# Über auflösbare Gruppen. III

Frobenius, Georg

Göttingen, [s.a.]

ETH-Bibliothek Zürich

Shelf Mark: Rar 1524

Persistent Link: https://doi.org/10.3931/e-rara-18874

# Über auflösbare Gruppen. III.

Von G. Frobenius.

In meiner Arbeit *Über auflösbare Gruppen*, Sitzungsberichte 1893 (im folgenden *A. I* citirt) habe ich folgenden Satz bewiesen:

*Sind die Primfactoren der Zahl a alle unter einander verschieden, und ist jeder Primfactor von b grösser als der grösste Primfactor von a, so giebt es in einer Gruppe $\mathfrak{H}$ der Ordnung ab genau b Elemente, deren Ordnung in b aufgeht.*

Mit Hülfe der Theorie der Gruppencharaktere will ich hier beweisen, dass diese $b$ Elemente eine Gruppe bilden, die als einzige ihrer Art eine charakteristische Untergruppe von $\mathfrak{H}$ sein muss. In meiner Arbeit *Über endliche Gruppen*, Sitzungsberichte 1895, habe ich (§ 2, II) gezeigt:

*Ist $\mathfrak{A}$ eine invariante Untergruppe von $\mathfrak{B}$, und $\mathfrak{B}$ eine invariante Untergruppe von $\mathfrak{C}$, sind a und ab die Ordnungen von $\mathfrak{A}$ und $\mathfrak{B}$, und sind a und b theilerfremd, so ist $\mathfrak{A}$ auch eine invariante Untergruppe von $\mathfrak{C}$.*

Demnach ist der allgemeine oben aufgestellte Satz eine unmittelbare Folge des specielleren Satzes:

I. *Ist die Ordnung h der Gruppe $\mathfrak{H}$ nur durch die erste Potenz der Primzahl p theilbar und ist $p-1$ zu h theilerfremd, so enthält $\mathfrak{H}$ eine und nur eine (demnach charakteristische) Untergruppe der Ordnung $h:p$. Diese wird gebildet von allen Elementen der Gruppe $\mathfrak{H}$, deren Ordnung nicht durch p theilbar ist.*

Die Bedingung, dass $p-1$ und $h$ theilerfremd sind, ist stets erfüllt, wenn $p$ der kleinste Primfactor von $h$ ist. Den obigen Satz beweist für die beiden Fälle $p = 3$ und 5 Hr. Burnside in der interessanten Arbeit *On some properties of groups of odd order (Proceedings of the London Math. Soc., vol. XXXIII)*, worin er zum ersten Male die Theorie der Gruppencharaktere zur Erforschung der Eigenschaften einer Gruppe benutzt hat. Aber auch in dem lange bekannten Falle $p = 2$ beruht der Beweis auf den nämlichen Grundlagen. Stellt man nämlich $\mathfrak{H}$ als transitive Gruppe von Permutationen von $h$ Symbolen

dar, so ist die Hälfte dieser Permutationen gerade, die Hälfte ungerade. Demnach hat $\mathfrak{H}$ einen Charakter ersten Grades, der für die geraden Permutationen den Werth $+1$, für die ungeraden den Werth $-1$ hat.

Eine Gruppe $\mathfrak{H}$, deren Ordnung $h$ durch die Primzahl $p$ theilbar ist, enthält ein Element $P$ der Ordnung $p$. Die Potenzen von $P$ bilden eine Gruppe $\mathfrak{P}$ und die mit $\mathfrak{P}$ vertauschbaren Elemente von $\mathfrak{H}$ eine Gruppe $\mathfrak{Q}$ der Ordnung $q$. Ist $Q$ ein Element von $\mathfrak{Q}$, so ist $Q^{-1}PQ = P^s$. Ist nun $p-1$ zu $q$ theilerfremd, so muss $s \equiv 1 \pmod{p}$, also $Q$ mit $P$ vertauschbar sein. Denn da $Q^q = E$ ist, so ist $P = Q^{-q}PQ^q = P^{(s^q)}$, und mithin ist $s^q \equiv 1 \pmod{p}$. Da auch $s^{p-1} \equiv 1$ ist, so ist, weil $q$ und $p-1$ theilerfremd sind, $s \equiv 1$ (*A. I*, § 3).

Die Elemente von $\mathfrak{H}$ mögen in $k$ Classen conjugirter Elemente zerfallen. Von den $p-1$ Elementen $P, P^2, \cdots P^{p-1}$ sind nicht zwei conjugirt. Denn ist $H^{-1}P^\alpha H = P^\beta$, und ist $\alpha\gamma \equiv 1 \pmod{p}$, so ist $H^{-1}PH = P^{\beta\gamma}$, also $H^{-1}\mathfrak{P}H = \mathfrak{P}$. Daher gehört $H$ der Gruppe $\mathfrak{Q}$ an, und folglich ist, wie eben gezeigt, $\beta\gamma \equiv 1$ und mithin $\alpha \equiv \beta$.

