$ in x, ihre Coefficienten sind von der oben erwähnten Beschaffenheit. Man erhält daher den Satz:

Die Gleichung $\varphi(\mu^h) = m^{h-1}(m-1)^{ten}$ Grades

$$\psi_h(x^4) = 0$$

von der die eigentliche μ^h Teilung der Periode abhängt ist irreducibel in $k(i)$.

Die Discriminante der Gleichung (9) enthält nur die Factoren μ und $1+i$, wie es sich durch genau dieselbe Betrachtung wie in §. 2. nachweisen lässt.

Um die Gruppe dieser Gleichung zu bestimmen, unterscheiden wir zwei Fälle:

Ist $\mu = \pi$ nicht reell, $m = p$ die Noun von π, so gibt es Primitivzahlen nach π^h. Es sei g eine derselben, dann sind die Wurzeln von (9) die Grösse

$$x_\lambda = sn\ g^\lambda.\frac{\Omega}{\mu^h} \qquad \lambda = 0, 1, \ldots\ldots p^{h-1}(p-1)-1.$$

Die Gleichung (9) bestimmt daher einen relativcyclischen Körper vom Relativgrade $p^{h-1}(p-1)$ in Bezug auf $k(i)$. In demselben ist enthalten als Teiler ein relativcyclischer Körper vom Relativgrade p^{h-1}, dessen Relativdiscriminante eine Potenz von π ist, und ein relativcyclischer Körper vom Relativgrade $p-1$, welcher nichts anders ist als derjenige, welcher aus der π-Teilung entspringt und welchen wir im vorigen mit C_π bezeichnet haben.

Ist aber $\mu=q$ reell, also $m=q^2$, so lassen sich die $q^{2(h-1)}(q^2-1)$ incongruenten zu q relativ primen Zahlclassen des Körpers $k(i)$ nach dem Modul q^h $(h>1)$ nicht durch die Potenzen einer Zahl repräsentiren. Ist nämlich γ eine Primitivzahl nach q in $k(i)$ so ist $\gamma^{q^2-1}\equiv 1$ (mod. q). Besteht diese Congruenz auch mod. q^2 so nehmen wir statt γ, $\gamma+\lambda q$ wo $\lambda\not\equiv 0$ (mod. q) und sind sicher, dass für diese neue Primitivzahl nach q, die wir einfach mit γ bezeichnen wollen, die obige Congruenz nur für mod. q besteht; also

$$\gamma^{q^2-1}=1+\xi q \qquad \xi\not\equiv 0 \ (mod.\ q)$$

Hieraus folgt der Reihe nach

$$\gamma^{q(q^2-1)}=1+\xi' q^2 \qquad \xi'\not\equiv 0 \ (mod.\ q)$$

.....

$$\gamma^{q^{h-1}(q^2-1)}=1+\xi^{(h-1)}q^h \qquad \xi^{(h-1)}\not\equiv 0 \ (mod.\ q)$$

Die Zahl γ gehört also mod. q^h dem Exponenten $q^{h-1}(q^2-1)$. Es folgt hieraus, dass für jede ganze Zahl α des Körpers $k(i)$ die Congruenz

$$\alpha^{q^{h-1}(q^2-1)}\equiv 1 \qquad (mod.\ q^h)$$

besteht.

Wenn nun γ' eine Zahl ist, deren Potenz für keinen kleineren Exponenten als q^{h-1} mod. q^h congruent mit einer Potenz von γ wird, so werden alle $q^{2(h-1)}(q^2-1)$ mod. q^h incongruenten zu q relativ primen Zahlclassen durch

$$\gamma^{\lambda}\gamma'^{\mu} \qquad \begin{pmatrix} \lambda=0,\ 1,\ldots\ldots q^{h-1}(q^2-1)-1 \\ \mu=0,\ 1,\ldots\ldots q^{h-1}-1 \end{pmatrix}$$

repräsentirt.

Um die Existenz einer solchen Zahl γ' nachzuweisen, betrachten wir die Gesamtheit der Zahlen α die mod. q^h zum Exponenten q^{h-1} gehören; für diese Zahlen wird dann $\alpha\equiv 1$ (mod. q.) nicht aber

mod. q^2; sie sind daher in q^2-1 mod. q^2 incongruenten Zahlclassen von der Form $a=1+\xi q$ ($\xi \not\equiv 0$ mod. q) enthalten. Von diesen sind nur $q-1$ verschiedene Classen unter den Potenzen von γ enthalten, nämlich $\gamma^{\lambda(q^2-1)}$ ($\lambda=1, 2, \ldots q-1$.) Wählt man daher γ' beliebig aus den übrigbleibenden Classen, so wird γ' in der Tat die gesuchte Zahl sein. Denn ist $a>0$ der kleinste Exponent, für den $\gamma'^a \equiv \gamma^\mu$ (mod. q^2) wird, so muss erstens a in q^{h-1} aufgehen, sodann muss μ teilbar sein durch a (q^2-1) und endlich wenn man $\mu=ba$ (q^2-1) setzt, muss die Zahl $\gamma'\gamma^{-b(q^2-1)}$ mod. q^h zum Exponenten a gehören. Wäre also $a<q^{h-1}$ so musste $\gamma'\gamma^{-b(q^2-1)} \equiv 1$ wenigstens mod. q^2, was aber durch die Wahl von γ' ausgeschlossen ist.

Hiernach lassen sich die Wurzeln der Gleichung (9) für $\mu=q$ in der Form darstellen

$$x_{\lambda,\mu}=sn\ \gamma^\lambda \gamma'^\mu \frac{\Omega}{q^h} \quad \begin{pmatrix} \lambda=0, 1, 2, \ldots\ldots q^{h-1}(q^2-1)-1 \\ \mu=0, 1, 2, \ldots\ldots q^{h-1}-1 \end{pmatrix}$$

Bezeichnen wir nun die Substitutionen (x_{00}, x_{10}) (x_{00}, x_{01}) resp. mit s, t so ist die Gruppe der Gleichung (9) eine Abel'sche und zwar mit den Elementen

$$s^\lambda t^\mu \quad \begin{pmatrix} \lambda=0, 1, 2, \ldots\ldots q^{h-1}(q^2-1)-1 \\ \mu=0, 1, 2, \ldots\ldots q^{h-1}-1 \end{pmatrix}$$

Der Teilungskörper ist also in diesem Falle relativ Abel'sch in Bezug auf $k(i)$. Dieser enthält als Teiler $q^{h-1}+1$ von einander verschiedene relativcyclische Körper vom Relativgrad q^{h-1} in Bezug auf $k(i)$. Die Relativdiscriminante jedes dieser Körper ist eine Potenz von q. Der in dem ganzen Teilungskörper enthaltene relativcyclische Unterkörper vom Relativgrade q^2-1 ist nichts anders als derjenige, welcher aus der q-Teilung entspringt.

§. 5.

Teilung durch die Potenz von $1+i$.—Wir bedienen uns in diesem Falle der Function $\wp u$: aus der Formel

$$\wp(1+i)\,u=\frac{\wp u^2-1}{2i\wp u}$$

erhält man durch Iteration

$$\wp(1+i)^h u=\frac{f_h(x)}{g_h(x)} \qquad x=\wp u$$

worin f_h, g_h ganze rationale ganzzahlige Functionen in $k(i)$ sind, welche durch die Recursionsformel

$$f_{\lambda+1}=f_\lambda^2-g_\lambda^2$$

$$g_{\lambda+1}=2i\,f_\lambda\,g_\lambda$$

in Verbindung mit

$$f_1=x^2-1, \qquad g_1=2ix$$

vollständig definirt werden.

