Ueber eine specielle Classe von Gruppen.

Von

E. WENDT in Elsfleth i./Old.

Unter allen Gruppen verdienen die *auflösbaren*, hauptsächlich wegen ihrer wichtigen Beziehungen zur Theorie der algebraischen Gleichungen, das grösste Interesse. Nach der gewöhnlichen Definition heisst eine Gruppe „*auflösbar*“, wenn die Factorgruppen ihrer Compositionsreihen von Primzahlordnung sind. Man kann dieser Definition aber noch eine andere Fassung geben, man kann eine Gruppe auch *auflösbar* nennen, wenn die Factorgruppen ihrer Hauptreihen (Hauptcompositionsreihen) von Primzahlpotenzordnung sind. Beide Definitionen*) decken sich. Um dem eigentlichen Ziel, alle Typen auflösbarer Gruppen von vorgeschriebener Ordnung zu bestimmen, näher zu kommen, hat man den Charakter der Auflösbarkeit für specielle Gruppen nachgewiesen. Die meisten unter diesen, wie z. B. die Gruppen von Primzahlpotenzordnung, die Gruppen von quadratfreier Ordnungszahl, die Gruppen, deren Untergruppen von Primzahlpotenzordnung cyklisch sind, etc. haben die Eigenschaft, dass sich unter ihren Compositionsreihen solche befinden, die zugleich Hauptreihen sind, oder, wie man besser sagt, dass die Factorgruppen ihrer Hauptreihen von Primzahlordnung sind. Alle mit dieser Eigenschaft versehenen Gruppen verdienen daher wohl eine besondere Beachtung.

Bei dem Versuch, alle derartigen Gruppen von vorgeschriebener Ordnung zu bestimmen, bin ich auf einen, wie ich glaube, merkwürdigen Satz gestossen, der ein interessantes von Herrn Hölder gefundenes Resultat**) als speciellen Fall enthält. Bevor ich denselben ausspreche, ist es nothwendig, auf eine für beliebige Gruppen gültige Thatsache aufmerksam zu machen. Unter allen invarianten Untergruppen einer Gruppe G ,

*) Jordan, *Traité des substitutions* (1870).

Hölder, Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen. *Math. Ann.* Bd. 34.

**) Siehe § 2.

die sich als das directe Product von Gruppen von Primzahlpotenzordnung darstellen, befindet sich eine, in der alle anderen Untergruppen dieser Art enthalten sind, welche also als die *grösste* derselben bezeichnet werden kann. Ist $\mathfrak{H}$ nämlich irgend eine solche invariante Untergruppe von $\mathfrak{G}$, sind $p_1, p_2, \dots$ die verschiedenen in der Ordnung von $\mathfrak{H}$ enthaltenen Primzahlen und $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots$ die höchsten in dieser Ordnung aufgehenden Potenzen dieser Primzahlen, so kann man $\mathfrak{H}$ als das directe Product von Gruppen $\mathfrak{P}_1, \mathfrak{P}_2, \dots$ darstellen, deren Ordnungszahlen bezw. $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots$ sind. Ist $\mathfrak{P}$ eine beliebige derselben, so muss sie, da sie die einzige Untergruppe von $\mathfrak{H}$ ihrer Art ist, also auch innerhalb $\mathfrak{G}$ keine conjugirten Gruppen besitzen kann, eine invariante Untergruppe nicht bloss von $\mathfrak{H}$, sondern auch von $\mathfrak{G}$ sein. Ist $\mathfrak{H}'$ eine andere Untergruppe von $\mathfrak{G}$ von derselben Art wie $\mathfrak{H}$, sind $p_1^{\alpha'_1}, p_2^{\alpha'_2}, \dots$ die verschiedenen höchsten in der Ordnung von $\mathfrak{H}'$ aufgehenden Primzahlpotenzen, und ist $\mathfrak{H}'$ das directe Product von Gruppen $\mathfrak{P}'_1, \mathfrak{P}'_2, \dots$, deren Ordnungszahlen bezw. $p_1^{\alpha'_1}, p_2^{\alpha'_2}, \dots$ sind, so ist jede derselben eine invariante Untergruppe nicht bloss von $\mathfrak{H}'$, sondern auch von $\mathfrak{G}$. Jedes Element P' irgend einer dieser Gruppen $\mathfrak{P}'$ transformirt $\mathfrak{P}$ in sich selbst, und jedes Element P von $\mathfrak{P}$ transformirt $\mathfrak{P}'$ in sich selbst. Betrachtet man das Element $P'^{-1}P^{-1}P'P$, so ist dieses, als Product von P'^{-1} und $P^{-1}P'P$ aufgefasst, ein Element von $\mathfrak{P}'$, als Product von $P'^{-1}P^{-1}P'$ und P aufgefasst, ein Element von $\mathfrak{P}$. Sind daher p und p' von einander verschieden, können also $\mathfrak{P}$ und $\mathfrak{P}'$ ausser der Einheit kein gemeinsames Element enthalten, so muss $P'^{-1}P^{-1}P'P=1$, d. h. P mit P' vertauschbar sein. Sind die Primzahlen p und p' einander gleich, so erzeugen die Elemente von $\mathfrak{P}$ und $\mathfrak{P}'$ zusammen eine Gruppe, deren Ordnung ebenfalls eine Potenz von $p = p'$ ist. Das kleinste gemeinschaftliche Vielfache von $\mathfrak{H}$ und $\mathfrak{H}'$ oder, was dasselbe ist, das kleinste gemeinschaftliche Vielfache der Gruppen $\mathfrak{P}_1, \mathfrak{P}_2, \dots$ und $\mathfrak{P}'_1, \mathfrak{P}'_2, \dots$ ist daher ebenfalls eine Gruppe, die das directe Product von Gruppen von Primzahlpotenzordnung ist. Und es ist auch eine invariante Untergruppe von $\mathfrak{G}$, weil es $\mathfrak{H}$ und $\mathfrak{H}'$ sind. Daraus folgt aber sofort die obige Behauptung, dass jede Gruppe eine *grösste* invariante Untergruppe besitzen muss, die das directe Product von Gruppen von Primzahlpotenzordnung ist.

Der Satz, dessen vorhin gedacht wurde, lautet nun:

Ist $\mathfrak{M}$ eine Gruppe, in deren Hauptreihen die Factorgruppen von Primzahlordnung sind, und ist $\mathfrak{N}$ die grösste invariante Untergruppe von $\mathfrak{M}$, die sich als das directe Product von Gruppen von Primzahlpotenzordnung darstellt, so ist die zu $\mathfrak{N}$ complementäre Gruppe $\frac{\mathfrak{M}}{\mathfrak{N}}$ eine Abel'sche.

