ÜBER GRUPPEN DER ORDNUNG $p^\alpha q^\beta$

VON

G. FROBENIUS

in BERLIN.

Angeregt durch die bahnbrechenden Arbeiten von GAUSS haben ABEL und GALOIS das Fundament der modernen Algebra geschaffen und insbesondere die Bedingungen für die Auflösbarkeit einer algebraische Gleichung entwickelt. Mit Hülfe derselben gelingt es in einer Reihe von Fällen, wo die Ordnung der Gleichung bekannt ist, ihre Auflösbarkeit allein aus der Art zu erkennen, wie diese Zahl aus Primfactoren zusammengesetzt ist. Auch in diesem Bereiche von Untersuchungen hat ABEL den ersten Schritt gethan, indem er bewies, dass jede Gleichung von Primzahlordnung auflösbar ist. Diesen Satz hat Herr SYLOW in einer für die Gruppentheorie grundlegenden Arbeit auf Gleichungen ausgedehnt, deren Ordnung eine Potenz einer Primzahl ist. Im Folgenden beschäftige ich mich mit Gleichungen, deren Ordnung nur durch zwei verschiedene Primzahlen theilbar ist.

In meiner Arbeit *Über endliche Gruppen*, Sitzungsberichte der Berliner Akademie 1895, habe ich folgenden Satz bewiesen:

I. *In einer Gruppe* $\mathfrak{H}$, *deren Ordnung genau durch die* α^{te} *Potenz der Primzahl* p *theilbar ist, und die mehr als eine Gruppe* $\mathfrak{A}$ *der Ordnung* p^α *enthält, wähle man zwei dieser Untergruppen so, dass die Ordnung* p^δ *ihres grössten gemeinsamen Divisors* $\mathfrak{D}$ *möglichst gross ist. Bilden die mit* $\mathfrak{D}$ *vertauschbaren Elemente von* $\mathfrak{H}$ *die Gruppe* $\mathfrak{D}'$ *der Ordnung* d', *so sei* p^β *die höchste in* d' *aufgehende Potenz von* p.

Acta mathematica. 26. Imprimé le 25 juin 1902.

Dann ist $\mathfrak{D}$ *eine charakteristische Untergruppe von* $\mathfrak{D}'$, *nämlich der grösste gemeinsame Divisor von je zwei in* $\mathfrak{D}'$ *enthaltenen Gruppen* $\mathfrak{B}$ *der Ordnung* p^β. *Jede Gruppe* $\mathfrak{B}$ *ist in einer und nur einer Gruppe* $\mathfrak{A}$ *enthalten, und jede durch* $\mathfrak{D}$ *theilbare Gruppe* $\mathfrak{A}$ *enthält eine und nur eine Gruppe* $\mathfrak{B}$. *Die Anzahl der durch* $\mathfrak{D}$ *theilbaren Gruppen* $\mathfrak{A}$ *ist gleich der Anzahl der Gruppen* $\mathfrak{B}$. *Sie ist* $\equiv 1 \pmod{p^{\beta-\delta}}$ *und* $> p^{\beta-\delta} > 1$. *Demnach ist* $\beta > \delta$, *und* d' *stets durch eine von* p *verschiedene Primzahl theilbar.*

Jedes Element von $\mathfrak{H}$, *das mit* $\mathfrak{D}'$ *vertauschbar ist, ist in* $\mathfrak{D}'$ *enthalten. Ist* $\mathfrak{B}$ *in* $\mathfrak{A}$ *enthalten, und bilden die mit* $\mathfrak{A}$ *vertauschbaren Elemente von* $\mathfrak{H}$ *die Gruppe* $\mathfrak{A}'$, *und die mit* $\mathfrak{B}$ *vertauschbaren Elemente von* $\mathfrak{D}'$ *die Gruppe* $\mathfrak{B}'$, *so ist* $\mathfrak{B}'$ *der grösste gemeinsame Divisor von* $\mathfrak{A}'$ *und* $\mathfrak{D}'$.

Aus diesem Princip ergiebt sich die Auflösbarkeit jeder Gruppe der Ordnung $p^\alpha q$, wo q eine von p verschiedene Primzahl ist, und allgemeiner der Ordnung $p^\alpha q^\mu$, wo μ der Exponent ist, zu dem $q \pmod p$ gehört (A. a. O. § 6), ferner der Ordnung $p^\alpha q^2$ (BURNSIDE, *Theory of groups*, § 244; C. JORDAN, Liouv. Journ. sér. 5, tome 4, 1898) und der Ordnung $p^\alpha q^\beta$, wo $\beta < 2\mu$ ist (BURNSIDE, § 243). Diese Sätze will ich hier etwas einfacher herleiten und auf Gruppen der Ordnung $p^\alpha q^{2\mu}$ ausdehnen, sowie auf solche Gruppen der Ordnung $p^\alpha q^\beta$, die nicht mehr als q^μ Gruppen der Ordnung p^α enthalten.

Um die Entwicklung nicht unterbrechen zu müssen, schicke ich folgenden Hülfssatz voraus:

II. *Ist eine Gruppe* $\mathfrak{H}$ *der Ordnung* h *mit jedem Elemente einer Gruppe* $\mathfrak{P}$ *vertauschbar, deren Ordnung eine Potenz einer Primzahl* p *ist, und bilden die Elemente von* $\mathfrak{H}$, *die mit jedem Elemente von* $\mathfrak{P}$ *vertauschbar sind, eine Gruppe* $\mathfrak{G}$ *der Ordnung* g, *so ist* $h \equiv g \pmod p$.