Die Gleichung $2^{h-1\text{ ten}}$ Grades

$$f_h(x)=0 \tag{10}$$

von welcher die $(1+i)^h$ Teilung abhängt, lässt sich in $k(i)$ in vier Gleichungen $2^{h-2\text{ ten}}$ Grades zerlegen

$$f_h(x)=(f_{h-2}-i\,g_{h-2})^2\,(f_{h-2}+i\,g_{h-2})^2=0$$

Aus

$$\wp\left(\frac{\Omega}{2}\right)=1 \qquad \wp\left(\frac{\Omega i}{2}\right)=-1$$

folgt durch die Auflösung der Gleichungen

$$\frac{x^2-1}{2i\,x}=\pm 1$$

dass

$$\wp\frac{\Omega}{4}(1+3i)=\wp\frac{\Omega}{4}(3+i)=i$$

$$\wp\frac{\Omega}{4}(1+i)=\wp\frac{\Omega}{4}(3+3i)=-i$$

Die Wurzeln der Gleichung

$$f_{h-2}(x)-i\,g_{h-2}(x)=o$$

sind daher die Grössen $\wp u$ mit

$$u=\frac{\xi+\eta i}{(1+i)^h}\,\Omega$$

worin

$$(\xi,\eta)\equiv(0,1),\quad(0,3),\quad(2,3),\quad(2,1),\quad mod.\ 4.$$

Da aber $\wp(-u)=\wp u$, so sind diese Grössen enthalten in

$$\wp\frac{\xi+\eta i}{(1+i)^h}\,\Omega\qquad\left(\begin{matrix}\xi\text{ gerade}\\ \eta\equiv 1\text{ mod. }4.\end{matrix}\right)$$

Die Wurzeln der Gleichung

$$f_{h-2}(x)+i\,g_{h-2}(x)=o$$

sind die Grössen

$$\wp\frac{\xi+\eta i}{(1+i)^h}\,\Omega\qquad\left(\begin{matrix}\xi\equiv 1\text{ mod. }4.\\ \eta\text{ gerade}\end{matrix}\right)$$

Berücksichtigt man aber, dass $\wp iu=-\wp u$, so sieht man, dass die beiden Gleichungen denselben Körper definiren.

Da ferner der Körper der $(1+i)^\lambda$-Teilung in demjenigen der $(1+i)^{\lambda+1}$-Teilung als Teiler enthalten ist, wollen wir uns auf die Gleichung der $(1+i)^{2m+3}$ Teilung

$$f_{2m}(x)+i\,g_{2m}(x)=o \tag{11}$$

beschränken, deren Wurzeln, die 2^{2m} Grössen

$$\wp \frac{\xi+\eta i}{(1+i)^{2m+3}}\Omega \qquad \begin{pmatrix}\xi=1,\ 5,\ldots\ldots 4(2^m-1)+1\\ \eta=0,\ 2,\ldots\ldots 2(2^m-1)\end{pmatrix}$$

sind.

Es sei γ eine ungerade ganze Zahl in $k(i)$ derart, dass erstens der reelle Teil derselben $\equiv 1$ mod. 4 und zweitens die mit ihr associrte primäre Zahl nicht $\equiv 1$ mod. 4 ist, wie z. B. die Zahl $1+2i$. Diese Zahl γ gehört dann mod. $(1+i)^{2^{m+3}}$ zum Exponenten 2^m; die 2^m Potenzen von γ mit den Exponenten $0, 1, 2, \ldots 2^m-1$ sind alle von der Form $\xi+\eta i$, $\xi\equiv 1$ mod. 4, η, gerade; und sind mit einander mod. $(1+i)^{2^{m+3}}$ incongruent. Es existiren nun ebenso wie γ beschaffene Zahlen, unter anderen die zu γ conjugirte Zahl γ', von welcher keine niedrigere Potenz als die $2^{m\text{te}}$ mit einer der Potenzen von γ mod. $(1+i)^{2^{m+3}}$ congruent wird. Dann sind die Wurzeln der Gleichung (11) die 2^{2m} Grössen

$$x_{\lambda,\lambda'}=\wp\,\gamma^{\lambda}\gamma'^{\lambda'}\frac{\Omega}{(1+i)^{2m+3}} \qquad (\lambda, \lambda'=0,\ 1,\ 2,\ldots\ldots 2^m-1)$$

Die Gleichung (11) reducirt sich nun in eine kette von $2m$ quadratischen Gleichungen:

$$y_0=-i=\frac{y_1^2-1}{2i\,y_1}$$

$$y_1 \quad =\frac{y_2^2-1}{2i\,y_2}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y_{2m-1} \quad =\frac{y_{2m}^2-1}{2i\,y_{2m}}$$

Betrachten wir eine dieser quadratischen Gleichungen

$$y_{n+1}^2-2i\,y_n\,y_{n+1}-1=0$$

so sehen wir zunächst aus der Discriminante derselben

$$d_{n+1} = -4\,(y_n^2 - 1) = -8i\, y_n\, y_{n-1}$$

dass, die Discriminante der Gleichung (11) und folglich auch die Relativdiscriminante des durch sie definirten Körpers in Bezug auf $k(i)$ nur den Primfactor $1+i$ enthalten, da die Zahlen y sämtlich Einheiten sind.

Ferner leuchtet ein, dass der Körper $k(y_{n+1})$ durch Adjunction der Zahl $\sqrt{y_n}$ aus dem Körper $k(y_n)$ hervorgeht. Um uns zu überzeugen, dass die Gleichung (11) wirklich einen Körper vom Relativgrade 2^{2m} definirt, genügt es zu zeigen, dass jedesmal der Körper $k(y_{n+1})$ wirklich von $k(y_n)$ verschieden ist, oder was dasselbe ist, dass die Zahl y_n keine Quadratzahl in $k(y_n)$ ist. Da $y_1 = 1 \pm \sqrt{2}$, so ist $k(y_1)$ wirklich von $k(i)$ verschieden. Wir nehmen also an, dass $k(y_n)$ vom Relativgrade 2^n ist, und wollen beweisen, dass dann der Körper $k(y_{n+1})$ wirklich vom Relativgrade 2^{n+1} sein muss. Wäre nämlich $y_n = (\alpha + \beta\, y_n)^2$ worin α, β zwei Zahlen des Körpers $k(y_{n-1})$ bedeuten, so folgt hieraus, wegen der vorausgesetzten Irreducibilität der Gleichung für y_n in $k(y_{n-1})$, dass

$$\beta^2 = -\alpha^2 = \frac{2\,\alpha\beta - 1}{-2i\, y_{n-1}}$$

d.h.

$$y_{n-1} \pm 1 = \left\{ \frac{1}{(1-i)\,\beta} \right\}^2$$

Die Norm der Zahl $y_{n-1} \pm 1$ in Bezug auf $k(y_{n-2})$ ist aber $\pm\, 2i\, y_{n-2}$; es sollte also y_{n-2} eine Quadratzahl in $k(y_{n-2})$ sein, was nach der Voraussetzung nicht möglich ist.

Die Gleichung (11) ist daher in $k(i)$ irreducibel, sie definirt einen relativ Abel'schen Körper vom Relativgrade 2^{2m} in Bezug auf $k(i)$.

