THEORIE DER ABEL'SCHEN ZAHLKÖRPER

VON

H. WEBER

in MARBURG.

IV. ÜBER DIE BILDUNG ABEL'SCHER KÖRPER MIT GEGEBENER GRUPPE.

In den drei vorangegangenen, die Abel'schen Zahlkörper betreffenden Arbeiten (Acta Mathematica, Bd. 8) ist die Identität des Begriffs der Abel'schen mit den Kreiskörpern nachgewiesen, und damit zugleich die Theorie aller Abel'schen Zahlkörper auf die allgemeine Theorie der Kreisteilungsperioden zurückgeführt.

Eine tiefer greifende Einteilung der Abel'schen Körper wird sich, wie bei algebraischen Fragen überhaupt, auf die Beschaffenheit der Gruppe zu gründen haben. Die Constitution einer Abel'schen Gruppe kann aber, wie zunächst gezeigt werden wird, vollständig charakterisiert werden durch eine gewisse Reihe ganzer Zahlen, die *Gruppeninvarianten,* und indem wir die Gruppe als durch ihre Invarianten definiert annehmen, stellen wir die Aufgabe

I. *Alle Abel'schen Körper von gegebener Gruppe zu bestimmen.*

Nach den Ergebnissen der vorangegangenen Arbeiten (I, § 5) hat man hierzu nur nöthig, *Kreisteilungsperioden* mit gewissen vorgeschriebenen Eigenschaften zu bilden.

Es ist aber bereits in der Abhandlung I, § 4, darauf hingewiesen, dass ein und derselbe Abel'sche Körper in *mehreren* vollständigen Kreiskörpern enthalten ist, d. h. durch Einheitswurzeln *verschiedener* Grade dargestellt werden kann, und hiernach muss die Aufgabe I noch dahin ergänzt werden

II. *Abel'sche Körper von beliebig gegebener Gruppe durch Einheitswurzeln möglichst niedrigen Grades darzustellen.*[1]

§ 1. *Die Gruppeninvarianten.*

Es ist, wie schon in der Abhandlung I, § 1, erwähnt, eine fundamentale Eigenschaft Abel'scher Gruppen, durch eine Basis darstellbar zu sein, und man kann die Elemente $g_1, g_2, \ldots, g_\nu$ einer solchen Basis so auswählen und anordnen, dass von den Graden $e_1, e_2, \ldots, e_\nu$ dieser Elemente jeder durch den folgenden teilbar ist. Die Bestimmung einer solchen Basis ist auf mehrfache Art möglich; wie diese aber auch gewählt sein mag, die *Zahlen* $e_1, e_2, \ldots, e_\nu$, *deren Product* e *gleich dem*

---

[1] Die Aufgabe I ist für Abel'sche Körper mit *regulärer Gruppe* (einfache Abel'sche Körper) von KRONECKER im Monatsbericht der Berliner Akademie vom 14ten April 1856 behandelt. (Vgl. auch den IIIten Brief in dem in den Göttinger Nachrichten vom 16ten Dez. 1885 veröffentlichten Briefwechsel zwischen DIRICHLET und KRONECKER.) Das dortige Resultat bedarf einer kleinen Ergänzung, in so fern, wenn man nach KRONECKER's Vorschrift verfährt, noch Perioden erhalten werden, welche einen verschwindenden Wert haben. Nimmt man z. B. $n = 6$, $m = 63$, $p_1 = 3$, $p_2 = 7$, $b_1 = 3$, $b_2 = 1$, so erhält man nach Formel II der KRONECKER'schen Abhandlung, wenn ρ eine primitive 63^{te} Einheitswurzel bedeutet, $\tilde{\omega}(\rho) = \rho + \rho^{22} + \rho^{43} + \rho^{-1} + \rho^{-22} + \rho^{-43}$, was den Wert 0 hat. Dies rührt daher, dass p_1 ein mehrfacher Factor von m und zugleich ein Teiler von b_1 ist. Um die Bedeutung unserer Forderung II gleich hier durch ein einfaches Beispiel ins Licht zu setzen, nehmen wir $n = 3$, $m = 35 = 5 \cdot 7$, woraus sich, wenn ρ eine primitive 35^{te} Einheitswurzel bedeutet, die Periode

$$\tilde{\omega}(\rho) = \rho + \rho^{8} + \rho^{22} + \rho^{29} + \rho^{-1} + \rho^{-8} + \rho^{-22} + \rho^{-29}$$

ergiebt, welche aber $= -(\rho^{15} + \rho^{-15})$ ist und also schon unter den Perioden der 7^{ten} Einheitswurzeln vorkommt. Etwas anders verhalten sich wieder die 91^{ten} Einheitswurzeln. Denn während man aus 35^{ten} Einheitswurzeln überhaupt keine Perioden bilden kann, welche die Wurzeln cubischer Gleichungen sind, die nicht bereits unter den Perioden der 7^{ten} Einheitswurzeln vorkommen, ist dies bei den 91^{ten} Einheitswurzeln möglich, während andere wieder bereits unter den Perioden der 7^{ten} oder der 13^{ten} Einheitswurzeln vorkommen. Dieser Unterschied beruht darauf, dass alle Primfactoren von 91 nach dem Modul 3 mit 1 congruent sind, was bei 35 nicht der Fall ist.

Grade der Gruppe ist, sind immer dieselben und werden daher nicht unpassend die *Invarianten der Gruppe genannt.* [1]

Es soll hier eine Eigenschaft dieser Zahlenreihe nachgewiesen werden, welche die erwähnte Invarianz in sich schliesst, aber noch schärfer die fundamentale Bedeutung dieser Zahlen, oder genauer gesagt der in ihnen enthaltenen Primzahlpotenzen hervortreten lässt.

Sind $p_1, p_2, \ldots, p_\nu$ *die höchsten Potenzen einer Primzahl* p, *welche in* $e_1, e_2, \ldots, e_\nu$ *enthalten sind, so sind unter den Gradzahlen der Elemente einer beliebigen Basis der Gruppe immer* ν *solche enthalten, welche durch* $p_1, p_2, \ldots, p_\nu$, *aber durch keine höhere Potenz von* p *teilbar sind, während die Gradzahlen der übrigen Elemente der Basis (falls solche vorhanden) durch* p *unteilbar sind.*

Wir können diesem Satz, ohne seinen Inhalt zu ändern, eine etwas weitere Fassung geben, welche zugleich den Beweis vereinfacht. Es seien

$$a_1, a_2, \ldots, a_\nu$$

mit den Graden

$$\alpha_1, \alpha_2, \ldots, \alpha_\nu$$

und

$$b_1, b_2, \ldots, b_\mu$$

mit den Graden

$$\beta_1, \beta_2, \ldots, \beta_\mu$$

irgend zwei Basen einer Gruppe $\mathfrak{A}$, so dass alle Elemente a der Gruppe $\mathfrak{A}$, und jedes nur einmal, dargestellt wird, wenn man in einem der beiden Ausdrücke

$$(1) \qquad a = a_1^{x_1} a_2^{x_2} \ldots a_\nu^{x_\nu}$$

$$(2) \qquad a = b_1^{y_1} b_2^{y_2} \ldots b_\mu^{y_\mu}$$

die Exponenten x_h je ein vollständiges Restsystem modulo α_h oder die Exponenten y_h ein solches modulo β_h durchlaufen lässt.

[1] Diese Bezeichnung ist zuerst gebraucht in der Abhandlung von FROBENIUS und STICKELBERGER, *Über Gruppen vertauschbarer Elemente,* (CRELLE's Journal, Bd. 86, § 7), woselbst sich zwei Beweise für den Satz finden. Im übrigen sind noch zu erwähnen SCHERING, *Die Fundamentalclassen der zusammensetzbaren arithmetischen Formen,* Abhandlungen der Gesellschaft der Wissenschaften zu Göttingen, Bd. 14; KRONECKER, Monatsbericht der Berliner Akademie 1 Dez. 1870; WEBER, *Beweis des Satzes etc.*, Mathematische Annalen, Bd. 20, S. 301.

Ist nun p eine im Grade von $\mathfrak{A}$ aufgehende Primzahl und

$$\alpha_1 = p_1\alpha_1', \qquad \alpha_2 = p_2\alpha_2', \quad \ldots, \quad \alpha_\nu = p_\nu\alpha_\nu' \tag{3}$$

$$\beta_1 = p_1'\beta_1', \qquad \beta_2 = p_2'\beta_2', \quad \ldots, \quad \beta_\mu = p_\mu'\beta_\mu' \tag{4}$$

worin die p_h, p_h' Potenzen von p und α_h', β_h' durch p unteilbar sind, so sind diejenigen unter den $p_1, p_2, \ldots, p_\nu$, welche grösser als 1 sind, auch unter den $p_1', p_2', \ldots, p_\mu'$ enthalten und umgekehrt.

