Die Ringe „ersten Ranges“.

Von L. RÉDEI in Szeged und T. SZELE in Debrecen (Ungarn).

§ 1. Einleitung.

Den Begriff des Ranges von Abelschen Gruppen[1]) haben BAER [1] und PRÜFER [2] für torsionsfreie Gruppen bzw. für Torsionsgruppen eingeführt. Beide Definitionen lassen sich ohne weiteres auf beliebige Abelsche Gruppen übertragen, sind aber miteinander nicht äquivalent, indem die Gruppen r-ten Ranges im Baerschen Sinne eine echte Untermenge derjenigen im Prüferschen Sinne bilden.

Insbesondere verstehen wir BAER folgend unter einer Gruppe *ersten Ranges* eine Gruppe mit folgender Eigenschaft, die wir zweckmäßig gleich in drei äquivalenten Formen angeben:

E_1: Keine Untergruppe[2]) ist eine direkte Summe.

E_2: Irgendzwei zyklische Untergruppen enthalten ein gemeinsames Element $\neq 0$. (Hier darf „zyklisch“ offenbar gestrichen werden.)[3])

E_3: Für irgendzwei Gruppenelemente α, β $(\neq 0)$ gibt es ganze Zahlen a, b mit $a\alpha = b\beta \neq 0$.[4])

Die Äquivalenz von E_1, E_2 sieht man so ein. Gilt E_1 nicht, so gibt es eine Untergruppe, die sich direkt zerlegen läßt; zwei direkte Summanden sind dann Untergruppen mit dem einzigen gemeinsamen Element 0, und so gilt E_2 nicht. Wenn umgekehrt E_2 nicht gilt, so gibt es zwei Untergruppen mit dem einzigen gemeinsamen Element 0; ihre direkte Summe ist eine Untergruppe und so gilt E_1 nicht. Man sieht auch, daß E_3 bloß eine mehr explizite Form von E_2 ist.

Dagegen benützt PRÜFER für die Definition der Gruppen ersten Ranges die Eigenschaft, daß jedes Paar (oder, was auf dasselbe hinauskommt, jedes

---

[1]) In dieser Arbeit soll unter „Gruppe“ stets eine *additiv* geschriebene *Abelsche* Gruppe verstanden werden.

[2]) Bequemlichkeitshalber schließen wir die Gruppen mit nur einem Element durchweg aus. Auch eine Untergruppe soll also aus mindestens zwei Elementen bestehen.

[3]) Es ist klar, daß dann jedes endliche System der Untergruppen von obiger Eigenschaft ist.

[4]) BAER nahm E_3 als definierende Eigenschaft der torsionsfreien Gruppen ersten Ranges an.

endliche System) von Elementen in einer zyklischen Untergruppe enthalten ist. Diese Eigenschaft läßt sich auch so formulieren:

E^*: Für irgendzwei Gruppenelemente α, β ($\alpha, \beta \neq 0$) gibt es ein Element δ und ganze Zahlen a, b derart, daß $\alpha = a\delta$, $\beta = b\delta$ gelten.

Die Eigenschaften E_3 und E^* lassen sich so gegenüberstellen: Irgendzwei Gruppenelemente ($\neq 0$) haben ein gemeinsames „Multiplum“ ($\neq 0$) bzw. einen gemeinsamen „Teiler“.

Man kann leicht einsehen, daß die Bedingung E_3 eine Folgerung von E^* ist[5]) und insbesondere E_3 und E^* für torsionsfreie Gruppen sowie für p-Gruppen[6]) gleichbedeutend sind. (Dies folgt übrigens aus den nachstehenden Sätzen.) Ein Beispiel für den Fall, wo E^* gilt, E_3 aber nicht, wird durch die zyklische Gruppe von der Ordnung 6 geliefert.