Allerdings ist dieser Satz nicht umkehrbar. Wenn nämlich $\mathfrak{G}'$ die

grösste unter allen invarianten Untergruppen einer Gruppe $\mathfrak{G}$ ist, die das directe Product von Gruppen von Primzahlpotenzordnung sind, und wenn $\frac{\mathfrak{G}}{\mathfrak{G}'}$ eine Abel'sche Gruppe ist, so ist die Gruppe $\mathfrak{G}$, wie sofort ersichtlich, auflösbar, aber es brauchen nicht die Factorgruppen ihrer Hauptreihen von Primzahlordnung zu sein. Herr Steinitz, dem ich auch die Fassung des obigen Satzes in der vorliegenden Form verdanke, hat mich auf ein einfaches Beispiel aufmerksam gemacht. Es ist die alternirende Gruppe von vier Ziffern, welche eine einzige invariante Untergruppe, nämlich die Gruppe vierter Ordnung

$$1, (0, 2) (1, 3), (0, 1) (2, 3), (0, 3) (1, 2)$$

enthält.

Ich schreite nun zum Beweise des obigen Satzes.

§ 1.

Es sei $\mathfrak{M}$ eine Gruppe der besagten Art,

$$(1) \quad \mathfrak{M} = \mathfrak{M}_0, \mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_\varrho = 1$$

eine Hauptreihe derselben, welche die zugehörige Indexreihe

$$(2) \quad j_0, j_1, j_2, \dots, j_{\varrho-1}$$

besitze. Dann sind diese letzteren Zahlen Primzahlen, und die Factorgruppen $\frac{\mathfrak{M}_\alpha}{\mathfrak{M}_{\alpha+1}}$ ($\alpha=0, 1, \dots, \varrho-1$) sind cyklische Gruppen von Primzahlordnung. Bedeutet daher M_α ($\alpha=0, 1, \dots, \varrho-1$) ein in $\mathfrak{M}_\alpha$, aber nicht in $\mathfrak{M}_{\alpha+1}$ enthaltenes Element, so zerfällt $\mathfrak{M}_\alpha$ in die Nebengruppen

$$\mathfrak{M}_{\alpha+1}, M_\alpha \mathfrak{M}_{\alpha+1}, M_\alpha^2 \mathfrak{M}_{\alpha+1}, \dots, M_\alpha^{j_\alpha-1} \mathfrak{M}_{\alpha+1},$$

welche die Elemente der Gruppe $\frac{\mathfrak{M}_\alpha}{\mathfrak{M}_{\alpha+1}}$ ausmachen. Die niedrigste in $\mathfrak{M}_{\alpha+1}$ enthaltene Potenz von M_α ist die j_α^{te} . Die Ordnung von M_α ist durch j_α theilbar, und jedes zu $\mathfrak{M}_\alpha$, aber nicht zu $\mathfrak{M}_{\alpha+1}$ gehörige Element hat die Form $M_\alpha^{k_\alpha} A_{\alpha+1}$, wo k_α einen der Werthe $1, 2, \dots, j_\alpha-1$ besitzt und $A_{\alpha+1}$ der Gruppe $\mathfrak{M}_{\alpha+1}$ angehört. Man kann auch stets solche Elemente M_α finden, deren Ordnungszahl eine Potenz der Primzahl j_α ist. Denn hat M_α etwa die Ordnung $j_\alpha^\alpha \cdot \mu_\alpha$, wo μ_α relativ prim zu j_α ist, so ist $M_\alpha^{\mu_\alpha}$ ein Element, das zu $\mathfrak{M}_\alpha$, aber nicht zu $\mathfrak{M}_{\alpha+1}$ gehört und dessen Ordnung gleich j_α^α ist.

Sei nun M_α ($\alpha=0, 1, \dots, \varrho-1$) ein in $\mathfrak{M}_\alpha$, aber nicht in $\mathfrak{M}_{\alpha+1}$ enthaltenes Element, und bedeute R irgend ein Element aus $\mathfrak{M}$, dessen

Ordnung r heisse. Da $\mathfrak{M}_\alpha$ eine invariante Untergruppe von $\mathfrak{M}$ ist, so muss eine Gleichung von der Form bestehen:

$$(3) \quad R^{-1} M_\alpha R = M_\alpha^{\nu_\alpha} S; \quad (0 < \nu_\alpha < j_\alpha)$$

wo S ein der Gruppe $\mathfrak{M}_{\alpha+1}$ angehöriges Element bezeichnet, oder auch von folgender Gestalt:

$$(4) \quad R^{-1} M_\alpha R \mathfrak{M}_{\alpha+1} = M_\alpha^{\nu_\alpha} \mathfrak{M}_{\alpha+1}.$$

Für beliebige positive ganze Zahlen σ und τ folgt hieraus

$$(5) \quad R^{-\tau} M_\alpha^\sigma R^\tau \mathfrak{M}_{\alpha+1} = M_\alpha^{\sigma \cdot \nu_\alpha^\tau} \mathfrak{M}_{\alpha+1},$$

weil R und M_α mit $\mathfrak{M}_{\alpha+1}$ vertauschbar sind. Setzt man hierin $\tau = r$, so ergibt sich, da $R^r = 1$ ist, $M_\alpha^\sigma \mathfrak{M}_{\alpha+1} = M_\alpha^{\sigma \cdot \nu_\alpha^r} \mathfrak{M}_{\alpha+1}$, und daraus

$$(6) \quad \nu_\alpha^r \equiv 1 \pmod{j_\alpha}.$$

Ist R' ein weiteres Element aus $\mathfrak{M}$, so gelten die den Gleichungen (4) und (5) entsprechenden Gleichungen

$$(7) \quad R'^{-1} M_\alpha R' \mathfrak{M}_{\alpha+1} = M_\alpha^{\nu'_\alpha} \mathfrak{M}_{\alpha+1}; \quad R'^{-\tau} M_\alpha^\sigma R'^\tau = M_\alpha^{\sigma \cdot \nu'^\tau_\alpha} \mathfrak{M}_{\alpha+1}.$$

Transformirt man beide Seiten der Gleichung (4) mit R' , so ergibt sich mit Hilfe von (7)

$$R'^{-1} R^{-1} M_\alpha R R' \mathfrak{M}_{\alpha+1} \quad \text{oder} \quad (R R')^{-1} M_\alpha (R R') \mathfrak{M}_{\alpha+1} = M_\alpha^{\nu_\alpha \cdot \nu'_\alpha} \mathfrak{M}_{\alpha+1}.$$

Transformirt man beide Seiten der ersteren der Gleichungen (7) mit R und benutzt die Gleichung (5), so erhält man

$$(R R')^{-1} M_\alpha (R R') \mathfrak{M}_{\alpha+1} = M_\alpha^{\nu_\alpha \cdot \nu'_\alpha} \mathfrak{M}_{\alpha+1}.$$