Beim Beweis dieses Satzes setzen wir die Anordnung der Elemente $a_1, a_2, \ldots, a_\nu; b_1, b_2, \ldots, b_\mu$ so voraus, dass

$$p_1 \geqq p_2 \geqq \cdots \geqq p_\nu$$

$$p_1' \geqq p_2' \geqq \cdots \geqq p_\mu'.$$

Ist α das kleinste gemeinschaftliche Multiplum von $\alpha_1', \alpha_2', \ldots, \alpha_\nu'$, so ist für alle Elemente a der Gruppe $\mathfrak{A}$

$$a^{\alpha p_1} = 1$$

woraus hervorgeht, dass αp_1 durch jede der Zahlen $\beta_1, \beta_2, \ldots, \beta_\mu$ teilbar ist. Es ist also p_1 teilbar durch p_1' und α durch das kleinste gemeinschaftliche Vielfache von $\beta_1', \beta_2', \ldots, \beta_\mu'$. Da nun in diesem Schluss die a_h mit den b_h vertauscht werden können, so folgt, dass α zugleich das kleinste gemeinschaftliche Vielfache von $\beta_1', \beta_2', \ldots, \beta_\mu'$ ist und dass ausserdem

$$p_1 = p_1'. \tag{5}$$

Wir setzen nun voraus, es sei für irgend eine Zahl s bewiesen

$$p_1 = p_1', \qquad p_2 = p_2', \quad \ldots, \quad p_{s-1} = p_{s-1}', \tag{6}$$

und bestimmen die Anzahl aller von einander verschiedenen in der Form $a^{\alpha p_s}$ enthaltenen Elemente der Gruppe a. Die Darstellung (1) liefert uns

$$a^{\alpha p_s} = a_1^{x_1 \alpha p_s} a_2^{x_2 \alpha p_s} \ldots a_{s-1}^{x_{s-1} \alpha p_s}, \tag{7}$$

woraus sich für die Anzahl der verschiedenen unter diesen Elementen

$$\frac{p_1}{p_s}\cdot\frac{p_2}{p_s}\cdots\frac{p_{s-1}}{p_s} \tag{8}$$

ergiebt. Ebenso gross ist aber auch nach unserer Voraussetzung die Anzahl der von einander verschiedenen in der Form

$$b_1^{y_1 a_{p_s}} b_2^{y_2 a_{p_s}} \cdots b_{s-1}^{y_{s-1} a_{p_s}} \tag{9}$$

enthaltenen Elemente, und daher müssen (nach der Darstellung (2)) alle Elemente von der Form

$$a^{a_{p_s}} = b_1^{y_1 a_{p_s}} b_2^{y_2 a_{p_s}} \cdots b_\mu^{y_\mu a_{p_s}}$$

in der Form (9) enthalten sein. Also muss, wegen der Fundamentaleigenschaft der Basis, p_s teilbar sein durch p_s'. Da man aber wieder ebenso den umgekehrten Schluss machen kann, so folgt

$$p_s = p_s', \tag{10}$$

womit unser Satz bewiesen ist.

Wie man also auch die Abel'sche Gruppe durch eine Basis darstellen mag, die Gradzahlen der Elemente dieser Basis sind stets aus denselben Primzahlpotenzen zusammengesetzt. Man kann die Basis unter anderen auch so wählen, dass die Grade ihrer Elemente diese Primzahlpotenzen selbst sind.

Um die Gruppeninvarianten zu erhalten ordnet man die Potenzen der verschiedenen Primzahlen in absteigender Reihe nach der Höhe des Exponenten und multipliciert dann die entsprechenden Glieder dieser Reihen, wobei man, um Reihen von gleicher Gliederzahl zu erhalten, die 1 zu Hülfe nehmen muss. Diese Zusammenfassung der Primzahlpotenzen ist nicht sehr wesentlich, soll aber zur Vereinfachung der Darstellung hier beibehalten werden.

Da in der Reihe der Gruppeninvarianten

$$e_1,\ e_2,\ \ldots,\ e_\nu$$

jede Zahl durch die folgende teilbar ist, so sind die Quotienten

$$\frac{e_1}{e_2} = \delta_1, \qquad \frac{e_2}{e_3} = \delta_2, \quad \ldots, \quad \frac{e_{\nu-1}}{e_\nu} = \delta_{\nu-1}, \qquad e_\nu = \delta_\nu \tag{11}$$

ganze Zahlen, aus denen sich die Gruppeninvarianten $e_1, e_2, \ldots, e_\nu$ und der Grad e der Gruppe in folgender Weise zusammensetzen

$$
\begin{aligned}
e_1 &= \delta_1\delta_2\delta_3\ldots\delta_\nu \\
e_2 &= \quad \delta_2\delta_3\ldots\delta_\nu \\
&\ldots\ldots\ldots\ldots \\
e_{\nu-1} &= \quad\quad \delta_{\nu-1}\delta_\nu \\
e_\nu &= \quad\quad\quad \delta_\nu
\end{aligned}
\tag{12}
$$

$$
e = \delta_1\delta_2^2\delta_3^3\ldots\delta_\nu^\nu. \tag{13}
$$

Die Zahlen δ sind ebenso wie die Zahlen e nur von der Natur der Gruppe abhängig und haben vor letzteren noch den Vorzug, dass sie keiner Beschränkung unterworfen sind. In gewissem Sinne würde es sich daher empfehlen, die Zahlen δ als die Invarianten der Gruppe zu bezeichnen. Wir wollen aber gleichwohl bei der anderweit schon gebrauchten Bezeichnung stehen bleiben.

Zwei Gruppen, deren Elemente sich einander in der Weise eindeutig zuordnen lassen, dass durch die Zusammensetzung entsprechender Elemente wieder entsprechende Elemente entstehen, heissen *isomorph*.[1]

Wenn nun zwei Gruppen dieselben Invarianten $e_1, e_2, \ldots, e_\nu$ haben, so sind die Gruppen isomorph.

Denn wählt man für jede derselben eine Basis $g_1, g_2, \ldots, g_\nu$ so, dass in der Form

$$g_1^{x_1}g_2^{x_2}\ldots g_\nu^{x_\nu}$$

alle Elemente, und jedes nur einmal, enthalten sind, wenn x_h modulo e_h genommen wird, so kann man diejenigen Elemente beider Gruppen einander entsprechen lassen, in welchen die Exponenten x_h dieselben Werte haben, woraus der Isomorphismus erhellt.

---

[1] C. JORDAN, von dem dieser Ausdruck herrührt, nennt solche Gruppen »holoëdrisch isomorph». Da der meriëdrische Isomorphismus hier gar nicht in Betracht kommt, so lassen wir diese Unterscheidung weg.

Löst man den Begriff der Gruppe gänzlich ab von der besonderen Bedeutung, welche die Elemente derselben in jedem einzelnen Falle haben, und fasst die Definition nur formal, so kann man isomorphe Gruppen auch schlechthin als identisch bezeichnen und in diesem Sinne sagen, dass durch die Invarianten die Gruppe vollständig bestimmt sei.

§ 2. *Die Gruppencharaktere.*

Eine Function $\chi(a)$, d. h. ein System von e (gleichen oder verschiedenen) von Null verschiedenen Zahlwerten, deren jeder einem bestimmten Element a der Gruppe $\mathfrak{A}$ zugeordnet ist, heisst ein *Gruppencharakter*, wenn für irgend zwei Elemente a, a' der Gruppe $\mathfrak{A}$ die Bedingung erfüllt ist

$$\chi(aa') = \chi(a)\chi(a'). \tag{1}$$

Solcher Gruppencharaktere existieren genau e von einander verschiedene, d. h. solche, deren je zwei mindestens für ein Element a in $\mathfrak{A}$ verschiedene Werte haben, und alle sind e^{te} Einheitswurzeln.

Denn zunächst folgt aus (1), indem man $a' = 1$ annimmt

$$\chi(a) = \chi(a)\chi(1),$$

also:

$$\chi(1) = 1. \tag{2}$$

Bedeutet nun wie in § 1 $g_1, g_2, \ldots, g_\nu$ eine Basis der Gruppe $\mathfrak{A}$, deren Elemente die Grade $e_1, e_2, \ldots, e_\nu$ haben, so ist für jedes Element a

$$a = g_1^{x_1} g_2^{x_2} \ldots g_\nu^{x_\nu}, \tag{3}$$

und aus (1) folgt

$$\chi(a) = \chi(g_1)^{x_1}\chi(g_2)^{x_2}\ldots\chi(g_\nu)^{x_\nu}, \tag{4}$$

und

$$\chi(g_1)^{e_1} = 1, \quad \chi(g_2)^{e_2} = 1, \quad \ldots, \quad \chi(g_\nu)^{e_\nu} = 1. \tag{5}$$

Verstehen wir also unter

$$\theta_1, \theta_2, \ldots, \theta_\nu$$

primitive Einheitswurzeln der Ordnung

$$e_1, e_2, \ldots, e_\nu,$$

so lassen sich die ganzen Zahlen $y_1, y_2, \ldots, y_\nu$ nach den Moduln $e_1, e_2, \ldots, e_\nu$ so bestimmen, dass

$$\chi(g_1) = \theta_1^{y_1}, \qquad \chi(g_2) = \theta_2^{y_2}, \quad \ldots, \quad \chi(g_\nu) = \theta_\nu^{y_\nu}, \tag{6}$$

und daher

$$\chi(a) = \theta_1^{y_1 x_1} \theta_2^{y_2 x_2} \ldots \theta_\nu^{y_\nu x_\nu} \tag{7}$$

wird.