Ist A ein Element von $\mathfrak{H}$, und P ein Element von $\mathfrak{P}$, so ist $P^{-1}AP = B$ auch ein Element von $\mathfrak{H}$. Zwei solche Elemente von $\mathfrak{H}$ nenne ich *conjugirt in Bezug auf* $\mathfrak{P}$. Sind zwei Elemente einem dritten conjugirt, so sind sie es auch unter einander. Daher kann man die h Elemente von $\mathfrak{H}$ in Classen conjugirter Elemente eintheilen. Jedes der g Elemente von $\mathfrak{G}$ bildet für sich eine Classe. Ist p^λ die Ordnung von $\mathfrak{P}$, ist A nicht in $\mathfrak{G}$ enthalten, so ist A mit $p^\alpha < p^\lambda$ Elementen von $\mathfrak{P}$ vertauschbar, und folglich mit $p^{\lambda-\alpha}$ Elementen von $\mathfrak{H}$ conjugirt. Ist B nicht in $\mathfrak{G}$ enthalten, und

auch nicht mit A conjugirt, so ist B mit $p^{\lambda-\beta} > 1$ Elementen von $\mathfrak{H}$ conjugirt. Daher ist $h = g + p^{\lambda-\alpha} + p^{\lambda-\beta} + \ldots \equiv g \pmod{p}$.

Nun sei $\mathfrak{H}$ eine Gruppe der Ordnung $h = p^\alpha q^\beta$. Sind dann $\mathfrak{A}$ und $\mathfrak{B}$ zwei Untergruppen der Ordnungen p^α und q^β, so ist $\mathfrak{H} = \mathfrak{AB}$. Ist allgemeiner $\mathfrak{G}$ eine Untergruppe der Ordnung $p^\alpha q^\sigma$, so ist auch $\mathfrak{H} = \mathfrak{GB}$. Demnach bilden die Elemente von $\mathfrak{B}$ ein vollständiges Restsystem von $\mathfrak{H}$ (mod. $\mathfrak{G}$), und man erhält die Untergruppen, die mit $\mathfrak{G}$ in $\mathfrak{H}$ conjugirt sind, schon sämmtlich indem man $\mathfrak{G}$ mit jedem Elemente von $\mathfrak{B}$ transformirt. Sei B ein von E verschiedenes invariantes Element von $\mathfrak{B}$. Ist dann B in $\mathfrak{G}$ enthalten, so zeigt diese Betrachtung, dass auch die mit $\mathfrak{G}$ conjugirten Gruppen alle das Element B enthalten. Der grösste gemeinsame Divisor $\mathfrak{D}$ dieser Gruppen ist aber eine invariante Untergruppe von $\mathfrak{H}$. Ist also $\sigma < \beta$, so ist $\mathfrak{H}$ zusammengesetzt. Ich schliesse daher in den Beweisen der beiden folgenden Sätze den Fall aus, wo ein invariantes Element B einer Gruppe $\mathfrak{B}$ in einer Untergruppe der Ordnung $p^\alpha q^\sigma$ $(\sigma < \beta)$ enthalten ist, oder wo ein invariantes Element A einer Gruppe $\mathfrak{A}$ in einer Untergruppe der Ordnung $p^\rho q^\beta$ $(\rho < \alpha)$ enthalten ist.

III. *Sind p und q zwei verschiedene Primzahlen, und gehört q (mod. p) zum Exponenten μ, so ist jede Gruppe der Ordnung $p^\alpha q^\beta$ auflösbar, die nicht mehr als q^μ Gruppen der Ordnung p^α enthält.*

Es genügt zu zeigen, dass eine Gruppe $\mathfrak{H}$ der Ordnung $h = p^\alpha q^\beta$, die nicht mehr als q^μ Gruppen $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots$ der Ordnung p^α enthält, stets eine invariante Untergruppe $\mathfrak{G}$ besitzt. Dann hat nämlich die Gruppe $\frac{\mathfrak{H}}{\mathfrak{G}}$ der Ordnung $p^\gamma q^\delta < h$ die Untergruppe $\frac{\mathfrak{AG}}{\mathfrak{G}}$ der Ordnung p^γ und die mit ihr conjugirten Untergruppen $\frac{\mathfrak{A}_1\mathfrak{G}}{\mathfrak{G}}, \frac{\mathfrak{A}_2\mathfrak{G}}{\mathfrak{G}}, \ldots$, deren Anzahl $\leq q^\mu$ ist.

Bilden die mit $\mathfrak{A}$ vertauschbaren Elemente von $\mathfrak{H}$ die Gruppe $\mathfrak{A}'$ der Ordnung $p^\alpha q^\lambda$, so enthält $\mathfrak{H}$ $q^{\beta-\lambda}$ Gruppen der Ordnung p^α, von denen je zwei conjugirt sind, und es ist $q^{\beta-\lambda} \equiv 1 \pmod{p}$. Ist daher $\beta - \lambda$ kleiner als der Exponent μ, zu dem q (mod. p) gehört, so ist $\beta - \lambda = 0$, also ist $\mathfrak{A}$ eine invariante Untergruppe von $\mathfrak{H}$. Sei also $\beta = \lambda + \mu$. Sind nicht je zwei der q^μ mit $\mathfrak{A}$ conjugirten Gruppen theilerfremd, so sei $\mathfrak{D}$ die in Satz I definirte Gruppe. Dann ist die Anzahl der durch $\mathfrak{D}$ theilbaren Gruppen $\mathfrak{A}$ höchstens gleich q^μ, grösser als 1, eine Potenz von q

und $\equiv 1 \pmod{p}$, also gleich q^μ. Daher ist $\mathfrak{D}$ der grösste gemeinsame Divisor aller q^μ mit $\mathfrak{A}$ conjugirten Gruppen, also eine invariante Untergruppe von $\mathfrak{H}$. Seien also je zwei der Gruppen $\mathfrak{A}$ theilerfremd. Dann ist $q^\mu \equiv 1 \pmod{p^\alpha}$. Ist nun $\lambda = 0$, $\beta = \mu$, so enthält $\mathfrak{H}$ $(p^\alpha - 1)q^\beta + 1$ Elemente, deren Ordnung in p^α aufgeht, also eine invariante Untergruppe $\mathfrak{B}$ der Ordnung q^β. Sei also $\lambda > 0$.