Da es keinen Körper über $k(i)$ mit der Relativdiscriminante 1 gibt, und da die Relativdiscriminante des Körpers $k(y_n)$ eine

Potenz von $1+i$ ist, so folgt dass die Zahl $1+i$ gleich einer 2^nten Potenz eines Primideals in $k(y_n)$ sein muss. Um zu zeigen, dass dieses Primideal ein Hauptideal ist, betrachten mir die Zahl

$$\zeta_n = \frac{2}{y_n - y_{n-1}}$$

des Körpers $k(y_n)$. Ihre relative Spur und Norm bez. $k(y_{n-1})$ sind

$$\zeta_n + \zeta_n' = \frac{2(1+i)}{y_{n-1} - y_{n-2}} \qquad \zeta_n \zeta_n' = \frac{i}{y_{n-1}} \cdot \frac{2}{y_{n-1} - y_{n-2}} \tag{12}$$

ζ_n ist also eine ganze Zahl, wenn $\zeta_{n-1} = \frac{2}{y^{n-1} - y^{n-2}}$ es ist.
Die Zahl

$$\zeta_1 = \frac{2}{y_1 - y_0} = \frac{2}{y_1 + i}$$

ist aber eine ganze Zahl, da

$$\zeta_1 + \zeta_1' = -2i \qquad \zeta_1 \zeta_1' = -(1+i) \tag{13}$$

Folglich ist ζ_n eine ganze Zahl. Die Relativnorm der Zahl ζ_n genommen in $k(y_n)$ und in Bezug auf $k(i)$ ist nach (12) gleich der Relativnorm von ζ_{n-1} genommen in $k(y_{n-1})$, bis auf eine Einheit. Es ist also nach (13)

$$N\,\zeta_n = \varepsilon\,(1+i)$$

wenn ε eine Einheit bedeutet; im Sinne der Idealengleichheit ist demnach

$$(\zeta_n)^{2^n} = (1+i)$$

Hieraus schliesst man ferner dass die Relativdifferente δ_n des Körpers $k(y_n)$ in Bezug auf $k(y_{n-1})$ der Relativdifferente der Zahl ζ_n in Bezug auf $k(y_{n-1})$ gleich ist; also bis auf eine Einheit

$$\delta_n = (1+i)\,\zeta_{n-1}$$

Die Relativdifferente des durch (11) definirten relativ Abel'schen Körpers in Bezug auf $k(i)$ ist daher

$$\mathfrak{D}_{2m}=(1+i)^{2m}\zeta_{2m-1}\,\zeta_{2m-2}\cdots\cdots\zeta_0$$

und endlich die Relativdiscriminante

$$D_{2m}=2^{(m+1)\,2^{2m}-1}$$

Dieser relativ Abel'sche Körper vom Relativgrade 2^{2m} enthält als Teiler 2^m+1 von einander verschiedene relativcyclische Körper vom Relativgrade 2^m, deren Relativdiscriminante nur den Primfactor $1+i$ enthält.

§. 6.

Durch die bisherigen Auseinandersetzungen wurde die Existenz der folgenden relativ-cyclischen Körper über $k(i)$ nachgewiesen:

1) Eines relativ-cyclischen Körpers vom Relativ-grade p^λ ($\lambda=1, 2, 3,\ldots h$) dessen Relativdiscriminante eine Potenz der ungeraden Primzahl μ des Körpers $k(i)$ ist. Hierin bedeutet die Zahl h den Exponenten der höchsten Potenz von p, die in $m-1$ aufgeht, wenn m die Norm von μ in $k(i)$ ist.

2) Eines relativ cyclischen Körpers vom Relativgrad p^λ (λ beliebig) dessen Relativdiscriminante eine Potenz von π ist. Hierin bedeutet π eine Primzahl ersten Grades des Körpers $k(i)$ und p ihre Norm.

3) $q^\lambda+1$ relativcyclischer Körper vom Relativgrade q^λ (λ beliebig) deren Relativdiscriminante eine Potenz von q ist, wenn q eine Primzahl zweiten Grades in $k(i)$ ist.

4) Eines relativcyclischen Körpers vom Relativgrade 2^λ ($\lambda=1, 2,\ldots h, h+1, h+2$) dessen Relativdiscriminante für $\lambda\leqq h$ nur den Factor μ, und für $\lambda=h+1, h+2$ ausserdem nur

noch den Factor $(1+i)$ enthält. Hierin bedeutet μ eine ungerade Primzahl des Körpers $k(i)$, und 2^h die höchste Potenz von 2, die in $\frac{1}{4}(m-1)$ aufgeht, wenn m die Norm von μ ist.

5) $2^\lambda+1$ relativcyclischer Körper vom Relativgrade 2^λ (λ beliebig) deren Relativdiscriminante eine Potenz von $1+i$ ist.

§. 7.

Primideale des Teilungskörpers. Es bedeute μ^λ eine gerade oder ungerade Primzahlpotenz des Körpers $k(i)$, K den Körper der μ-Teilung, M den Relativgrad desselben in Bezug auf $k(i)$.

Wir haben gezeigt, dass die Primzahl μ gleich der M^{ten} Potenz eines primen Hauptideals $\mathfrak{M}$ in K ist. $\mathfrak{M}$ ist vom ersten Grade in Bezug auf $k(i)$.

Es sei nun ν eine ungerade, primäre, von μ verschiedene Primzahl des Körpers $k(i)$, n deren Norm.

Bedeutet

$$x = sn\, u$$

eine Wurzel der Gleichung der μ^h Teilung, so ist jedenfalls

$$x' = sn\, \nu u$$

auch Wurzel derselben Gleichung. Es ist nun

$$x' = x\frac{x^{n-1}+\nu\gamma}{\nu\gamma'+1}$$

wenn γ, γ' gewisse ganze Zahlen des Körpers K bedeuten. Es folgt hieraus

$$x' \equiv x^n \qquad (mod.\ \nu)$$

Eine solche Congruenz besteht aber nicht für eine andere Wurzel x'' der Teilungsgleichung, weil $x'-x''$ nur durch diejenigen Primideale des Körpers K teilbar ist, die in μ oder in $1+i$ aufgehen.

Bezeichnen wir nun mit s die Substitution (x, x') des Körpers K, so ist

$$x \mid s^2 \equiv x^{n^2}, \ldots\ldots \qquad x \mid s^\lambda \equiv x^{n^\lambda} \qquad (mod.\ \nu)$$

Ist daher f der Grad von s,

$$x^{n^f} \equiv x \qquad (mod.\ \nu)$$

Jede ganze Zahl γ des Körpers K lässt sich nun in der Form darstellen

$$c.\ \gamma = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_{M-1} x^{M-1}$$

wenn $a_0, a_1 \ldots a_{M-1}$ ganze Zahlen des Körpers $k(i)$ und c eine gewisse Potenz von $(1+i)$ bedeuten. Hieraus folgt für jede ganze Zahl des Körpers K

$$\gamma^{n^f} \equiv \gamma \qquad (mod.\ \nu)$$

Ist daher $\mathfrak{N}$ ein Primideal des Körpers K, welches in ν aufgeht, und $n^{f'}$ die absolute Norm derselben, so muss $f' \leqq f$. Da aber

$$x^{n^{f'}} \equiv x \qquad (mod.\ \mathfrak{N})$$

nicht für $f' < f$ bestehn kann, so ist $f' = f$

Die Zahl f, als die Gradzahl der Substitution s, muss in die Gradzahl M des Körpers aufgehen; ist $M = ef$, so zerfällt die Zahl ν in e von einander verschiedene Primideale in K. Diese Primideale sind vom f^{ten} Grade in Bezug auf $k(i)$.

Die Zahl f ist aber nichts anders als der Exponent, zu welchem die Zahl ν gehört mod. μ^h.

Es bleibt noch für ungerades μ die Zerlegung der Zahl $1+i$ zu untersuchen. Wir bezeichnen den einzigen Unterkörper von K vom Index 4 mit K', den Relativgrad desselben $\frac{M}{4}$ mit M'. Eine Basis von K' bilden die Potenzen der Zahl (§. 2)

$$y=\frac{x^4-a}{4}, \quad a=1+2i$$

sodass jede ganze Zahl γ des Körpers K' in der Form

$$\gamma=a_0+a_1\,y+a_2\,y^2+\ldots\ldots+a_{M'-1}\,y^{M'-1}$$

darstellbar ist, wenn $a_0,\ a_1,\ldots a_{M'-1}$ ganze Zahlen des Körpers $k(i)$ bedeuten.

Nun ist die Zahl

$$x'=sn\,(1+i)\,u=\frac{(1+i)\,sn\,u}{cn\,u\,dn\,u}$$

eine Wurzel der Teilungs-gleichung, und

$$y'=\frac{x'^4-a}{4}$$

eine zu y conjugirte Zahl. Es ist aber

$$y'=-\frac{4\,x^4}{(x^4-1)^2}-\frac{a}{4}=\frac{(4y+a)+a(2y-i)^2}{4(2y-i)^2}$$
$$=\frac{-a\,y^2+(1-i\,a)y}{(2y-i)^2}$$

sodass

$$y'\equiv y^2 \qquad (mod.\ 1+i)$$

Da ferner $y'-y''$ eine mit $\mathfrak{M}$ associrte Zahl ist, so besteht eine solche Congruenz nicht für ein anderes y''.