Nehmen wir umgekehrt das Zahlensystem $y_1, y_2, \ldots, y_\nu$ beliebig an, so genügt (7) der Bedingung (1) und ist daher ein Gruppencharakter. Auch sind die auf diese Weise gebildeten e Gruppencharaktere alle von einander verschieden; denn wählen wir in (7) zwei verschiedene Exponentensysteme y, welchen die beiden Charaktere χ, χ' entspringen, so kann man stets ein System der x, d. h. ein Element a finden, so dass $\chi(a)$ von $\chi'(a)$ verschieden wird.

Ebenso aber giebt es, wenn a, a' verschiedene Elemente in $\mathfrak{A}$ sind, unter den Charakteren χ gewiss immer solche für welche $\chi(a)$ von $\chi(a')$ verschieden ist.

Ein Element a ist also vollständig und eindeutig bestimmt durch die Zahlenwerte der e Charaktere $\chi(a)$.[1]

Jedem System der Zahlen y entspricht nach der Formel

$$a' = g_1^{y_1} g_2^{y_2} \ldots g_\nu^{y_\nu} \tag{8}$$

ein und nur ein Element a' der Gruppe $\mathfrak{A}$, *so dass sich die durch* (7) *bestimmten e Charaktere selbst in eindeutiger Weise den Elementen der Gruppe* $\mathfrak{A}$ *zuordnen lassen.* Indem wir diese Zuordnung in die Bezeichnung aufnehmen, setzen wir, wenn die Zahlensysteme x, y durch (3) und (8) bestimmt sind

$$\chi_{a'}(a) = \chi_a(a') = \theta_1^{y_1 x_1} \theta_2^{y_2 x_2} \ldots \theta_\nu^{y_\nu x_\nu}. \tag{9}$$

Verstehen wir unter $\chi_{a'}\chi_{a''}$ den Charakter $\chi_{a'a''}(a)$, so bilden nach dieser Zusammensetzung *die Charaktere unter sich eine Abel'sche Gruppe, welche mit der gegebenen Gruppe* $\mathfrak{A}$ *isomorph ist.*

---

[1] Diese Sätze sind bewiesen in der oben citierten Abhandlung des Verfassers und sind in der Abhandlung I zum Teil benutzt. Des leichteren Verständnisses halber sind die Beweise in obigen Text, zum Teil etwas vereinfacht, wiederholt.

§ 3. *Divisoren Abel'scher Gruppen.*

Wir betrachten jetzt eine Abel'sche Gruppe $\mathfrak{R}$ vom Grade N, deren Elemente mit n und deren Charaktere mit $\chi_{n'}(n)$ bezeichnet sein mögen.

Ist $\mathfrak{A}$ eine in $\mathfrak{R}$ enthaltene Gruppe, d. h. ein System von in $\mathfrak{R}$ enthaltenen Elementen a von der Art, dass das Product zweier a immer wieder ein Element in $\mathfrak{A}$ ist, so lässt sich die Gruppe $\mathfrak{R}$ in *Reihen* von gleich viel Elementen in folgender Weise zerfällen.

Ist a_1 ein in $\mathfrak{R}$ aber nicht in $\mathfrak{A}$ enthaltenes Element, so sind auch alle Elemente aa_1 zwar in $\mathfrak{R}$ aber nicht in $\mathfrak{A}$ enthalten. Die Gesammtheit dieser Producte $a_1 a$, welche ebenso viele Zahlen wie $\mathfrak{A}$ selbst enthält, werde mit $\mathfrak{A}_1$ bezeichnet.

Ist a_2 ein in $\mathfrak{R}$, aber weder in $\mathfrak{A}$ noch in $\mathfrak{A}_1$ enthaltenes Element, so gilt das gleiche von allen Producten $a_2 a$, und deren Gesammtheit bildet ein System $\mathfrak{A}_2$ von ebenso vielen Elementen wie $\mathfrak{A}$. Fährt man auf diese Weise fort, bis die Gruppe $\mathfrak{R}$ erschöpft ist, so wird $\mathfrak{R}$ in eine bestimmte Anzahl von *Reihen*

$$\mathfrak{A},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots,\ \mathfrak{A}_{e-1} \tag{1}$$

zerlegt, deren jede gleichviel, also $N:e$ Elemente enthält, von denen aber nur die erste eine Gruppe ist.

Wenn man nun die Zusammensetzung dieser Reihen in der Weise erklärt, dass $\mathfrak{A}_h \mathfrak{A}_k$ die aus den Elementen $a_h a_k a$ gebildete Reihe sein soll, so bilden diese Reihen unter sich eine Abel'sche Gruppe $\mathfrak{R}$ vom Grade e, in welcher die Gruppe $\mathfrak{A}$ als Einheit gilt.

Wie die Charaktere der Gruppe $\mathfrak{R}$ aus denen der Gruppe $\mathfrak{R}$ hergeleitet werden, ist schon in der Abhandlung I, § 3, gezeigt. Wir kommen hier in der Kürze darauf zurück.

Ist $\xi(\mathfrak{A}_k)$ einer dieser Charaktere, so können wir setzen:

$$\xi(\mathfrak{A}_k) = \xi(a_k a) = \xi(n) \tag{2}$$

wodurch eine Function $\xi(n)$ für jedes Element von $\mathfrak{R}$ definiert ist, welche für alle Elemente einer der Reihen (1) einen und denselben Wert hat, und für alle Elemente der Gruppe $\mathfrak{A}$ den Wert 1.

Diese Function genügt aber der Bedingung

$$\xi(\mathfrak{A}_h)\xi(\mathfrak{A}_k) = \xi(\mathfrak{A}_h\mathfrak{A}_k),$$

d. h. nach der Erklärung der Zusammensetzung der Reihen $\mathfrak{A}_h$, $\mathfrak{A}_k$,

$$\xi(n)\xi(n') = \xi(nn'), \tag{3}$$

und ist also nach § 2 unter den Charakteren $\chi(n)$ der Gruppe $\mathfrak{N}$ enthalten.

Ist umgekehrt $\xi(n)$ einer der Charaktere $\chi(n)$, welcher der Bedingung

$$\xi(a) = 1 \tag{4}$$

genügt, so ist auch

$$\xi(a_k a) = \xi(a_k) \tag{5}$$

für alle a und kann daher mit $\xi(\mathfrak{A}_k)$ bezeichnet werden. Es besteht aber zugleich die Relation

$$\xi(\mathfrak{A}_h)\xi(\mathfrak{A}_k) = \xi(\mathfrak{A}_h\mathfrak{A}_k) \tag{6}$$

und es ist also diese Function einer der Charaktere von $\mathfrak{N}$.

Es folgt hieraus, dass die Bedingung (4) für genau e unter den Charakteren $\chi(n)$ erfüllt ist.

Wenden wir also die am Schlusse des vorigen Paragraphen eingeführte Bezeichnung an, so erhalten wir die Charaktere der Gruppe $\mathfrak{N}$ in der Form $\chi_b(n)$, wenn wir alle diejenigen Elemente b in der Gruppe $\mathfrak{N}$ aufsuchen, welche für *alle Elemente* a der Bedingung genügen

$$\chi_b(a) = 1. \tag{7}$$

Diese Elemente b bilden eine in $\mathfrak{N}$ enthaltene Gruppe $\mathfrak{B}$, welche mit $\mathfrak{N}$ isomorph ist, und der zu $\mathfrak{A}$ reciproke Divisor von $\mathfrak{N}$ genannt sein soll.

Die Gruppe $\mathfrak{B}$ ist durch die Gruppe $\mathfrak{A}$ vollständig bestimmt und die Beziehung beider ist eine gegenseitige. Das Product der Grade zweier reciproker Teiler von $\mathfrak{N}$ ist gleich dem Grade von $\mathfrak{N}$.

