e-rara.ch

Verallgemeinerung des Sylow'schen Satzes

Frobenius, Ferdinand Georg

Göttingen, [s. a.]

ETH-Bibliothek Zürich

Signatur: Rar 1524

Persistenter Link: http://dx.doi.org/10.3931/e-rara-18880

Verallgemeinerung des Sylow'schen Satzes.

Von G. Frobenius.

Jede endliche Gruppe, deren Ordnung durch die Primzahl p theilbar ist, enthält Elemente der Ordnung p. (Cauchy, *Mémoire sur les arrangements que l'on peut former avec des lettres données.* Exercices d'analyse et de physique Mathématique, tome III, §. XII pag. 250.) Die Anzahl derselben ist, wie ich hier zeigen werde, stets eine Zahl der Form $(p-1)(np+1)$. Aus jenem Satze hat Sylow den allgemeineren hergeleitet, dass eine Gruppe, deren Ordnung h durch $p^\varkappa$ theilbar ist, Untergruppen der Ordnung $p^\varkappa$ besitzen muss. (*Théorèmes sur les groupes de substitutions*, Math. Ann. Bd. V.) Einen einfachen Beweis dafür habe ich in meiner Arbeit *Neuer Beweis des Sylow'schen Satzes*, Crelle's Journal Bd. 100, gegeben. Die Anzahl dieser Untergruppen muss, wie ich hier zeigen werde, immer $\equiv 1 \pmod{p}$ sein. Ist p^λ die höchste in h enthaltene Potenz von p, so hat Sylow diesen Satz nur für den Fall bewiesen, dass $\varkappa = \lambda$ ist. Dann sind je zwei in $\mathfrak{H}$ enthaltene Gruppen der Ordnung p^λ conjugirt, und ihre Anzahl $np+1$ ist ein Divisor von h, während dies für $\varkappa < \lambda$ im Allgemeinen nicht eintrifft. Die angeführten Ergebnisse erhalte ich auf einem neuen Wege aus einem Satze der Gruppentheorie, der bisher noch nicht bemerkt zu sein scheint:

In einer Gruppe der Ordnung h ist die Anzahl der Elemente, deren Ordnung in g aufgeht, durch den grössten gemeinsamen Divisor von g und h theilbar.

§. 1.

Ist p eine Primzahl, so hat eine Gruppe $\mathfrak{P}$ der Ordnung p^λ eine Reihe von invarianten Untergruppen (Hauptreihe) $\mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}_{\lambda-1}$ der Ordnungen $p, p^2 \ldots p^{\lambda-1}$, von denen jede in der folgenden enthalten ist. Dies Resultat leitet Sylow (a. a. O. S. 588) aus dem Satze ab:

I. *Jede Gruppe der Ordnung p^λ enthält ein invariantes Element der Ordnung p.*

Ein *invariantes Element einer Gruppe* $\mathfrak{H}$ ist ein Element von $\mathfrak{H}$, das mit jedem Element von $\mathfrak{H}$ vertauschbar ist. Enthält $\mathfrak{P}$ das in-

variante Element P der Ordnung p, so bilden die Potenzen von P eine invariante Untergruppe $\mathfrak{P}_1$ von $\mathfrak{P}$, deren Ordnung p ist. Ebenso hat $\frac{\mathfrak{P}}{\mathfrak{P}_1}$ eine invariante Untergruppe $\frac{\mathfrak{P}_2}{\mathfrak{P}_1}$ der Ordnung p, also hat $\mathfrak{P}$ eine invariante Untergruppe $\mathfrak{P}_2$ der Ordnung p^2, welche $\mathfrak{P}_1$ enthält, u. s. w. Ich habe in meiner Arbeit *Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul*, Crelle's Journal Bd. 101 (§. 3, IV) zu jenem Theorem die folgende Bemerkung gefügt:

II. *Jede in einer Gruppe der Ordnung p^λ enthaltene Gruppe der Ordnung $p^{\lambda-1}$ ist eine invariante Untergruppe.*

Andere Beweise dafür habe ich in meiner Arbeit *Über endliche Gruppen*, Sitzungsberichte 1895 (§. 2, III, IV, V; §. 4, II) entwickelt. Aus dem Satze I kann man dies auf folgende Weise erhalten: Sei $\mathfrak{H}$ eine Gruppe der Ordnung p^λ, $\mathfrak{G}$ eine Untergruppe der Ordnung $p^{\lambda-1}$, P ein invariantes Element von $\mathfrak{H}$, dessen Ordnung p ist, und $\mathfrak{P}$ die Gruppe der Potenzen von $\mathfrak{P}$. Ist $\mathfrak{G}$ durch $\mathfrak{P}$ theilbar, so ist $\frac{\mathfrak{G}}{\mathfrak{P}}$ eine invariante Untergruppe von $\frac{\mathfrak{H}}{\mathfrak{P}}$, weil man den Satz II für Gruppen, deren Ordnung kleiner als p^λ ist, schon als bewiesen annehmen kann. Mithin ist auch $\mathfrak{G}$ eine invariante Untergruppe von $\mathfrak{H}$. Ist $\mathfrak{G}$ nicht durch $\mathfrak{P}$ theilbar, so ist $\mathfrak{H} = \mathfrak{G}\mathfrak{P}$, oder es kann jedes Element von $\mathfrak{H}$ auf die Form $H = GP^\nu$ gebracht werden, wo G ein Element von $\mathfrak{G}$ ist. Nun ist G mit $\mathfrak{G}$ vertauschbar, und P sogar mit jedem Elemente von $\mathfrak{G}$. Mithin ist auch H mit $\mathfrak{G}$ vertauschbar.