1) Sei O ein Element von $\mathfrak{H}$, dessen Ordnung eine Potenz von q ist, $\mathfrak{B}$ eine durch O theilbare Untergruppe der Ordnung q^β, B ein invariantes Element von $\mathfrak{B}$. Dann ist B nicht in der Gruppe $\mathfrak{A}'$ der Ordnung $p^\alpha q^\lambda$ enthalten, also nicht mit $\mathfrak{A}$ vertauschbar, die Gruppe $B^{-1}\mathfrak{A}B$ ist demnach von $\mathfrak{A}$ verschieden. Die mit O vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppe $\mathfrak{G}$ der Ordnung $p^\rho q^\sigma$. $\mathfrak{G}$ enthält das Element B und eine Gruppe $\mathfrak{R}$ der Ordnung p^ρ, also auch die Gruppe $B^{-1}\mathfrak{R}B$. Sei $\mathfrak{A}$ eine durch $\mathfrak{R}$ theilbare Gruppe der Ordnung p^α.

Ist $\rho > 0$, so ist $B^{-1}\mathfrak{R}B$ von $\mathfrak{R}$ verschieden. Denn sonst wäre $\mathfrak{R} = B^{-1}\mathfrak{R}B$ ein gemeinsamer Divisor der beiden verschiedenen Gruppen $\mathfrak{A}$ und $B^{-1}\mathfrak{A}B$. Demnach enthält $\mathfrak{G}$ mehrere Gruppen $\mathfrak{R}$, $\mathfrak{R}_1, \ldots, \mathfrak{R}_x, \ldots$ der Ordnung p^ρ. Zwei dieser Gruppen, $\mathfrak{R}$ und $\mathfrak{R}_1$, können nicht in derselben Gruppe $\mathfrak{A}$ der Ordnung p^α enthalten sein. Denn sonst wären sie auch in dem grössten gemeinsamen Divisor von $\mathfrak{A}$ und $\mathfrak{G}$ enthalten dessen Ordnung höchstens p^ρ sein kann. Ist also $\mathfrak{R}_x$ in $\mathfrak{A}_x$ enthalten, so sind die Gruppen $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots$ alle unter einander verschieden. Daher ist die Anzahl der Gruppen $\mathfrak{R}_x$ höchstens gleich q^μ, grösser als 1, eine Potenz von q und $\equiv 1 \pmod{p}$, also gleich q^μ. Nun ist O mit $\mathfrak{R}_x$ vertauschbar, also auch mit $\mathfrak{A}_x$, weil sonst die beiden verschiedenen Gruppen $\mathfrak{A}_x$ und $O^{-1}\mathfrak{A}_x O$ beide durch $\mathfrak{R}_x$ theilbar wären. Folglich ist O in $\mathfrak{A}'_x$ enthalten, also haben die q^μ mit $\mathfrak{A}'$ conjugirten Gruppen $\mathfrak{A}'_x$ alle einen Theiler gemeinsam, und demnach ist $\mathfrak{H}$ zusammengesetzt.

Sei also $\rho = 0$ für jedes O; dann ist ein Element von $\mathfrak{H}$, dessen Ordnung eine Potenz von p ist, nie mit einem Elemente vertauschbar, dessen Ordnung eine Potenz von q ist, und $\mathfrak{H}$ enthält kein Element, dessen Ordnung durch p und q theilbar ist.

2) Die Untergruppe $\mathfrak{A}'$ der Ordnung $p^\alpha q^\lambda$ enthält p^α Elemente, deren Ordnungen in p^α aufgehen, und kein Element, dessen Ordnung durch pq theilbar ist, also $p^\alpha(q^\lambda - 1) + 1$ Elemente, deren Ordnungen in q^λ aufgehen, Dies ist aber möglich, wenn $\mathfrak{A}'$ p^α verschiedene Untergruppen $\mathfrak{B}$

der Ordnung q^λ enthält, und je zwei derselben theilerfremd sind. Daher ist $p^\alpha \equiv 1 \pmod{q^\lambda}$, und weil $q^\mu \equiv 1 \pmod{p^\alpha}$ ist, so ist $\lambda < \mu$.

Seien $\mathfrak{L}, \mathfrak{L}_1, \ldots, \mathfrak{L}_x, \ldots$ die p^α in $\mathfrak{A}'$ enthaltenen Gruppen der Ordnung q^λ (> 1). Eine Gruppe $\mathfrak{B}$ der Ordnung q^β kann nicht zwei dieser Gruppen enthalten, weil die Ordnung des grössten gemeinsamen Divisors von $\mathfrak{B}$ und $\mathfrak{A}'$ höchstens gleich q^λ sein kann. Ist also $\mathfrak{L}_x$ in $\mathfrak{B}_x$ enthalten, so sind die p^α Gruppen $\mathfrak{B}, \mathfrak{B}_1, \mathfrak{B}_2, \ldots$ alle unter einander verschieden. Daher enthält $\mathfrak{H}$ nicht weniger und auch nicht mehr als p^α Gruppen $\mathfrak{B}$ der Ordnung q^β.