§ 4. *Die Gruppe der Potenzreste für einen zusammengesetzten Modul.*

Wir verstehen jetzt unter $\mathfrak{N}$ die Gruppe der nach irgend einem Modul m genommenen *zu* m *teilerfremden* Zahlen n, welche sich, wenn zwei nach dem Modul m congruente Zahlen als nicht verschieden betrachtet werden, durch Multiplication, welche hier die Stelle der Zusammensetzung vertritt, reproducieren.

Sei also

$$m = 2^{\lambda} q_1^{k_1} q_2^{k_2} \dots \tag{1}$$

der Modul, $q_1, q_2, \dots$ von einander verschiedene ungerade Primzahlen, $k_1, k_2, \dots$ positive Exponenten und λ entweder $= 0$ oder $\geqq 2$, ($\lambda = 1$ hat für unsere Aufgabe kein Interesse).

Bedeuten $c_1, c_2, \dots$ primitive Wurzeln von $q_1^2, q_2^2, \dots$ so sind, wie aus der Theorie der Potenzreste für zusammengesetzte Moduln bekannt ist, für jede Zahl n die Exponenten $\gamma_1, \gamma_2, \dots$ nach den Moduln

$$q_1^{k_1-1}(q_1 - 1),\ q_2^{k_2-1}(q_2 - 1),\ \dots$$

vollständig und eindeutig dadurch bestimmt, dass

$$n \equiv c_1^{\gamma_1} \pmod{q_1^{k_1}}, \qquad n \equiv c_2^{\gamma_2} \pmod{q_2^{k_2}}, \quad \dots$$

Ist $\lambda = 2$, so ist ebenso α nach dem Modul 2 durch die Congruenz

$$n \equiv (-1)^{\alpha} \pmod 4$$

und ist $\lambda > 2$ so sind α, β nach den Moduln 2, $2^{\lambda-2}$ durch die Congruenz

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

bestimmt.

Die auf diese Weise bestimmten Exponenten, nämlich

$$\begin{aligned} &\gamma_1, \gamma_2, \dots && \text{wenn } m \text{ ungerade} \\ &\alpha, \gamma_1, \gamma_2, \dots && \text{wenn } m \equiv 4 \pmod 8 \\ &\alpha, \beta, \gamma_1, \gamma_2, \dots && \text{wenn } m \equiv 0 \pmod 8 \end{aligned}$$

heissen die *Indices* der Zahl n und sollen in irgend einer Reihenfolge mit

$$\alpha_1, \alpha_2, \ldots, \alpha_\mu$$

bezeichnet werden, während wir die Moduln, nach welchen diese Indices genommen sind, nämlich

$$\begin{aligned} & q_1^{k_1-1}(q_1-1),\ q_2^{k_2-1}(q_2-1),\ \ldots && \text{wenn } m \text{ ungerade} \\ 2,\ & q_1^{k_1-1}(q_1-1),\ q_2^{k_2-1}(q_2-1),\ \ldots && \text{wenn } m \equiv 4 \pmod 8 \\ 2,\ 2^{\lambda-2},\ & q_1^{k_1-1}(q_1-1),\ q_2^{k_2-1}(q_2-1),\ \ldots && \text{wenn } m \equiv 0 \pmod 8 \end{aligned}$$

mit

$$m_1, m_2, \ldots, m_\mu$$

bezeichnen, und zwar so dass α_1 der zum Modul m_1 gehörige Index heisst.

Die Anzahl μ der Indices ist also gleich der Anzahl der von einander verschiedenen in m aufgehenden Primzahlen, oder, falls m durch 8 teilbar ist, um eins grösser.

Ist ein System von Zahlwerten für die Indices $\alpha_1, \alpha_2, \ldots, \alpha_\mu$ nach dem System der Moduln $m_1, m_2, \ldots, m_\mu$ beliebig gegeben, so gehört dazu umgekehrt eine nach dem Modul m vollständig bestimmte Zahl n. Die Indices eines Productes zweier Zahlen sind die Summen der entsprechenden Indices der einzelnen Factoren.

Wenn wir also jeden der Indices ein vollständiges Restsystem nach seinem Modul durchlaufen lassen, so erhalten wir die ganze Gruppe $\mathfrak{N}$ vom Grade

$$\varphi(m) = m_1 m_2 \ldots m_\mu.$$

Um die Charaktere der Gruppe $\mathfrak{N}$ zu erhalten, wählen wir ein System primitiver Einheitswurzeln der Ordnung $m_1, m_2, \ldots, m_\mu$

$$\omega_1, \omega_2, \ldots, \omega_\mu.$$

Sind alsdann $\alpha_1', \alpha_2', \ldots, \alpha_\mu'$ die Indices irgend einer Zahl n' in $\mathfrak{N}$, so erhält man die $\varphi(n)$ Charaktere $\chi_{n'}(n)$ in der Form

$$\chi_{n'}(n) = \omega_1^{\alpha_1'\alpha_1}\omega_2^{\alpha_2'\alpha_2}\ldots\omega_\mu^{\alpha_\mu'\alpha_\mu}.$$

§ 5. *Die Kreisteilungsperioden.*

Bedeutet r eine primitive m^{te} Einheitswurzel, und $\mathfrak{A}$ irgend eine in $\mathfrak{R}$ enthaltene Gruppe, so heisst die Summe

$$\eta = \sum^{a} r^{a} \tag{1}$$

eine *Kreisteilungsperiode* und man hat nun zunächst auf zwei Umstände zu achten:

1. Nach Abhandlung I, § 5, verschwindet η *dann* und *nur dann* wenn für irgend eine *mehrfach* in m aufgehende Primzahl q alle der Bedingung

$$a \equiv 1 \pmod{\frac{m}{q}}$$

genügende Zahlen n in $\mathfrak{A}$ enthalten sind.

2. Wenn die in 1 erwähnte Bedingung nicht, dagegen für einen *einfachen* Primfactor q von m *alle in* $\mathfrak{R}$ *enthaltenen* der Bedingung

$$a \equiv 1 \pmod{\frac{m}{q}}$$

genügende Zahlen zugleich in $\mathfrak{A}$ enthalten sind, aber auch *nur* unter dieser Voraussetzung kann η durch Einheitswurzeln von niedrigerer Ordnung ausgedrückt werden. (I, § 4.)

Es lässt sich diese Darstellung auch leicht finden; denn es besteht in diesem Falle $\mathfrak{A}$ aus lauter Zahlen von der Form

$$a'\left(1 + h\frac{m}{q}\right),$$

worin h die Reihe der Zahlen $0, 1, \ldots, q-1$ mit Ausnahme derjenigen, für welche

$$1 + h\frac{m}{q} = kq$$

ein Vielfaches von q ist, und a' eine Gruppe $\mathfrak{A}'$ für den Modul $m:q$ durchläuft. Dann ergiebt sich aber

$$\eta = \sum^{a} r^{a} = -\sum^{a'} r^{qka'},$$

also η (vom Vorzeichen abgesehen) gleich einer aus Einheitswurzeln der Ordnung $m:q$ gebildeten Periode.

Es sei nun wieder $\mathfrak{A}$ irgend eine in $\mathfrak{R}$ enthaltene Gruppe vom Grade $\varphi(m):e$, und es werde überhaupt an den Bezeichnungen der §§ 3, 4 festgehalten. Unter den mit η *conjugierten* Perioden

$$\eta_n = \sum_{a}^{a} r^{na} \tag{2}$$

sind, wenn nicht der Ausnahmefall 1 eintritt, in welchem dieselben alle verschwinden, e von einander verschieden, entsprechend den e Reihen $\mathfrak{A}$, $\mathfrak{A}_1$, ..., $\mathfrak{A}_{e-1}$ des § 3, nämlich

$$\eta,\ \eta_{a_1},\ \eta_{a_2},\ \ldots,\ \eta_{a_{e-1}}, \tag{3}$$

und diese sind die Wurzeln einer irreducibeln ganzzahligen Gleichung e^{ten} Grades (I, § 5). Die rationalen Functionen von η mit rationalen Zahlencoefficienten constituiren einen Kreiskörper, und es ist das Hauptergebniss der drei vorangegangenen Abhandlungen, dass man auf diese Weise alle Abel'schen Körper erhält, und, wenn man den Ausnahmefall 2 noch ausschliesst, jeden nur einmal.

Die Permutationsgruppe des auf diese Weise gebildeten Körpers (oder die Galois'sche Gruppe der Gleichung für η) besteht aus den e Substitutionen

$$(\eta,\ \eta_{a_k}) = (\eta_{a_h},\ \eta_{a_h a_k}), \tag{4}$$

und ist also isomorph mit der Gruppe $\mathfrak{R}$ der Reihen $\mathfrak{A}$, $\mathfrak{A}_1$, ..., $\mathfrak{A}_{e-1}$, oder auch *isomorph mit der zu* $\mathfrak{A}$ *reciproken Gruppe* $\mathfrak{B}$.

