Über den Fundamentalsatz der Abelschen Gruppen von endlicher Ordnung.

Von L. RÉDEI in Szeged.

Der verblüffend kurze Beweis von KORSELT—FRANZ[1]) für den im Titel genannten Satz erfordert vom Leser wegen der darin vorkommenden künstlichen Doppelminimalannahme anstrengendes Nachdenken, bietet auch wenig Einblick in die wahren Verhältnisse Abelscher Gruppen und keine Vorschrift zur Konstruktion einer Basis. VAN DER WAERDEN[2]) schließt dagegen immer noch kurz genug, auf den Begriff der Faktorgruppen stützend, wobei man den Eindruck hat, daß der passendste Weg gegangen wurde. Will man aber Faktorgruppen vermeiden — ein Standpunkt, der unter Umständen zweckmäßig sein kann — so scheint folgender Beweis unter den zahlreichen anderen von ähnlicher Natur von Vorteil zu sein.

Es sei G eine Abelsche Gruppe von endlicher Ordnung. Es bezeichne (G) die Ordnung von G, (A) die eines Elements A von G, E das Einheitselement von G. Die von E verschiedenen Elemente $A_1, \ldots, A_r$ von G nennen wir eine Basis von G, wenn sie alle von Primzahlpotenzordnung sind, alle Elemente von G in der Form

$$(1) \qquad A_1^{x_1} \ldots A_r^{x_r} \qquad (x_i = 0, 1, \ldots, (A_i) - 1\,;\, i = 1, 2, \ldots, r)$$

darstellbar sind und auch

$$(2) \qquad (G) = (A_1) \ldots (A_r)\ ^3)$$

[1]) W. FRANZ, Zur vorstehenden Arbeit von Herrn A. Korselt, *Journal für Math.*, **164** (1931), S. 63.

[2]) B. L. VAN DER WAERDEN, *Moderne Algebra* II (Berlin, 1940), S. 116.

[3]) Offenbar läßt sich (2) mit der Bedingung ersetzen, daß die Produkte (1) verschieden sind, wodurch die übliche Definition der Basis entsteht. Mit der obigen Form der Definition kommen wir ökonomischer aus.

gilt. Der Fundamentalsatz lautet dann: Ist $G \neq E$, so hat G eine Basis.

Dem Beweis schicken wir die aus der Definition unmittelbar folgende Bemerkung voran:

a. Ist $A_1, \ldots, A_r$ Basis einer Gruppe und sind $x_1, \ldots, x_r$ beliebige ganze rationale Zahlen, so ist (1) nur für $(A_i) | x_i$ $(i = 1, \ldots, r)$ gleich E.

Es sei G_0 eine Untergruppe von G mit möglichst großem (G_0), die eine Basis $B_1, \ldots, B_s$ hat. Ein solches G_0 existiert sicher, denn G hat ein Element von Primzahlordnung, das dann Basis der von ihm erzeugten Gruppe ist. Man darf $G_0 \neq G$ annehmen, da sonst der Satz richtig ist. Dann gibt es ein Element A in G, das in G_0 nicht enthalten ist. Da jedes Element als ein Produkt von Elementen von Primzahlpotenzordnung darstellbar ist, so läßt sich annehmen, daß die Ordnung von A die Potenz einer Primzahl p ist. Auch läßt sich annehmen, daß A^p in G_0 enthalten ist, da man sonst statt A das letzte Element der Folge $A^p, A^{p^2}, A^{p^3}, \ldots, E$ nehmen könnte, das in G_0 noch nicht enthalten ist. Dann bestehen die Nebengruppen $G_0, AG_0, A^2G_0, \ldots, A^{p-1}G_0$ aus allen verschiedenen Elementen von $\{A, G_0\}$, wobei $\{\}$ das Zeichen für die durch die eingeklammerten Elemente erzeugte Gruppe ist. Also gilt

$$(\{A, G_0\}) = p(B_1) \ldots (B_s). \tag{3}$$

Es ist mit einer geeigneten Reihenfolge von $B_1, \ldots, B_s$

$$A^p = B_1^{y_1} \ldots B_t^{y_t} \qquad (0 \leq t \leq s), \tag{4}$$

wobei die Potenzen rechts von E verschieden sind ($t = 0$ bedeutet, daß die rechte Seite gleich E ist). Erhebt man (4) zur (A)-ten Potenz, so folgt nach **a** $(B_i) | (A) y_i$ $(i = 1, \ldots, t)$. Wegen $(B_i) \nmid y_i$ ist also $p | (B_i)$, d. h. die Ordnungen von $B_1, \ldots, B_t$ sind Potenzen von p. Es genügt weiter den Fall zu betrachten, in dem kein y_i durch p teilbar ist, denn ist z. B. $p | y_t$, so ist auch $A' = AB_t^{-\frac{y_t}{p}}$ ein in G_0 nicht enthaltenes Element, wofür A'^p in G_0 enthalten ist, uns dann läßt sich A von vornherein durch A' ersetzen, wodurch man in ein paar Schritten zum Ziele kommt.

Ist dann $t = 0$, so ist $(A) = p$. Das bedeutet wegen (3), daß $A, B_1, \ldots, B_s$ eine Basis von $\{A, G_0\} = \{A, B_1, \ldots, B_s\}$ ist, das ein Widerspruch ist.

Ist dagegen $t > 0$, so wählt man eine solche Reihenfolge von $B_1, \ldots, B_t$, daß die Ordnung von B_1 möglichst groß ausfällt. Nach (4) und **a** ist $A^{p(B_1)} = E$, $A^{(B_1)} \neq E$, woraus $(A) = p(B_1)$ folgt. Wegen $p \nmid y_1$ gibt es ein ganzes rationales z mit $y_0 z \equiv 1 \pmod{(B_1)}$ und dann ist nach (4) $B_1 = (B_1^{y_0})^z$ in $\{A, B_2, \ldots, B_s\}$ enthalten. Hieraus folgt, daß diese Gruppe gleich $\{A, G_0\}$ und also nach (3) $A, B_2, \ldots, B_s$ eine Basis von ihr ist. Dieser Widerspruch beweist den Satz.

(Eingegangen am 14. August 1941.)