Hieraus schliesst man genau in derselben Weise wie vorher, dass, wenn f den kleinsten Exponenten bedeutet, für den

$$(1+i)^f\equiv 1 \qquad (mod.\ \mu^h)$$

und wenn

$$M'=ef$$

gesetzt wird, die Zahl $1+i$ in e von einander verschiedene Primideale in K' zerfällt.

Wir haben schon bewiesen, dass jedes dieser Primideale in 4 identische Primideale in K zerfällt; diese Ideale sind daher vom f^{ten} Grade in Bezug auf $k(i)$.

Die Zerlegung der Primideale des Körpers $k(i)$ im Körper der μ^h Teilung ist daher genau demselben Gesetz unterworfen, wie bei der Kreisteilungstheorie.

Ist $M=\varphi(\mu^h)=m^{h-1}(m-1)$ so findet in K die Zerlegung statt:

$$\mu=\mathfrak{M}^M: \qquad \mathfrak{M}=\left(sn\frac{\Omega}{\mu^h}\right)$$

$$\nu=\mathfrak{N}_1\mathfrak{N}_2\ldots\ldots\mathfrak{N}_e: \qquad ef=M,\ \nu^f\equiv 1\ (mod.\ \mu^h)$$

$$1+i=(\mathfrak{Z}_1\mathfrak{Z}_1\ldots\ldots\mathfrak{Z}_e)^t: \qquad ef=\frac{M}{4},\ (1+i)^f\equiv 1\ (mod.\ \mu^h)$$

$\mathfrak{M}$ ist vom ersten, $\mathfrak{N}$, $\mathfrak{Z}$ vom f^{ten} Grade in Bezug auf $k(i)$.

§. 8.

Teilung durch eine Zusammengesetzte Zahl. Ist λ eine Zusammengesetzte Zahl des Körpers $k(i)$ und $\lambda=\mu\nu$ worin μ, ν relativprime Zahlen sind, so durchläuft die Zahl

$$\zeta=\eta\mu+\xi\nu$$

alle zu λ relativ primen $\varphi(\lambda)$ incongruenten Zahlclassen mod. λ, wenn man ξ die zu μ relativ primen $\varphi(\mu)$ incongruenten Zahlclassen mod. μ, und η die zu ν relativ primen $\varphi(\nu)$ incongruenten Zahlclassen mod. ν. durchlaufen lässt.

Setzt man daher

$$w=sn\frac{\xi\Omega}{\lambda}, \quad u=sn\frac{\xi\Omega}{\mu}, \quad v=sn\frac{\eta\Omega}{\nu}$$

so wird

$$sn\ w=sn\ (u+v)=\frac{sn\ u\ cn\ v\ dn\ v+sn\ v.\ cn\ u.\ dn\ u}{1+sn^2\ u\ sn^2\ v}$$

und $sn\ w$ durchläuft alle Wurzeln der Gleichung, von der die eigentliche λ-Teilung abhängt, wenn man in diesem Ausdruck resp. $sn\ u$, $sn\ v$ alle Wurzeln der Gleichungen der μ-, ν- Teilung durchlaufen lässt.

Es lassen sich nun jedenfalls $cn\ u.\ dn\ u$ durch $sn\ u$, $cn\ v.\ dn\ v$ durch $sn\ v$ in $k(i)$ rational ausdrücken, sodass wenn

$$z = sn\ w, \qquad x = sn\ u, \qquad y = sn\ \nu$$

gesetzt wird

$$z = f(x, y)$$

und es ist f eine rationale Function in $k(i)$, deren Coefficienten von μ und ν, nicht aber von der Wahl der Wurzeln x, y abhängen

Der Körper der λ-Teilung ist daher gewiss im demjenigen Körper enthalten, welcher durch die Zusammensetzung der Körper der μ- und ν- Teilung entsteht.

Jeder Teilungskörper ist daher in einem aus einer Anzahl gewisser elementaren Körper des §. 6. zusammengesetzten Körper enthalten, ist also relativ Abel'sch in Bezug auf $k(i)$; desgleichen auch für jeden Unterkörper eines Teilungskörpers.

Nach Analogie des Hilbert'schen Kreiskörpers nenne ich einen *Lemniscatenkörper* einen jeden Teilungskörper und seinen Unterkörper wie sie im vorigen in Betracht gezogen wurden, sowie einen jeden aus solchen zusammengesetzten Körper.

§. 9.

Wir kommen nun an den Zielpunkt dieser Abhandlung; es handelt sich darum, nachzuweisen, dass

jeder im Bereich der rationalen complexen Zahlen Abel'sche Körper ein Lemniskatenkörper ist.

Da sich jeder Abel'sche Körper aus den cyclischen Körpern, deren Grad eine Primzahlpotenz ist, zusammensetzen lässt, genügt es zu beweisen, dass jeder relativcyclische Körper über $k(i)$, dessen Grad eine Primzahlpotenz ist, in einem aus den elementaren Lemniskatenkörpern des §. 6. zusammengesetzten Körper als Teiler enthalten ist.

Wir schicken die folgenden Hülfssätze voran:

1) Jeder im natürlichen Rationalitätsbereich Galois'sche Körper, welcher die Zahl i enthält, und in Bezug auf $k(i)$ relativ cyclisch ist, ist ein Kreiskörper.

Beweis. Es sei K ein solcher Körper, R derjenige Unterkörper von K, welcher aus allen in K enthaltenen reellen Zahlen besteht. Da K als ein im natürlichen Rationalitätsbereich Galois'scher Körper zu jeder seiner Zahlen die conjugirt complexe enthält, und da K ausserdem die Zahl i enthält, so muss K aus R und $k(i)$ zusammengesetzt sein.

Der Körper K kann daher durch eine Zahl $\theta = \rho + yi$ erzeugt werden, wenn ρ eine den Körper R erzeugende Zahl und y eine passend gewählte rationale Zahl bedeutet. Es sei G die Gruppe des Körpers K; dann hat G einen Teiler C vom Index 2, zu welchem die Zahl i gehört. Diese Untergruppe C muss aber cyclisch sein, da K relativcyclisch ist in Bezug auf $k(i)$. Durch die Substitutionen dieser Untergruppe gehe θ in $\theta', \theta'', \ldots$ und ρ in $\rho', \rho'' \ldots$ über. Ist sodann $\theta' = F(\theta)$ worin F eine rationale Function in $k(i)$ bedeutet, so ist

$$\rho' + yi = F(\rho + yi)$$

woraus dann folgt

$$\rho' = \Re F(\rho + yi) = \varphi(\rho)$$

worin $\Re$ für "reeller Teil von" steht. Da $\theta'' = F(\theta')$ so muss auch

$$\rho'' = \varphi(\rho')$$

sein; also ist R cyclisch im natürlichen Rationalitätsbereich, und folglich ist K ein Kreiskörper.

2) Durch Zusammensetzung zweier Abel'scher Körper entsteht wiederum ein Abel'scher Körper. Ist A ein Abel'scher Körper vom Grade $m=p^{h_1}\ p^{h_2}\ldots$, welcher aus den cyclischen Körpern C_1, $C_2,\ldots$ vom Grade p^{h_1}, $p^{h_2},\ldots$zusammengesetzt ist, B ein cyclischer Körper vom Grade $\varkappa=p^k$, wobei k keinen der Exponenten h_1, $h_2,\ldots$übertrifft, habe ferner A, B einen gemeinsamen Teiler vom Grade g, so kann der aus A und B zusammengesetzte Körper K auch aus A und einem zu A teilerfremden cyclischen Körper vom Grade $mn:g$ zusammengesetzt werden. Als Rationalitätsbereich wird hier jeder beliebige algebraische Körper vorausgesetzt.