Will man also Abel'sche Körper bilden, deren Gruppe vorgeschriebene Invarianten e_1, e_2, ..., e_ν hat, so wird man zunächst nicht auf die Bildung der Gruppe $\mathfrak{A}$, sondern auf die der reciproken Gruppe $\mathfrak{B}$ ausgehen, welche eben diese Invarianten besitzt. Hieraus ergeben sich die beiden folgenden, zusammen zu beantwortenden Fragen:

I. *Welche Moduln m sind geeignet, um mit ihrer Hilfe Gruppen* $\mathfrak{B}$ *mit den vorgeschriebenen Invarianten* e_1, e_2, ..., e_ν *zu bilden, und zwar so, dass die zu* $\mathfrak{B}$ *reciproke Gruppe* $\mathfrak{A}$ *nicht unter die beiden Ausnahmefälle* 1, 2 *fällt?* [1]

[1] Dass für beliebig gegebene Invarianten immer solche Moduln existieren, ist in der

II. *Wie findet man diese Gruppen für einen gegebenen dazu geeigneten Modul?*

§ 6. *Bedingungen für den Modul* m.

Es ist zunächst erforderlich, die Bedingungen, 1, 2 welche die auszuschliessenden Gruppen $\mathfrak{A}$ charakterisieren, auf solche für die Gruppe $\mathfrak{B}$ zu übertragen.

Wir bezeichnen die Indices einer jeden Zahl a in $\mathfrak{A}$ mit

$$\alpha_1, \alpha_2, \ldots, \alpha_\mu,$$

die einer jeden Zahl b in $\mathfrak{B}$ mit

$$\beta_1, \beta_2, \ldots, \beta_\mu,$$

so dass also die Zahlen b dadurch definiert sind, dass für alle Zahlen a

$$\omega_1^{\alpha_1\beta_1}\omega_2^{\alpha_2\beta_2}\ldots\omega_\mu^{\alpha_\mu\beta_\mu} = 1. \tag{1}$$

Wir haben nun wenn q ein Primfactor von m ist, diejenigen Zahlen a zu betrachten, welche der Bedingung

$$a \equiv 1 \left(\mathrm{mod}\frac{m}{q}\right) \tag{2}$$

genügen, und unterscheiden dabei folgende drei Fälle:

1. Es sei q eine k mal in m aufgehende ungerade Primzahl und $k > 1$. Die Indices aller der Bedingung (2) genügenden Zahlen a sind dann gleich Null mit Ausnahme des zum Modul $q^{k-1}(q-1)$ gehörigen, und dieser letztere kann jeden Wert annehmen, der durch $q^{k-2}(q-1)$ teilbar ist. Die Gruppe $\mathfrak{A}$ wird also dann und nur dann die sämmtlichen der Bedingung (2) genügende Zahlen a enthalten, *wenn die zum Modul* $q^{k-1}(q-1)$ *gehörigen Indices* β *alle durch* q *teilbar sind.*

2. Ist $q = 2$ so schliesst man ebenso, dass alle der Bedingung (2) genügenden Zahlen a dann und nur dann in $\mathfrak{A}$ enthalten sind, wenn die zum Modul 2 oder $2^{\lambda-2}$ gehörigen Indices β alle gerade sind, je nachdem $m \equiv 4$ oder $m \equiv 0 \pmod 8$ ist.

---

oben citierten Arbeit von FROBENIUS und STICKELBERGER gezeigt. Jedoch ist dort die Frage nicht berührt, wie man *alle* diese Moduln erhält.

Schliessen wir diese Fälle aus, so kann die Kreisteilungsperiode η nicht verschwinden.

3. Ist q ein einfacher Primfactor von m, so sind die der Bedingung (2) genügenden Zahlen a dadurch charakterisiert, dass die Indices derselben alle verschwinden mit Ausnahme des zum Modul $q-1$ gehörigen, welcher jeden beliebigen Wert haben kann. Es tritt also hiernach der zweite Ausnahmefall, nämlich die Reduction auf Einheitswurzeln niedrigerer Ordnung, *dann* und *nur dann* ein, *wenn die zum Modul* $q-1$ *gehörigen Indices* β *alle gleich Null sind.*

Nun ist nach der Definition der Invarianten e_1 die kleinste positive Zahl, welche für alle Elemente b den Bedingungen genügt:

$$(3)\quad e_1\beta_1 \equiv 0 \pmod{m_1}, \qquad e_1\beta_2 \equiv 0 \pmod{m_2}, \quad \ldots, \quad e_1\beta_\mu \equiv 0 \pmod{m_\mu}.$$

Sollen also die beiden Ausnahmefälle ausgeschlossen sein, so ergeben sich nach 1, 2, 3 für den Modul m die folgenden Bedingungen.

Eine ungerade Primzahl q_1 darf nicht öfter in m_1 enthalten sein als in e_1 (weil sonst nach (3) sämmtliche β_1 durch q_1 teilbar wären), also:

A. *Eine in* e_1 *nicht enthaltene ungerade Primzahl kann nur einfach in* m *enthalten sein und eine in* e_1 *enthaltene ungerade Primzahl kann höchstens einmal mehr in* m *als in* e_1 *aufgehen.*

B. *Ist* e_1 *ungerade, so muss auch* m *ungerade sein, und ist* e_1 *durch eine Potenz von* 2 *teilbar, so kann* m *den Factor* 2 *höchstens zweimal öfter enthalten als* e_1.

C. *Ist* q *eine einfach in* m *aufgehende Primzahl, so muss* $q-1$ *wenigstens durch eine der in* e_1 *aufgehenden Primzahlen teilbar sein.*

Diese Bedingungen erweisen sich als notwendig. Es wird sich später noch eine weitere Bedingung ergeben, die dann mit diesen zusammen auch hinreichend ist.

§ 7. *Bestimmung der Gruppe* $\mathfrak{B}$.

Wenn eine Gruppe $\mathfrak{B}$ mit den Invarianten $e_1, e_2, \ldots, e_\nu$ existiert, so giebt es eine Basis von ν Elementen $g_1, g_2, \ldots, g_\nu$ von den Graden $e_1, e_2, \ldots, e_\nu$, so dass jedes Element b in der Form darstellbar ist

$$(1)\qquad b \equiv g_1^{x_1} g_2^{x_2} \ldots g_\nu^{x_\nu} \pmod{m},$$

und jedes nur einmal, wenn $x_1, x_2, \ldots, x_\nu$ je ein vollständiges Restsystem mod $e_1, e_2, \ldots, e_\nu$ durchlaufen.

Sind nun

$$\begin{array}{llll} \beta_{1,1}, \beta_{1,2}, \ldots, \beta_{1,\mu} & \text{die Indices von } g_1, \\ \beta_{2,1}, \beta_{2,2}, \ldots, \beta_{2,\mu} & \text{»} \quad \text{»} \quad \text{»} \quad g_2, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ \beta_{\nu,1}, \beta_{\nu,2}, \ldots, \beta_{\nu,\mu} & \text{»} \quad \text{»} \quad \text{»} \quad g_\nu, \end{array}$$

so erhält man die Indices $\beta_1, \beta_2, \ldots, \beta_\mu$ eines beliebigen Elementes b in der Form:

$$(2) \qquad \begin{array}{l} \beta_1 \equiv \beta_{1,1}x_1 + \beta_{2,1}x_2 + \ldots + \beta_{\nu,1}x_\nu \pmod{m_1} \\ \beta_2 \equiv \beta_{1,2}x_1 + \beta_{2,2}x_2 + \ldots + \beta_{\nu,2}x_\nu \pmod{m_2} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \beta_\mu \equiv \beta_{1,\mu}x_1 + \beta_{2,\mu}x_2 + \ldots + \beta_{\nu,\mu}x_\nu \pmod{m_\mu}. \end{array}$$

Umgekehrt liefert auch jedes System der

$$x_1 \pmod{e_1}, \qquad x_2 \pmod{e_2}, \quad \ldots, \quad x_\nu \pmod{e_\nu}$$

in (2) eingesetzt, die Indices einer und nur einer Zahl b.

Hieraus ergeben sich mit Rücksicht auf 1, 2, 3 des vorigen Paragraphen die nicht nur *notwendigen* sondern auch *hinreichenden* Bedingungen für die Indices $\beta_{h,k}$ des Basis.