Von nun an werden wir die Bezeichnung „ersten Ranges“ für die Gruppen von der Eigenschaft E_3 beibehalten. Die Gruppen von der Eigenschaft E^* wollen wir (wie es heute schon üblich ist) *lokal-zyklische* Gruppen nennen. Auch einen Ring[7]) nennen wir „ersten Ranges“ bzw. „lokal-zyklisch“, falls seine additive Gruppe die Eigenschaft E_3 bzw. E^* besitzt. Der Zweck dieser Arbeit ist die Ringe ersten Ranges und die lokal-zyklischen Ringe zu bestimmen, und zwar werden wir uns hauptsächlich mit den Ringen ersten Ranges beschäftigen. Nach Bestimmung dieser Ringe ergeben sich die lokal-zyklischen Ringe sehr leicht.

Jetzt führen wir einige Bezeichnungen und Redeweisen ein. Für einen Ring R bezeichne R^+ die additive Gruppe von R Mit $\mathfrak{R}$ bezeichnen wir den rationalen Zahlkörper. Dann ist $\mathfrak{R}^+$ die additive Gruppe sämtlicher rationaler Zahlen (auch „rationale Gruppe“ genannt), Ferner soll $\mathfrak{Z}(p^e)$ folgende p-Gruppe bezeichnen, wobei e eine natürliche Zahl oder $e = \infty$ sein kann. Im ersten Fall ist $\mathfrak{Z}(p^e)$ die zyklische Gruppe von der Ordnung p^e, dagegen ist $\mathfrak{Z}(p^\infty)$ die engste Gruppe, die alle $\mathfrak{Z}(p^e)$ ($e = 1, 2, 3, \ldots$) enthält. Hierdurch ist $\mathfrak{Z}(p^\infty)$ eindeutig bestimmt als die durch die unendlichvielen Elemente $\alpha_1, \alpha_2, \ldots$ erzeugte Abelsche Gruppe $\{\alpha_1, \alpha_2, \ldots\}$[8]) mit den definierenden Gleichungen

$$(1) \qquad p\alpha_1 = 0,\; p\alpha_2 = \alpha_1,\; p\alpha_3 = \alpha_2, \ldots .$$

---

[5]) Diese Behauptung ist aber nur für Abelsche Gruppen gültig, denn eine beliebige Gruppe mit der Eigenschaft E^* ist notwendig kommutativ, wogegen E_3 sehr wohl auch einer nichtkommutativen Gruppe zukommen kann, wie dies das Beispiel der Quaternionengruppe (von 8-ter Ordnung) lehrt.

[6]) Unter einer *p-Gruppe* (auch *primäre* Gruppe genannt) werden wir durchweg eine (endliche oder unendliche) Gruppe verstehen, deren Elemente lauter Potenzen einer und derselben Primzahl p zur Ordnung haben. — Die Bezeichnung „*p-Ring*“ soll dementsprechend einen (nicht notwendig kommutativen) Ring bedeuten, dessen additive Gruppe eine p-Gruppe ist.

[7]) Es sind nicht nur kommutative Ringe gemeint.

[8]) { } soll die durch die eingeklammerten Elemente erzeugte (additive) Gruppe bezeichnen.

PRÜFER nennt $\mathfrak{Z}(p^\infty)$ „die Gruppe vom Typ p^∞". Dabei läßt sich $\mathfrak{Z}(p^\infty)$ auch aus $\mathfrak{R}^+$ (durch nacheinanderfolgende Untergruppen- und Faktorgruppenbildung) gewinnen:

(2) $$\mathfrak{Z}(p^\infty) \cong \left\{\frac{1}{p}, \frac{1}{p^2}, \frac{1}{p^3}, \ldots\right\} \Big/ \{1\},$$

d. h. $\mathfrak{Z}(p^\infty)$ ist isomorph der Faktorgruppe der Gruppe der rationalen Zahlen von der Form $\frac{a}{p^n}$ nach dem Normalteiler der ganzen Zahlen. Letztere ist eine Untergruppe der Faktorgruppe $\mathfrak{R}^+/\{1\}$, die wir im folgenden mit $\mathfrak{Z}$ bezeichnen. $\mathfrak{Z}$ ist offensichtlich lokal-zyklisch. Außerdem ist $\mathfrak{Z}(p^\infty)$ bzw. $\mathfrak{Z}$ isomorph mit der multiplikativen Gruppe der komplexen Einheitswurzeln von p-Potenzordnung bzw. aller komplexen Einheitswurzeln.