Die beiden letzten Gleichungen lehren, dass der Complex $M_\alpha \mathfrak{M}_{\alpha+1}$ durch jedes der Elemente RR' und $R'R$ in den Complex $M_\alpha^{\nu_\alpha \cdot \nu'_\alpha} \mathfrak{M}_{\alpha+1}$ transformirt wird, folglich muss er durch das Element

$$N = (R R')^{-1} (R R') = R^{-1} R'^{-1} R R'$$

in sich selbst transformirt werden. Dieses Element N ist also mit anderen Worten mit dem Complex $M_\alpha \mathfrak{M}_{\alpha+1}$ und daher mit allen Elementen der Factorgruppe $\frac{\mathfrak{M}_\alpha}{\mathfrak{M}_{\alpha+1}}$ vertauschbar. Die Zahl α stellt hierbei irgend einen der Werthe $0, 1, \dots, \rho - 1$ vor, und R und R' bedeuten zwei beliebige Elemente aus $\mathfrak{M}$. Es gilt also allgemein die Gleichung

$$(8) \quad R'^{-1} R R' = R N,$$

wo N ein Element ist, das mit allen Elementen der sämtlichen Factorgruppen $\frac{\mathfrak{M}_\alpha}{\mathfrak{M}_{\alpha+1}}$ ($\alpha = 0, 1, \dots, \rho - 1$) vertauschbar ist.

Nun bilden alle Elemente von $\mathfrak{M}$, die wie N mit allen Elementen der Factorgruppen $\frac{\mathfrak{M}_\alpha}{\mathfrak{M}_{\alpha+1}}$ ($\alpha = 0, 1, \dots, \varrho - 1$) vertauschbar sind, eine Gruppe $\mathfrak{N}$. Denn, wenn zwei Elemente mit einem Complex $M_\alpha \mathfrak{M}_{\alpha+1}$ vertauschbar sind, so ist auch deren Product mit diesem vertauschbar. Lässt man in Gleichung (8) R alle Elemente von $\mathfrak{N}$, R' alle Elemente von $\mathfrak{M}$ durchlaufen, so erkennt man, dass $\mathfrak{N}$ eine invariante Untergruppe von $\mathfrak{M}$ ist, weil ja jedes Element R von $\mathfrak{N}$ wieder in ein Element RN von $\mathfrak{N}$ transformirt wird. Die Gleichung (8) lässt sich für beliebige Elemente R und R' von $\mathfrak{M}$ aber auch in die Form setzen

$$(9) \quad RR'\mathfrak{N} = R'R\mathfrak{N},$$

und diese Gleichung drückt aus, dass die zu $\mathfrak{N}$ complementäre Gruppe $\frac{\mathfrak{M}}{\mathfrak{N}}$ eine Abel'sche ist.

Aus Gleichung (8) lässt sich noch eine weitere Folgerung ziehen, wenn man unter R und R' zwei Elemente aus $\mathfrak{N}$ versteht. Es möge R noch in $\mathfrak{M}_\beta$, aber nicht mehr in $\mathfrak{M}_{\beta+1}$ enthalten sein, wo β einen der Werthe $0, 1, \dots, \varrho - 1$ bedeutet. Da im vorliegenden Falle R' mit den Elementen der Factorgruppe $\frac{\mathfrak{M}_\beta}{\mathfrak{M}_{\beta+1}}$ vertauschbar ist, so gehört das in der Gleichung (8) auftretende Element N der Gruppe $\mathfrak{M}_{\beta+1}$ an. Nimmt man an, dass dasselbe, falls es von 1 verschieden ist, noch in der Gruppe $\mathfrak{M}_\gamma$ ($\gamma > \beta$), aber nicht mehr in der Gruppe $\mathfrak{M}_{\gamma+1}$ enthalten ist, und schreibt die Gleichung (8) in der Form

$$R'^{-1}RR'\mathfrak{M}_{\gamma+1} = RN\mathfrak{M}_{\gamma+1},$$

so folgt, da nach Voraussetzung R und R' Elemente von $\mathfrak{N}$ sind und als solche mit dem Complex $N\mathfrak{M}_{\gamma+1}$ vertauschbar sein müssen, für beliebige positive ganze Zahlen σ und τ

$$R'^{-\tau}R^\sigma R'^\tau \mathfrak{M}_{\gamma+1} = R^\sigma N^{\sigma \cdot \tau} \mathfrak{M}_{\gamma+1}.$$

Sind r und r' die Ordnungen von R und R' , so folgt für $\tau = r'$, $\sigma = 1$ aus dieser Gleichung $\mathfrak{M}_{\gamma+1} = N^{r'} \mathfrak{M}_{\gamma+1}$, und für $\tau = 1$, $\sigma = r$ ergibt sich $\mathfrak{M}_{\gamma+1} = N^r \mathfrak{M}_{\gamma+1}$. Es gehören also N^r und $N^{r'}$ der Gruppe $\mathfrak{M}_{\gamma+1}$ an. In dem Falle, dass r und r' theilerfremd sind, würde demnach folgen, dass N selbst in $\mathfrak{M}_{\gamma+1}$ enthalten wäre. Da das aber der gemachten Annahme widerspricht, so muss in diesem Falle $N = 1$ und daher nach (8) $RR' = R'R$ sein. Alle zu $\mathfrak{N}$ gehörigen Elemente, deren Ordnungszahlen theilerfremd sind, sind demnach vertauschbar. Daraus folgt weiter in bekannter Weise mit Hülfe des Sylow'schen Satzes, dass $\mathfrak{N}$ das directe Product von Gruppen von Primzahlpotenzordnung ist.

Bedeutet nun wie in der Einleitung $\mathfrak{N}$ die grösste unter allen invarianten Untergruppen von $\mathfrak{M}$, die sich als das directe Product von Gruppen von Primzahlpotenzordnung darstellen, so ist $\mathfrak{N}'$ eine invariante Untergruppe von $\mathfrak{N}$, und, weil, wie vorher bewiesen, $\frac{\mathfrak{M}}{\mathfrak{N}}$ eine Abel'sche Gruppe ist, so muss erst recht $\frac{\mathfrak{M}}{\mathfrak{N}}$ eine solche sein.