I. *Die $\beta_{h,k}$ müssen so beschaffen sein, dass die Congruenzen*

$$(3) \qquad \begin{array}{l} \beta_{1,1}x_1 + \beta_{2,1}x_2 + \ldots + \beta_{\nu,1}x_\nu \equiv 0 \pmod{m_1} \\ \beta_{1,2}x_1 + \beta_{2,2}x_2 + \ldots + \beta_{\nu,2}x_\nu \equiv 0 \pmod{m_2} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \beta_{1,\mu}x_1 + \beta_{2,\mu}x_2 + \ldots + \beta_{\nu,\mu}x_\nu \equiv 0 \pmod{m_\mu} \end{array}$$

die Congruenzen

$$(4) \qquad x_1 \equiv 0 \pmod{e_1}, \qquad x_2 \equiv 0 \pmod{e_2}, \quad \ldots, \quad x_\nu \equiv 0 \pmod{e_\nu}$$

zur notwendigen Folge haben.

II. *Ist q ein mehrmals in m aufgehender Primfactor und $m_h = q^{k-1}(q-1)$,*

oder falls $q = 2$ *ist,* $m_h = 2^{\lambda-2}$ *oder* $= 2$, *je nachdem* m *durch* 8 *teilbar ist oder nicht, so dürfen die* ν *Zahlen*

$$\beta_{1,h},\ \beta_{2,h},\ \ldots,\ \beta_{\nu,h} \tag{5}$$

nicht alle durch q *teilbar sein.*

III. *Soll auch der zweite Ausnahmefall ausgeschlossen sein, so dürfen, wenn* q *ein einfacher Primfactor von* m *und* $m_h = q - 1$ *ist, die Zahlen*

$$\beta_{1,h},\ \beta_{2,h},\ \ldots,\ \beta_{\nu,h}$$

nicht alle durch $q - 1$ *teilbar sein.*

Um die Möglichkeit der Erfüllung dieser Bedingungen beurteilen zu können, bezeichnen wir mit

$$d_{k,h} \qquad \begin{pmatrix} k=1,2,\ldots,\nu \\ h=1,2,\ldots,\mu \end{pmatrix} \tag{6}$$

den grössten gemeinschaftlichen Teiler von e_k und m_h, so dass, wegen der von den e_k vorausgesetzten Eigenschaft in der Zahlenreihe

$$d_{1,h},\ d_{2,h},\ \ldots,\ d_{\nu,h} \tag{7}$$

jede Zahl durch die folgende teilbar ist, und setzen ferner

$$\begin{aligned} e_k &= d_{k,1}e_{k,1} = d_{k,2}e_{k,2} = \ldots = d_{k,\mu}e_{k,\mu}, \\ m_h &= d_{1,h}m_{1,h} = d_{2,h}m_{2,h} = \ldots = d_{\nu,h}m_{\nu,h}, \end{aligned} \tag{8}$$

so dass $e_{k,h}$ und $m_{k,h}$ relative Primzahlen sind, und wegen (7) in der Zahlenreihe

$$m_{1,h},\ m_{2,h},\ \ldots,\ m_{\nu,h} \tag{9}$$

jede Zahl durch die *vorangegangene* teilbar ist.

Die Zahlen $d_{k,h}$, $e_{k,h}$, $m_{k,h}$ sind durch die Invarianten $e_1, e_2, \ldots, e_\nu$ und den Modul m allein bestimmt, und wenn m den Bedingungen A, B, C des vorigen Paragraphen genügt, *so ist* $m_{1,h}$ *im Falle* II *nicht durch* q, *im Falle* III *nicht durch* $q - 1$ *teilbar*, wie aus

$$e_1 = d_{1,h}e_{1,h}, \qquad m_h = d_{1,h}m_{1,h}$$

hervorgeht.

Da nun e_k der Grad von g_k ist, und $\beta_{k,1}, \beta_{k,2}, \ldots, \beta_{k,\mu}$ die Indices von g_k, so ist e_k die kleinste positive Zahl, welche den Congruenzen

$$e_k \beta_{k,h} \equiv 0 \pmod{m_h} \qquad (h=1,2,\ldots,\mu) \tag{10}$$

genügt. Daraus folgt aber mittelst (8)

$$d_{k,h} e_{k,h} \beta_{k,h} \equiv 0 \pmod{d_{k,h} m_{k,h}},$$

und daraus, da $e_{k,h}$ und $m_{k,h}$ relativ prim sind,

$$\beta_{k,h} \equiv 0 \pmod{m_{k,h}}.$$

Wir setzen daher, indem wir unter $\gamma_{k,h}$ neue ganze Zahlen verstehen, die nach dem Modul $d_{k,h}$ zu nehmen sind

$$\beta_{k,h} = m_{k,h} \gamma_{k,h}, \tag{11}$$

und formen damit die Congruenzen (3) um.

Man erhält zunächst durch einsetzen von (8) und (11) in (3):

$$m_{1,h}\gamma_{1,h}x_1 + m_{2,h}\gamma_{2,h}x_2 + \ldots + m_{\nu,h}\gamma_{\nu,h}x_\nu \equiv 0 \pmod{m_{1,h}d_{1,h}}$$

und daraus mittelst der Relationen

$$\frac{m_{k,h}}{m_{1,h}} = \frac{d_{1,h}}{d_{k,h}} = \frac{e_1}{e_k}\frac{e_{k,h}}{e_{1,h}} = \delta_1\delta_2\ldots\delta_{k-1}\frac{e_{k,h}}{e_{1,h}}, \tag{12}$$

worin wie in § 1 (11)

$$\frac{e_1}{e_2} = \delta_1, \quad \frac{e_2}{e_3} = \delta_2, \quad \ldots, \quad \frac{e_{\nu-1}}{e_\nu} = \delta_{\nu-1}, \quad e_\nu = \delta_\nu, \quad e_1 = \delta_1\delta_2\ldots\delta_\nu \tag{13}$$

gesetzt ist,

$$e_{1,k}\gamma_{1,k}x_1 + e_{2,k}\gamma_{2,k}\delta_1 x_2 + \ldots + e_{\nu,k}\gamma_{\nu,k}\delta_1\delta_2\ldots\delta_{\nu-1}x_\nu \equiv 0 \pmod{e_1}, \tag{14}$$

und die Bedingung I ist nun darauf zurückgeführt, *dass die für* $k = 1, 2, \ldots, \mu$ *gültigen Congruenzen* (14), *die sich auf einen und denselben Modul beziehen, die Congruenzen* (4) *zur notwendigen Folge haben.*

Bei den weiteren Folgerungen aus dieser Forderung stützen wir uns auf das nachstehende, leicht zu beweisende *Lemma.*

Die nach irgend einem Modul δ genommenen Congruenzen

$$\begin{aligned} &a_{1,1}x_1 + \ldots + a_{1,\nu}x_\nu \equiv 0 \\ &\ldots\ldots\ldots\ldots \pmod{\delta} \\ &a_{\mu,1}x_1 + \ldots + a_{\mu,\nu}x_\nu \equiv 0 \end{aligned}$$

können befriedigt werden ohne dass sämmtliche $x_1, \ldots, x_\nu$ durch δ teilbar sind, wenn $\nu > \mu$ ist oder wenn zwar $\nu \leqq \mu$ aber alle aus den Reihen der Coefficienten $a_{k,h}$ zu bildenden ν-reihigen Determinanten mit δ einen gemeinschaftlichen Teiler haben, im andern Fall ist dies nicht möglich. [1]

Da nun die Congruenz (14) auch für den Modul e_ν gültig sein und die Folgerung

$$x_1 \equiv 0, \qquad x_2 \equiv 0, \quad \ldots, \quad x_\nu \equiv 0 \pmod{e_\nu}$$

ergeben muss, so erhalten wir eine vierte Bedingung für den Modul m.

D. *Es muss die Anzahl μ der Indices für den Modul m gleich oder grösser sein als die Anzahl ν der Invarianten.*

Die Congruenzen (14) lassen sich nun successive durch die folgenden ersetzen:

$$e_{1,k}\gamma_{1,k}x_1 \equiv 0 \pmod{\delta_1}, \tag{15}$$

welche die Bedingung ergiebt:

$$e_{1,1}\gamma_{1,1},\ e_{1,2}\gamma_{1,2},\ \ldots,\ e_{1,\mu}\gamma_{1,\mu} \tag{δ_1}$$

dürfen keinen gemeinschaftlichen Teiler mit δ_1 haben.

Dann folgt aus (15)

$$x_1 = \delta_1 x_1', \tag{16}$$

und aus (14)

$$e_{1,k}\gamma_{1,k}x_1' + e_{2,k}\gamma_{2,k}x_2 \equiv 0 \pmod{\delta_2}, \tag{17}$$

---

[1] Es ist kaum nötig, auf den Beweis dieses Satzes hier einzugehen, der fast wörtlich aus der Theorie der linearen homogenen Gleichungen entnommen werden kann. (Man vgl. z. B. LIPSCHITZ, *Lehrbuch der Analysis*, Bd. I, Cap. IV.)

woraus die zweite Bedingung:

(δ_2) *Nicht alle aus*

$$e_{1,1}\gamma_{1,1},\ e_{1,2}\gamma_{1,2},\ \ldots,\ e_{1,\mu}\gamma_{1,\mu}$$

$$e_{2,1}\gamma_{2,1},\ e_{2,2}\gamma_{2,2},\ \ldots,\ e_{2,\mu}\gamma_{2,\mu}$$

zu bildenden zweireihigen Determinanten dürfen einen gemeinschaftlichen Teiler mit δ_2 haben.

