# Ein Beweis des Ruffini—Abelschen Satzes.

Von László Kalmár in Szeged.

Die Herleitung des Satzes von Ruffini und Abel — laut dessen die allgemeine algebraische Gleichung $n$-ten Graden für $n \geqq 5$ nicht durch Radikale lösbar ist — aus dem Galoisschen Kriterium für die algebraische Lösbarkeit erfolgt gewöhnlich unter Berufung auf die Tatsache, daß die alternierende Gruppe $\mathfrak{A}_n$ von $n$ Elementen für $n \geqq 5$ einfach ist. Statt dessen würde auch die weniger scharfe Tatsache genügen, daß $\mathfrak{A}_n$ für $n \geqq 5$ keinen Normalteiler vom Primzahlindex besitzt. Für diese letztere Tatsache werden wir einen einfachen Beweis geben, wodurch ein für Vorlesungszwecke[1]) besonders geeigneter Beweis des Ruffini—Abelschen Satzes entsteht.

Es genügt folgenden Satz zu beweisen:

*Es sei $\mathfrak{G}$ ein echter Normalteiler der alternierenden Gruppe $\mathfrak{A}_n$ von n Elementen; ferner sei p eine ungerade Primzahl $\leqq n$. Dann gibt es eine Untergruppe $\mathfrak{U}$ von $\mathfrak{A}_n$, die $\mathfrak{G}$ als Untergruppe vom Index p enthält.*

In der Tat folgt hieraus, daß der Index von $\mathfrak{G}$ in bezug auf $\mathfrak{A}_n$ durch jede ungerade Primzahl $p \leqq n$ teilbar ist, also kann für $n \geqq 5$ keine Primzahl sein.

Zum Beweise sei $Z$ ein nicht zu $\mathfrak{G}$ gehöriger $p$-gliedriger Zyklus[2]); $G_1, G_2, \ldots, G_g$ seien die Elemente von $\mathfrak{G}$. Wir betrachten die Permutationen

[1]) Wir meinen eine Vorlesung, in der der in Rede stehende Satz nicht independent, sondern als eine Anwendung des Galoischen Kriteriums bewiesen wird.

[2]) Gehört jeder $p$-gliedriger Zyklus der Gruppe $\mathfrak{G}$ an (wobei $p$ *irgendeine ungerade* Zahl bedeutet), so gehört bekanntlich überhaupt jede gerade Permutation $\mathfrak{G}$ an, also ist $\mathfrak{G}$ kein *echter* Normalteiler von $\mathfrak{A}_n$.

(1) $$Z^i\, G_j \qquad (i=0,\ 1,\ 2,\ldots,\ p-1,\quad j=1,\ 2,\ 3,\ldots,\ g);$$

dieselben gehören sämtlich $\mathfrak{A}_n$ an. Ferner sind sie verschieden. In der Tat folgt aus

(2) $$Z^{i_1}\, G_{j_1} = Z^{i_2}\, G_{j_2},$$

daß $Z^{i_1-i_2} = G_{j_2} G_{j_1}^{-1}$ zu $\mathfrak{G}$ gehört; wäre hier $i_1 \neq i_2$, also $(i_1-i_2,\ p)=1$, so könnte man die ganzen Zahlen $x$ und $y$ so bestimmen, daß sie die diophantische Gleichung

$$(i_1-i_2)\, x + p\, y = 1$$

erfüllen; daher ergäbe sich, daß $Z = Z^{1-py} = Z^{(i_1-i_2)x} = (Z^{i_1-i_2})^x$ gegen der Voraussetzung $\mathfrak{G}$ angehört. Daher ist $i_1 = i_2$, also, wegen (2), $G_{j_1} = G_{j_2}$, d. h. $j_1 = j_2$.

Wir zeigen nun, daß die $g\,p$ Permutationen (1) eine Gruppe $\mathfrak{U}$ bilden. In der Tat ist

$$\begin{aligned} Z^{i_1} G_{j_1} . Z^{i_2} G_{j_2} &= Z^{i_1+i_2} Z^{-i_2} G_{j_1} Z^{i_2} G_{j_2} = \\ &= Z^{i_1+i_2} G_{j_3} G_{j_2} = \\ &= Z^{i_3} G_{j_4}, \end{aligned}$$

wobei $i_3$, $j_3$, $j_4$ aus

$$\begin{aligned} &i_3 \equiv i_1 + i_2 \pmod{p}, \qquad 0 \leqq i_3 \leqq p-1, \\ &G_{j_3} = (Z^{i_2})^{-1}\, G_{j_1}\, Z^{i_2}, \\ &G_{j_4} = G_{j_3}\, G_{j_2} \end{aligned}$$

zu bestimmen sind, was wegen der Voraussetzung, daß $\mathfrak{G}$ ein Normalteiler von $\mathfrak{A}_n$ sein soll, bzw. wegen der Gruppeneigenschaft von $\mathfrak{G}$ möglich ist.

Da die Gruppe $\mathfrak{G}$ eine Untergruppe von $\mathfrak{U}$ vom Index $p$ ist, so ist die Behauptung bewiesen.

*(Eingegangen am 6. August 1932.)*