Die $k$ verschiedenen Charaktere von $\mathfrak{H}$ seien

$$\chi^{(\varkappa)}(R) \qquad (\varkappa = 0, 1, \cdots k-1).$$

Dann ist (*Über die Primfactoren der Gruppendeterminante*, Sitzungsberichte 1896; im folgenden *Pr.* citirt; § 7, (8.)).

$$(1.) \qquad \sum_{\varkappa} \chi^{(\varkappa)}(R^{-1})\chi^{(\varkappa)}(R) = \frac{h}{h_R},$$

wo $h_R$ die Anzahl der mit $R$ conjugirten Elemente bezeichnet; dagegen

$$(2.) \qquad \sum_{\varkappa} \chi^{(\varkappa)}(R^{-1})\chi^{(\varkappa)}(S) = 0,$$

wenn die Elemente $R$ und $S$ nicht conjugirt sind.

Daher ist unter den obigen Voraussetzungen

$$(3.) \qquad \sum_{\varkappa} \chi^{(\varkappa)}(P^{-1})\chi^{(\varkappa)}(P^\alpha) = 0, \qquad (\alpha = 2, 3, \cdots p-1)$$

aber

$$(4.) \qquad \sum_{\varkappa} \chi^{(\varkappa)}(P^{-1})\chi^{(\varkappa)}(P) = \frac{h}{h_P}.$$

Ist $\chi^{(\varkappa)}(E) = f^{(\varkappa)}$, so ist $\chi^{(\varkappa)}(P)$ eine Summe von $f^{(\varkappa)}$ Wurzeln der Gleichung $x^p = 1$ (*Pr.* § 12, (6.)), die einzeln dadurch bestimmt sind, dass $\chi^{(\varkappa)}(P^\alpha)$ die Summe ihrer $\alpha^{\text{ten}}$ Potenzen ist. Ist daher $\rho$ eine primitive $p^{\text{te}}$ Wurzel der Einheit, so ist

$$(5.) \qquad \begin{aligned} \chi^{(\varkappa)}(P) &= r_0^{(\varkappa)} + r_1^{(\varkappa)}\rho + \cdots + r_{p-1}^{(\varkappa)}\rho^{p-1}, \\ \chi^{(\varkappa)}(P^\alpha) &= r_0^{(\varkappa)} + r_1^{(\varkappa)}\rho^\alpha + \cdots + r_{p-1}^{(\varkappa)}\rho^{(p-1)\alpha}, \\ \chi^{(\varkappa)}(E) &= r_0^{(\varkappa)} + r_1^{(\varkappa)} + \cdots + r_{p-1}^{(\varkappa)}, \end{aligned}$$

wo $r_0^{(\varkappa)}, r_1^{(\varkappa)} \cdots r_{p-1}^{(\varkappa)}$ nicht negative ganze Zahlen sind. Mithin ist nach (3.) und (4.)

$$\sum_{\varkappa}(r_0^{(\varkappa)} + r_1^{(\varkappa)}\rho^{-1} + r_2^{(\varkappa)}\rho^{-2} + \cdots + r_{p-1}^{(\varkappa)}\rho^{-p+1})(r_0^{(\varkappa)} + r_1^{(\varkappa)}\rho^{\alpha} + r_2^{(\varkappa)}\rho^{2\alpha} + \cdots + r_{p-1}^{(\varkappa)}\rho^{(p-1)\alpha}) = 0$$

für $\alpha = 2, 3, \cdots p-1$, aber $= \frac{h}{h_P}$ für $\alpha = 1$.

Ich benutze auch die Zeichen $r_p^{(\varkappa)}, r_{p+1}^{(\varkappa)}, \cdots$, indem ich $r_\alpha^{(\varkappa)} = r_\beta^{(\varkappa)}$ setze, wenn $\alpha \equiv \beta \pmod p$ ist. Auf der linken Seite ist dann, wenn man sie mittelst der Gleichung $\rho^p = 1$ reducirt, das von $\rho$ unabhängige Glied gleich

$$\sum_{\varkappa}(r_0^{(\varkappa)}r_0^{(\varkappa)} + r_\alpha^{(\varkappa)}r_1^{(\varkappa)} + r_{2\alpha}^{(\varkappa)}r_2^{(\varkappa)} + \cdots + r_{(p-1)\alpha}^{(\varkappa)}r_{p-1}^{(\varkappa)}) = \sum_{\varkappa} r_0^{(\varkappa)}r_0^{(\varkappa)} + \sum_{\varkappa}\sum_{\beta} r_{\alpha\beta}^{(\varkappa)}r_\beta^{(\varkappa)},$$

wo $\beta$ die Werthe $1, 2, \cdots p-1$ durchläuft.

