

Neuer Beweis eines Fundamentaltheorems aus der Theorie der Substitutionslehre.

Von

E. NETTO in Berlin.

So einfach der Lagrange'sche Fundamentalsatz der Substitutionstheorie: „dass die Ordnung einer Gruppe durch die Ordnung jeder in ihr enthaltenen Gruppe theilbar sei“ in seinem Beweise sich stellt, so versteckt liegt der Beweis für die durch Cauchy gegebene Umkehrung: „dass wenn die Ordnung einer Gruppe durch eine Primzahl theilbar ist, die Gruppe eine Substitution jener Primzahlordnung enthalte.“ Er stützt sich auf zwei Hülffsätze, von denen der eine die Beziehung zwischen zwei Gruppen untersucht, welche keine ähnlichen Substitutionen enthalten, während der zweite die Existenz einer Gruppe der Ordnung p^f und des Grades n darlegt, wo p^f die höchste $n!$ theilende Potenz der Primzahl p ist. In glücklicher Weise hat Herr Sylow*) den Cauchy'schen Satz dahin erweitert: „dass wenn die Ordnung einer Gruppe durch eine Primzahlpotenz theilbar ist, die Gruppe eine andere von der Ordnung jener Primzahlpotenz enthalte.“ Sein Beweis stützt sich auf den des Cauchy'schen Satzes; es schien daher wünschenswerth eine davon unabhängige und wenn möglich einfachere Darlegung dieses allgemeinen Theorems zu geben. Das soll im Folgenden geschehen. Der Beweis beruht allein auf dem zweiten oben angeführten Cauchy'schen Lemma, dessen Ableitung der Kürze halber übergangen ist. Es findet sich dieselbe z. B. in dem *Traité des Substitutions etc.* §. 41 des Herrn C. Jordan. —

Enthält die Gruppe G des Grades n und der Ordnung k eine andere Gruppe der Ordnung p^ω , so kann man diese so gewählt denken, dass in G keine andere Gruppe eines Grades p^β vorhanden ist, wo $\beta > \omega$ wäre. φ sei nun eine Function der n Elemente x_1, \dots, x_n , welche für alle Substitutionen von G und nur für diese ungeändert bleibt; dann wird für alle möglichen Substitutionen der Grössen x die Function φ im Ganzen $\frac{n!}{k}$ verschiedene Werthe $\varphi_1, \varphi_2, \varphi_3, \dots$ an-

*) Siehe diese Zeitschrift. Bd. V, S. 584—594.

nehmen, wo φ_1 aus φ durch Anwendung der Substitution s_1 entstanden sein möge. — Ist nun p' die höchste Potenz von p , welche $n!$ theilt, so kann man eine Gruppe H der n Grössen x von der Ordnung p' aufstellen. ψ sei eine nur für die Gruppe H unveränderliche Function; unter den möglichen Werthen von φ und ψ seien φ_1 und ψ_1 so gewählt, dass die Ordnung p^α der Gruppe Γ_1 , welche diese beiden Functionen ungeändert lässt, möglichst gross ist.

Sind ferner a und b unbestimmte Constanten, so wird $a\varphi_1 + b\psi_1$ für die Substitutionen der x unter sich $\frac{n!}{p^\alpha}$ verschiedene Werthe annehmen, da es nur für die p^α Substitutionen von Γ_1 , welche den Gruppen G_1 und H_1 gleichzeitig angehören, ungeändert bleibt. Gibt es nun unter den $\frac{n!}{k} \cdot \frac{n!}{p'}$ möglichen Werthen $a\varphi_\lambda + b\psi_\mu$ ($\lambda = 1 \dots \frac{n!}{k}$; $\mu = 1 \dots \frac{n!}{p'}$) andere von den aus $a\varphi_1 + b\psi_1$ erlangten verschiedene, z. B. $a\varphi_s + b\psi_s$, so kommt unter denselben auch $a\varphi_{s_1 \dots s_{s-1}} + b\psi_{s_1 \dots s_{s-1}} = a\varphi_1 + b\psi_1$ nicht vor. Diese Function $a\varphi_1 + b\psi_1$ giebt für die Substitutionen der x $\frac{n!}{p^s}$ Werthe, wenn die Ordnung der Gruppe, welche φ_1 und ψ_1 gemeinsam ungeändert lässt, p^s ist. Der Annahme nach ist $\beta \leq \alpha$. Gibt es ausser diesen $\frac{n!}{p^\alpha} + \frac{n!}{p^\beta}$ Ausdrücken noch andere $a\varphi_\lambda + b\psi_\mu$, so kann man in gleicher Weise fortfahren und erhält, da sich offenbar keiner der Ausdrücke wiederholen kann,

$$\frac{n!}{k} \cdot \frac{n!}{p'} = \frac{n!}{p^\alpha} + \frac{n!}{p^\beta} + \dots = \frac{n!}{p^\alpha} \cdot s,$$

wo s eine ganze Zahl ist, da $p^\alpha \geq p^\beta$, p^γ , \dots sein muss. Diese Gleichung giebt aber

$$p^\alpha \cdot n! = p' \cdot k \cdot s.$$

Die höchste Potenz von p , die links vorkommt, ist $p^{\alpha+s}$, k kann daher höchstens durch p^α theilbar sein. Andererseits muss k nach dem Lagrange'schen Satze mindestens durch p^α theilbar sein; daraus folgt, dass $k = p^\alpha \cdot \kappa$ ist, wo κ zu p relativ prim ist. Folglich ist $\alpha = \omega$; was zu beweisen war.

Die weiteren von Herrn Sylow (l. c.) gezogenen Schlüsse über die Ordnung k von G ergeben sich unmittelbar in derselben Weise wie dort, nur mit der Vereinfachung, dass wir bereits wissen, κ habe keinen Factor p .

Berlin, 22. November 1877.