Beweis. Es bedeute α, β, $\varkappa=x\alpha+y\beta$ resp. die den Körper A, B, K erzeugende Zahl. Da sowold α als auch β rational durch $\varkappa$, ausdrückbar sind, so ist, wenn $\varkappa'=x\alpha'+y\beta'$ eine zu $\varkappa$ conjugirte Zahl bedeutet, α' durch α, β' durch β folglich beide und daher auch $\varkappa'$ rational durch $\varkappa$ ausdrückbar. K ist daher gewiss ein Galois'scher Körper. Daher gibt es in der Gruppe G von K nur eine Substitution, die unter den conjugirten von α, und unter denjenigen ~~von β, eine~~ bestimmte Permutation hervorruft. Die Gesamtheit derjenigen Substitutionen von G, die die Zahl α ungeändert lassen, bildet einen Normalteiler S von G vom Grade $n:g$. Die complementäre Gruppe G/S ist aber mit der Gruppe des Körpers A isomorph, also Abel'sch. Dies besagt aber, dass, wenn σ, σ' zwei Substitutionen der Gruppe G sind, $\sigma\sigma'$ und $\sigma'\sigma$ dieselbe Permutation unter den conjugirten von α hervorrufen. Da dasselbe auch in Bezug auf β gelten muss, so rufen $\sigma\sigma'$ und $\sigma'\sigma$ dieselbe Permutation unter den conjugirten von β hervor. Es muss daher $\sigma\sigma'=\sigma'\sigma$; der Körper K ist in der Tat Abel'sch.

Um den zweiten Teil des Satzes zu beweisen, bemerken wir

zunächst, dass die Gruppe S cyclisch sein muss, weil der Körper B nach der Vorraussetzung cyclisch ist. Es sei uun α_1 eine den Körper C_1 erzeugende Zahl, $\alpha_1, \alpha_1', \ldots$ ihre conjugirten, ferner seien $\alpha_2, \alpha_2', \ldots; \alpha_3, \alpha_3', \ldots$; u.s.w. die entsprechenden Zahlen für $C_2, C_3, \ldots$ Unter den Substitutionen der Gruppe G, welche nicht in S enthalten sind, gibt es dann eine, die wir s_1 nennen wollen, welche α_1 zu α_1' überführt, $\alpha_2, \alpha_3, \ldots$ aber ungeändert lässt; in folge der über den Grad von B gemachten Annahme ist dann diese Substitution s_1 vom Grade p^{h_1}. Sind nun $s_2, s_3, \ldots$ ähnliche den Körpern $C_2, C_3, \ldots$ entsprechende Substitutionen, so sind $s_2, s_3, \ldots$ resp. vom Grade $p^{h_2}, p^{h_3}, \ldots$ Diese Substitutionen $s_1, s_2, \ldots$ erzeugen, eine mit der Gruppe von A isomorphe Untergruppe T von G, vom Grade m; und es ist $G = S.T$. Zu dieser Untergruppe T gehört ein Unterkörper D von K vom Grade $n:g$, und welcher zu A teilerfremd ist. Es ist daher $K = A.D$. Die Gruppe von D ist aber isomorph mit der complementären Gruppe G/T, daher auch mit S, woraus dann folgt, dass D cyclisch sein muss.

§ 10.

Wir können jetzt den folgenden Satz beweisen:

Es sei μ eine Primzahl des Körpers $k(i)$, m deren Norm, p^h die höchste Potenz einer natürlichen Primzahl p die in m-1 aufgeht. Jeder relativcyclische Körper Γ vom Relativgrade $p^{h'}$ $(h' \leqq h)$ dessen Relativdiscriminante keinen Primfactor ausser μ enthält, stimmt dann mit dem entsprechenden elementaren Lemniskatenkörper C überein, deren Existenz in §. 6. nachgewiesen wurde.

Beweis. Wäre Γ verschieden von C, so sei K der aus Γ und C zusammengesetzte Körper, dessen Relativgrad p^n gewiss zwischen $p^{h'}$ und $p^{2h'}$ liegt; K enthält keinen relativcyclischen Körper von

höherem als dem $p^{h'\text{ten}}$ Relativgrad als Teiler. Der Verzweigungskörper von μ in K ist K selbst, der Trägheitskörper genau vom Grade $p^{n-h'}$. Die Annahme $n>h'$ führt daher zu dem unzulässigen Resultat, dass es einen Relativkörper über $k(i)$ gibt mit der Relativdiscriminante 1. Es muss daher $n=h'$, d.h. $\Gamma=C$.

Dieser Satz gilt auch für $p=2$, wenn 2^h die höchste in $\frac{1}{4}(m-1)$ aufgehende Potenz von 2 ist.

Wenn die Zahl μ in dem obigen Satze reell ist, so ist der entsprechende Körper ein Kreiskörper.

Ist nämlich C' der in Bezug auf den natürlichen Rationalitätsbereich zu C conjugirte Körper, so ist C' auch relativcyclisch über $k(i)$ und hat dieselbe Relativdiscriminante wie C. Daher ist $C=C'$; d.h. C ist ein Galois'scher Körper im natürlichen Rationalitätsbereich, und folglich ein Kreiskörper nach dem Hülfssatz 1. des §. 9.

§. 11.

Es sei nun C_h ein relativcyclischer Körper vom Relativgrade p^h, wo p eine beliebige natürliche Primzahl bedeutet, C_k $(k \leqq h)$ der einzige in C_h enthaltene relativcyclische Körper vom Relativgrad p^k. Wir nehmen ferner an, dass die Relativdiscriminante von C_h eine zu p relativ prime Primzahl μ des Körpers $k(i)$ sei.

Wäre C_{h_0} der grösste in C_h enthaltene Kreiskörper, dessen Relativdiscriminante in Bezug auf $k(i)$ ausschliesslich den Factor p enthält, so bezeichnen wir mit E_h denjenigen Kreiskörper, welcher i enthält, relativcyclisch vom Relativgrade p^h in Bezug auf $k(i)$ ist, und dessen Relativdiscriminante eine Potenz von p ist. Der grösste gemeinsame Teiler von C_h und E_h ist C_{h_0}. Durch Zusammensetzung der beiden Körper C_h, E_h entsteht dann ein Körper K,

welcher auch aus E_h und einem zu E_h teilerfremden relativcyclischen Körper C^* vom Relativgrade p^{h-h_0} zusammengesetzt wird. Diesen letzten Körper nennen wir dann einfach C_h, seinen Relativgrad p^h. Die Relativdiscriminante dieses Körpers enthält jedenfalls den Factor μ.

Es sei nun ζ eine primitive $p^{h\text{te}}$ Einheitswurzel, der durch ζ und i erzeugte Körper Z ist relativcyclisch in Bezug auf $k(i)$. Die Relativgruppe von Z besteht aus den Potenzen der Substitutionen s, welche die Zahl ζ zu ζ^g überführt, wenn g für ungerades p eine Primitivzahl nach p^h, und für $p=2$, die Zahl 5 bedeutet.

Die beiden Körper C_h und Z haben nach dem obigen keinen gemeinsamen Teiler über $k(i)$. Durch ihre Zusammensetzung entsteht ein relativ Abel'scher Körper K, welcher auch dadurch aus Z hervorgeht, dass demselben die p^{te} Wurzel einer gewissen Zahl $\varkappa$ von Z adjungirt wird, welche der Bedingung genügt, dass

$$\varkappa \mid s = \varkappa^g \cdot a^{p^h}$$

wenn a eine Zahl des Körpers Z bedeutet.

Die Zahl $\varkappa$ kann nicht relativ prim zu μ sein; denn wäre $\varkappa$ relativ prim zu μ, so musste die Relativdiscriminante von K in Bezug auf Z, und folglich auch in Bezug auf $k(i)$ relativ prim zu μ sein, was zur Folge hätte, dass auch die Relativdiscriminante von C_h gegen die Voraussetzung relativ prim zu μ ist.