Damit ist der in der Einleitung aufgeführte Satz bewiesen. Ich will noch einige Bemerkungen hinzufügen. Da $\mathfrak{N}$ eine invariante Untergruppe von $\mathfrak{M}$ ist, so kann man eine Hauptreihe von $\mathfrak{M}$ bilden, in welcher $\mathfrak{N}$ vorkommt. Sei die Reihe (1) von dieser Beschaffenheit. Von $\mathfrak{N}$ an laute dieselbe

$$\mathfrak{N} = \mathfrak{M}_{\varphi'}, \mathfrak{M}_{\varphi'+1}, \dots, \mathfrak{M}_{\varphi-1}, \mathfrak{M}_{\varphi} = 1.$$

Es bedeute R ein beliebiges Element von $\mathfrak{N}$, dessen Ordnung r eine Potenz einer Primzahl p sei. Unter α verstehe man zunächst eine der Zahlen $\varphi', \varphi' + 1, \dots, \varphi$, und sei M_{α} ein Element von der Ordnung j_{α}^c , das in $\mathfrak{M}_{\alpha}$, aber nicht in $\mathfrak{M}_{\alpha+1}$ enthalten sei. Sind p und j_{α} von einander verschieden, so ist R mit M_{α} vertauschbar. Ist aber $p = j_{\alpha}$, so folgt aus der Congruenz (6), da r im vorliegenden Falle keinen Factor mit $j_{\alpha} - 1 = p - 1$ gemeinsam haben kann, dass $\nu_{\alpha} = 1$ ist. In jedem Falle ergibt sich mithin, dass R mit den Elementen der sämtlichen Factorgruppen $\frac{\mathfrak{M}_{\alpha}}{\mathfrak{M}_{\alpha+1}}$ ($\alpha = \varphi', \varphi' + 1, \dots, \varphi - 1$) vertauschbar ist. Mit den Elementen der übrigen Factorgruppen $\frac{\mathfrak{M}_{\alpha}}{\mathfrak{M}_{\alpha+1}}$ ($\alpha < \varphi'$) ist R aber auch vertauschbar, denn es ist für $\alpha < \varphi'$:

$$R(M_{\alpha}\mathfrak{M}_{\alpha+1}) = R\mathfrak{M}_{\alpha+1}M_{\alpha} = \mathfrak{M}_{\alpha+1}M_{\alpha} = M_{\alpha}\mathfrak{M}_{\alpha+1} = (M_{\alpha}\mathfrak{M}_{\alpha+1})R,$$

weil R ein Element in $\mathfrak{M}_{\varphi'}$, also auch von $\mathfrak{M}_{\alpha+1}$ ($\alpha < \varphi'$) ist. Alle diejenigen Elemente von $\mathfrak{N}$, deren Ordnung eine Primzahlpotenz ist, sind also mit den Elementen der Factorgruppen von $\mathfrak{M}$ vertauschbar. Da man sich nun $\mathfrak{N}$ durch Composition aus solchen Elementen entstanden denken kann, so haben alle Elemente von $\mathfrak{N}$ ohne Ausnahme die Eigenschaft, mit den Elementen der sämtlichen Factorgruppen von $\mathfrak{M}$ vertauschbar zu sein. Nun erzeugen aber nach den Untersuchungen dieses Paragraphen alle mit dieser Eigenschaft versehenen Elemente von $\mathfrak{M}$ eine invariante Untergruppe $\mathfrak{N}'$ von $\mathfrak{M}$, die ebenso wie $\mathfrak{N}$ das directe Product von Gruppen von Primzahlpotenzordnung ist, folglich muss $\mathfrak{N}' = \mathfrak{N}$ sein, und es darf also kein Element von $\mathfrak{M}$, das nicht zu $\mathfrak{N}$ gehört, mit den Elementen aller Factorgruppen $\frac{\mathfrak{M}_{\alpha}}{\mathfrak{M}_{\alpha+1}}$ ($\alpha \geq \varphi'$) vertauschbar sein. Diese Bedingung ist gleichbedeutend mit der, dass $\mathfrak{N}$ die grösste invariante Untergruppe von $\mathfrak{M}$ ist,

die sich als das directe Product von Gruppen von Primzahlpotenzordnung darstellt.

Es sei q die grösste der in der Ordnung von $\mathfrak{M}$ aufgehenden Primzahlen und q^e die höchste darin enthaltene Potenz von q . Bedeutet R ein Element von $\mathfrak{M}$, dessen Ordnung eine Potenz von q ist, so folgt aus der Congruenz (6) $\nu_\alpha = 1$. Denn, wenn diese Congruenz von 1 verschiedene Wurzeln haben soll, so müssen r und $j_\alpha - 1$ einen von 1 verschiedenen Theiler besitzen. Das ist aber im vorliegenden Falle nicht möglich, da ja r eine Potenz von q und $q \geq j_\alpha$ ist. Alle Elemente also, und daher auch alle Untergruppen von $\mathfrak{M}$, deren Ordnung eine Potenz der grössten in der Ordnung von $\mathfrak{M}$ aufgehenden Primzahl ist, sind mit den Elementen der Factorgruppen von $\mathfrak{M}$ vertauschbar und daher in $\mathfrak{N}'$ und auch in $\mathfrak{N}$ enthalten. Da $\mathfrak{N}$ das directe Product von Gruppen von Primzahlpotenzordnung ist, so giebt es folglich nur eine einzige Untergruppe von $\mathfrak{M}$ von der Ordnung q^e , und diese ist also eine in $\mathfrak{N}$ enthaltene invariante Untergruppe von $\mathfrak{M}$.

Eine algebraische Gleichung mit der Galois'schen Gruppe $\mathfrak{M}$ wird gelöst, indem man zuerst eine irreducible Abel'sche Gleichung, deren Grad gleich der Ordnung von $\frac{\mathfrak{M}}{\mathfrak{N}}$ ist, bildet, dann eine Wurzel dieser Gleichung dem Rationalitätsbereich adjungirt und darauf im erweiterten Bereich mehrere irreducible Normalgleichungen löst, deren Gradzahlen gleich den verschiedenen in der Ordnung von $\mathfrak{N}$ aufgehenden höchsten Primzahlpotenzen sind. Umgekehrt erhält man alle Normalkörper von vorgeschriebenem Grade m , deren Galois'sche Gruppe eine der hier betrachteten Art ist, auf folgende Weise. Es sei m' irgend ein Divisor von m und $m = m' \cdot n$, und y sei eine Wurzel einer irreduciblen Abel'schen Gleichung vom Grade m' . Die verschiedenen in n aufgehenden höchsten Primzahlpotenzen seien $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots$. Es bedeute z_1 eine Wurzel einer irreduciblen Normalgleichung vom Grade $p_1^{\alpha_1}$, deren Coefficienten rationale Functionen von y sind, z_2 eine Wurzel einer solchen vom Grade $p_2^{\alpha_2}$, $\dots$. Dann ist, wenn K den zu Grunde gelegten Rationalitätsbereich bezeichnet, der Körper $K(y, z_1, z_2, \dots)$ ein Normalkörper der verlangten Art.

