Einfacher Beweis des Frobeniusschen Fundamentalsatzes der Gruppentheorie für den Fall eines quadratfreien Exponenten

Von HORST SACHS in Halle/Saale (Deutschland)

Professor L. Rédei zum 60. Geburtstag gewidmet

Der Satz von FROBENIUS besagt in seiner ursprünglichen Fassung:

Es seien $\mathfrak{G}$ eine endliche Gruppe der Ordnung g, n ein Teiler von g. Dann gilt: Die Anzahl N der Elemente X von $\mathfrak{G}$, welche der Gleichung $X^n = 1$ genügen, ist durch n teilbar.

Die bekannten Beweise sind, verglichen mit der einfachen Aussage des Satzes, recht kompliziert und wenig befriedigend. Es ist daher wohl der Mühe wert, nach neuen Beweismotiven zu suchen.[1])

Im Folgenden wird mittels elementar-kombinatorischer Methoden ein schwächerer Satz bewiesen, welcher immerhin im Falle eines quadratfreien Exponenten n dasselbe aussagt wie der Satz von FROBENIUS.

*

Satz. *Es seien $\mathfrak{G}$ eine endliche Gruppe der Ordnung g, n ein Teiler von g, p ein Primteiler von n. Dann gilt: Die Anzahl N der Elemente X von $\mathfrak{G}$, welche der Gleichung*

$$X^n = 1 \tag{1}$$

genügen, ist durch p teilbar.

Folgerung. *Ist n quadratfrei, so gilt: N ist durch n teilbar.*

Beweis. Die Gleichung

$$Y^{\frac{n}{p}} = 1 \tag{2}$$

habe in $\mathfrak{G}$ genau die r Lösungen $Y_1, \ldots, Y_r$ (es ist $r \geqq 1$, weil $Y = 1$ eine

---

[1]) Man vergleiche auch H. ZASSENHAUS, *Lehrbuch der Gruppentheorie.* I (Leipzig—Berlin, 1937 (Nachdruck 1948)), Seite 26: „*Der folgende Satz* [von FROBENIUS] *ist noch nicht in befriedigender Weise in einen größeren Zusammenhang gefügt.*"

Lösung von (2) ist). Die Gesamtheit der Lösungen X von (1) stimmt überein mit der Gesamtheit derjenigen X von $\mathfrak{G}$, welche einer der Gleichungen

$$X^p = Y_\varrho \qquad (\varrho = 1, \ldots, r)$$

genügen.

Es durchlaufe A_i $(i = 1, \ldots, g)$ die sämtlichen Elemente der Gruppe $\mathfrak{G}$. Wir betrachten die Gesamtheit der geordneten $(p-1)$-tupel

$$T_{i_1 \ldots i_{p-1}} = \{A_{i_1}, \ldots, A_{i_{p-1}}\},$$

wo die Indizes unabhängig voneinander die Werte $1, \ldots, g$ durchlaufen; ihre Anzahl ist g^{p-1}. Zu jedem solchen $(p-1)$-tupel sind durch die Bedingungen $A_{i_1} A_{i_2} \ldots A_{i_{p-1}} A_{i_p} = Y_\varrho$ $(\varrho = 1, \ldots, r)$ genau r verschiedene (von $T_{i_1 \ldots i_{p-1}}$ und ϱ abhängende) Elemente A_{i_p} bestimmt. Wir betrachten nun die Menge $\mathfrak{M}$ der so entstandenen geordneten p-tupel

$$\{A_{i_1}, \ldots, A_{i_p}\};$$

sie sind paarweise verschieden, ihre Anzahl ist $M = r \cdot g^{p-1}$. In $\mathfrak{M}$ sind alle geordneten p-tupel $\{A_{j_1}, \ldots, A_{j_p}\}$ und nur solche mit der Eigenschaft

$$A_{j_1} \ldots A_{j_p} = Y_\varrho \qquad (\varrho = 1, \ldots, r)$$

enthalten.

Die Anzahl N ist offenbar gleich der Anzahl derjenigen p-tupel von $\mathfrak{M}$, die lauter gleiche Elemente enthalten; diese bilden eine Untermenge $\mathfrak{N}$ von $\mathfrak{M}$. Wir haben

$$p \mid r \cdot g^{p-1} = M = N + (M - N);$$

können wir nun zeigen, daß $p \mid M - N$, so folgt $p \mid N$, und das ist gerade die zu beweisende Behauptung.

$M - N$ ist die Anzahl der p-tupel von $\mathfrak{M} - \mathfrak{N}$, also die Anzahl derjenigen p-tupel von $\mathfrak{M}$, welche mindestens zwei verschiedene Elemente enthalten.

Durch zyklische Umordnung der Elemente eines p-tupels von $\mathfrak{M} - \mathfrak{N}$ entstehen wieder p-tupel von $\mathfrak{M} - \mathfrak{N}$, denn aus $A_{i_1} \ldots A_{i_p} = Y$ mit $Y^{\frac{n}{p}} = 1$ folgt $A_{i_p} A_{i_1} \ldots A_{i_{p-1}} = A_{i_p} Y A_{i_p}^{-1} = Z$ mit $Z^{\frac{n}{p}} = 1$ usw.; auf diese Weise gewinnen wir aus einem p-tupel von $\mathfrak{M} - \mathfrak{N}$ genau p offenbar paarweise verschiedene p-tupel von $\mathfrak{M} - \mathfrak{N}$. Die Menge $\mathfrak{M} - \mathfrak{N}$ zerfällt so in (elementfremde) Klassen zyklisch-äquivalenter p-tupel, deren jede genau p p-tupel enthält. Folglich ist $M - N$ durch p teilbar. Das war zu zeigen.

(Eingegangen am 14. April 1960)