Es sei nun

$$\mu = \mathfrak{M}_1 . \mathfrak{M}_2 \ldots\ldots \mathfrak{M}_e$$

die Zerlegung in die Primideale von μ in Z, und

$$\varkappa = \mathfrak{M} . \mathfrak{K}$$

worin $\mathfrak{M}$ das Product aller in $\varkappa$ aufgehenden Potenzen von $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ bedeutet, und $\mathfrak{K}$ infolgedessen prim zu μ ist. Es ist dann

$$\zeta = \frac{\varkappa \mid s^e}{\varkappa} = \varkappa^{g^e-1}\beta^{p^h}$$

eine zu μ fremde Zahl. Ist $p^{h'}$ die höchste Potenz von p, die in g^e-1 aufgeht, so bestimmt die Zahl $\sqrt[p^h]{\zeta}$ einen Unterkörper von K, welcher nichts anders ist, als der aus $C_{h-h'}$ und Z zusammengesetzte Körper. Es folgt dann, dass die Relativdiscriminante von $C_{h-h'}$ prim zu μ ist.

Ist anderseits m die Norm von μ und p^a die höchste Potenz von p, die in $m-1$ aufgeht, so wird

$$m^{p^{h-a}} = 1 \qquad (mod.\ p^h)$$

und p^{h-a} ist zugleich der kleinste Expotent, für den diese Congruenz bestehen kann. Dann zerfällt die Zahl μ in $e=p^{a-1}(p-1)$ von einander verschiedene Primideale in Z; und zugleich ist p^a die höchste Potenz von p, die in g^e-1 aufgeht. Es ist also $a=h'$, und wir schliessen:[1]

Damit μ in der Relativdiscriminante von C_k als Factor auftreten kann, ist es notwendig, dass

$$m \equiv 1 \qquad (mod.\ p^{h-k+1})$$

Sollte daher die Zahl μ überhaupt in der Relativdiscriminante von C_h auftreten können, so muss $m-1$ durch p teilbar sein; sollte μ schon in der Relativdiscriminante von C_1 auftreten, so muss $m \equiv 1$, mod p^h.

§. 12.

Trete die Zahl μ in der Relativdiscriminante von C_1 auf, sodass

1) Dies ist die Verallgemeinerung des Hilbert'schen Satzes (l.c. S. 342.) in etwas schärferer Fassung. Hierzu ist zu vgl.: A. Wiman, zur Theorie der relativabelschen Zahlkörper, Acta Univ. Lundensis 36. welche Abhandlung mir nur dem Berichte in den "Fortschritte der Mathematik (Jahrgang 1900) nach bekannt ist.

$m \equiv 1$ mod. p^h, so sei M derjenige relativcyclische Körper vom Relativgrade p^h, dessen Relativdiscriminante ausschliesslich den Primfactor μ enthält. Möglicherweise haben dann C_h und M einen gemeinsamen Teiler ausser $k(i)$. Der zusammengesetzte Körper $C_h M$. ist dann relativ Abel'sch vom Relativgrade $p^{h+h'}$ $(h' \leqq h)$ in Bezug auf $k(i)$. Seine Relativgruppe G ist von der Form

$$s^\lambda t^\mu, \quad \left(\begin{array}{l} \lambda = 0, 1, \ldots\ldots p^h - 1 \,; \quad s^{p^h} = 1 \\ \mu = 0, 1, \ldots\ldots p^{h'} - 1 \,; \quad t^{p^{h'}} = 1 \end{array} \right)$$

Die Trägkeitsgruppe T der Zahl μ in $C_h M$ ist cyclisch und vom Grade p^h ; T besteht daher aus den Potenzen einer Substituion st^ν. Der Trägheitskörper ist vom Relativgrade $p^{h'}$; die Gruppe desselben ist isomorph mit der complementären Gruppe G/T, und daher cyclisch. Der Trägheitskörper ist demnach relativcyclisch in Bezug auf $k(i)$, wir nennen ihn $C'_{h'}$. Dieser hat keinen Teiler ausser $k(i)$ mit M gemein. Daher ist

$$C_h M = C'_{h'} M \,;$$

die Relativdiscriminante von $C'_{h'}$ enthält alle in der Relativdiscriminante von C_h auftretenden Primfactoren mit Ausnahme der Zahl μ.

Wir nehmen jetzt allgemein an, die Zahl μ trete erst in der Relativdiscriminante von C_{k+1} auf, sodass $m \equiv 1$ mod. p^{h-k}. Es existirt daher ein relativcyclischer Körper M vom Relativgrade p^{h-k}, dessen Relativdiscriminante eine Potenz von μ ist. Nach dem vorhin gesagten, können wir nun annehmen, dass C_h und M keinen gemeinsamen Teiler ausser $k(i)$ besitzen. Der zusammengesetzte Körper MC_h ist dann relativ Abel'sch vom Relativgrade p^{2h-k}, die Relativgruppe G desselben von der Form

$$s^{\lambda}\, t^{\mu}, \quad \begin{pmatrix} \lambda=0,\ 1,\ 2,\ldots\ldots p^{h}-1\,; & s^{p^{h}} & =1. \\ \mu=0,\ 1,\ 2,\ldots\ldots p^{h-k}-1\,; & t^{p^{h-k}} & =1. \end{pmatrix}$$

worin s, t resp. die Substitutionen bedeuten, welche den Körper M, C_h ungeändert lassen. Dann gehört der Unterkörper C_k zu der Untergruppe G' von der Form

$$s^{*\lambda}\, t^{\mu}, \quad \begin{pmatrix} \lambda,\ \mu=0,\ 1,\ldots\ldots p^{h-k}-1. \\ s^{*}=s^{p^{k}} \end{pmatrix}$$

Nimmt man daher C_k zum Rationalitätsbereich, so wird G' die Relativgruppe von MC_h in diesem Rationalitätsbereich.

In C_k zerfalle μ in eine Anzahl von einander verschiedener Primideale, etwa $\mu=\mathfrak{M}\mathfrak{M}'\ldots\ldots$ Ist nun $\mathfrak{M}^*$ das Primideal des Körpers MC_h, welches in $\mathfrak{M}$ aufgeht, so muss $\mathfrak{M}^*$ wenigstens zur p^{h-k}ten Potenz in $\mathfrak{M}$ enthalten sein ; die Trägheitsgruppe von $\mathfrak{M}$ in dem Relativkörper MC_h muss daher wenigstens vom Grade p^{h-k} sein. Die Verzweigungsgruppe von $\mathfrak{M}$ ist aber eine Einheitsgruppe. Daher muss die Trägheitsgruppe von $\mathfrak{M}$ cyclisch sein, und da es in G' keinen cyclischen Teiler von einem höheren als p^{h-k}ten Grade gibt, so muss die Trägheitsgruppe von $\mathfrak{M}$ genau vom Grade p^{h-k} sein. Daraus folgt, dass $\mathfrak{M}^*$ genau zu der p^{h-k}ten Potenz in $\mathfrak{M}$ und folglich in μ enthalten sein muss.

Wir kehren nun zu dem ursprünglichen Rationalitätsbereich $k(i)$ zurück. Die Trägheitsgruppe T von $\mathfrak{M}^*$ ist cyclisch und vom Grade p^{h-k}, der Trägheitskörper C'_h von $\mathfrak{M}^*$ ist vom Relativgrade p^h, und es ist $MC_h=MC'_h$. Die Gruppe T besteht daher aus den Potenzen einer Substitution von der Form $s^a t$. Die Gruppe des Körpers C'_h, isomorph mit G/T, ist also cyclisch, sodass C'_h relativcyclisch in Bezug auf $k(i)$ ist. Die Relativdiscriminante von C'_h enthält alle in derjenigen von C_h auftretenden Primfactoren mit Ausnahme der Zahl μ.

Wir operiren sodann in ähnlicher Weise mit dem Körper C', falls die Relativdiscriminante desselben noch eine zu p prime Primzahl μ' enthält, und erhalten dann einen Körpes C'', dessen Relativdiscriminante alle in derjenigen von C vorkommenden Primfactoren enthält mit Ausnahme der Zahlen μ, μ'.