Das Eingangs erwähnte Theorem lässt sich noch nach einer anderen Richtung hin vervollständigen:

III. *Jede invariante Untergruppe der Ordnung p von einer Gruppe der Ordnung p^λ besteht aus den Potenzen eines invarianten Elementes.*

Sei $\mathfrak{H}$ eine Gruppe der Ordnung p^λ, $\mathfrak{P}$ eine invariante Untergruppe der Ordnung p. Ist Q irgend ein Element von $\mathfrak{H}$ und $q = p^\kappa$ seine Ordnung, so bilden die Potenzen von Q eine in $\mathfrak{H}$ enthaltene Gruppe $\mathfrak{Q}$ der Ordnung q. Ist $\mathfrak{P}$ ein Divisor von $\mathfrak{Q}$, so ist jedes Element P von $\mathfrak{P}$ eine Potenz von Q, also mit Q vertauschbar. Ist $\mathfrak{P}$ nicht ein Divisor von $\mathfrak{Q}$, so sind $\mathfrak{P}$ und $\mathfrak{Q}$ theilerfremd. $\mathfrak{P}$ ist mit jedem Elemente von $\mathfrak{H}$, also auch mit jedem von $\mathfrak{Q}$ vertauschbar. Daher ist $\mathfrak{P}\mathfrak{Q}$ eine Gruppe der Ordnung $p^{\kappa+1}$, und $\mathfrak{P}$ ist eine invariante Untergruppe derselben. Nach dem Satze II ist aber auch $\mathfrak{Q}$ eine solche. Mithin ist P mit Q vertauschbar nach dem Satze:

IV. *Ist jede der beiden theilerfremden Gruppen $\mathfrak{A}$ und $\mathfrak{B}$ mit jedem Elemente der andern vertauschbar, so ist auch jedes Element von $\mathfrak{A}$ mit jedem Elemente von $\mathfrak{B}$ vertauschbar.*

Denn ist A ein Element von $\mathfrak{A}$ und B ein Element von $\mathfrak{B}$, so ist das Element

$$A(BA^{-1}B^{-1}) = (ABA^{-1})B^{-1}$$

sowohl in $\mathfrak{A}$ als auch in $\mathfrak{B}$ enthalten, und ist daher das Hauptelement E.

Ich will den Satz III noch auf eine zweite Art beweisen: Ist $Q^{-1}PQ = P^a$, so ist $Q^{-q}PQ^q = P^{a^q}$. Ist also $Q^q = E$, so ist $a^q \equiv 1 \pmod{p}$. Nun ist $a^{p-1} \equiv 1 \pmod{p}$, also da q und $p-1$ theilerfremd sind, auch $a \equiv 1 \pmod{p}$, und mithin $PQ = QP$.

Endlich ergiebt sich der Satz drittens aus dem allgemeineren Satze:

V. *Jede invariante Untergruppe einer Gruppe $\mathfrak{H}$ der Ordnung p^λ enthält ein invariantes Element von $\mathfrak{H}$, dessen Ordnung p ist.*

Man theile die Elemente von $\mathfrak{H}$ in Classen conjugirter Elemente (conjugirt in Bezug auf $\mathfrak{H}$). Besteht eine Classe aus nur einem Element, so ist dies ein invariantes, und umgekehrt bildet jedes invariante Element von $\mathfrak{H}$ für sich eine Classe. Sei $\mathfrak{G}$ eine invariante Untergruppe von $\mathfrak{H}$ und $p^\varkappa$ ihre Ordnung. Enthält dann die Gruppe $\mathfrak{G}$ ein Element einer Classe, so enthält sie alle Elemente derselben. Man wähle aus jeder der n in G enthaltenen Classen ein Element aus, $G_1, G_2, \ldots G_n$. Bilden die mit G_ν vertauschbaren Elemente von $\mathfrak{H}$ eine Gruppe der Ordnung p^{λ_ν}, so ist die Anzahl der mit G_ν conjugirten Elemente von $\mathfrak{H}$, also die Anzahl der Elemente der durch G repraesentirten Classe, gleich $p^{\lambda-\lambda_\nu}$ (CRELLE's Journal Bd. 100 S. 181). Daher ist

$$p^\varkappa = p^{\lambda-\lambda_1} + p^{\lambda-\lambda_2} + \cdots + p^{\lambda-\lambda_n}.$$

Ist G_1 das Hauptelement E, so ist $\lambda = \lambda_1$. Daher können die letzten $n-1$ Glieder auf der rechten Seite dieser Gleichung nicht alle durch p theilbar sein. Es muss daher noch einen Index $\nu > 1$ geben, für den $\lambda_\nu = \lambda$ ist. Dann ist G_ν ein invariantes Element von $\mathfrak{H}$, dessen Ordnung $p^\mu > 1$ ist, und die $p^{\mu-1}$te Potenz von G_ν ist ein in $\mathfrak{G}$ enthaltenes invariantes Element von $\mathfrak{H}$ der Ordnung p.

§. 2.

I. *Sind a und b relative Primzahlen, so kann ein Element der Ordnung ab stets und nur in einer Weise als Product von zwei Elementen dargestellt werden, deren Ordnungen a und b sind, und die mit einander vertauschbar sind.*

Sind A und B zwei mit einander vertauschbare Elemente, deren Ordnungen a und b relative Primzahlen sind, so hat $AB = C$ die Ordnung ab. Sei umgekehrt C irgend ein Element der Ordnung ab. Bestimmt man dann die ganzen Zahlen x und y so, dass $ax + by = 1$

wird, und setzt man $ax = \beta$, $by = \alpha$, so ist $C = C^{\alpha}C^{\beta}$, und C^{α} hat, da y zu a theilerfremd ist, die Ordnung a, und C^{β} die Ordnung b. (Cauchy, a. a. O. §. V, pag. 179.) Sei nun auch $C = AB$, wo A und B die Ordnungen a und b haben und mit einander vertauschbar sind. Dann ist $C^{\alpha} = A^{\alpha}B^{\alpha}$, $B^{\alpha} = B^{by} = E$, $A^{\alpha} = A^{1-\beta} = A$, also $A = C^{\alpha}$ und $B = C^{\beta}$. Als Potenzen von C gehören A und B jeder Gruppe an, der C angehört.

II. *Ist die Ordnung einer Gruppe durch n theilbar, so ist die Anzahl derjenigen Elemente der Gruppe, deren Ordnung in n aufgeht, ein Vielfaches von n.*

Sei $\mathfrak{H}$ eine Gruppe der Ordnung h und n ein Divisor von h. Für jede Gruppe, deren Ordnung $h' < h$ ist, und für jeden Divisor n' von h' setze ich den Satz als bewiesen voraus. Die Anzahl der Elemente von $\mathfrak{H}$, deren Ordnung in n aufgeht, ist, falls $n = h$ ist, gleich n. Ist also $n < h$, so kann ich annehmen, der Satz sei bereits bewiesen für jeden Divisor von h, der $> n$ ist. Ist dann p eine in $\frac{h}{n}$ aufgehende Primzahl, so ist die Anzahl der Elemente von h, deren Ordnung in np aufgeht, durch np theilbar, also auch durch n. Sei $np = p^{\lambda}r$, wo r nicht durch p theilbar ist und $\lambda \geq 1$ ist. Sei $\mathfrak{K}$ der Complex derjenigen Elemente von $\mathfrak{H}$, deren Ordnung in np, aber nicht in n aufgeht, also durch p^{λ} theilbar ist, und sei k die Ordnung dieses Complexes. Dann ist nur noch zu zeigen, dass die Zahl k, falls sie von Null verschieden ist, durch n theilbar ist. Zu dem Zweck beweise ich, dass k durch $p^{\lambda-1}$ und durch r theilbar ist.