Die erhaltenen Gleichungen bleiben bestehen, wenn man $\rho$ durch $\rho^2, \rho^3, \cdots \rho^{p-1}$ ersetzt. Für $\rho = 1$ aber ist

$$\sum_{\varkappa}(r_0^{(\varkappa)} + r_1^{(\varkappa)} + \cdots + r_{p-1}^{(\varkappa)})^2 = \sum_{\varkappa} f^{(\varkappa)2} = h.$$

Addirt man die $p$ so gefundenen Gleichungen, so ergiebt sich

$$\sum_{\varkappa} r_0^{(\varkappa)}r_0^{(\varkappa)} + \sum_{\varkappa}\sum_{\beta} r_{\alpha\beta}^{(\varkappa)}r_\beta^{(\varkappa)} = \frac{h}{p}$$

für $\alpha = 2, 3, \cdots p-1$, dagegen gleich $\frac{h}{p} + (p-1)\frac{h}{ph_P}$ für $\alpha = 1$. Multiplicirt man mit $\alpha$ und summirt nach $\alpha$ von 1 bis $p-1$, so erhält man

$$\tfrac{1}{2}p(p-1)\sum_{\varkappa} r_0^{(\varkappa)}r_0^{(\varkappa)} + \sum_{\varkappa}\sum_{\alpha,\beta}\alpha\, r_{\alpha\beta}^{(\varkappa)}r_\beta^{(\varkappa)} = \tfrac{1}{2}(p-1)h + (p-1)\frac{h}{ph_P}.$$

Daher besteht, wenn $p$ ungerade ist, die Congruenz

$$\sum_{\varkappa}\sum_{\alpha,\beta}\alpha\, r_{\alpha\beta}^{(\varkappa)}r_\beta^{(\varkappa)} \equiv -\frac{h}{ph_P} \pmod p,$$

wo sowohl $\alpha$ als $\beta$ $p-1$ Zahlen durchläuft, die den Zahlen $1, 2, \cdots p-1 \pmod p$ congruent sind. Unter $\beta^{-1} \pmod p$ verstehe ich die ganze Zahl $\gamma$, die der Congruenz $\beta\gamma \equiv 1$ genügt. Ersetzt man dann in der obigen Congruenz den Summationsbuchstaben $\alpha$ durch $\alpha\beta^{-1}$, so erhält man

$$\sum_{\varkappa}(\sum_{\alpha}\alpha r_\alpha^{(\varkappa)})(\sum_{\beta}\beta^{-1}r_\beta^{(\varkappa)}) \equiv -\frac{h}{ph_P} \pmod p.$$

Ich nehme jetzt an, dass $h$ nur durch die erste Potenz von $p$ theilbar ist. Dann ist $\frac{h}{ph_P}$ nicht durch $p$ theilbar. Daher giebt es einen Werth von $\varkappa$, für welchen

$$\sum_{\alpha}\alpha r_\alpha^{(\varkappa)} = r_1^{(\varkappa)} + 2r_2^{(\varkappa)} + \cdots + (p-1)r_{p-1}^{(\varkappa)}$$

nicht durch $p$ theilbar ist. Der letzte Ausdruck ist der Exponent der Potenz von $\rho$, die gleich dem Producte der $f^{(\varkappa)}$ Einheitswurzeln in der

Summe (5.) ist. Dieses Product $\vartheta(P)$ ist aber ein Charakter ersten Grades von $\mathfrak{H}$ (*Pr.* § 12, (9.)). Die Gruppe $\mathfrak{H}$ besitzt also einen Charakter ersten Grades, der für $R = P$ gleich einer primitiven $p^{\text{ten}}$ Einheitswurzel ist.

Für ein Element $S$ der Ordnung $s$ ist $\vartheta(S)$ eine $s^{\text{te}}$ Wurzel der Einheit. Ist $g = \frac{h}{p}$, so ist $\vartheta(R)^g = \chi(R)$ auch ein Charakter ersten Grades von $\mathfrak{H}$, dessen Werth für $R = P$ eine primitive $p^{\text{te}}$ Wurzel der Einheit ist, für jedes Element $R$ aber, dessen Ordnung in $g$ aufgeht, gleich 1 ist. Nun habe ich (*Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen*, Sitzungsberichte 1898; § 4, II; im folgenden mit *Rel.* citirt) gezeigt:

*Ist $\chi(R)$ ein Charakter $f^{\text{ten}}$ Grades der Gruppe $\mathfrak{H}$, so bilden alle Elemente $R$ von $\mathfrak{H}$, für die $\chi(R) = f$ ist, eine invariante Untergruppe $\mathfrak{G}$ von $\mathfrak{H}$, und der Charakter $\chi$ gehört zu der Gruppe $\frac{\mathfrak{H}}{\mathfrak{G}}$.*

Daher hat $\mathfrak{H}$ eine invariante Untergruppe $\mathfrak{G}$, gebildet von allen Elementen von $\mathfrak{H}$, für die $\chi(R) = 1$ ist. Diese enthält das Element $P$ nicht, ist also $< \mathfrak{H}$. Sie enthält aber alle Elemente von $\mathfrak{H}$, deren Ordnung in $g$ aufgeht. Ist, in Primfactoren zerlegt, $g = a^\alpha b^\beta c^\gamma \cdots$, so enthält $\mathfrak{H}$ Untergruppen der Ordnung $a^\alpha$, $b^\beta$, $c^\gamma$, $\cdots$. Da diese alle in $\mathfrak{G}$ enthalten sind, so ist die Ordnung von $\mathfrak{G}$ durch $a^\alpha$, $b^\beta$, $c^\gamma$, $\cdots$, also durch $g$ theilbar, und folglich, weil sie $< h$ ist, gleich $g$. Für die in der Arbeit *A. I* entwickelten Sätze, die hier nicht vorausgesetzt sind, ist damit zugleich ein neuer Beweis gewonnen.

In dem Satze I. wird verlangt, dass $p-1$ zu $h$ theilerfremd ist. Wie der Beweis zeigt, genügt es aber schon, wenn $p-1$ zu $q$ theilerfremd ist. Z. B. ist nach Sylow die Ordnung einer transitiven Gruppe $\mathfrak{H}$ von Permutationen von $p$ Symbolen eine Zahl der Form

$$h = pq \ (np+1),$$

wo $q$ ein Divisor von $p-1$ ist, und $np+1$ die Anzahl der in $\mathfrak{H}$ enthaltenen Gruppen $\mathfrak{P}$ der Ordnung $p$ ist. Die mit einer solchen Gruppe $\mathfrak{P}$ vertauschbaren Elemente von $\mathfrak{H}$ bilden eine metacyklische Gruppe $\mathfrak{Q}$ der Ordnung $pq$. Nun hat Mathieu bemerkt: »*Ist $q = 1$, so ist $n = 0$.*« Denn dann hat $\mathfrak{H}$ nach dem Satze I. eine und nur eine Untergruppe $\mathfrak{G}$ der Ordnung $np+1$. Nun bilden aber die Permutationen der transitiven Gruppe $\mathfrak{H}$, die $x_\alpha$ ungeändert lassen, eine solche Gruppe $\mathfrak{G}$. Daher lässt jede Permutation von $\mathfrak{G}$ das Symbol $x_\alpha$, d. h. $x_0, x_1, \ldots x_{p-1}$ ungeändert, und mithin ist $\mathfrak{G}$ die Hauptgruppe und ihre Ordnung $np+1 = 1$.

## § 2.

In ähnlicher Weise lassen sich die allgemeineren Betrachtungen vervollständigen und vereinfachen, die ich in meiner Arbeit *Über auf-*

*lösbare Gruppen* II, Sitzungsberichte 1895 (im folgenden *A. II* citirt), angestellt habe. Sei $\mathfrak{F}$ eine Untergruppe von $\mathfrak{H}$, von deren Elementen nicht zwei in Bezug auf $\mathfrak{H}$ conjugirt sind. Sind $A$ und $B$ zwei Elemente von $\mathfrak{F}$, so ist daher das mit $A$ conjugirte Element $B^{-1}AB$ von $\mathfrak{F}$ gleich $A$, oder es sind je zwei Elemente von $\mathfrak{F}$ vertauschbar, $AB = BA$.

Sei $m$ der Rang der commutativen Gruppe $\mathfrak{F}$, sei $L_1, L_2 \cdots L_m$ eine Basis von $\mathfrak{F}$, und sei $l_\mu$ die Ordnung von $L_\mu$. Dann kann jedes Element $P$ von $\mathfrak{F}$, und zwar nur in einer Art auf die Form $P = L_1^{\lambda_1} L_2^{\lambda_2} \cdots L_m^{\lambda_m}$ gebracht werden. Ist ferner $\rho_\mu$ eine primitive $l_\mu^{\text{te}}$ Wurzel der Einheit, und sind $\alpha_1, \alpha_2 \cdots \alpha_m$ irgend $m$ Zahlen, so ist