Von den p^α Gruppen $\mathfrak{B}$ können nicht je zwei theilerfremd sein. Sonst enthielten sie zusammen $(q^\beta - 1)p^\alpha + 1$ Elemente, und folglich enthielte $\mathfrak{H}$ nur eine Gruppe $\mathfrak{A}$. Wählt man zwei der Gruppen $\mathfrak{B}$ so, dass die Ordnung q^δ ihres grössten gemeinsamen Divisors $\mathfrak{D}$ möglichst gross ist, so ist $\delta > 0$. Die mit $\mathfrak{D}$ vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppe $\mathfrak{D}'$ der Ordnung $p^\rho q^\sigma$, wo $\rho > 0$ und $\sigma > \delta$ ist. Ist $\rho = \alpha$, so ist $\mathfrak{H}$ zusammengesetzt, nämlich falls $\sigma < \beta$ ist, weil $\mathfrak{D}'$ jedes invariante Element B jeder durch $\mathfrak{D}$ theilbaren Gruppe $\mathfrak{B}$ enthält, und falls $\sigma = \beta$ ist, weil $\mathfrak{D}$ eine invariante Untergruppe von $\mathfrak{H}$ ist.

3) Die Annahme $\rho < \alpha$ aber ist unzulässig. Denn sei $\mathfrak{R}$ eine in $\mathfrak{D}'$ enthaltene Gruppe der Ordnung p^ρ. Dann ist $\mathfrak{D}$ mit jedem Elemente von $\mathfrak{R}$ vertauschbar, aber kein Element von $\mathfrak{D}$ ausser E. Nach Satz II ist folglich $q^\delta \equiv 1 \pmod{p}$, also $\delta = \mu$, mithin $\sigma > \mu > \lambda$.

Da $\rho < \alpha$ ist, so ist $\mathfrak{R}$ in einer Gruppe der Ordnung $p^{\rho+1}$ als invariante Untergruppe enthalten. Sei P ein Element dieser Gruppe, das nicht in der Gruppe $\mathfrak{D}'$ der Ordnung $p^\rho q^\sigma$ enthalten ist. Dann ist $P^{-1}\mathfrak{D}P = \mathfrak{D}_1$ von $\mathfrak{D}$ verschieden und mit jedem Elemente von $P^{-1}\mathfrak{R}P = \mathfrak{R}$ vertauschbar.

$\mathfrak{D}$ und $\mathfrak{D}_1$ haben keinen Theiler gemeinsam. Denn ihr grösster gemeinsamer Theiler wäre mit jedem Elemente von $\mathfrak{R}$ vertauschbar, aber keines seiner Elemente ausser E. Daher wäre nach Satz II seine Ordnung $\equiv 1 \pmod{p}$, also gleich q^μ, der Ordnung von $\mathfrak{D}$.

Aus demselben Grunde haben $\mathfrak{D}_1$ und $\mathfrak{D}'$, die beide mit jedem Elemente von $\mathfrak{R}$ vertauschbar sind, kein Element gemeinsam. Denn sonst wäre die Ordnung ihres grössten gemeinsamen Theilers gleich q^μ, dieser Theiler wäre $\mathfrak{D}_1$, wäre in $\mathfrak{D}'$ enthalten, $\mathfrak{D}$ wäre also mit jedem Elemente von $\mathfrak{D}_1$ vertauschbar. Folglich wäre $\mathfrak{D}\mathfrak{D}_1$ eine Gruppe der Ordnung $q^{2\mu}$, während h nur durch q^β theilbar ist, und $\beta = \lambda + \mu < 2\mu$ ist.

Kein Element von $\mathfrak{D}_1$ ausser E ist in $\mathfrak{D}'$ enthalten, also mit $\mathfrak{D}$ vertauschbar. Transformirt man daher $\mathfrak{D}$ mit jedem Elemente von $\mathfrak{D}_1$, so erhält man q^μ verschiedene mit $\mathfrak{D}$ conjugirte Gruppen. Da $\mathfrak{D}$ mit $p^\rho q^\sigma$ Elementen von $\mathfrak{H}$ vertauschbar ist, so enthält $\mathfrak{H}$ genau $p^{\alpha-\rho}q^{\beta-\sigma}$ mit $\mathfrak{D}$ conjugirte Gruppen. Folglich ist $q^\mu < p^{\alpha-\rho}q^{\beta-\sigma}$. Nun ist $q^\mu = 1 + rp^\alpha$ und $p^\alpha \equiv 1 \pmod{q^\lambda}$, also da $\lambda < \mu$ ist, $r \equiv -1 \pmod{q^\lambda}$. Daher ist

$$q^\mu = 1 - p^\alpha + sp^\alpha q^\lambda > p^\alpha(q^\lambda - 1).$$

Mithin ist

$$p^\alpha(q^\lambda - 1) < p^{\alpha-\rho}q^{\beta-\sigma}, \qquad p^\rho(q^\lambda - 1) < q^{\lambda-(\sigma-\mu)}.$$

Da aber $\rho > 0$ und $\sigma > \mu$ ist, so ist

$$p^\rho > 1, \qquad q^\lambda - 1 > q^{\lambda-(\sigma-\mu)}.$$

Daher kann der betrachtete Fall ($\rho < \alpha$) nicht eintreten.