§ 2.

Der in § 1 hergeleitete Satz enthält den von Herrn Hölder über Gruppen von quadratfreier Ordnungszahl bewiesenen Satz*) als besonderen Fall.

In Bezug auf Gruppen, deren Untergruppen von Primzahlpotenzordnung commutativ sind, ist unter gewissen Bedingungen nachgewiesen

*) Hölder, Gött. Nachr. 1895.

worden, dass sie auflösbar sind, z. B. dann, wenn jene Untergruppen cyklisch sind*). Ist $\mathfrak{M}$ eine Gruppe der letzteren Art und $m = p_1^{x_1} \cdot p_2^{x_2} \cdot p_3^{x_3} \cdots$ ihre Ordnung, wo $p_1, p_2, p_3, \cdots$ Primzahlen bedeuten und $p_1 < p_2 < p_3 < \cdots$ ist, so besitzt sie invariante Untergruppen von jeder Ordnung

$$p_i^{x'_i} \cdot p_{i+1}^{x'_{i+1}} \cdot p_{i+2}^{x'_{i+2}} \cdots (x'_i \leq x_i); (i = 1, 2, 3, \cdots).$$

Die Factorgruppen ihrer Hauptreihen sind daher von Primzahlordnung**). Der in § 1 bewiesene Satz nimmt jetzt die besondere Gestalt an:

Ist $\mathfrak{N}$ die grösste invariante cyklische Untergruppe von $\mathfrak{M}$, so ist die zu $\mathfrak{N}$ complementäre Gruppe $\frac{\mathfrak{M}}{\mathfrak{N}}$ cyklisch.

Zunächst ist nämlich klar, dass, da $\mathfrak{N}$ ein Theiler von $\mathfrak{M}$ ist, die Untergruppen von $\mathfrak{N}$ von Primzahlpotenzordnung cyklisch sind. Das gilt aber auch für die Gruppe $\frac{\mathfrak{M}}{\mathfrak{N}}$. Denn ist p irgend eine in der Ordnung m' von $\frac{\mathfrak{M}}{\mathfrak{N}}$ aufgehende Primzahl und ist sie in m genau κ mal, in m' genau λ mal, in der Ordnung $n = \frac{m}{m'}$ von $\mathfrak{N}$ also genau $\kappa - \lambda$ mal enthalten, so muss $\mathfrak{M}$ nach dem Sylow'schen Satze eine Untergruppe von der Ordnung p^κ , und, weil diese nach Voraussetzung cyklisch ist, ein Element P von der Ordnung p^κ enthalten, und es kann keine niedere als die p^{λ} te Potenz von P der Gruppe $\mathfrak{N}$ angehören. Denn der Exponent der niedrigsten in $\mathfrak{N}$ enthaltenen Potenz von P muss ein Divisor der Ordnung von P , also von der Form $p^{\lambda'}$ sein, und wäre nun etwa $\lambda' < \lambda$, so müsste $\mathfrak{N}$ die ganze durch $P^{p^{\lambda'}}$ erzeugte cyklische Gruppe von der Ordnung $p^{\kappa - \lambda'}$ enthalten, es müsste also n durch $p^{\kappa - \lambda'}$ theilbar sein, während doch die Primzahl p nur $\kappa - \lambda$ mal in n aufgehen soll. Es enthält demnach die Gruppe $\frac{\mathfrak{M}}{\mathfrak{N}}$ eine durch ihr Element $P\mathfrak{N}$ erzeugte cyklische Gruppe von der Ordnung p^{λ} , ihre Untergruppen von Primzahlpotenzordnung sind also cyklisch. Da nun $\frac{\mathfrak{M}}{\mathfrak{N}}$ als Abel'sche Gruppe ebenso wie $\mathfrak{N}$ das directe Product von Gruppen von Primzahlpotenzordnung ist, so folgt, dass $\mathfrak{N}$ und $\frac{\mathfrak{M}}{\mathfrak{N}}$ cyklisch sind.

Das erzeugende Element von $\mathfrak{N}$ heisse N , dass von $\frac{\mathfrak{M}}{\mathfrak{N}}$ heisse $M\mathfrak{N}$, wo M ein Element von $\mathfrak{M}$ bedeutet, dessen niedrigste in $\mathfrak{N}$ enthaltene Potenz die m' te ist. Es sei

$$(1) \quad M^{m'} = N^{n'}; \quad N^n = 1.$$

*) Frobenius, Ueber auflösbare Gruppen, II. Berl. Sitz. 1895.

Burnside, Proc. L. M. S. Vol. XXVI, 1895.

**) Derartige Gruppen besitzen demnach Hauptreihen, deren zugehörige Indices eine nicht absteigende Reihe von Primzahlen bilden. Dasselbe gilt auch für die allgemeinen in § 1 betrachteten Gruppen, wie leicht nachzuweisen ist.

Das Element N kann man sich so gewählt denken, dass n' ein Divisor von n ist*) Denn, ist d der grösste gemeinsame Divisor von n und n' , sind also $\frac{n}{d}$ und $\frac{n'}{d}$ relativ prim zu einander, so giebt es eine zu d und deswegen auch zu n theilerfremde Zahl x , welche den gleichberechtigten Congruenzen $x \equiv \frac{n'}{d} \pmod{\frac{n}{d}}$ und $dx \equiv n' \pmod{n}$ genügt. Setzt man nun $N' = N^x$, so ist zufolge (1) $M^{m'} = N^{n'} = N^{x \cdot d} = N'^d$; man braucht also nur N durch N' zu ersetzen, um den gewünschten Erfolg zu haben.

Ist N derartig gewählt, dass n durch n' theilbar ist, so ist die Ordnung von M gleich $m' \cdot \frac{n}{n'}$, da die von $N^{n'}$ gleich $\frac{n}{n'}$ ist.

Weiter kann man nun das Element M so wählen, dass die Zahl $\frac{n}{n'}$ nur Primfactoren besitzt, die in m' aufgehen, oder, was dasselbe ist, dass n' alle diejenigen Divisoren von n enthält, die zu m' relativ prim sind. Denn, ist d der grösste Divisor von $\frac{n}{n'}$, der zu m' relativ prim ist, so würde M^d die gewünschte Bedingung erfüllen, weil $(M^d)^{m'} = N^{n' \cdot d}$ ist. Es wird sich späterhin ergeben, dass n' relativ prim zu m' ist.