Ich theile die Elemente von $\mathfrak{K}$ in Systeme, indem ich zwei Elemente zu demselben System rechne, wenn jedes eine Potenz des anderen ist. Alle Elemente eines Systems haben dieselbe Ordnung m. Ihre Anzahl ist $\phi(m)$. Durch jedes seiner Elemente A ist das System vollständig bestimmt, es wird gebildet von den Elementen A^{μ}, wo μ die $\phi(m)$ Zahlen durchläuft, die $< m$ und relativ prim zu m sind. Ist A ein Element des Complexes $\mathfrak{K}$, so gehören auch alle Elemente des durch A repraesentirten Systems dem Complexe $\mathfrak{K}$ an. Dann ist die Ordnung m von A durch p^{λ}, also $\phi(m)$ durch $p^{\lambda-1}$ theilbar. Da die Anzahl der Elemente jedes der Systeme, in die $\mathfrak{K}$ zerlegt ist, durch $p^{\lambda-1}$ theilbar ist, so muss auch k durch $p^{\lambda-1}$ theilbar sein.

Um zweitens zu zeigen, dass k auch durch r theilbar ist, theile ich wieder die Elemente von $\mathfrak{K}$ in Systeme, aber von anderer Art, doch ebenfalls so, dass die Anzahl der Elemente jedes Systems durch r theilbar ist. Jedes Element von $\mathfrak{K}$ kann, und zwar nur in einer Art, dargestellt werden als Product von einem Elemente P der Ordnung p^{λ} und einem damit vertauschbaren Elemente Q, dessen Ordnung in r

aufgeht. Umgekehrt gehört jedes so erhaltene Product PQ dem Complexe $\mathfrak{K}$ an.

Sei P irgend ein bestimmtes Element der Ordnung p^λ. Alle Elemente von $\mathfrak{H}$, die mit P vertauschbar sind, bilden eine Gruppe $\mathfrak{Q}$, deren Ordnung q durch p^λ theilbar ist. Die Potenzen von P bilden eine Gruppe $\mathfrak{P}$ der Ordnung p^λ, die eine invariante Untergruppe von $\mathfrak{Q}$ ist. Die Elemente Q von $\mathfrak{Q}$, die der Gleichung $Y^r = E$ genügen, sind mit denen identisch, die der Gleichung $Y^t = E$ genügen, wo t der grösste gemeinsame Divisor von q und r ist. Es handelt sich zunächst darum, die Anzahl dieser Elemente zu bestimmen.

Jedes Element von $\mathfrak{Q}$ lässt sich, und zwar nur in einer Weise als Product darstellen von einem Element A, dessen Ordnung eine Potenz p ist, und einem damit vertauschbaren Elemente B, dessen Ordnung nicht durch p theilbar ist.

Wenn die $t$te Potenz von AB der Gruppe $\mathfrak{P}$ angehört, so ist

$$(AB)^t = A^t B^t = P^s, \quad \text{also} \quad A^t = P^s, \quad B^t = E,$$

weil sich auch dies Element nur in einer Weise auf die angegebene Art zerlegen lässt. Demnach gehört A^t der Gruppe $\mathfrak{P}$ an, mithin auch A selbst, weil t nicht durch p theilbar ist. Die Ordnung der Gruppe $\frac{\mathfrak{Q}}{\mathfrak{P}}$ ist $\frac{q}{p^\lambda} < h$. Die Anzahl der (complexen) Elemente dieser Gruppe, die der Gleichung $Y^t = E$ genügen, ist daher ein Vielfaches von t, etwa tu. Ist $\mathfrak{P}AB$ ein solches Element, so ist, weil A der Gruppe $\mathfrak{P}$ angehört, $\mathfrak{P}A = \mathfrak{P}$, also $\mathfrak{P}AB = \mathfrak{P}B$. Da B als Element von $\mathfrak{Q}$ mit P vertauschbar ist, so enthält der Complex $\mathfrak{P}B$ nur ein Element, dessen Ordnung in t aufgeht, nämlich B selbst, während die Ordnung jedes anderen Elementes von $\mathfrak{P}B$ durch p theilbar ist. Seien

$$\mathfrak{P}B + \mathfrak{P}B_1 + \mathfrak{P}B_2 + \cdots$$

die tu verschiedenen (complexen) Elemente der Gruppe $\frac{\mathfrak{Q}}{\mathfrak{P}}$, deren $t$te Potenz in $\mathfrak{P}$ enthalten ist, dann sind in diesem Complexe auch alle Elemente von $\mathfrak{Q}$ enthalten, deren $t$te Potenz (absolut) gleich E ist. Diese Eigenschaft haben aber nur die Elemente $B, B_1, B_2, \cdots$. Mithin enthält $\mathfrak{Q}$ genau tu Elemente, die der Gleichung $Y^t = E$ genügen, oder es giebt, wenn P ein bestimmtes Element der Ordnung p^λ ist, genau tu Elemente, die mit P vertauschbar sind, und deren Ordnung in r aufgeht.

Die Anzahl der mit P vertauschbaren Elemente von $\mathfrak{H}$ ist q. Die Anzahl der Elemente $P, P_1, P_2, \cdots$ von $\mathfrak{H}$, die mit P conjugirt sind in Bezug auf $\mathfrak{H}$, ist daher $\frac{h}{q}$. Es giebt dann auch genau tu

Elemente Q_1 in $\mathfrak{H}$, die mit P_1 vertauschbar sind, und deren Ordnung in r aufgeht. Setzt man für X der Reihe nach jedes der $\frac{h}{q}$ Elemente $P, P_1, P_2, \cdots$ und für Y jedes Mal die tu mit X vertauschbaren Elemente, die der Gleichung $Y^r = E$ genügen, so erhält man ein System $\mathfrak{K}'$ vor

$$k' = \frac{h}{q} tu$$

verschiedenen Elementen XY des Complexes $\mathfrak{K}$. Nun ist h durch jede der beiden Zahlen q und r theilbar, also auch durch ihr kleinstes gemeinschaftliches Vielfache $\frac{qr}{t}$. Mithin ist k' durch r theilbar. Das System $\mathfrak{K}'$ ist durch jedes seiner Elemente vollständig bestimmt. Zwei verschiedene der Systeme $\mathfrak{K}', \mathfrak{K}'', \cdots$ haben kein Element gemeinsam. Ihre Ordnungen $k', k'', \cdots$ sind alle durch r theilbar. Mithin ist auch $k = k' + k'' + \cdots$ durch r theilbar.