$$\psi(P) = \rho_1^{\alpha_1\lambda_1} \rho_2^{\alpha_2\lambda_2} \cdots \rho_m^{\alpha_m\lambda_m}$$

ein Charakter von $\mathfrak{F}$. Ist $A = L_1^{\alpha_1} L_2^{\alpha_2} \cdots L_m^{\alpha_m}$, so bezeichne ich diesen Charakter mit $\psi_A(P)$. Ist $f$ die Ordnung von $\mathfrak{F}$, so sind dadurch die $f$ Charaktere von $\mathfrak{F}$ den Elementen $A$ zugeordnet, doch ist diese Zuordnung von der Wahl der Basis und der Wahl der Wurzeln $\rho_1, \cdots \rho_m$ abhängig (vergl. H. WEBER, *Theorie der ABEL'schen Zahlkörper*, Act. Math. Bd. 9, Seite 112). Das Product zweier Charaktere (ersten Grades) ist wieder ein solcher, und zwar ist $\psi_A(P)\psi_B(P) = \psi_{AB}(P)$. Der zu $\psi_A(P)$ inverse Charakter ist $\psi_A(P)^{-1} = \psi_A(P^{-1}) = \psi_{A^{-1}}(P)$.

Zwischen den Charakteren $\chi^{(\varkappa)}(R)$ der Gruppe $\mathfrak{H}$ und den Charakteren $\psi_A(P)$ von $\mathfrak{F}$ bestehen (*Rel.* § 1) Relationen der Form

$$\chi^{(\varkappa)}(P) = \sum_A r_A^{(\varkappa)} \psi_A(P), \tag{6.}$$

deren Coefficienten $r_A^{(\varkappa)}$ positive ganze Zahlen sind. Die Summe erstreckt sich über alle Elemente $A$ von $\mathfrak{F}$. Nach der Voraussetzung gilt die Gleichung (2.), § 1 für je zwei verschiedene Elemente von $\mathfrak{F}$. Daher ist

$$\sum_\varkappa \sum_{A,B} r_A^{(\varkappa)} \psi_A(P^{-1})\, r_B^{(\varkappa)} \psi_B(Q) = 0,$$

aber wenn $P = Q$ ist, gleich $\frac{h}{h_P}$. Setzt man

$$\sum_\varkappa r_A^{(\varkappa)} r_B^{(\varkappa)} = s_{A,B} = s_{B,A},$$

so ist

$$\sum_{A,B} s_{A,B} \psi_A(P^{-1}) \psi_B(Q) = 0$$

oder $\frac{h}{h_P}$. Daher ist

$$\sum_Q \psi_B(Q) \Big( \sum_{A,C} s_{A,C} \psi_A(P) \psi_C(Q^{-1}) \Big) = \frac{h}{h_P}\, \psi_B(P).$$

Nun ist $\sum_Q \psi_B(Q)\psi_C(Q^{-1}) = 0$, aber wenn $B = C$ ist, gleich $f$. Daher ist

$$\sum_A s_{A,B} \psi_A(P) = \frac{h}{f h_P}\, \psi_B(P),$$

und in derselben Weise ergiebt sich aus dieser Gleichung

$$s_{A,B} = \frac{h}{f^2} \sum_P \frac{1}{h_P} \psi_A(P^{-1}) \psi_B(P).$$

Nun ist $\psi_A(P^{-1}) = \psi_{A^{-1}}(P)$ und $\psi_{A^{-1}}(P)\psi_B(P) = \psi_{A^{-1}B}(P)$. Setzt man also

$$s_{A,E} = s_A = \frac{h}{f^2} \sum_P \frac{1}{h_P} \psi_A(P),$$

so ist

$$s_{A,B} = s_{B,A} = s_{A^{-1}B} = s_{AB^{-1}}.$$

Ferner ist $\sum_A \psi_A(P) = 0$, aber wenn $P = E$ ist, gleich $f$. Daher ist

$$\sum_A s_A = \frac{h}{f} = g.$$

Die Formel (6.) gilt für jedes Element $P$ von $\mathfrak{G}$, also auch für $P^\varkappa$ und für $E$. Daher enthält sie die Darstellung von $\chi^{(\varkappa)}(P)$ als Summe von $f^{(\varkappa)}$ Einheitswurzeln. Das Product derselben

$$\vartheta^{(\varkappa)}(P) = \prod_A \psi_A(P)^{r_A^{(\varkappa)}}$$

ist ein Charakter ersten Grades von $\mathfrak{H}$, genauer, es giebt einen Charakter $\vartheta^{(\varkappa)}(R)$, der für die Elemente $P$ der Gruppe $\mathfrak{F}$ die angegebenen Werthe hat. Daher ist auch