IV. *Sind p und q zwei verschiedene Primzahlen, gehört q (mod. p) zum Exponenten μ, und ist $\beta \leqq 2\mu$, so ist jede Gruppe der Ordnung $p^\alpha q^\beta$ auflösbar.*

Auch hier genügt es zu zeigen dass $\mathfrak{H}$ keine einfache Gruppe ist. Dies ergiebt sich aus dem Satze III, wenn $\mathfrak{A}'$ die Ordnung $p^\alpha q^{\beta-\mu}$ hat, also stets, wenn $\beta < 2\mu$ ist. Es ist also nur der Fall zu betrachten, wo $\beta = 2\mu$ und $\mathfrak{A}' = \mathfrak{A}$ ist. Dann enthält $\mathfrak{H}$ $q^{2\mu}$ Gruppen $\mathfrak{A}$. Sind je zwei derselben theilerfremd, so ist $\mathfrak{B}$ eine invariante Untergruppe von $\mathfrak{H}$. Seien also $\mathfrak{D}$ und $\mathfrak{D}'$ die in Satz I definirten Gruppen, und seien ihre Ordnungen $p^\delta > 1$ und $d' = p^\rho q^\sigma$. Dann werde ich zunächst zeigen, dass $\mathfrak{H}$ zusammengesetzt ist, wenn nicht 1) $\sigma = \mu$ und 2) $\rho = \alpha$ ist.

1) $\sigma = \mu$: Die Gruppe $\mathfrak{D}'$ enthält mehrere Gruppen $\mathfrak{R}$ der Ordnung p^ρ, also q^μ oder $q^{2\mu}$. Im letzteren Falle ist $\mathfrak{D}$ in allen $q^{2\mu}$ mit $\mathfrak{A}$ conjugirten Gruppen enthalten, und eine invariante Untergruppe von $\mathfrak{H}$. Sei also q^μ die Anzahl der Gruppen $\mathfrak{R}$, demnach $\sigma \geqq \mu$.

Sei $\mathfrak{S}$ eine in $\mathfrak{D}'$ enthaltene Gruppe der Ordnung q^σ, und $\mathfrak{B}$ eine durch $\mathfrak{S}$ theilbare Gruppe der Ordnung $q^{2\mu}$. Ist $\mathfrak{A}$ durch $\mathfrak{D}$ theilbar, so ist $\mathfrak{D}$ mit p^ρ Elementen von $\mathfrak{A}$ vertauschbar. Transformirt man also $\mathfrak{D}$ mit den p^α Elementen von $\mathfrak{A}$, so erhält man $p^{\alpha-\rho}$ mit $\mathfrak{D}$ conjugirte Gruppen, deren eine gleich $\mathfrak{D}$ ist. Dasselbe gilt für jede der q^μ Gruppen $\mathfrak{A}$, die durch $\mathfrak{D}$ theilbar sind. Je zwei derselben haben ausser $\mathfrak{D}$ keinen Theiler gemeinsam.

Sie enthalten daher zusammen $(p^{\alpha-\rho}-1)q^\mu+1$ verschiedene Gruppen, die mit $\mathfrak{D}$ in $\mathfrak{H}$ conjugirt sind. Im ganzen enthält $\mathfrak{H}$, da $\mathfrak{D}$ mit $p^\rho q^\sigma$ Elementen vertauschbar ist, $p^{\alpha-\rho}q^{2\mu-\sigma}$ solche Gruppen. Daher ist

$$(p^{\alpha-\rho}-1)q^\mu < p^{\alpha-\rho}q^{2\mu-\sigma}, \qquad (p^{\alpha-\rho}-1)q^{\sigma-\mu} < p^{\alpha-\rho}.$$

Folglich ist nicht $\sigma > \mu$, sondern $\sigma = \mu$.

Zu demselben Ergebniss führt die Bemerkung, dass die Gruppe $\mathfrak{D}'$ in dem Falle $\sigma > \mu$ ein Element O der Ordnung q enthielte, das mit $\mathfrak{R}$, aber nicht mit $\mathfrak{A}$ vertauschbar wäre. Zwei verschiedene Gruppe $\mathfrak{A}$ und $O^{-1}\mathfrak{A}O$ können aber nicht eine Gruppe $\mathfrak{R} = O^{-1}\mathfrak{R}O$ der Ordnung $p^\rho > p^{\hat{\rho}}$ gemeinsam haben.

2) $\rho = \alpha$: Es giebt in $\mathfrak{H}$ $p^{\alpha-\rho}q^\mu$ mit $\mathfrak{D}$ conjugirte Gruppen, von denen mindestens $p^{\alpha-\rho}q^\mu - q^\mu + 1$ in den q^μ Gruppen $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots$ enthalten sind, die durch $\mathfrak{D}$ theilbar sind. Jede dieser q^μ Gruppen $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots$ enthält eine der q^μ Gruppen $\mathfrak{R}, \mathfrak{R}_1, \mathfrak{R}_2, \ldots$ der Ordnung p^ρ, durch die $\mathfrak{D}'$ theilbar ist. Da $\mathfrak{D}' = \mathfrak{R}\mathfrak{S}$ ist, so giebt es in $\mathfrak{S}$ ein solches Element S, dass $S^{-1}\mathfrak{R}S = \mathfrak{R}_x$ ist. Ist also $\mathfrak{R}$ in $\mathfrak{A}$ enthalten, so ist $\mathfrak{R}_x$ in $\mathfrak{A}_x = S^{-1}\mathfrak{A}S$ enthalten. Je zwei der Gruppen $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots$ können also durch ein Element von $\mathfrak{S}$ in einander transformirt werden.