Die Anzahl der Elemente einer Gruppe, die der Gleichung $X^n = E$ genügen, ist mn, die ganze Zahl m ist > 0, weil stets $X = E$ jene Gleichung befriedigt.

III. *Ist die Ordnung einer Gruppe $\mathfrak{H}$ durch n theilbar, so erzeugen die Elemente von $\mathfrak{H}$, deren Ordnung in n aufgeht, eine charakteristische Untergruppe von $\mathfrak{H}$, deren Ordnung durch n theilbar ist.*

Sei $\mathfrak{N}$ der Complex der Elemente von $\mathfrak{H}$, die der Gleichung $X^n = E$ genügen. Ist X ein Element von $\mathfrak{N}$, und R irgend ein mit $\mathfrak{H}$ vertauschbares Element, so ist auch $R^{-1}XR$ ein Element von $\mathfrak{N}$. Mithin ist $R^{-1}\mathfrak{N}R = \mathfrak{N}$. Der Complex $\mathfrak{N}$ erzeuge eine Gruppe $\mathfrak{G}$ der Ordnung g. Dann ist auch $R^{-1}\mathfrak{G}R = \mathfrak{G}$, also ist $\mathfrak{G}$ eine charakteristische Untergruppe von $\mathfrak{H}$.

Ist q^α die höchste in n aufgehende Potenz der Primzahl q, so geht q^α auch in h auf. Mithin enthält $\mathfrak{H}$ eine Gruppe $\mathfrak{Q}$ der Ordnung q^α. Nun ist $\mathfrak{N}$ durch $\mathfrak{Q}$ theilbar, also auch $\mathfrak{G}$, und folglich ist g durch q^α theilbar. Da dies für jede in n aufgehende Primzahl q gilt, so ist g durch n theilbar.

Über die Beziehung des Complexes $\mathfrak{N}$ zu der Gruppe $\mathfrak{G}$ bemerke ich noch Folgendes: Ich habe *Über endliche Gruppen*, § 1 die Potenzen $\mathfrak{N}, \mathfrak{N}^2, \mathfrak{N}^3, \cdots$ eines Complexes $\mathfrak{N}$ betrachtet. Ist in ihrer Reihe $\mathfrak{N}^{r+s}$ die erste, die einer früheren $\mathfrak{N}^r$ gleich ist, so ist stets und nur dann $\mathfrak{N}^\rho = \mathfrak{N}^\sigma$, wenn $\rho \equiv \sigma \pmod{s}$ und ρ und σ beide $\geqq r$ sind. Sei t die durch die Bedingungen $t \equiv 0 \pmod{s}$ und $r \leqq t < r + s$ eindeutig bestimmte Zahl. Dann ist $\mathfrak{N}^t$ die einzige in der Reihe jener Potenzen enthaltene Gruppe. Enthält $\mathfrak{N}$ das Hauptelement E, so ist $\mathfrak{N}^{t+1}$ durch $\mathfrak{N}^t$ theilbar. Mithin ist $\mathfrak{G} = \mathfrak{N}^t$ durch $\mathfrak{N}$ theilbar. Ist N ein Element der Gruppe $\mathfrak{G}$, so ist $\mathfrak{G}N = \mathfrak{G}$. Ist also allgemeiner $\mathfrak{N}$ ein in der

Gruppe $\mathfrak{G}$ enthaltener Complex von Elementen, so ist $\mathfrak{G}\mathfrak{N} = \mathfrak{G}$. Daher ist $\mathfrak{N}^{t+1} = \mathfrak{N}^t$, also $s = 1$ und $t = r$. In der Reihe der Potenzen von $\mathfrak{N}$ ist folglich $\mathfrak{N}^r = \mathfrak{N}^{r+1}$ die erste, die einer folgenden gleich ist, und diese ist die von dem Complex $\mathfrak{N}$ erzeugte Gruppe.

IV. *Ist die Ordnung einer Gruppe $\mathfrak{H}$ durch die beiden theilerfremden Zahlen r und s theilbar, giebt es in $\mathfrak{H}$ genau r Elemente A, deren Ordnung in r aufgeht, und genau s Elemente B, deren Ordnung in s aufgeht, so ist jedes der r Elemente A mit jedem der s Elemente B vertauschbar, und es giebt in $\mathfrak{H}$ genau rs Elemente, deren Ordnung in rs aufgeht, nämlich die rs verschiedenen Elemente $AB = BA$.*

Denn jedes Element C von $\mathfrak{H}$, dessen Ordnung in rs aufgeht, kann als Product von zwei mit einander vertauschbaren Elementen A und B dargestellt werden, deren Ordnungen in r und s aufgehen. Nun enthält $\mathfrak{H}$ nicht mehr als r Elemente A und nicht mehr als s Elemente B. Wäre also nicht jedes der r Elemente A mit jedem der s Elemente B vertauschbar, und wären nicht ausserdem die rs Elemente AB alle verschieden, so enthielte $\mathfrak{H}$ weniger als rs Elemente C. Dies widerspricht aber dem Satze II.

§. 3.

Ist die Ordnung h der Gruppe $\mathfrak{H}$ durch die Primzahl p theilbar, so enthält $\mathfrak{H}$ Elemente der Ordnung p, und zwar $mp-1$, weil es in $\mathfrak{H}$ mp Elemente giebt, deren Ordnung in p aufgeht. Aus diesem Satze von CAUCHY hat SYLOW den allgemeineren abgeleitet, dass jede Gruppe, deren Ordnung durch $p^\varkappa$ theilbar ist, eine Untergruppe der Ordnung $p^\varkappa$ besitzt. Er bedient sich bei seinem Beweise der Sprache der Substitutionentheorie. Will man diese vermeiden, so hat man das Verfahren anzuwenden, das ich in meiner Arbeit *Über endliche Gruppen* beim Beweise der Sätze V und VIII, §. 2 benutzt habe.