Fahren wir aber in dieser Weise fort, so gelangen wir schliesslich zu einem relativcyclischen Körper C^* vom Relativgrade p^{h^*} $(h^* \leqq h)$ dessen Relativdiscriminante nur noch die in p aufgehenden Primzahlen des Körpers $k(i)$ enthält.

Es handelt sich hiernach nur noch darum, unseren Hauptsatz für einen solchen Körper zu beweisen.

§. 13.

Jeder relativ cyclische Körper von Relativgrade p, dessen Relativdiscriminante eine Potenz von π ist, stimmt mit dem entsprechenden elementaren Lemniskatenkörper überein, deren Existenz in §. 6. *nachgewiesen wurde;* hierin bedeutet p eine natürliche Primzahl von der Form $4h+1$, und π einen Primfactor von p in $k(i)$

Beweis. Gebe es zwei verschiedene Körper C, C' von der angegebenen Beschaffenheit, so entsteht durch ihre Zusammensetzung und die Adjunction einer primitiven p^{ten} Einheitswurzel ζ ein Körper K vom Relativgrad $p^2(p-1)$.

In dem durch ζ und i erzeugten Körper Z zerfällt p in $2(p-1)$ Primideale ersten Grades

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

und es ist

$$p=\pi\pi'\,; \quad \pi=\mathfrak{p}^{p-1}, \quad \pi'=\mathfrak{p}'^{p-1} \quad (\eta)=(1-\zeta)=\mathfrak{p}\mathfrak{p}'$$

Der Körper $k(C, \zeta)$ geht dadurch aus Z hervor, dass man diesem

letzteren die $p$te Wurzel einer Zahl $\varkappa$ von Z adjungirt. Diese Zahl $\varkappa$ genügt der bekannten Bedingung[1])

$$\varkappa \mid s = \varkappa^{g} . \alpha^{p}$$

Wir können aber $\varkappa$ so wählen, dass $\varkappa \equiv 1 \pmod{\mathfrak{p}}$ wird; denn leistet $\varkappa$ dieser Bedingung nicht Genüge, so können wir statt $\varkappa$ eine Zahl $\varkappa^*$ von der Form

$$\varkappa^* = \alpha^{p(p-1)} \left(\frac{\varkappa \mid s}{\varkappa} \right)^{p-1}$$

nehmen, wobei wir die natürliche ganze Zahl a passend wählen, und erhalten in $\varkappa^*$ eine ganze Zahl, der die Eigenschaft zukommt, dass

$$(c) \qquad \varkappa^* \mid s = \varkappa^{*g-1} \alpha^{*p},$$

$$k(C, \zeta) = k(\zeta, \sqrt[p]{\varkappa^*}) \qquad \varkappa^* \equiv 1 \qquad (mod.\ \mathfrak{p})$$

Da nun $\mathfrak{p}$ ein Primideal ersten Grades ist, auch in Bezug auf den natürlichen Rationalitätsbereich, so wird die Congruenz

$$\varkappa^* \equiv 1 + a\eta \qquad (mod.\ \mathfrak{p}^2)$$

$$(\eta = 1 - \zeta)$$

durch eine natürliche ganze Zahl a befriedigt. Hierbei kann aber nicht $a \equiv 0 \pmod{p}$ sein. Wäre nämlich a durch p teilbar, so wird $\varkappa^* \equiv 1 \pmod{\mathfrak{p}^2}$, woraus mit Hülfe von (c) folgt

$$\varkappa^* \equiv 1 \qquad (mod.\ \mathfrak{p}^{\nu})$$

Ist nun ν eine durch $\mathfrak{p}'$ aber nicht durch $\mathfrak{p}$ teilbare ganze Zahl des Körpers Z, so ist die Zahl

$$\omega = \frac{\nu}{\eta}(1 - \sqrt[p]{\varkappa^*})$$

welche der Gleichung $(\lambda\omega - \nu)^p + \nu^p \varkappa^* = 0$ genügt, eine ganze Zahl.

1) Vgl. z. B. Hilbert, l.c.

Die Zahl ω erzeugt aber offenbar den Körper $k(C, \zeta)$. Die Relativdiscriminante dieser Zahl in Bezug auf Z ist $\nu^{p(p-1)}\,\varkappa^{*p-1}$, also prim zu $\mathfrak{p}$. Daher muss die Relativdiscriminante von $k(C, \zeta)$ in Bezug auf Z auch prim zu $\mathfrak{p}$ sein. Bedeutet nun $\mathfrak{P}$ ein Primideal des Körpers $k(C, \zeta)$, welches in $\mathfrak{p}$ aufgeht, so geht $\mathfrak{P}$ nur zu der $p-1^{\text{ten}}$ Potenz in π auf. Der Trägheitskörper von π ist dann vom Relativgrade p in Bezug auf $k(i)$, und seine Relativdiscriminante muss 1 sein, was aber unmöglich ist. Es ist daher

$$\varkappa^* = 1 + a\eta \quad (mod.\ \mathfrak{p}^2), \quad a \not\equiv o \quad (mod.\ p)$$

Genau dieselbe Erwägungen führen uns zu dem Resultat:

$$k\,(C', \zeta) = k\,(\zeta, \sqrt[p]{\rho})$$

mit $$\rho \equiv 1 + b\,\eta \quad (mod.\ \mathfrak{p}^2)$$

wo $$b \not\equiv 0 \quad (mod.\ p)$$

Bestimmt man nun die natürliche ganze Zahl c aus der Congruenz

$$a + bc \equiv 0 \quad (mod.\ p)$$

so folgt

$$\theta = \varkappa^*.\ \rho^c \equiv 1 \quad (mod.\ \mathfrak{p}^2)$$

und es ist

$$\theta \mid s = \theta^{g-1}.\ \gamma^p$$

Wäre also $C \neq C'$ so würde θ gewiss nicht eine $p$te Potenz in Z sein. Da aber $k(\zeta, \sqrt[p]{\theta})$ gewiss in $K = k(C, C', \zeta)$ enthalten ist, würde die Conruenz $\theta \equiv 1$ $(\mathfrak{p}^2)$ genau wie vorher zu einem unzulässsigen Resultat führen. Demnach muss, wie bewiesen werden sollte,

$$C = C'.$$

Jeder relativcyclische Körper vom Relativgrad p^h, dessen Relativ-

discriminante eine Potenz von π ist, stimmt mit dem entsprechenden elementaren Körper des §. 6. *überein.*

Um den Satz durch vollständige Induction zu beweisen, nehmen wir ihn als bewiesen an, für alle kleinere Werte von h. Sind sodann C, C' zwei verschiedene Körper von der angegebenen Beschaffenheit, so müssen die in ihnen enthaltenen relativcyclischen Körper vom Relativgrad p^{h-1} auf Grund der Voraussetzung mit einander übereinstimmen. Durch Zusammensetzung entsteht daher aus C, C' ein Körper K vom Relativgrad p^{h+1}, welcher auch aus C, und einem zu C teilerfremden relativcyclischen Körper C_1 vom Relativgrad p zusammengesetzt werden kann. Da aber die Relativdiscriminante von C_1 nur den Primfactor π enthalten kann, und da C_1 nicht in C enthalten sein soll, so musste die Relativdiscriminante von C_1 gleich 1 sein, was unmöglich ist.

Die beiden elementaren Körper vom Relativgrade p^h, deren Relativdiscriminante resp. eine Potenz von π und π' sind bezeichnen wir bez. mit Π_h und Π'_h. Durch die Zusammensetzung der beiden entsteht ein relativ Abel'scher Körper P_h vom Relativgrade p^{2h}; in demselben sind enthalten als Teiler die p^h+1 von einander verschiedenen relativcyclischen Körper vom Relativgrad p^h, deren Relativdiscriminante ausschliesslich die Primzahlen π, π' enthalten. Es ist jetzt zu beweisen, dass es ausser diesen keinen Körper von dieser Beschaffenheit gibt.