Nun sei $\mathfrak{S}$ *irgend* eine in $\mathfrak{D}'$ enthaltene Gruppe der Ordnung q^μ, und $\mathfrak{B}$ *irgend* eine durch $\mathfrak{S}$ theilbare Gruppe der Ordnung $q^{2\mu}$. Dann ist $\mathfrak{S}$ der grösste gemeinsame Theiler von $\mathfrak{D}'$ und $\mathfrak{B}$, und $\mathfrak{D}$ ist mit den q^μ Elementen von $\mathfrak{S}$, aber mit keinen anderen Elemente von $\mathfrak{B}$ vertauschbar. Transformirt man daher $\mathfrak{D}$ mit den $q^{2\mu}$ Elementen von $\mathfrak{B}$, so erhält man q^μ verschiedene mit $\mathfrak{D}$ conjugirte Gruppen $\mathfrak{D}, \mathfrak{D}_1, \ldots, \mathfrak{D}_x, \ldots$, deren eine gleich $\mathfrak{D}$ ist. Von den $q^\mu - 1$ übrigen ist keine in einer der q^μ Gruppen $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots$ enthalten, die durch $\mathfrak{D}$ theibar sind. Denn sei O ein Element von $\mathfrak{B}$, und sei $O\mathfrak{D}O^{-1}$ in $\mathfrak{A}$ enthalten. Dann ist $\mathfrak{D}$ in $O^{-1}\mathfrak{A}O = \mathfrak{A}_x$ enthalten. Wie oben gezeigt, ist aber auch $S^{-1}\mathfrak{A}S = \mathfrak{A}_x$, wo S ein Element von $\mathfrak{S}$, also auch von $\mathfrak{B}$ ist. Daher ist OS^{-1} mit $\mathfrak{A}$ vertauschbar, also in $\mathfrak{A}' = \mathfrak{A}$ enthalten, aber auch in $\mathfrak{B}$, und folglich ist $OS^{-1} = E$, also ist $O = S$ in $\mathfrak{S}$ enthalten. Ist also O in $\mathfrak{B}$, aber nicht in $\mathfrak{S}$ enthalten, so ist $O\mathfrak{D}O^{-1}$ in keiner der q^μ Gruppen $\mathfrak{A}$ enthalten, die durch $\mathfrak{D}$ theilbar sind. Ist

$$\mathfrak{B} = \mathfrak{S} + \mathfrak{S}O_1 + \mathfrak{S}O_2 + \ldots$$

so ist $O_1O_2^{-1}$ nicht in $\mathfrak{S}$ enthalten. Transformirt man also $\mathfrak{D}$ mit allen Ele-

menten von $\mathfrak{B}$, so erhält man q^μ Gruppen $\mathfrak{D}$, $\mathfrak{D}_1 = O_1^{-1}\mathfrak{D}O_1$, $\mathfrak{D}_2 = O_2^{-1}\mathfrak{D}O_2, \ldots$, von denen ausser $\mathfrak{D}$ keine in einer der q^μ Gruppen $\mathfrak{A}$, $\mathfrak{A}_1$, $\mathfrak{A}_2$, ... enthalten ist. Diese aber enthalten von den $p^{\alpha-\rho}q^\mu$ mit $\mathfrak{D}$ conjugirten Gruppen mindestens $p^{\alpha-\rho}q^\mu - q^\mu + 1$. Daher enthalten sie auch nicht mehr, genau $q^\mu - 1$ der mit $\mathfrak{D}$ conjugirten Gruppen, etwa $\mathfrak{D}_1$, $\mathfrak{D}_2$, ..., $\mathfrak{D}_x$, ... sind in keiner durch $\mathfrak{D}$ theilbaren Gruppe $\mathfrak{A}$ enthalten, und die q^μ Gruppen $\mathfrak{D}$, $\mathfrak{D}_1$, $\mathfrak{D}_2$, ... und keine anderen findet man, indem man $\mathfrak{D}$ mit den $q^{2\mu}$ Elementen *irgend* einer Gruppe $\mathfrak{B}$ transformirt, die mit $\mathfrak{D}'$ einen Theiler $\mathfrak{S}$ der Ordnung q^μ gemeinsam hat. Diese geistreiche Überlegung bildet den Kern des Beweises, den Herr C. Jordan für die Auflösbarkeit der Gruppen der Ordnung $p^\alpha q^2$ gegeben hat.

Nun sei P irgend ein Element von $\mathfrak{D}'$, und O irgend ein Element von $\mathfrak{B}$. Dann kann man zu den q^μ Gruppen $\mathfrak{D}$, $\mathfrak{D}_1$, $\mathfrak{D}_2$, ..., $\mathfrak{D}_x$, ... auch gelangen, indem man statt $\mathfrak{B}$ die Gruppe $P^{-1}\mathfrak{B}P$ benutzt, die mit $\mathfrak{D}'$ die Gruppe $P^{-1}\mathfrak{S}P$ gemeinsam hat. Transformirt man also $\mathfrak{D}$ mit dem Elemente $P^{-1}OP$ der Gruppe $P^{-1}\mathfrak{B}P$, so erhält man eine jener Gruppe $\mathfrak{D}_x$. Es giebt aber auch in $\mathfrak{B}$ ein Element O', das $\mathfrak{D}$ in $\mathfrak{D}_x$ transformirt. Daher ist $P^{-1}OPO'^{-1}$ mit $\mathfrak{D}$ vertauschbar, also in $\mathfrak{D}'$ enthalten. Mithin ist auch $OPO'^{-1} = P'$ in $\mathfrak{D}'$ enthalten. Sind also P und O irgend zwei Elemente von $\mathfrak{D}'$ und $\mathfrak{B}$, so giebt es in diesen Gruppen zwei solche Elemente P' und O', dass $OP = P'O'$ ist. Daher sind $\mathfrak{B}'$ und $\mathfrak{D}$ mit einander vertauschbar, ihr Product $\mathfrak{B}'\mathfrak{D} = \mathfrak{D}\mathfrak{B}'$ ist eine Gruppe, deren Ordnung gleich $p^\rho q^{2\mu}$ ist, weil der grösste gemeinsame Divisor $\mathfrak{S}$ von $\mathfrak{D}$ und $\mathfrak{B}'$ die Ordnung q^μ hat.