Da $\mathfrak{N}$ eine invariante cyklische Untergruppe von $\mathfrak{M}$ ist, so muss eine Gleichung von der Form

$$(2) \quad M^{-1}NM = N^v$$

bestehen. Für positive ganze Zahlen σ und τ folgt hieraus

$$(3) \quad M^{-\tau}N^\sigma M^\tau = N^{\sigma \cdot v^\tau} \quad \text{oder} \quad N^\sigma M^\tau = M^\tau N^{\sigma \cdot v^\tau}.$$

Setzt man hierin $\tau = m'$, so ergiebt sich mit Hülfe von (1) $N^\sigma = N^{\sigma \cdot v^{m'}}$, folglich

$$(4) \quad v^{m'} \equiv 1 \pmod{n}.$$

Versteht man aber unter σ eine durch n' theilbare Zahl $\sigma = n' \cdot \sigma'$, so wird die linke Seite der Gleichung (3) mit Rücksicht auf Gleichung (1) gleich $M^{-\tau}(N^{n'})^{\sigma'} M^\tau = M^{-\tau}(M^{m'})^{\sigma'} M^\tau = (M^{m'})^{\sigma'} = N^{n' \cdot \sigma'}$, es muss also $N^{n' \cdot \sigma'} = N^{n' \cdot \sigma' \cdot v^\tau}$ für alle Werthe von σ' und τ sein. Daraus folgt $n' \cdot \sigma' \cdot (v^\tau - 1) \equiv 0 \pmod{n}$ und speciell für $\tau = 1$, $\sigma' = 1$:

$$(5) \quad n'(\nu - 1) \equiv 0 \pmod{n}.$$

Diëse Congruenz ist auch hinreichend für das Bestehen der allgemeiner aussehenden Congruenz.

Erfüllen umgekehrt die Zahlen m, n, m', n', ν die bisher aufgestellten Bedingungen, ist also $m = m' \cdot n$, bedeutet ferner n' einen Factor von n ,

*) Für den Fall $M^{m'} = 1$ gelten die folgenden Schlüsse, wenn man sich in diesem Falle n' gleich n gewählt denkt.

der durch alle zu m' relativ primen Divisoren von n theilbar ist, und genügt die Zahl ν den Congruenzen (4) und (5), so definiren, wie leicht zu sehen, die Gleichungen (1) und (2) eine Gruppe $\mathfrak{M}$ von der Ordnung $m = m' \cdot n$, welche die cyklische Gruppe $\mathfrak{N} = N, N^2, \dots, N^{n-1}, 1$ als invariante Untergruppe enthält, deren complementäre Gruppe $\frac{\mathfrak{M}}{\mathfrak{N}}$ ebenfalls cyklisch ist. Jedes beliebige Element von $\mathfrak{M}$ lässt sich auf die Form $M^x N^y$ ($x = 0, 1, \dots, m' - 1$; $y = 0, 1, \dots, n - 1$) bringen, und zwei Elemente $M^{x_1} N^{y_1}$ und $M^{x_2} N^{y_2}$ setzen sich nach Gleichung (3) nach folgender Regel zusammen

$$(6) \quad (M^{x_1} N^{y_1}) (M^{x_2} N^{y_2}) = M^{x_1 + x_2} N^{y_1 \cdot \nu^{x_2} + y_2}.$$

Nun ist noch weiter der Bedingung Rechnung zu tragen, dass $\mathfrak{N}$ die *grösste* invariante cyklische Untergruppe von $\mathfrak{M}$ ist, und auch die Forderung, dass die Untergruppen von $\mathfrak{M}$ von Primzahlpotenzordnung cyklisch sind, ist noch weiter auszunutzen.

Die Zahl ν muss nothwendig zum Exponenten m' (mod. n) gehören. Denn wäre etwa schon $\nu^{m'} \equiv 1$, wo m'' ein Theiler von m' ist, so würde aus der Gleichung (3) für $\tau = m''$ folgen, dass $M^{-m''} N^\sigma M^{m''} = N^\sigma$, d. h. dass $M^{m''}$ mit allen Elementen von $\mathfrak{N}$ vertauschbar wäre. Das Element $M^{m''}$ würde also mit der Gruppe $\mathfrak{N}$ zusammen eine Abel'sche Gruppe erzeugen, die, da sie als (invarianter) Theiler von $\mathfrak{M}$ die Eigenschaft haben muss, dass ihre Untergruppen von Primzahlpotenzordnung cyklisch sind, sogar cyklisch sein muss. Es würde also eine grössere invariante cyklische Untergruppe von $\mathfrak{M}$ existiren als $\mathfrak{N}$, und das ist gegen die Annahme. Die Bedingung, dass ν zum Exponenten m' (mod. m) gehört, ist, wie leicht ersichtlich, auch hinreichend dafür, dass $\mathfrak{N}$ die *grösste* invariante cyklische Untergruppe von $\mathfrak{M}$ ist.

Durch wiederholte Anwendung der Regel (6) ergibt sich

$$(7) \quad (M^x N^y)^{\sigma'} = M^{\sigma \cdot x} N^{(\nu^{(\sigma-1)x} + \nu^{(\sigma-2)x} + \dots + \nu + 1)y} \\ = M^{\sigma \cdot x} N^{\frac{\nu^{\sigma \cdot x} - 1}{\nu^x - 1} \cdot y}.$$

Der Bruch $\frac{\nu^{\sigma \cdot x} - 1}{\nu^x - 1}$ nimmt für $\sigma = m'$, nach dem Modul einer in n aufgehenden Primzahl betrachtet, zufolge der Congruenz (4) entweder den Werth m' oder 0 an, je nachdem $\nu^x - 1$ durch den Modul theilbar ist oder nicht. Wäre nun p ein gemeinschaftlicher Primfactor von m' und n' , also auch von n , so würde der Bruch in jedem Falle $\equiv 0$ (mod. p) sein, also die Form $k \cdot p$ haben. Aus Gleichung (7) würde demnach für $\sigma = m'$ mit Benutzung von Gleichung (1) folgen

$$(M^x N^y)^{m'} = N^{n' \cdot x} N^{p \cdot k} = N^{p \cdot k},$$

und daraus $(M^x N^y)^{\frac{m}{p}} = 1$ für alle Werthe von x und y . Es könnte dann aber kein Element in $\mathfrak{M}$ existiren, dessen Ordnung gleich der höchsten in m enthaltenen Potenz von p wäre, weil nach der letzten Gleichung die Ordnung ja stets ein Divisor von $\frac{m}{p}$ sein müsste, und das ist gegen die Voraussetzung. Es ist also n' relativ prim zu m' , und da n' nach dem Vorigen alle diejenigen Divisoren von n enthält, die zu m' relativ prim sind, so stellt demnach n' den grössten Divisor von n dar, der zu m' relativ prim ist.