$$\vartheta_B(P) = \prod_\varkappa \vartheta^{(\varkappa)}(P)^{r_B^{(\varkappa)}} = \prod_A \psi_A(P)^{s_{AB^{-1}}}$$

ein Charakter ersten Grades von $\mathfrak{H}$, oder wenn man $A$ durch $AB$ ersetzt,

$$\vartheta_B(P) = \prod_A \psi_{AB}(P)^{s_A} = \psi_B(P)^g \prod_A \psi_A(P)^{s_A}$$

und endlich auch

$$\frac{\vartheta_B(P)}{\vartheta_C(P)} = \psi_{BC^{-1}}(P)^g,$$

oder wenn man $BC^{-1} = A$ setzt, $\psi_A(P)^g$.

Nimmt man jetzt an, dass $f$ und $g$ theilerfremd sind, so folgt daraus, dass $\psi_A(P)$ selbst ein Charakter von $\mathfrak{H}$ ist, d. h. es giebt einen oder mehrere Charaktere ersten Grades $\chi(R)$ von $\mathfrak{H}$, die für die Elemente $P$ der Gruppe $\mathfrak{F}$ die Werthe $\psi_A(P)$ haben. Sei $\mathfrak{G}$ der Complex der Elemente von $\mathfrak{H}$, deren Ordnung in $g$ aufgeht. Ist dann $gg' \equiv 1 \pmod{f}$, so ist $\chi(R)^{gg'}$ ein Charakter ersten Grades von $\mathfrak{H}$, der dieselbe Eigenschaft besitzt, und der für die Elemente des Complexes $\mathfrak{G}$ gleich 1 ist. Einen solchen Charakter bezeichne ich mit

$\chi_A(R)$. Alle Elemente von $\mathfrak{H}$, für die jeder der $f$ verschiedenen Charaktere $\chi_A(R) = 1$ ist, bilden eine invariante Untergruppe von $\mathfrak{H}$, und diese ist gleich $\mathfrak{G}$. Sei nämlich $R$ ein Element von $\mathfrak{H}$, das dem Complexe $\mathfrak{G}$ nicht angehört. Dann ist die Ordnung von $R$ durch einen Primfactor $p$ von $f$ theilbar. Sei $p^\lambda$ die höchste in $f$ aufgehende Potenz von $p$, sei $\mathfrak{P}$ eine Untergruppe der Ordnung $p^\lambda$ von $\mathfrak{F}$. Dann ist $R^{h:p^\lambda} = Q$ ein von $E$ verschiedenes Element von $\mathfrak{H}$, dessen Ordnung eine Potenz von $p$ ist. Nun sind aber je zwei in $\mathfrak{H}$ enthaltene Gruppen der Ordnung $p^\lambda$ conjugirt, und $Q$ ist in einer dieser Gruppen enthalten. Daher ist ein mit $Q$ conjugirtes Element $P$ in $\mathfrak{P}$ enthalten. Nun kann man den Charakter $\psi_A$ so wählen, dass der Werth $\psi_A(P)$ von 1 verschieden ist. Dieser Werth ist aber gleich $\chi_A(P) = \chi_A(Q)$. Folglich ist auch $\chi_A(R)$ von 1 verschieden.

Die Gruppe $\mathfrak{G}$ ist durch $\mathfrak{P}$ theilbar, also ihre Ordnung durch $p^\lambda$, und mithin, weil für $p$ jede in $g$ aufgehende Primzahl gesetzt werden kann, durch $g$. Sie enthält aber keine in $f$ aufgehende Primzahl $l$, weil es sonst in $\mathfrak{G}$ ein Element der Ordnung $l$ gäbe. Die Ordnung von $\mathfrak{G}$ ist daher gleich $g$. Damit ist der Satz bewiesen:

II. *Sind $f$ und $g$ theilerfremde Zahlen, und enthält eine Gruppe $\mathfrak{H}$ der Ordnung $fg$ eine Gruppe $\mathfrak{F}$ der Ordnung $f$, von deren Elementen nicht zwei in Bezug auf $\mathfrak{H}$ conjugirt sind, so enthält $\mathfrak{H}$ eine und nur eine charakteristische Untergruppe der Ordnung $g$. Diese wird gebildet von allen Elementen von $\mathfrak{H}$, deren Ordnung in $\mathfrak{G}$ aufgeht.*

Es ist dann $\mathfrak{H} = \mathfrak{F}\mathfrak{G} = \mathfrak{G}\mathfrak{F}$, die Gruppe $\mathfrak{F}$ ist der Gruppe $\frac{\mathfrak{H}}{\mathfrak{G}}$ isomorph, und die Charaktere von $\mathfrak{F}$ oder $\frac{\mathfrak{H}}{\mathfrak{G}}$ sind zugleich Charaktere von $\mathfrak{H}$. Sie haben für jedes Element des Complexes $\mathfrak{G}P$ denselben Werth $\chi(P) = \psi(P)$.