Es wird genügen, den Satz nur für den Fall, wo $h=1$, zu beweisen; das übrige folgt unmittelbar durch die vollständige Induction.

Es sei also C ein relativcyclischer Körper vom Relativgrad p, dessen Relativdiscriminante ausschliesslich die Primzahlen π, π' enthält,

ζ wie vorher eine primitive p^{te} Einheitswurzel, $\mathfrak{p}$, $\mathfrak{p}'$ die beiden von einander verschiedenen Primideale des Körpers $Z=k(\zeta, i)$, die in p aufgehen.

Wir betrachten nun die Zahl $\varkappa$, welche in der bekannten Weise den Körper CZ erzeugt. Wir nehmen wie vorher an, es sei

$$\varkappa \equiv 1 + a\eta \quad (mod.\ \mathfrak{p}^2)$$

$$a \not\equiv 0 \quad (mod.\ p)$$

sodass

$$\rho = \zeta^{-a}\varkappa \equiv 1 \quad (mod.\ \mathfrak{p}^2)$$

Bezeichnen wir nun die Körper $k(C, \sqrt[p]{\zeta})$, $k(\zeta, \sqrt[p]{\rho})$ bez. mit K, K', so ist K' gewiss in K enthalten. Die Relativdiscriminante von K' in Bezug auf Z ist aber prim zu $\mathfrak{p}$, sie muss daher ausschliesslich den Primteiler $\mathfrak{p}'$ enthalten, sodass $K=k(Z, \Pi_1')$ sein muss. Ähnlicherweise enthält K auch den Körper $Z\Pi_1$ als Teiler. Daher ist

$$K = Z.\ P_1$$

woraus dann folgt, dass in der That C in P_1 enthalten sein muss, q. e. d.

§. 14.

Wir haben gesehen, dass es q^h+1 von einander verschiedene relativcyclische Körper vom Relativgrade q^h gibt, deren Relativdiscriminanten ausschliesslich den Primfactor q enthalten, dass diese q^h+1 Körper Teiler eines relativ Abelschen Körpers Q_h vom Relativgrad q^{2h} sind; hierbei bedendet q eine natürliche Primzahl von der Form $4h+3$, sodass q eine Primzahl zweiten Grades in $k(i)$ ist.

Wir wollen jetzt zeigen, dass es ausser diesen keinen anderen Körper von der angegebenen Beschaffenheit gibt; begnügen uns aber auch hier den Satz nur für den Fall, wo $h=1$ ist, zu beweisen.

Da es nur einen Kreiskörper gibt, welcher relativcyclish über $k(i)$ vom Relativgrade q ist, und dessen Relativdiscriminante nur den Primfactor q enthält, nämlich denjenigen, welcher in dem durch i und eine primitive q^2te Einheitswurzel erzeugten Körper enthalten ist, so sind wir sicher, dass es einen Körper C von der angegebenen Beschaffenheit gibt, der kein Kreiskörper ist, und infolgedessen von dem in Bezug auf den natürlichen Rationalitätsbereich zu C conjugirten Körper C' verschieden ist (§. 8), so-dass $CC'=Q_1$. Der Körper Q_1 enthält aber den oben erwähnten Kreiskörper als Teiler; bedeutet daher ζ eine primitive q^{te} Einheitswurzel, so wird $k(Q_1, \zeta)=k(C, \sqrt[q]{\zeta})$ sein. Gebe es nun einen Körper $\bar{C}$ von der angegebenen Beschaffenheit, der jedoch nicht in Q_1 enthalten ist, so entsteht durch Composition ein relativ Abel'scher Körper $k(Q_1, \bar{C}, \zeta)=k(C, \bar{C}, \sqrt[q]{\zeta})$ vom Relativgrad $q^3(q-1)$.

Bezeichnen wir nun mit Z den durch i und ζ erzeugten Körper, so ist die Zahl q die $(q-1)^{te}$ Potenz eines Primideals $\mathfrak{q}$ in Z, welches vom zweiten Grade in Bezug auf den natürlichen Rationalitätsbereich, aber vom ersten in Bezug auf $k(i)$ ist; es ist ferner $\mathfrak{q}$ das durch die Zahl $\eta=1-\zeta$ erzeugte Hauptideal.

Wir denken uns nun die Zahlen $\varkappa$, θ wie im vorigen Paragraphen aufgestellt, sodass

$$k(\zeta, C)=k(\zeta, \sqrt[q]{\varkappa}); \quad \varkappa \mid s=\varkappa^{g-1}\alpha^q; \quad \varkappa\equiv 1\ (\mathfrak{q}) \not\equiv 1\ (\mathfrak{q}^2)$$

$$k(\zeta, \bar{C})=k(\zeta, \sqrt[q]{\theta}); \quad \theta \mid s=\theta^{g-1}\beta^q; \quad \theta\equiv 1\ (\mathfrak{q}) \not\equiv 1\ (\mathfrak{q}^2)$$

Da $\mathfrak{q}$ ein Primideal ersten Grades in Bezug auf $k(i)$ ist, so können wir zwei nicht durch q teilbare ganze Zahlen des Körpers $k(i)$ finden, sodass

$$\varkappa\equiv 1+(a+b\,i)\eta \quad (mod.\ \mathfrak{q}^2)$$

$$\theta\equiv 1+(a'+b'i)\eta \quad (mod.\ \mathfrak{q}^2)$$

Nehmen wir noch die Congruenz zu Hülfe

$$\zeta^r \equiv 1 - r\eta \qquad (mod.\ \mathfrak{q}^2)$$

und setzen

$$\rho = \zeta^r \varkappa.\ \theta^c \equiv 1 + (u + iv)\eta \qquad (mod.\ \mathfrak{q}^2)$$

so ist

$$u = a + ca' - r, \quad v = b + cb'.$$

Man kann nun die natürlichen ganzen Zahlen c, r so bestimmen, dass

$$u \equiv 0, \quad v \equiv 0 \quad (mod.\ q)$$

wird. Dann ist

$$\rho \equiv 1 \qquad (mod.\ \mathfrak{q}^2)$$

wir können nun genau in derselben Weise fortfahren wie im vorigen Paragraphen, um nuns zu überzeugen, dass der Körper $\overline{C}$ in der Tat in Q_1 enthalten ist.

§. 15.

Um endlich den entsprechenden Satz für den Fall zu beweisen, wo der Relativgrad eine Potenz von 2, und die Relativdiscriminante eine Potenz von $1+i$ ist, betrachten wir den relativ Abel'schen Körper D_1 vom Relativgrad 4, welcher aus der Teilung der Periode von $\wp(u)$ durch $(1+i)^7$ entspringt. Dieser Körper ist durch die Zahl y erzeugt, welche der Gleichung genügt:

$$y^2 - 2ixy - 1 = 0$$

$$(x^2 - 2x - 1 = 0)$$

Es ist aber

$$D_1 = k(y) = k(\sqrt{x}, i) \qquad x = 1 \pm \sqrt{2}$$

Setzt man nun

$$\alpha=\sqrt{2}+1 \qquad \beta=\sqrt{2}-1$$

so wird

$$2(1\pm i)=(\sqrt{\alpha}\pm i\sqrt{\beta})^2$$

D_1 enthält daher $\sqrt{1+i}$, $\sqrt{1-i}$, und demnach auch $\sqrt{i}$, Die drei in D_1 enthaltenen relativ quadratischen Körper, sind $k(\sqrt{1+i})$, $k(\sqrt{1-i})$ und $k(\sqrt{i})$

Anderseits leuchtet ein, dass es ausser diesen, keinen relativ quadratischen Körper gibt dessen Relativdiscriminante eine Potenz von $1+i$ ist.

Hieraus schliesst man durch vollständige Induction, dass es ausser den in §. 6. (5) angegebenen, keinen anderen Körper ihrer Art gibt.

Göttingen, im Frühjahr, 1901.