Einen anderen Beweis erhält man, indem man die $mp-1$ in $\mathfrak{H}$ enthaltenen Elemente P der Ordnung p in Classen conjugirter Elemente theilt. Bilden die mit P vertauschbaren Elemente von $\mathfrak{H}$ die Gruppe $\mathfrak{G}$ der Ordnung g, so ist die Anzahl der mit P conjugirten Elemente $\frac{h}{g}$. Mithin ist

$$mp-1 = \sum \frac{h}{g},$$

wo die Summe über die verschiedenen Classen zu erstrecken ist, in welche die Elemente P zerfallen. Aus dieser Gleichung folgt, dass die Summanden $\frac{h}{g}$ nicht alle durch p theilbar sind. Sei p^λ die höchste in h enthaltene Potenz von p, und sei $\varkappa \leqq \lambda$. Ist $\frac{h}{g}$ nicht durch p

theilbar, so ist g durch p^λ theilbar. Die Potenzen von P bilden eine Gruppe $\mathfrak{P}$ der Ordnung p, die eine invariante Untergruppe von $\mathfrak{G}$ ist. Die Ordnung der Gruppe $\frac{\mathfrak{G}}{\mathfrak{P}}$ ist $\frac{g}{p} < h$. Für diese Gruppe dürfen wir mithin die Sätze, die wir für die Gruppe $\mathfrak{H}$ beweisen wollen, schon als bekannt voraussetzen. Sie enthält also eine Gruppe $\frac{\mathfrak{P}_\varkappa}{\mathfrak{P}}$ der Ordnung $p^{\varkappa-1}$, und falls $\varkappa < \lambda$ ist, eine durch $\frac{\mathfrak{P}_\varkappa}{\mathfrak{P}}$ theilbare Gruppe $\frac{\mathfrak{P}_{\varkappa+1}}{\mathfrak{P}}$ der Ordnung $p^\varkappa$. Folglich enthält $\mathfrak{H}$ die Gruppe $\mathfrak{P}_\varkappa$ der Ordnung $p^\varkappa$ und die durch $\mathfrak{P}_\varkappa$ theilbare Gruppe $\mathfrak{P}_{\varkappa+1}$ der Ordnung $p^{\varkappa+1}$.

§. 4.

I. *Ist die Ordnung einer Gruppe durch die $\varkappa$te Potenz der Primzahl p theilbar, so ist die Anzahl der darin enthaltenen Gruppen der Ordnung $p^\varkappa$ eine Zahl der Form $np+1$.*

Sei $r_\varkappa$ die Anzahl der in $\mathfrak{H}$ enthaltenen Gruppen der Ordnung $p^\varkappa$. Dann ist die Anzahl der Elemente von $\mathfrak{H}$, deren Ordnung p ist, gleich $r_1(p-1)$. Diese Zahl hat, wie oben gezeigt, die Form $mp-1$. Mithin ist

$$r_1 \equiv 1 \pmod{p}. \tag{1.}$$

Sei $r_{\varkappa-1} = r$, $r_\varkappa = s$, und seien

$$\mathfrak{A}_1, \mathfrak{A}_2, \cdots \mathfrak{A}_r \tag{2.}$$

die r in $\mathfrak{H}$ enthaltenen Gruppen der Ordnung $p^{\varkappa-1}$ und

$$\mathfrak{B}_1, \mathfrak{B}_2, \cdots \mathfrak{B}_s \tag{3.}$$

die s Gruppen der Ordnung $p^\varkappa$. Die Gruppe $\mathfrak{A}_\varrho$ sei in a_ϱ der Gruppen (3.) enthalten. Die Gruppe $\mathfrak{B}_\sigma$ sei durch b_σ der Gruppen (2.) theilbar. Dann ist

$$a_1 + a_2 + \cdots + a_r = b_1 + b_2 + \cdots + b_s \tag{4.}$$

die Anzahl der verschiedenen Paare von Gruppen $\mathfrak{A}_\varrho$, $\mathfrak{B}_\sigma$, für die $\mathfrak{A}_\varrho$ in $\mathfrak{B}_\sigma$ enthalten ist.

Sei $\mathfrak{A}$ eine der Gruppen (2.). Von den Gruppen (3.) seien $\mathfrak{B}_1, \mathfrak{B}_2, \cdots \mathfrak{B}_a$ die, welche durch $\mathfrak{A}$ theilbar sind. Nach §. 3 ist $a > 0$, und nach Satz II, §. 1 ist $\mathfrak{A}$ eine invariante Untergruppe von jeder dieser a Gruppen, also auch von ihrem kleinsten gemeinschaftlichen Vielfachen $\mathfrak{G}$. Mithin enthält die Gruppe $\frac{\mathfrak{G}}{\mathfrak{A}}$ die a Gruppen $\frac{\mathfrak{B}_1}{\mathfrak{A}}, \frac{\mathfrak{B}_2}{\mathfrak{A}}, \cdots \frac{\mathfrak{B}_a}{\mathfrak{A}}$ der Ordnung p und keine weitere. Denn ist $\frac{\mathfrak{B}}{\mathfrak{A}}$ eine in $\frac{\mathfrak{G}}{\mathfrak{A}}$ enthaltene

Gruppe der Ordnung p, so ist $\mathfrak{B}$ eine durch $\mathfrak{A}$ theilbare Gruppe der Ordnung $p^\varkappa$. Nach Formel (1.) ist daher $a \equiv 1 (\text{mod. } p)$. Mithin ist

$$(5.) \qquad a_\varrho \equiv 1,\ a_1 + a_2 + \cdots + a_r \equiv r (\text{mod. } p).$$

Nunmehr brauche ich den Hülfssatz:

Die Anzahl der Gruppen der Ordnung $p^{\lambda-1}$, die in einer Gruppe der Ordnung p^λ enthalten sind, ist $\equiv 1 (mod.\ p)$.

Ich nehme an, dies Lemma sei schon bewiesen für Gruppen der Ordnung $p^\varkappa$, falls $\varkappa < \lambda$ ist. Ist dann in der obigen Entwicklung $\varkappa < \lambda$, so ist

$$(6.) \qquad b_\tau \equiv 1,\ b_1 + b_2 + \cdots + b_s \equiv s (\text{mod. } p).$$

Daher ist $r \equiv s$ oder $r_{\varkappa-1} \equiv r_\varkappa (\text{mod. } p)$, und da diese Congruenz für jeden Werth $\varkappa < \lambda$ gilt, so ist

$$1 \equiv r_1 \equiv r_2 \equiv \cdots \equiv r_{\lambda-1} (\text{mod. } p).$$

Wendet man dies Ergebniss auf eine Gruppe $\mathfrak{H}$ an, deren Ordnung p^λ ist, so ist demnach für eine solche $r_{\lambda-1} \equiv 1 (\text{mod. } p)$, und damit ist das obige Lemma auch für Gruppen der Ordnung p^λ bewiesen, falls es für Gruppen der Ordnung $p^\varkappa < p^\lambda$ gilt, es ist also allgemein gültig. Für jeden Werth $\varkappa$ ist folglich $r_\varkappa \equiv r_{\varkappa-1}$, und daher $r_\varkappa \equiv 1 (\text{mod. } p)$.