Dann folgt aus (17)

$$x_1' = \delta_2 x_1'', \qquad x_1 = \delta_1\delta_2 x_1'', \qquad x_2 = \delta_2 x_2''.$$

Indem man diese Schlussweise fortsetzt, gelangt man schliesslich zu der Bedingung

(δ_ν) *Nicht alle aus*

$$e_{1,1}\gamma_{1,1},\ e_{1,2}\gamma_{1,2},\ \ldots,\ e_{1,\mu}\gamma_{1,\mu}$$

$$e_{2,1}\gamma_{2,1},\ e_{2,2}\gamma_{2,2},\ \ldots,\ e_{2,\mu}\gamma_{2,\mu}$$

$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

$$e_{\nu,1}\gamma_{\nu,1},\ e_{\nu,2}\gamma_{\nu,2},\ \ldots,\ e_{\nu,\mu}\gamma_{\nu,\mu}$$

zu bildenden ν-reihigen Determinanten dürfen einen gemeinsamen Teiler mit δ_ν haben.

Wenn nun q eine in $e_1, e_2, \ldots, e_\rho$ aber nicht in $e_{\rho+1}, \ldots, e_\nu$ aufgehende Primzahl, also ein Teiler von δ_ρ nicht aber von $\delta_{\rho+1}, \delta_{\rho+2}, \ldots, \delta_\nu$ ist, so fordert die Bedingung (δ_ρ), dass man über die $\gamma_{k,h}$ so verfüge, dass wenigstens eine der ρ-reihigen Determinanten, etwa

$$\begin{vmatrix} e_{1,1}\gamma_{1,1}, & e_{1,2}\gamma_{1,2}, & \ldots, & e_{1,\rho}\gamma_{1,\rho} \\ e_{2,1}\gamma_{2,1}, & e_{2,2}\gamma_{2,2}, & \ldots, & e_{2,\rho}\gamma_{2,\rho} \\ \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot \\ e_{\rho,1}\gamma_{\rho,1}, & e_{\rho,2}\gamma_{\rho,2}, & \ldots, & e_{\rho,\rho}\gamma_{\rho,\rho} \end{vmatrix} \qquad (\Delta)$$

nicht durch q teilbar sei, und wenn dieser Forderung für alle in e_1 aufgehenden Primzahlen q genügt ist, so sind auch die Bedingungen (δ_1), (δ_2), ..., (δ_ν) erfüllt.

Hieraus ergiebt sich die letzte Bedingung für den Modul m:

E. *Ist q eine in $e_1, e_2, \ldots, e_\rho$ aber nicht in $e_{\rho+1}$ aufgehende Primzahl, so muss eine Anordnung der $m_1, m_2, \ldots, m_\mu$ derart möglich sein, dass das Product*

$$e_{1,1}e_{2,2}\ldots e_{\rho,\rho}$$

nicht durch q teilbar ist. (Selbstverständlich braucht diese Anordnung für die verschiedenen Primzahlen q nicht dieselbe zu sein.)

Ist die Bedingung E erfüllt, so kann man über die $\gamma_{k,h}$ so verfügen, dass auch die Bedingung (Δ) befriedigt ist; man hat nur z. B.

$$\gamma_{1,1}, \gamma_{2,2}, \ldots, \gamma_{\rho,\rho} \quad \text{durch } q \text{ nicht teilbar}$$

$$\gamma_{2,1}, \gamma_{3,1}, \gamma_{3,2}, \ldots, \gamma_{\rho,1}, \gamma_{\rho,2}, \ldots, \gamma_{\rho,\rho-1} \quad \text{durch } q \text{ teilbar}$$

anzunehmen, und da hiernach an $\gamma_{1,h}$ noch keine Anforderung gestellt ist, so bleibt noch die Möglichkeit, den Bedingungen II, III zu genügen. Denn nach (11) geschieht diesen Forderungen genüge, wenn ein bestimmtes $m_{1,h}\gamma_{1,h}$, nicht durch q oder nicht durch $q-1$ teilbar ist, während $m_{1,h}$ durch q oder $q-1$ nicht teilbar ist.

Auch für die verschiedenen in Betracht kommenden Primzahlen q sind diese Forderungen offenbar mit einander verträglich.

§ 8. *Bestimmung der Gruppe* $\mathfrak{A}$.

Die Coefficienten $\gamma_{k,h}$ lassen sich den Bedingungen des vorigen Paragraphen gemäss im Allgemeinen auf mehrfache Weise bestimmen. Unter diesen Bestimmungsarten können mehrere zu derselben Gruppe $\mathfrak{B}$ führen; es können aber auch verschiedene Gruppen $\mathfrak{B}$ und folglich auch verschiedene Gruppen $\mathfrak{A}$ auftreten. Man muss also, um alle diese Gruppen zu bilden, die verschiedenen Bestimmungsweisen der Coefficienten $\gamma_{k,h}$ in Betracht ziehen. Man kann aber dann, wenn man die $\gamma_{k,h}$ gewählt hat, ohne erst auf die Gruppe $\mathfrak{B}$ einzugehen, direct zur Bildung der Gruppe $\mathfrak{A}$ schreiten, wie jetzt noch gezeigt werden soll.

Sind wie oben $\alpha_1, \alpha_2, \ldots, \alpha_\mu$ die Indices irgend einer Zahl in $\mathfrak{A}$, $\beta_1, \beta_2, \ldots, \beta_\mu$ die einer Zahl in $\mathfrak{B}$, ist ferner

$$(1) \qquad M = m_1 m_1' = m_2 m_2' = \ldots = m_\mu m_\mu'$$

das kleinste gemeinschaftliche Vielfache von $m_1, m_2, \ldots, m_\mu$ so sind die beiden Gruppen $\mathfrak{A}$, $\mathfrak{B}$ dadurch charakterisiert, dass stets

$$m_1'\beta_1\alpha_1 + m_2'\beta_2\alpha_2 + \ldots + m_\mu'\beta_\mu\alpha_\mu \equiv 0 \pmod{M} \tag{2}$$

oder dass die sämmtlichen

$$\frac{\beta_1\alpha_1}{m_1} + \frac{\beta_2\alpha_2}{m_2} + \ldots + \frac{\beta_\mu\alpha_\mu}{m_\mu} \tag{3}$$

ganze Zahlen sind. Nach § 7 (2) hat man also alle diejenigen Zahlensysteme $\alpha_1, \alpha_2, \ldots, \alpha_\mu \pmod{m_1, m_2, \ldots, m_\mu}$ aufzusuchen, für welche

$$\frac{\beta_{k,1}\alpha_1}{m_1} + \frac{\beta_{k,2}\alpha_2}{m_2} + \ldots + \frac{\beta_{k,\mu}\alpha_\mu}{m_\mu} \qquad (k=1,2,\ldots,\nu) \tag{4}$$

ganze Zahlen sind. Die Ausdrücke (4) lassen sich aber nach (8), (11) § 7 so darstellen

$$\frac{\gamma_{k,1}\alpha_1}{d_{k,1}} + \frac{\gamma_{k,2}\alpha_2}{d_{k,2}} + \ldots + \frac{\gamma_{k,\mu}\alpha_\mu}{d_{k,\mu}}, \tag{5}$$

so dass man die einzelnen Terme auf den gemeinschaftlichen Nenner e_k bringen kann. Hiernach ergeben sich dann zur directen Bestimmung der Indices α_h die Congruenzen

$$e_{k,1}\gamma_{k,1}\alpha_1 + e_{k,2}\gamma_{k,2}\alpha_2 + \ldots + e_{k,\mu}\gamma_{k,\mu}\alpha_\mu \equiv 0 \pmod{e_k}. \qquad (k=1,2,\ldots,\nu) \tag{6}$$

§ 9. *Besondere Fälle.*

Es hat nicht die geringste Schwierigkeit, nach den bisher gegebenen Vorschriften Zahlenbeispiele in beliebiger Menge durchzuführen. Wir überlassen dies dem Leser und heben hier nur noch zwei Fälle allgemeinerer Art hervor, in welchen den Resultaten eine einfachere Gestalt gegeben werden kann.