Diese Bedingung ist auch hinreichend dafür, dass die Untergruppen von Primzahlpotenzordnung der durch (1), (2), (4), (5) definirten Gruppen cyklisch sind. Dazu ist nachzuweisen, dass, wenn eine Primzahl p genau κ mal in m aufgeht, ein Element von der Ordnung p^κ existirt. Es sei p genau λ mal in m' und infolgedessen genau $\kappa - \lambda$ mal in n enthalten. Dann muss p auch genau $\kappa - \lambda$ mal in $\frac{n}{n'}$ aufgehen, weil ja n' relativ prim zu m' und daher nicht durch p theilbar ist. Daraus folgt, dass die Zahl $m' \cdot \frac{n}{n'}$, welche die Ordnung von M darstellt, durch p^κ theilbar ist, und eine gewisse Potenz von M hat daher die Ordnung p^κ .

Somit ist folgender Satz bewiesen:

Alle Gruppen von gegebener Ordnung m , deren Untergruppen von Primzahlpotenzordnung cyklisch sind, und nur solche, werden durch folgende Gleichungen defnirt:

$$M^{-1}NM = N^v; M^{m'} = N^{n'}; N^n = 1; m = m' \cdot n,$$

wo n einen Divisor von m und n' den grössten Divisor von n bezeichnet, der zu m' relativ prim ist, und wo die Zahl v zum Exponenten m' nach dem Modul n gehört und ausserdem die Congruenz $(v - 1)n' \equiv 0 \pmod{n}$ befriedigt.

Die gruppentheoretische Aufgabe ist damit auf die rein zahlen-theoretische zurückgeführt, zu den verschiedenen Divisoren n von m die brauchbaren Reste v zu finden. Auf diese Aufgabe, welche nach Art der Untersuchungen des Herrn Hölder zu erledigen ist, gehe ich nicht weiter ein. Ich will bloss bemerken, dass mir Herr Steinitz ein Verfahren mitgetheilt hat, wie man den allgemeinen Fall auf den speciellen zurückführen kann, wo n quadratfrei ist, und dass, wenn $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots$ ist und $p_1, p_2, \cdots$ verschiedene Primzahlen bedeuten und $\bar{n} = p_1 \cdot p_2 \cdots$ gesetzt wird, es ebensoviele verschiedene Gruppen $\mathfrak{M}$ giebt, deren grösste invariante cyklische Untergruppe $\mathfrak{N}$ die Ordnung n hat, als es solche giebt, in denen $\mathfrak{N}$ die Ordnung $\bar{n}$ hat.

Zwei auf oben beschriebene Weise erhaltene Gruppen sind dann und nur dann (eindeutig) isomorph, wenn die Zahlen n und m' in beiden dieselben sind und wenn die Zahlen v modulo n Potenzen von einander sind.

Den Beweis dieser letzteren Behauptung unterdrücke ich, weil die von Herrn Hölder in der citirten Abhandlung über Gruppen von quadratfreier Ordnungszahl auf S. 220 gegebene Darstellung nur zu wiederholen wäre.

§ 3.

Ich kehre zu dem in § 1 behandelten allgemeineren Falle zurück. Wollte man die Aufgabe, alle möglichen Gruppen $\mathfrak{M}$ von vorgeschriebener Ordnung m zu bestimmen, ebenso weit durchführen, wie es in § 2 für die speciellen Gruppen geschehen ist, deren Untergruppen von Primzahlpotenzordnung cyklisch sind, so müsste man erst die bis jetzt ungelöste Aufgabe erledigen, alle verschiedenen Gruppen von Primzahlpotenzordnung zu bestimmen. Bei dem Versuch, die erstere so weit als möglich auf die letztere zurückzuführen, bin ich auf einen Satz aufmerksam geworden, der, selbst wenn seine Kenntniss auch nicht durchaus nothwendig zur Lösung der Aufgabe sein sollte, mir doch hinreichend Interesse zu verdienen scheint, um hier hergeleitet zu werden. Er bezieht sich auf den Isomorphismus, welchen die Gruppe $\mathfrak{M}$ erfährt, wenn man dieselbe durch gewisse Elemente von $\mathfrak{M}$ transformirt.

Man betrachte eine invariante Untergruppe von $\mathfrak{M}$, welche eine Primzahlpotenzordnung p^α zur Ordnung hat. Dieselbe ist natürlich in $\mathfrak{M}$ enthalten. Es lässt sich eine Hauptreihe von $\mathfrak{M}$ bilden, in der $\mathfrak{P}$ vorkommt. Dieselbe laute von $\mathfrak{P}$ ab folgendermassen

$$(1) \quad \mathfrak{P} = \mathfrak{P}_0, \mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_\alpha = 1.$$

Die Ordnungszahlen der Factorgruppen $\frac{\mathfrak{P}_s}{\mathfrak{P}_{s+1}}$ ($s = 0, 1, \dots, \alpha - 1$) sind alle gleich p . Für jedes beliebige Element M von $\mathfrak{M}$ hat man

$$(2) \quad M^{-1} P_s M \mathfrak{P}_{s+1} = \mathfrak{P}_s^{\nu_s} \mathfrak{P}_{s+1}; \quad (s = 0, 1, \dots, \alpha - 1),$$

woraus für beliebige positive ganze Zahlen σ und τ die Gleichung folgt:

$$(3) \quad M^{-\sigma} P_s^\sigma M^\tau \mathfrak{P}_{s+1} = P_s^{\sigma \cdot \nu_s^\tau} \mathfrak{P}_{s+1}.$$

Setzt man hierin τ gleich der Ordnung μ von M , so ergibt sich

$$P_s^\sigma \mathfrak{P}_{s+1} = P_s^{\sigma \cdot \nu_s^\mu} \mathfrak{P}_{s+1},$$

folglich

$$\nu_s^\mu \equiv 1 \pmod{p}.$$

Zu jeder Wurzel ν_s dieser Congruenz lässt sich bekanntlich eine ganz

bestimmte zu ν , (mod. p) congruente Zahl finden, deren μ^a Potenz der Einheit sogar nach dem Modul p^a congruent ist. Da P_s der Gruppe $\mathfrak{P}_{s+1}$ angehört, so kann man ν , selbst gleich derartig gewählt denken. Dann ist

$$(4) \quad \nu_s^{\mu} \equiv 1 \pmod{p^a}.$$

Ich führe die Untersuchung für den Fall weiter, dass μ relativ prim zu p ist. Die Gleichung (2) schreibe man in der Form

$$(5) \quad M^{-1} P_s M \mathfrak{P}_{s+1} = P_s^{\nu_s} \mathfrak{P}_{s+1}; \quad (s' > s),$$

wo P_s , falls es von 1 verschieden ist, noch in $\mathfrak{P}_s$, aber nicht mehr in $\mathfrak{P}_{s+1}$ enthalten sei. Entsprechend den Gleichungen (2) und (3) hat man

$$(6) \quad M^{-1} P_s M \mathfrak{P}_{s+1} = P_s^{\nu_s} \mathfrak{P}_{s+1}; \quad M^{-\tau} P_s^{\sigma} M^{\tau} \mathfrak{P}_{s+1} = P_s^{\sigma \cdot \nu_s^{\tau}} \mathfrak{P}_{s+1}.$$