Genau auf dieselbe Weise beweist man den allgemeineren Satz:

II. *Ist die Ordnung einer Gruppe $\mathfrak{H}$ durch die $\varkappa$te Potenz der Primzahl p theilbar, ist $\mathfrak{d} \leqq \varkappa$ und $\mathfrak{P}$ eine in $\mathfrak{H}$ enthaltene Gruppe der Ordnung $p^\mathfrak{d}$, so ist die Anzahl der in $\mathfrak{H}$ enthaltenen Gruppen der Ordnung $p^\varkappa$, die durch $\mathfrak{P}$ theilbar sind, eine Zahl der Form $np + 1$.*

§. 5.

Das in §. 4 benutzte Lemma kann man auch in folgender Art beweisen, indem man sich auf den Satz stützt: Jede Gruppe $\mathfrak{H}$ der Ordnung p^λ hat eine Untergruppe $\mathfrak{A}$ der Ordnung $p^{\lambda-1}$, und eine solche Untergruppe ist stets eine invariante. Seien $\mathfrak{A}$ und $\mathfrak{B}$ zwei verschiedene in $\mathfrak{H}$ enthaltene Gruppen der Ordnung $p^{\lambda-1}$, und sei $\mathfrak{D}$ ihr grösster gemeinsamer Divisor. Da $\mathfrak{A}$ und $\mathfrak{B}$ invariante Untergruppen von $\mathfrak{H}$ sind, so ist auch $\mathfrak{D}$ eine solche, und da $\mathfrak{H}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{A}$ und $\mathfrak{B}$ ist, so hat $\mathfrak{D}$ die Ordnung $p^{\lambda-2}$. Mithin ist $\frac{\mathfrak{H}}{\mathfrak{D}}$ eine Gruppe der Ordnung p^2. Eine solche hat, je nachdem sie eine cyklische Gruppe ist oder nicht, 1 oder $p+1$ Untergruppen der Ordnung p, in unserem Falle also $p+1$, da $\frac{\mathfrak{A}}{\mathfrak{D}}$ und $\frac{\mathfrak{B}}{\mathfrak{D}}$ zwei verschiedene Gruppen dieser Art sind. Demnach enthält $\mathfrak{H}$ genau $p+1$ verschiedene Gruppen der Ordnung $p^{\lambda-1}$, die durch $\mathfrak{D}$ theilbar sind.

Die Gruppe $\mathfrak{H}$ enthält immer eine Gruppe $\mathfrak{A}$ der Ordnung $p^{\lambda-1}$. Enthält sie noch eine andere, so hat $\mathfrak{H}$ eine invariante Untergruppe $\mathfrak{D}$ der Ordnung $p^{\lambda-2}$, die in $\mathfrak{A}$ enthalten ist, und für welche die Gruppe $\frac{\mathfrak{H}}{\mathfrak{D}}$ nicht eine cyklische ist. Seien $\mathfrak{D}_1, \mathfrak{D}_2, \cdots \mathfrak{D}_n$ die sämmtlichen Gruppen dieser Art. Dann giebt es in $\mathfrak{H}$ ausser $\mathfrak{A}$ noch p durch $\mathfrak{D}_1$ theilbare Gruppen der Ordnung $p^{\lambda-1}$

$$(1.) \qquad \mathfrak{A}_1, \mathfrak{A}_2, \cdots \mathfrak{A}_p,$$

ebenso p durch $\mathfrak{D}_2$ theilbare Gruppen

$$(2.) \qquad \mathfrak{A}_{p+1}, \mathfrak{A}_{p+2}, \cdots \mathfrak{A}_{2p},$$

u. s. w., endlich p durch $\mathfrak{D}_n$ theilbare Gruppen

$$(3.) \qquad \mathfrak{A}_{(n-1)p+1}, \mathfrak{A}_{(n-1)p+2}, \cdots \mathfrak{A}_{np}.$$

Die $np+1$ Gruppen $\mathfrak{A}, \mathfrak{A}_1, \cdots \mathfrak{A}_{np}$ sind die sämmtlichen in $\mathfrak{H}$ enthaltenen Gruppen der Ordnung $p^{\lambda-1}$, da jede solche Gruppe $\mathfrak{B}$ mit $\mathfrak{A}$ einen gewissen Divisor $\mathfrak{D}$ gemeinsam haben muss, der eine der n Gruppen $\mathfrak{D}_1, \mathfrak{D}_2 \cdots \mathfrak{D}_n$ ist. Sie sind ferner alle verschieden. Denn wäre $\mathfrak{A}_1 = \mathfrak{A}_{p+1}$, so wäre $\mathfrak{A}_1$ durch die beiden Gruppen $\mathfrak{D}_1$ und $\mathfrak{D}_2$ theilbar, also auch durch ihr kleinstes gemeinschaftliches Vielfaches $\mathfrak{A}$. Ist $\mathfrak{P}$ eine in $\mathfrak{H}$ enthaltene Gruppe der Ordnung p^φ, so kann man auch die oben betrachteten Untergruppen von $\mathfrak{H}$ alle der Bedingung unterwerfen, durch $\mathfrak{P}$ theilbar zu sein. Ist umgekehrt $\mathfrak{H}$ eine invariante Untergruppe einer Gruppe $\mathfrak{P}$ der Ordnung p^φ, so kann man fordern, dass sie alle invariante Untergruppen von $\mathfrak{P}$ seien.

Mit Hülfe des Satzes V, § 1 ist leicht zu beweisen, dass die Anzahl der Gruppen der Ordnung $p^{\lambda-1}$, die in einer Gruppe $\mathfrak{H}$ der Ordnung p^λ enthalten sind, nur dann gleich 1 ist, wenn $\mathfrak{H}$ eine cyclische Gruppe ist.