Ist aber A ein invariantes Element einer der durch $\mathfrak{D}$ theilbaren Gruppen $\mathfrak{A}$, so ist A in $\mathfrak{D}'$, also auch in $\mathfrak{B}\mathfrak{D}'$ enthalten. Ist also $\rho < \alpha$, so ist $\mathfrak{H}$ zusammengesetzt.

3) Ist $\rho = \alpha$ und $\sigma = \mu$, so enthält $\mathfrak{H}$ genau q^μ mit $\mathfrak{D}$ conjugirte Gruppen $\mathfrak{D}_x$. Die mit $\mathfrak{D}_x$ vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppe $\mathfrak{D}'_x$ der Ordnung $p^\alpha q^\mu$. Sie enthält von den q^μ mit $\mathfrak{D}$ conjugirten Gruppen nur die eine $\mathfrak{D}_x$, und von den $q^{2\mu}$ mit $\mathfrak{A}$ conjugirten Gruppen genau q^μ, nämlich die, welche durch $\mathfrak{D}_x$ theilbar sind. Jede der $q^{2\mu}$ Gruppen $\mathfrak{A}$ enthält nur eine der q^μ Gruppen $\mathfrak{D}$. Jede der q^μ Gruppen $\mathfrak{D}$ ist in q^μ der $q^{2\mu}$ Gruppen $\mathfrak{A}$ enthalten, und diese sind alle in $\mathfrak{D}'$ enthalten. Zwei verschiedene Gruppen $\mathfrak{D}'$ und $\mathfrak{D}'_1$ haben keine Gruppe $\mathfrak{A}$ gemeinsam.

Man wähle $\mathfrak{D}'$ und $\mathfrak{D}'_1$ so, dass sie beide durch eine Gruppe $\mathfrak{T}$ theilbar

sind, deren Ordnung p^τ eine möglichst hohe Potenz von p ist. Dann ist $\tau < \alpha$. Ist $\tau > 0$, so hat $\mathfrak{H}$ stets eine invariante Untergruppe: Die mit $\mathfrak{T}$ vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppen $\mathfrak{T}'$, deren Ordnung $p^\rho q^\sigma < h$ sei. Da $\tau < \alpha$ ist, so ist $\rho > \tau$. Ist $\sigma = 2\mu$, so ist $\mathfrak{H}$ zusammengesetzt, weil $\mathfrak{T}'$ ein Element A enthält, das in einer Gruppe $\mathfrak{A}$ invariant ist. Sei also $\sigma < 2\mu$.

Die in $\mathfrak{T}'$ enthaltenen Gruppen $\mathfrak{R}, \mathfrak{R}_1, \mathfrak{R}_2, \ldots$ der Ordnung p^ρ können nicht alle in $\mathfrak{D}'$ enthalten sein. Denn $\mathfrak{T}$ ist mit den Elementen einer in $\mathfrak{D}_1'$ enthaltenen Gruppe der Ordnung $p^{\tau+1}$ vertauschbar. Diese ist also in $\mathfrak{T}'$, mithin in einer der Gruppen $\mathfrak{R}, \mathfrak{R}_1, \ldots$, also in $\mathfrak{D}'$ enthalten, während die Ordnung des grössten gemeinsamen Theilers von $\mathfrak{D}$ und $\mathfrak{D}_1'$ nur durch p^τ theilbar ist. Damit ist der Fall erledigt, wo $\mathfrak{T}'$ nur eine Gruppe $\mathfrak{R}$ enthält.

Im anderen Falle enthält $\mathfrak{T}'$, da $\sigma < 2\mu$ ist, q^μ Gruppen $\mathfrak{R}, \mathfrak{R}_1, \ldots$. Von diesen sind nicht zwei in $\mathfrak{D}'$ enthalten. Denn sonst wäre der grösste gemeinsame Theiler von $\mathfrak{T}'$ und $\mathfrak{D}'$ eine Gruppe der Ordnung $p^\rho q^\psi$ und enthielte zwei, also q^μ der Gruppen $\mathfrak{R}$, und folglich wären die q^μ Gruppen $\mathfrak{R}$ alle in $\mathfrak{D}'$ enthalten. Ist also $\mathfrak{R}_\varkappa$ in $\mathfrak{D}_\varkappa'$ enthalten, so sind die q^μ Gruppen $\mathfrak{D}', \mathfrak{D}_1', \mathfrak{D}_2', \ldots$ alle unter einander verschieden. Die q^μ mit $\mathfrak{D}'$ conjugirten Gruppen sind folglich alle durch $\mathfrak{T}$ theilbar, also ist $\mathfrak{H}$ zusammengesetzt.