Ich behaupte, dass, wenn P_s nicht gleich 1 ist, ν_s und $\nu_{s'}$ von einander verschieden sein müssen. Wäre nämlich $\nu_s = \nu_{s'}$, so würde, da P_s als Element von $\mathfrak{N}$ mit den Elementen der Factorgruppe $\frac{\mathfrak{P}_s}{\mathfrak{P}_{s+1}}$ vertauschbar ist (s. § 1), aus Gleichung (5) mit Hülfe von Gleichung (6) für beliebige positive ganze Zahlen σ und τ

$$M^{-\tau} P_s^{\sigma} M^{\tau} \mathfrak{P}_{s+1} = P_s^{\sigma \cdot \nu_s^{\tau}} P_s^{\sigma \cdot \nu_{s'}^{\tau-1}} \mathfrak{P}_{s+1}$$

folgen, und daraus mit Hülfe der Congruenz (4) für $\tau = \mu$, $\sigma = 1$

$$P_s \mathfrak{P}_{s+1} = P_s P_s^{\mu \cdot \nu_s^{\mu-1}} \mathfrak{P}_{s+1},$$

weil $P_s^{\mu} = 1$, oder

$$\mathfrak{P}_{s+1} = P_s^{\mu \cdot \nu_s^{\mu-1}} \mathfrak{P}_{s+1}.$$

Das Bestehen einer solchen Gleichung ist aber unmöglich, weil der Exponent $\mu \cdot \nu_s^{\mu-1}$ von P_s nicht durch p theilbar ist. Es müssen also ν_s und $\nu_{s'}$ von einander verschieden sein. Daraus folgt weiter, dass man eine Zahl x_s bestimmen kann, welche der Congruenz

$$1 \equiv x_s (\nu_s - \nu_{s'}) \pmod{p}$$

genügt. Mit Hülfe dieser Congruenz und der Gleichungen (5) und (6) erhält man

$$M^{-1} (P_s P_{s'}^{\nu_{s'}}) M \mathfrak{P}_{s+1} = P_s^{\nu_s} P_{s'}^{1 + \nu_{s'} \cdot \nu_s} \mathfrak{P}_{s+1} = P_s^{\nu_s} P_{s'}^{\nu_{s'}} \mathfrak{P}_{s+1} = (P_s P_{s'}^{\nu_{s'}})^{\nu_s} \mathfrak{P}_{s+1},$$

also, wenn

$$(7) \quad P_s P_{s'}^{\nu_{s'}} = P_{s'}$$

gesetzt wird,

$$(8) \quad M^{-1} P_{s'} M \mathfrak{P}_{s+1} = P_{s'}^{\nu_{s'}} \mathfrak{P}_{s+1}; \quad (s' > s).$$

Das Element $P_{s'}$ gehört ebenso wie P_s noch der Gruppe $\mathfrak{P}_s$, aber nicht mehr der Gruppe $\mathfrak{P}_{s+1}$ an.

Falls s' noch nicht gleich α ist, lässt sich das Verfahren, das soeben angewendet wurde, um aus Gleichung (2) die Gleichung (8) zu gewinnen, für die letztere wiederholen. Man findet dann ein in $\mathfrak{P}_s$, aber nicht in $\mathfrak{P}_{s+1}$ enthaltenes Element P_s'' , welches die Gleichung befriedigt

$$M^{-1}P_s''M\mathfrak{P}_{s''+1} = P_s''^{\nu_s}\mathfrak{P}_{s''+1}; \quad (s'' > s' > s).$$

Durch genügend häufige Wiederholung des Verfahrens muss man schliesslich zu einem in $\mathfrak{P}_s$, aber nicht in $\mathfrak{P}_{s+1}$ enthaltenen Element gelangen, welches durch M in eine Potenz von sich selbst transformirt wird. Dieses Ergebniss gilt für alle Werthe $s = 0, 1, \dots, \alpha - 1$ und jedes beliebige Element M , dessen Ordnung relativ prim zu p ist.

Hat man irgend welche Elemente $P_s (s = 0, 1, \dots, \alpha - 1)$ gewählt, die noch zu $\mathfrak{P}_s$, aber nicht mehr zu $\mathfrak{P}_{s+1}$ gehören, so lässt sich, wie leicht zu sehen, jedes Element von P auf eine und nur eine Weise in die Form setzen

$$(9) \quad P_0^{\kappa_0} P_1^{\kappa_1} \dots P_{\alpha-1}^{\kappa_{\alpha-1}}; \quad \begin{pmatrix} \kappa_0 & = 0, 1, \dots, p-1 \\ \kappa_1 & = 0, 1, \dots, p-1 \\ \cdot & \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ \kappa_{\alpha-1} & = 0, 1, \dots, p-1 \end{pmatrix}$$

und $P_s^p; (s = 0, 1, \dots, \alpha - 1)$ ist die niedrigste Potenz von P_s , welche sich durch die Elemente $P_{s+1}, P_{s+2}, \dots, P_{\alpha-1}$ darstellen lässt.

Es besteht also folgender Satz:

Ist $\mathfrak{M}$ eine Gruppe, in deren Hauptreihen die Factorgruppen von Primzahlordnung sind, und bedeutet $\mathfrak{P}$ eine invariante Untergruppe von $\mathfrak{M}$, welche eine Primzahlpotenz p^α zur Ordnung hat, ist ferner M ein Element von $\mathfrak{M}$, dessen Ordnung μ relativ prim zu p ist, so lassen sich in $\mathfrak{P}$ α mit folgenden Eigenschaften versehene Elemente

$$P_0, P_1, \dots, P_{\alpha-1}$$

finden:

1) *Jedes von ihnen wird durch M in eine Potenz von sich selbst transformirt, deren Exponent eine Wurzel der Congruenz $\nu^\mu \equiv 1 \pmod{p^\alpha}$ ist;*

2) *Jedes Element von $\mathfrak{M}$ lässt sich auf eine einzige Weise in der Form (9) darstellen:*

3) *$P_s^p; (s = 0, 1, \dots, \alpha - 1)$ ist die niedrigste Potenz von P_s , welche sich durch die Elemente $P_{s+1}, P_{s+2}, \dots, P_{\alpha-1}$ darstellen lässt.*