1. *Es sei* $\nu = 1$, *also die Gruppe* $\mathfrak{B}$ *regulär*

$$m = 2^\lambda q_1^{k_1} q_2^{k_2} \ldots$$

Es ist in diesem Fall nach § 7 (8)

$$e_1 = d_{1,1}e_{1,1} = d_{1,2}e_{1,2} = \ldots = d_{1,\mu}e_{1,\mu}$$
$$m_1 = d_{1,1}m_{1,1}, \qquad m_2 = d_{1,2}m_{1,2}, \quad \ldots, \quad m_\mu = d_{1,\mu}m_{1,\mu}$$

und die Bedingung E reduciert sich darauf, dass

$$e_{1,1},\ e_{1,2},\ \ldots,\ e_{1,\mu}$$

keinen gemeinschaftlichen Teiler haben. Die Zahlen $\gamma_{1,1},\ \gamma_{1,2},\ \ldots,\ \gamma_{1,\mu}$ hat man dann so zu wählen, dass auch

$$e_{1,1}\gamma_{1,1},\ e_{1,2}\gamma_{1,2},\ \ldots,\ e_{1,\mu}\gamma_{1,\mu}$$

keinen gemeinschaftlichen Teiler mit e_1 haben, und überdiess zur Vermeidung der Ausnahmefälle, so dass, wenn q Primfactor von m ist und m_1 der zugehörige Indexmodul, $e_{1,1}\gamma_{1,1}$ nicht durch $q-1$ oder nicht durch $q]$ teilbar ist, je nachdem q einmal oder mehrmals in m aufgeht, eine Forderung, welcher wegen der Voraussetzungen A, B, C stets genügt werden kann. Für die Indices α erhält man dann die eine Bedingung

$$(1)\qquad e_{1,1}\gamma_{1,1}\alpha_1 + e_{1,2}\gamma_{1,2}\alpha_2 + \ldots + e_{1,\mu}\gamma_{1,\mu}\alpha_\mu \equiv 0 \pmod{e_1}.$$

Dies ist der von KRONECKER in der oben erwähnten Abhandlung behandelte Fall.

2. Es sei ν beliebig, dagegen

$$(2)\qquad e_1 = e_2 = \ldots = e_\nu = p$$

gleich einer und derselben Primzahl (einschliesslich der Primzahl 2). Alle von p verschiedenen in m aufgehenden Primzahlen müssen in diesem Falle $\equiv 1 \pmod{p}$ sein und können nur einfache Factoren von m sein. Der Factor p selbst kann zweimal und wenn $p = 2$ ist, dreimal in m enthalten sein, aber nicht nur einmal (wegen C).

Wir nehmen zuerst an, es sei:

$$m = q_1 q_2 \ldots q_\mu$$

$$q_1 \equiv 1,\qquad q_2 \equiv 1,\quad \ldots,\quad q_\mu \equiv 1 \pmod{p},\qquad \mu \overline{\overline{\gtrless}} \nu$$

$$m_1 = q_1 - 1,\qquad m_2 = q_2 - 1,\quad \ldots,\quad m_\mu = q_\mu - 1.$$

Dann ist

$$d_{k,h} = p,\qquad e_{k,h} = 1,\qquad m_{k,h} = \frac{q_h - 1}{p}.$$

Die Zahlen $\gamma_{k,h}$ hat man so anzunehmen, dass nicht alle ν-reihigen Determinanten aus

$$\gamma_{1,1},\ \gamma_{1,2},\ \ldots,\ \gamma_{1,\mu}$$
$$\gamma_{2,1},\ \gamma_{2,2},\ \ldots,\ \gamma_{2,\mu}$$
$$\ldots\ldots\ldots\ldots$$
$$\gamma_{\nu,1},\ \gamma_{\nu,2},\ \ldots,\ \gamma_{\nu,\mu}$$

durch p teilbar sind, und dann erhält man die Gruppe $\mathfrak{A}$, indem man alle Zahlen α aufsucht welche den Congruenzen

$$(3)\qquad \begin{aligned} \gamma_{1,1}\alpha_1 + \gamma_{1,2}\alpha_2 + \ldots + \gamma_{1,\mu}\alpha_\mu &\equiv 0 \\ \gamma_{2,1}\alpha_1 + \gamma_{2,2}\alpha_2 + \ldots + \gamma_{2,\mu}\alpha_\mu &\equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ \gamma_{\nu,1}\alpha_1 + \gamma_{\nu,2}\alpha_2 + \ldots + \gamma_{\nu,\mu}\alpha_\mu &\equiv 0 \end{aligned} \pmod{p}$$

genügen. Durch diese Congruenzen sind ν von den Zahlen α_h durch die übrigen $\mu - \nu$, welche willkürlich sind, nach dem Modul p bestimmt. Nun kann jede Zahl α_h, ohne die Bedingungen (3) zu verletzen, ersetzt werden durch

$$(4)\qquad \alpha_h + s_h p, \qquad s_h = 0,\ 1,\ 2,\ \ldots,\ \frac{q_h - 1}{p} - 1.$$

Bezeichnen wir also mit c_1, c_2, ... primitive Wurzeln von q_1, q_2, ... so ist

$$a \equiv c_1^{\alpha_1} \pmod{q_1}$$
$$a \equiv c_2^{\alpha_2} \pmod{q_2}$$
$$\ldots\ldots\ldots$$

und daher, wenn r_1, r_2, ... primitive Einheitswurzeln der Ordnung q_1, q_2, ... bedeuten

$$r^a = r_1^{c_1^{\alpha_1}} r_2^{c_2^{\alpha_2}} \ldots$$

und also, nach (4)

$$(5)\qquad \eta = \sum^{a}\sum^{s_k} r_1^{c_1^{\alpha_1 + s_1 p}} r_2^{c_2^{\alpha_2 + s_2 p}} \ldots$$

worin die mit α bezeichnete Summe auf alle den Congruenzen (3) genügenden Zahlen α_h, die kleiner als q und nicht negativ sind, erstreckt ist.

Setzen wir also

$$(6)\qquad \eta_{\alpha_h}^{(k)} = \sum_{0,\ \frac{q_h-1}{p}-1}^{s} r_k^{c_k^{\alpha_h + sp}}$$

was nichts anderes als die von GAUSS eingeführten $q_h - 1 : p$-gliedrigen Perioden sind, so erhält (5) die Form

$$\eta = \sum^{\alpha} \eta^{(1)}_{a_1} \eta^{(2)}_{a_2} \dots \tag{7}$$

worin die Summe nach α ebenso zu erklären ist wie in (5).

Ist insbesondere $\mu = \nu$, so werden die in (7) vorkommenden α alle $= 0$ und man erhält η dargestellt als ein Product von ν einfachen GAUSS'schen Perioden.

Nicht viel anders gestaltet sich das Resultat, wenn wir

$$m = p^2 q_1 q_2 \dots \tag{8}$$

setzen. Wir nehmen eine primitive Wurzel c_0 von p^2 und definieren α_0 nach dem Modul $p(p-1)$ durch die Congruenz

$$a \equiv c_0^{\alpha_0} \pmod{p^2}.$$

Ist dann r_0 eine primitive Einheitswurzel der Ordnung p^2, und $\eta^{(0)}_{\alpha_0}$ die $(p-1)$-gliedrige Periode

$$\eta^{(0)}_{\alpha_0} = \sum_{0, p-2}^{s} r_0^{c_0^{\alpha_0 + sp}}$$

so wird jetzt

$$\eta = \sum^{\alpha} \eta^{(0)}_{a_0} \eta^{(1)}_{a_1} \eta^{(2)}_{a_2} \dots \tag{9}$$

worin die Summe nach α über alle den Congruenzen

$$\gamma_{h,0}\alpha_0 + \gamma_{h,1}\alpha_1 + \gamma_{h,2}\alpha_2 + \dots \equiv 0 \pmod{p} \qquad (h = 1, 2, \dots, \nu) \tag{10}$$

genügenden Werte α erstreckt ist, die kleiner als p und nicht negativ sind.

Ist endlich $p = 2$ und

$$m = 8 q_1 q_2 \dots$$

so bestimmt man α_0, α'_0 nach dem Modul 2 aus der Congruenz

$$(-1)^{\alpha_0} 5^{\alpha'_0} \equiv a \pmod{8} \tag{11}$$

und erhält für η den Ausdruck

$$\eta = \sum^{\alpha} e^{\frac{\pi i}{4}(-1)^{\alpha_0} 5^{\alpha'_0}} \eta^{(1)}_{a_1} \eta^{(2)}_{a_2} \dots \tag{12}$$

worin wieder die nach α genommene Summe über alle den Congruenzen

$$\gamma_{h,0}\alpha_0 + \gamma'_{h,0}\alpha'_0 + \gamma_{h,1}\alpha_1 + \gamma_{h,2}\alpha_2 + \dots \equiv 0 \pmod{2} \tag{13}$$

genügenden Werte α, die gleich 0 oder 1 gesetzt werden können, erstreckt ist.

Marburg, im October 1886.