Sei demnach $\tau = 0$. Dann haben zwei der q^μ Gruppen $\mathfrak{D}'$ kein Element gemeinsam, dessen Ordnnng eine Potenz von p ist. Nun enthält $\mathfrak{D}'$ q^μ Gruppen $\mathfrak{A}$, die durch $\mathfrak{D}$ theilbar sind, sonst aber kein Element gemeinsam haben. Daher enthält $\mathfrak{D}'$ ausser dem Hauptelemente $(p^\alpha - p^\delta)q^\mu + p^\delta - 1$ Elemente, deren Ordnungen in p^α aufgehen, und die q^μ mit $\mathfrak{D}'$ conjugirten Gruppen enthalten

$$p^\alpha q^{2\mu} - (q^\mu - 1)(p^\delta q^\mu + 1)$$

solche Elemente. Die Anzahl der Elemente von $\mathfrak{H}$, deren Ordnungen in p^α aufgehen, ist aber durch p^α theilbar. Daher ist $q^\mu \equiv 1 \pmod{p^\alpha}$.

4) Sei O ein Element von $\mathfrak{H}$, dessen Ordnung eine Potenz von q ist. Die mit O vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppe $\mathfrak{G}$ der Ordnung $p^\rho q^\sigma$. Man kann O so wählen, dass $\rho > 0$ ist. Denn sonst enthielte $\mathfrak{H}$ kein Element, dessen Ordnung durch p und q theilbar ist, also

$$(q^\mu - 1)(p^\delta q^\mu + 1) + 1 = p^\delta q^{2\mu} - (p^\delta - 1)q^\mu$$

Elemente, deren Ordnungen in $q^{2\mu}$ aufgehen. Diese Anzahl muss durch $q^{2\mu}$ theilbar sein. Daher wäre $p^\delta \equiv 1 \pmod{q^\mu}$, während $q^\mu \equiv 1 \pmod{p^\alpha}$ ist.

Seien $\mathfrak{R}$ und $\mathfrak{S}$ zwei in $\mathfrak{T}$ enthaltene Gruppen der Ordnungen p^ρ und q^σ, $\mathfrak{B}$ eine durch $\mathfrak{S}$ theilbare Gruppe der Ordnung $q^{2\mu}$, B ein invariantes Element von $\mathfrak{B}$. Dann ist B in $\mathfrak{G}$ enthalten. Ist also $\rho = \alpha$, so ist $\mathfrak{H}$ zusammengesetzt. Sei also $0 < \rho < \alpha$. B ist nicht in der Gruppe $\mathfrak{D}'$ der Ordnung $p^\alpha q^\mu$ enthalten, also nicht mit $\mathfrak{D}$, und auch nicht mit $\mathfrak{D}'$ vertauschbar. Daher ist $\mathfrak{R}$ von $B^{-1}\mathfrak{R}B$ verschieden. Denn sonst wäre $\mathfrak{R} = B^{-1}\mathfrak{R}B$ in den beiden verschiedenen Gruppen $\mathfrak{D}'$ und $B^{-1}\mathfrak{D}'B$ enthalten, während diese nach der gemachten Annahme keinen Theiler gemeinsam haben, dessen Ordnung eine Potenz von p ist. Folglich enthält $\mathfrak{G}$ mehrere Gruppen $\mathfrak{R}, \mathfrak{R}_1, \mathfrak{R}_2, \ldots$, also q^μ oder $q^{2\mu}$. Im letzteren Falle wäre $\sigma = 2\mu$, und wäre $\mathfrak{R}$ mit keinem Elemente von $\mathfrak{G}$ vertauchbar, dessen Ordnung eine Potenz von q ist. Da aber $\mathfrak{R}$ mit O vertauschbar ist, so enthält $\mathfrak{G}$ genau q^μ Gruppen $\mathfrak{R}$. Von diesen sind nicht zwei in $\mathfrak{D}'$ enthalten. Denn sonst enthielte auch der grösste gemeinsame Theiler von $\mathfrak{G}$ und $\mathfrak{D}'$ zwei, also q^μ, also alle Gruppen $\mathfrak{R}$. Mithin enthielte $\mathfrak{D}'$ die Gruppe $B\mathfrak{R}B^{-1}$, und $\mathfrak{R}$ wäre in den beiden verschiedenen Gruppen $\mathfrak{D}'$ und $B^{-1}\mathfrak{D}'B$ enthalten.

Ist also $\mathfrak{R}_x$ in $\mathfrak{D}'_x$ enthalten, so sind die q^μ Gruppen $\mathfrak{D}'_x$ alle unter einander verschieden. Nun ist O mit $\mathfrak{R}_x$ vertauschbar, also auch mit $\mathfrak{D}'_x$, weil sonst die beiden Gruppen $\mathfrak{D}'_x$ und $O^{-1}\mathfrak{D}'_x O$ verschieden und beide durch $\mathfrak{R}_x$ theilbar wären. Folglich ist O in $\mathfrak{D}'_x$ enthalten, also in allen mit $\mathfrak{D}'$ conjugirten Gruppen, und mithin ist $\mathfrak{G}$ keine einfache Gruppe.

Zum Beweise der Auflösbarkeit jeder Gruppe $\mathfrak{H}$ der Ordnung $p^\alpha q^2$ reichen die unter 1) und 2) angestellten Überlegungen aus. Denn jede Gruppe $\mathfrak{B}$ der Ordnung q^2 ist eine commutative. Enthält daher $\mathfrak{H}$ eine Gruppe der Ordnung $p^\alpha q$, so ist ein darin enthaltenes Element B der Ordnung q ein invariantes Element jeder durch B theilbaren Gruppe $\mathfrak{B}$ der Ordnung q^2.

Damit ist der Beweis durch rein gruppentheoretische Betrachtungen geführt, ohne jede Hülfe der Substitutionstheorie, d. h. ohne Benutzung irgend einer Darstellung der Gruppe $\mathfrak{G}$.