Allgemeiner gilt der Satz (vergl. die Arbeit *Über Gruppen von vertauschbaren Elementen*, Journal für Math., Band 86, § 3, V):

III. *Enthält eine Gruppe $\mathfrak{H}$ der Ordnung $fg$ eine Gruppe $\mathfrak{F}$ der Ordnung $f$, von deren Elementen nicht zwei in Bezug auf $\mathfrak{H}$ conjugirt sind, bilden die $g^{ten}$ Potenzen der Elemente von $\mathfrak{F}$ eine Gruppe $\mathfrak{A}$ der Ordnung $a$, und ist $\mathfrak{B}$ die Gruppe der Elemente von $\mathfrak{F}$, deren $g^{te}$ Potenz gleich $E$ ist, so enthält $\mathfrak{H}$ eine invariante Untergruppe, zu der alle Elemente von $\mathfrak{H}$ gehören, deren Ordnung zu $a$ theilerfremd ist, und die mit $\mathfrak{F}$ den grössten gemeinsamen Theiler $\mathfrak{B}$ hat.*

In dem Satze, den ich *A. II*, § 3 bewiesen habe, kommt eine Gruppe $\mathfrak{H}_1$ der Ordnung $a_1 b$ vor, die eine Gruppe $\mathfrak{A}_1$ der Ordnung $a_1$ enthält. Die Zahlen $a_1$ und $b$ sind theilerfremd, und jedes Element von $\mathfrak{A}_1$ ist mit jedem von $\mathfrak{H}_1$ vertauschbar, bildet also für sich eine Classe conjugirter Elemente von $\mathfrak{H}_1$. Daher enthält $\mathfrak{H}_1$ eine Gruppe der Ordnung $b$,

und daraus folgt, dass die dort mit $a_1$ bezeichnete Zahl gleich 1 ist. Demnach kann man jenem Satze die präcisere Form geben:

IV. *Enthält eine Gruppe $\mathfrak{H}$ der Ordnung $fg$ eine invariante Untergruppe $\mathfrak{F}$ der Ordnung $f$, und sind $g$ und $f$ $\mathfrak{H}(\mathfrak{F})$ theilerfremd, so ist $\mathfrak{H}$ das Product aus $\mathfrak{F}$ in eine Gruppe $\mathfrak{G}$ der Ordnung $g$, deren Elemente mit denen von $\mathfrak{F}$ vertauschbar sind.*

§ 3.

Wir haben vorausgesetzt: »Zwei Elemente von $\mathfrak{F}$, die in Bezug auf $\mathfrak{H}$ conjugirt sind, sind gleich.« Daraus folgt: »Jedes Element von $\mathfrak{H}$, das mit $\mathfrak{F}$ vertauschbar ist, ist mit jedem Elemente von $\mathfrak{F}$ vertauschbar.« Denn ist $R^{-1}\mathfrak{F}R = \mathfrak{F}$, so ist für jedes Element $P$ von $\mathfrak{F}$ auch $R^{-1}PR = Q$ ein Element von $\mathfrak{F}$. Da $P$ und $Q$ conjugirt sind, so ist $P = Q$.