I. *Die Anzahl der in einer Gruppe der Ordnung p^λ enthaltenen invarianten Untergruppen der Ordnung $p^\varkappa$ ist eine Zahl der Form $np+1$.*

Sei $\mathfrak{H}$ eine Gruppe der Ordnung h, sei p^λ die höchste in h enthaltene Potenz von p, sei $\varkappa \leqq \lambda$ und $\mathfrak{P}_\varkappa$ irgend eine in $\mathfrak{H}$ enthaltene Gruppe der Ordnung $p^\varkappa$. Jede Gruppe $\mathfrak{P}_\varkappa$ ist in $np+1$, also in mindestens einer Gruppe $\mathfrak{P}_\lambda$ enthalten. Ich theile die Gruppen $\mathfrak{P}_\varkappa$ in zwei Arten. Für eine Gruppe der ersten Art giebt es eine Gruppe $\mathfrak{P}_\lambda$, von der $\mathfrak{P}_\varkappa$ eine invariante Untergruppe ist, für eine der zweiten Art giebt es eine solche nicht. Die Anzahl der mit $\mathfrak{P}_\varkappa$ vertauschbaren Elemente von $\mathfrak{H}$ ist im ersten Falle durch p^λ theilbar, im zweiten nicht. Die Anzahl der mit $\mathfrak{P}_\varkappa$ conjugirten Gruppen ist daher im zweiten Falle durch p theilbar, im ersten nicht. Theilt man also die Gruppen $\mathfrak{P}_\varkappa$ in Classen conjugirter Gruppen, so erkennt man, dass

die Anzahl der Gruppen $\mathfrak{P}_\varkappa$ der zweiten Art durch p theilbar ist. Folglich ist die Anzahl der Gruppen $\mathfrak{P}_\varkappa$ der ersten Art $\equiv 1 \pmod{p}$.

II. *Ist $\mathfrak{H}$ eine Gruppe der Ordnung p^λ und $\mathfrak{G}$ eine invariante Untergruppe von $\mathfrak{H}$, deren Ordnung durch $p^\varkappa$ theilbar ist, so ist die Anzahl der in $\mathfrak{G}$ enthaltenen Gruppen der Ordnung $p^\varkappa$, die invariante Untergruppen von $\mathfrak{H}$ sind, eine Zahl der Form $np+1$.*

Sei auch hier allgemeiner p^λ die höchste Potenz der Primzahl p, die in der Ordnung h von $\mathfrak{H}$ aufgeht. Sei $\mathfrak{G}$ eine invariante Untergruppe von $\mathfrak{H}$, deren Ordnung g durch $p^\varkappa$ theilbar ist. Die Anzahl aller in $\mathfrak{G}$ enthaltenen Gruppen $\mathfrak{P}_\varkappa$ der Ordnung $p^\varkappa$ ist $\equiv 1 \pmod{p}$. Ich theile sie in Gruppen erster und zweiter Art (in Bezug auf $\mathfrak{H}$) und weiter in Classen conjugirter Gruppen. Ist $\mathfrak{G}$ durch $\mathfrak{P}_\varkappa$ theilbar, so ist $\mathfrak{G}$ auch durch jede mit $\mathfrak{P}_\varkappa$ conjugirte Gruppe theilbar. Daraus ergiebt sich die Behauptung in derselben Weise wie oben. Man kann sie aber auch mit Hülfe der in §. 4 benutzten Methode leicht direct beweisen:

Die Ordnung von $\mathfrak{H}$ sei $h = p^\lambda$. Nach Satz V, §. 1 enthält $\mathfrak{G}$ Elemente der Ordnung p, die invariante Elemente von $\mathfrak{H}$ sind. Sie bilden, zusammen mit dem Hauptelemente, eine Gruppe. Ist p^α ihre Ordnung, so ist $p^\alpha - 1$ die Anzahl jener Elemente. Nach Satz III, §. 1 besteht jede invariante Untergruppe von $\mathfrak{H}$, deren Ordnung p ist, aus den Potenzen eines solchen Elementes. Daher giebt es in $\mathfrak{G}$ $r = \frac{p^\alpha - 1}{p-1}$ Gruppen der Ordnung p, die invariante Untergruppen von $\mathfrak{H}$ sind. Diese Zahl ist

$$r \equiv 1 \pmod{p}. \tag{4.}$$

Seien

$$\mathfrak{A}_1, \mathfrak{A}_2, \cdots \mathfrak{A}_r \tag{5.}$$

diese r Gruppen, und seien

$$\mathfrak{B}_1, \mathfrak{B}_2, \cdots \mathfrak{B}_s \tag{6.}$$

die s in $\mathfrak{G}$ enthaltenen Gruppen der Ordnung $p^\varkappa$, die invariante Untergruppen von $\mathfrak{H}$ sind. Sei $\mathfrak{B}$ eine der Gruppen (6.). Unter den Gruppen (5.) seien $\mathfrak{A}_1, \mathfrak{A}_2, \cdots \mathfrak{A}_b$ in $\mathfrak{B}$ enthalten. Nach (4.) ist dann $b \equiv 1 \pmod{p}$. Sei $\mathfrak{A}$ eine der Gruppen (5.). Unter den Gruppen (6.) seien $\mathfrak{B}_1, \mathfrak{B}_2, \cdots \mathfrak{B}_a$ durch $\mathfrak{A}$ theilbar. Dann sind $\frac{\mathfrak{B}_1}{\mathfrak{A}}, \frac{\mathfrak{B}_2}{\mathfrak{A}}, \cdots \frac{\mathfrak{B}_a}{\mathfrak{A}}$ die in $\frac{\mathfrak{G}}{\mathfrak{A}}$ enthaltenen Gruppen der Ordnung $p^{\varkappa-1}$, die invariante Untergruppen von $\frac{\mathfrak{H}}{\mathfrak{A}}$ sind. Nach der Methode der Induction ist demnach $a \equiv 1 \pmod{p}$. Bedient man sich also derselben Bezeichnungen, wie in §. 4, so ist

$$1 \equiv r \equiv a_1 + a_2 + \cdots + a_r \equiv b_1 + b_2 + \cdots + b_s \equiv s \pmod{p}.$$

Ich füge noch einige Bemerkungen hinzu über die Anzahl der Gruppen $\mathfrak{P}_\varkappa$ der ersten Art, die mit einer bestimmten conjugirt sind, und über die Anzahl der Classen conjugirter Gruppen, in welche die Gruppen $\mathfrak{P}_\varkappa$ zerfallen.

