Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 20 (1947)

Artikel: Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört.
Autor: Szele, T.
DOI: https://doi.org/10.5169/seals-18061

Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört

Von T. Szele, Szeged (Ungarn)

Es gilt folgender Satz: *Zu einer Ordnungszahl n gehört dann und nur dann nur eine (und zwar die zyklische) Gruppe, wenn* $(n, \varphi(n)) = 1$ *ist*[1]).

Offenbar ließe sich dieser Satz leicht als Korollar aus einem Satz von *Rédei*[2]) gewinnen (s. unten), wir werden aber obigen Satz sehr einfach, nur auf folgendem Satz von *Frobenius*[3]) stützend beweisen: *Es gibt in jeder Gruppe von der Ordnung ab genau b Elemente, deren Ordnung in b aufgeht, falls a quadratfrei und jeder Primfaktor von b größer als der größte Primfaktor von a ist.*

Der Satz von *Rédei* lautet so: *Zu einer Ordnungszahl n gehören dann und nur dann nur kommutative Gruppen, wenn n von der Form*

$$n = p_1 \dots p_i q_1^2 \dots q_j^2 \quad (p_1, \dots, q_j \text{ verschiedene Primzahlen})$$

und zu

$$(p_1 - 1) \dots (p_i - 1) \cdot (q_1^2 - 1) \dots (q_j^2 - 1)$$

prim ist. Rédei gewinnt diesen merkwürdigen und allgemeineren Satz als Nebenresultat seiner Untersuchungen über die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen.

Der wesentliche Inhalt unseres Satzes ist die Behauptung, daß *eine Gruppe mit* $(n, \varphi(n)) = 1$ *notwendig kommutativ ist.* Dies ist nichts anderes, als ein Satz von *Szép*[4]), den er ebenfalls sehr einfach, aber mit Anwendung mehrerer Sätze der Gruppentheorie beweist.

---

[1]) Offenbar kann die Bedingung $(n, \varphi(n)) = 1$ nur für quadratfreie n erfüllt sein, und dann ist sie gleichbedeutend damit, daß die Anzahl der zu n primen Zahlen aus $1, \dots, n$ selbst ein zu n primes Element dieser Folge ist.

[2]) Siehe die vorstehende Arbeit von *L. Rédei:* „Das „schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören (Satz 10).

[3]) *Netto:* Gruppen- und Substitutionentheorie (Leipzig 1908), S. 110.

[4]) Siehe die zweitvorstehende Arbeit von *J. Szép:* On finite groups which are necessarily commutative.

Wir beweisen zuerst, daß jede Gruppe $\mathfrak{G}$ von n-ter Ordnung mit $(n, \varphi(n)) = 1$ zyklisch ist, und zwar verwenden wir dabei eine vollständige Induktion nach der Anzahl der Primfaktoren von n (denn die Behauptung ist im Falle $n =$ Primzahl offenbar richtig). Es sei p der größte Primfaktor von n. Nach obigem Satz von *Frobenius* (angewandt auf den Fall $b = p$) gibt es in $\mathfrak{G}$ genau p Elemente, deren Ordnung ein Teiler von p ist. Die Menge $\mathfrak{N}$ dieser Elemente ist eine normale Untergruppe von $\mathfrak{G}$, da einerseits $\mathfrak{N}$ aus den Potenzen eines ihrer Elemente besteht, andererseits jede Konjugierte eines Elementes ($\neq 1$) von $\mathfrak{N}$ wieder ein Element p-ter Ordnung ist, also zu $\mathfrak{N}$ gehört. Betrachten wir nun die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$. Diese ist nach der Induktionsvoraussetzung zyklisch, weil sie die Ordnung $\frac{n}{p}$ (mit weniger Primfaktoren als n) hat. Es gibt also in $\mathfrak{G}$ Elemente A, B so, daß durch

$$A^x B^y \quad \left(x = 0, \ldots, p-1\,;\;\; y = 0, \ldots, \frac{n}{p} - 1\right)$$

die ganze Gruppe $\mathfrak{G}$ erschöpft ist, und für die Ordnungen gilt $(A) = p$, $(B) = n$ oder $\frac{n}{p}$. Im Fall $(B) = n$ ist $\mathfrak{G}$ in der Tat die zyklische Gruppe $\{B\}$. Im Fall $(B) = \frac{n}{p}$ setzen wir

$$B^{-1}AB = A^r \qquad (1 \leqq r \leqq p-1)\,.$$

Dann ist (wegen $B^{\frac{n}{p}} = 1$)

$$B^{-\frac{n}{p}} A B^{\frac{n}{p}} = A^{r^{\frac{n}{p}}} = A\,,$$

d. h.

$$r^{\frac{n}{p}} \equiv 1 \pmod{p}\,.$$

Andererseits ist nach Fermat

$$r^{p-1} \equiv 1 \pmod{p}\,.$$

Aus $(n, \varphi(n)) = 1$ folgt aber $\left(\frac{n}{p},\; p-1\right) = 1$, und so ist $r \equiv 1 \pmod{p}$, d. h. $r = 1$. Das bedeutet, daß $B^{-1}AB = A$ und so $(AB) = (A)(B) = p \cdot \frac{n}{p} = n$ ist, woraus $\mathfrak{G} = \{AB\}$ folgt. Die Behauptung ist also bewiesen.

Wir müssen noch zeigen, daß es im Falle $(n, \varphi(n)) > 1$ auch eine nicht-zyklische Gruppe n-ter Ordnung gibt. Da $(n, \varphi(n)) > 1$ ist, enthält n entweder einen Teiler p^2 (p = Primzahl), oder ist n quadratfrei und enthält Primfaktoren p, q mit $p \equiv 1 \pmod{q}$. Im ersten Fall bilden wir das direkte Produkt aus der Abelschen Gruppe mit den Invarianten p, p, und aus einer beliebigen Gruppe mit der Ordnung $\frac{n}{p^2}$. Die so erhaltene Gruppe ist offenbar nichtzyklisch. Im zweiten Fall genügt es zu zeigen, daß eine nicht-Abelsche Gruppe von der Ordnung pq existiert. Eine solche Gruppe wird bekanntlich durch die folgenden Gleichungen definiert:

$$A^p = B^q = 1\,, \quad B^{-1}AB = A^r, \quad r = g^{\frac{p-1}{q}}\,,$$

g ist eine primitive Kongruenzwurzel mod p.

(Eingegangen den 5. Januar 1947.)