Die zweite Eigenschaft von $\mathfrak{F}$ sagt also weniger aus als die erste. Ist aber die Ordnung $f = p^\lambda$ von $\mathfrak{F}$ die höchste Potenz einer in $h$ enthaltenen Primzahl $p$, so folgt aus der zweiten Eigenschaft auch die erste. Bezeichnen wir jetzt $\mathfrak{F}$ mit $\mathfrak{P}$. Die mit $\mathfrak{P}$ vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppe $\mathfrak{Q}$. Dann verlangt die Voraussetzung, dass jedes Element von $\mathfrak{Q}$ mit jedem Elemente von $\mathfrak{P}$ vertauschbar ist. Sei $P$ ein Element von $\mathfrak{P}$. Die mit $P$ vertauschbaren Elemente von $\mathfrak{H}$ bilden eine Gruppe $\mathfrak{R}$. Dann ist $\mathfrak{P} < \mathfrak{Q} < \mathfrak{R} < \mathfrak{H}$, wo das Zeichen $<$ das Enthaltensein ausdrückt. Es soll nun bewiesen werden: Sind $P$ und $P'$ zwei Elemente von $\mathfrak{P}$, die in Bezug auf $\mathfrak{H}$ conjugirt sind, so ist $P = P'$. Sei nämlich $H^{-1}P'H = P$. Da $P'$ der Gruppe $\mathfrak{P}$ angehört, so ist $P$ ein Element der Gruppe $H^{-1}\mathfrak{P}H = \mathfrak{P}'$. Auch in $\mathfrak{P}'$ sind, wie in $\mathfrak{P}$, je zwei Elemente mit einander vertauschbar. Mithin ist $P$ mit jedem Elemente von $\mathfrak{P}$ und jedem von $\mathfrak{P}'$ vertauschbar, oder $\mathfrak{R}$ ist durch $\mathfrak{P}$ und $\mathfrak{P}'$ theilbar. Nun ist aber $p^\lambda$ die höchste Potenz von $p$, die in der Ordnung von $\mathfrak{R}$ aufgeht. Nach dem Sylow-schen Satze giebt es daher in $\mathfrak{R}$ ein solches Element $R$, dass $R^{-1}\mathfrak{P}'R = \mathfrak{P}$ ist. Mithin ist $\mathfrak{P}HR = HR\mathfrak{P}$, also ist $HR = Q$ ein Element der Gruppe $\mathfrak{Q} < \mathfrak{R}$. Daher ist auch $H = QR^{-1}$ in $\mathfrak{R}$ enthalten, also mit $P$ vertauschbar und folglich ist $P' = HPH^{-1} = P$ (vergl. *A. II*, § 5).

Seien $p^{\lambda_1}, p^{\lambda_2} \cdots p^{\lambda_m}$ die (oben mit $l_1, l_2 \cdots l_m$ bezeichneten) Invarianten der commutativen Gruppe $\mathfrak{P}$, sei $\varkappa_\lambda$ die Anzahl der Zahlen $\lambda_1, \lambda_2 \cdots \lambda_m$, die $\geq \lambda$ sind[1], und sei $\varkappa$ die grösste der Differenzen $\varkappa_1 - \varkappa_2$, $\varkappa_2 - \varkappa_3 \cdots$. Dann habe ich *A. II*, § 1

$$\mathfrak{s}(\mathfrak{P}) = (p-1)\,(p^2-1)\cdots(p^\varkappa-1)$$

[1] Dann sind $\lambda = \lambda_1 + \lambda_2 + \cdots$ und $\lambda = \varkappa_1 + \varkappa_2 + \cdots$ zwei Zerlegungen der Zahl $\lambda$, die man als *associirte* bezeichnen kann (*Über die Charaktere der symmetrischen Gruppe*, Sitzungsberichte 1900, § 6).

gesetzt. Ist nun $p^\lambda q$ die Ordnung der Gruppe $\mathfrak{Q}$, und ist $q$ zu $\mathfrak{H}(\mathfrak{P})$ theilerfremd, so ist jedes Element $R$ von $\mathfrak{Q}$ mit jedem Elemente von $\mathfrak{P}$ vertauschbar. Denn ist $p'q'$ die Ordnung von $R$, wo $p'$ eine Potenz von $p$ und $q'$ ein Theiler von $q$ ist, so ist $R = PQ$, wo $P$ und $Q$ die Ordnungen $p'$ und $q'$ haben und gleich Potenzen von $R$ sind. Das Element $P$ gehört der Gruppe $\mathfrak{P}$ an, ist also mit jedem Elemente von $\mathfrak{P}$ vertauschbar. Dieselbe Eigenschaft hat $Q$, weil $q'$ zu $p\mathfrak{H}(\mathfrak{P})$ theilerfremd ist (*A. II*, § 2). Daher ist auch $R$ mit jedem Elemente von $\mathfrak{P}$ vertauschbar. Demnach gilt der Satz:

V. *Ist $p^\lambda$ die höchste Potenz der Primzahl $p$, die in der Ordnung $h = p^\lambda g$ der Gruppe $\mathfrak{H}$ aufgeht, ist $\mathfrak{P}$ eine in $\mathfrak{H}$ enthaltene Gruppe der Ordnung $p^\lambda$, sind je zwei Elemente von $\mathfrak{P}$ mit einander vertauschbar, und ist $g$ zu $\mathfrak{H}(\mathfrak{P})$ theilerfremd, so enthält $\mathfrak{H}$ eine und nur eine (demnach charakteristische) Untergruppe der Ordnung $g$. Diese wird gebildet von allen Elementen der Gruppe $\mathfrak{H}$, deren Ordnung nicht durch $p$ theilbar ist.*

Sind z. B. $g$ und $p(p^2-1)$ theilerfremd, so enthält eine Gruppe der Ordnung $p^2g$ eine und nur eine Untergruppe der Ordnung $g$.

---

Ausgegeben am 7. August.



Berlin, gedruckt in der Reichsdruckerei.