Sei $\mathfrak{P}$ eine in $\mathfrak{H}$ enthaltene Gruppe der Ordnung p^λ, und $\mathfrak{Q}$ eine invariante Untergruppe von $\mathfrak{P}$ der Ordnung $p^\varkappa$. Die mit $\mathfrak{P}(\mathfrak{Q})$ vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppe von $\mathfrak{P}'(\mathfrak{Q}')$ der Ordnung $p'(q')$. Der grösste gemeinsame Divisor von $\mathfrak{P}'$ und $\mathfrak{Q}'$ sei die Gruppe $\mathfrak{R}$ der Ordnung r. Die Gruppen $\mathfrak{P}'$, $\mathfrak{Q}'$ und $\mathfrak{R}$ sind durch $\mathfrak{P}$ theilbar. Sei p^δ die Ordnung des grössten gemeinsamen Divisors von $\mathfrak{P}$ und einer in Bezug auf $\mathfrak{H}$ conjugirten Gruppe, die so gewählt ist, dass δ ein Maximum ist. Dann ist (*Über endliche Gruppen*, §. 2, VIII)

$$\frac{h}{p'} \equiv 1 \,(\mathrm{mod.}\, p^{\lambda-\delta}).$$

Die Gruppe $\mathfrak{R}$ besteht aus allen Elementen von $\mathfrak{Q}'$, die mit $\mathfrak{P}$ vertauschbar sind. Mithin ist auch

$$\frac{q'}{r} \equiv 1 \,(\mathrm{mod.}\, p^{\lambda-\delta}).$$

Folglich ist

$$\frac{h}{q'} \equiv \frac{p'}{r} \,(\mathrm{mod.}\, p^{\lambda-\delta}). \tag{7.}$$

Hier ist $\frac{h}{q'}$ die Anzahl der Gruppen, die mit $\mathfrak{Q}$ in Bezug auf $\mathfrak{H}$ conjugirt sind, und $\frac{p'}{r}$ die Anzahl der Gruppen, die mit $\mathfrak{Q}$ in Bezug auf $\mathfrak{P}'$ conjugirt sind. Denn die Gruppe $\mathfrak{R}$ besteht aus allen Elementen von $\mathfrak{P}'$, die mit $\mathfrak{Q}$ vertauschbar sind. Die Anzahl der Gruppen einer bestimmten Classe in $\mathfrak{H}$ ist also der Anzahl der Gruppen der entsprechenden Classe in $\mathfrak{P}'$ congruent (mod. $p^{\lambda-\delta}$).

Ferner ist die Anzahl der verschiedenen Classen (in welche die Gruppen $\mathfrak{P}_\varkappa$ der ersten Art zerfallen) in $\mathfrak{H}$ der Anzahl dieser Classen in $\mathfrak{P}'$ gleich. Dies ergiebt sich aus dem Satze:

III. *Sind zwei invariante Untergruppen von* $\mathfrak{P}$ *conjugirt in Bezug auf* $\mathfrak{H}$, *so sind sie es auch in Bezug auf* $\mathfrak{P}'$.

Seien $\mathfrak{Q}$ und $\mathfrak{Q}_0$ zwei invariante Untergruppen von $\mathfrak{P}$. Sind sie conjugirt in Bezug auf $\mathfrak{H}$, so giebt es in $\mathfrak{H}$ ein solches Element H, dass

$$H^{-1}\mathfrak{Q}_0 H = \mathfrak{Q} \tag{4.}$$

ist. Da $\mathfrak{Q}_0$ eine invariante Untergruppe von $\mathfrak{P}$ ist, so ist $H^{-1}\mathfrak{Q}_0 H = \mathfrak{Q}$ eine invariante Untergruppe von

$$H^{-1}\mathfrak{P}H = \mathfrak{P}_0.$$

Mithin ist $\mathfrak{Q}'$ durch $\mathfrak{P}$ und durch $\mathfrak{P}_0$ theilbar. Folglich (*Über endliche Gruppen*, §. 2, VII) giebt es in $\mathfrak{Q}'$ ein solches Element Q, dass

$$Q^{-1}\mathfrak{P}_0 Q = \mathfrak{P},$$

also

$$\mathfrak{P}HQ = HQ\mathfrak{P}$$

ist. Daher ist $HQ = P$ ein Element von $\mathfrak{P}'$. Setzt man den Ausdruck $H = PQ^{-1}$ in die Gleichung (4.) ein, so erhält man, da Q mit $\mathfrak{Q}$ vertauschbar ist,

$$P^{-1}\mathfrak{Q}_0 P = Q^{-1}\mathfrak{Q}Q = \mathfrak{Q}.$$

Es giebt also in $\mathfrak{P}'$ ein Element P, das $\mathfrak{Q}_0$ in $\mathfrak{Q}$ transformirt.

Man theile nun die in $\mathfrak{H}$ enthaltenen Gruppen $\mathfrak{P}_\varkappa$ (der ersten Art) in Classen conjugirter Gruppen (in Bezug auf $\mathfrak{H}$), und wähle aus jeder Classe einen Repraesentanten. Ist $\mathfrak{Q}_0$ ein solcher, so ist $\mathfrak{Q}_0$ eine Gruppe der Ordnung $p^\varkappa$, die in einer gewissen Gruppe $\mathfrak{P}_0$ als invariante Untergruppe enthalten ist. Ist $H^{-1}\mathfrak{P}_0 H = \mathfrak{P}$, so ist $H^{-1}\mathfrak{Q}_0 H = \mathfrak{Q}$ eine invariante Untergruppe von $\mathfrak{P}$. Man kann also die Repraesentanten der verschiedenen Classen so wählen, dass sie alle invariante Untergruppen einer bestimmten Gruppe $\mathfrak{P}$ der Ordnung p^λ sind. Jede invariante Untergruppe der Ordnung $p^\varkappa$ von $\mathfrak{P}$ ist dann einer dieser Gruppen in Bezug auf $\mathfrak{H}$, also auch in Bezug auf $\mathfrak{P}'$, conjugirt. Die invarianten Untergruppen $\mathfrak{P}_\varkappa$ von $\mathfrak{P}$ mögen zerfallen in s Classen von Gruppen, die in Bezug auf $\mathfrak{P}'$ conjugirt sind. Dann zerfallen auch die Gruppen $\mathfrak{P}_\varkappa$ der ersten Art von $\mathfrak{H}$ in s Classen von Gruppen, die in Bezug auf $\mathfrak{H}$ conjugirt sind.

Ausgegeben am 7. November.