Unter einem *Zeroring* verstehen wir (wie üblich) einen solchen Ring, in dem jedes Elementenprodukt gleich 0 ist. Ein Zeroring R ist durch R^+ eindeutig bestimmt und dabei kann R^+ jede vorgegebene Abelsche Gruppe sein. In diesem Sinne gehört zu jeder Gruppe mit der Eigenschaft E_3 bzw. E^* ein Zeroring ersten Ranges bzw. ein lokal-zyklischer Zeroring. Indem wir also im folgenden alle solchen Ringe bestimmen, so werden wir auch einen Überblick über sämtliche Gruppentypen von der Eigenschaft E_3 bzw. E^* gewinnen. Letztere Gruppen sind übrigens schon oft untersucht worden.

§ 2. Sätze.

Den vollständigen Überblick über die Gruppen mit der Eigenschaft E_3 ermöglichen uns folgende Sätze 1, 1a:

Satz 1. *Die Untergruppen von $\mathfrak{R}^+$ und $\mathfrak{Z}(p^\infty)$ (für sämtliche p) sind gerade alle Gruppen ersten Ranges.*

Alle Untergruppen einer Gruppe $\mathfrak{Z}(p^\infty)$ sind offenbar diese Gruppe selbst und die zyklischen p-Gruppen. Man sieht auch, daß zwei Untergruppen von $\mathfrak{Z}(p^\infty)$ nur dann isomorph sind, wenn sie identisch sind. Dagegen gilt ähnliches für die Untergruppen von $\mathfrak{R}^+$ nicht, wie das der folgende Satz lehrt:

Satz 1a. *Die Untergruppen der additiven Gruppe $\mathfrak{R}^+$ der rationalen Zahlen und die nichtisomorphen unter ihnen lassen sich so angeben:*

Bezeichne $\mathfrak{P}$ eine nichtleere Menge von Primzahlpotenzen $P_1, P_2, \ldots$ $(\geqq 1)$ so beschaffen, daß mit einem Element p^e alle Teiler $1, p, \ldots, p^e$ unter den P_i vorkommen, ferner bezeichne n eine zu allen P_i prime natürliche Zahl. Wir führen dann die kurze Bezeichnung ein:

(3) $$\frac{n}{\mathfrak{P}} = \left\{\frac{n}{P_1}, \frac{n}{P_2}, \ldots\right\}.$$ [9]

Diese sind alle Untergruppen von $\mathfrak{R}^+$.

[9]) Es ist klar, daß n die kleinste in der Gruppe (3) enthaltene natürliche Zahl ist.

Isomorph sind zwei solche Gruppen $\frac{n}{\mathfrak{P}}, \frac{n'}{\mathfrak{P}'}$ *dann und nur dann, wenn* $\mathfrak{P}$ *und* $\mathfrak{P}'$ *bis auf endlich viele Elemente übereinstimmen. (Insbesondere sind alle* $\frac{n}{\mathfrak{P}}$ *isomorph zu* $\frac{1}{\mathfrak{P}}$.)

Bemerkungen. Der Inhalt der Sätze 1, 1a ist im wesentlichen schon bekannt. Und zwar bewies BAER [1], daß die Untergruppen von $\mathfrak{R}^+$ die sämtlichen torsionsfreien Gruppen ersten Ranges sind. PRÜFER [2] bewies, daß die Untergruppen von $\mathfrak{Z}(p^\infty)$ alle lokal-zyklischen p-Gruppen erschöpfen.[10]) Bezüglich Satz 1a bemerken wir, daß eine im wesentlichen übereinstimmende Charakterisierung (mit Hilfe der Steinitzschen G-Zahlen) der Untergruppen von $\mathfrak{R}^+$ auch aus einem viel allgemeineren Satz von BAER ([1], Theorem 2. 8) folgt.

Beide Sätze 1, 1a geben eine vollständige Aufklärung über die Gruppen ersten Ranges. Nennen wir zwei Mengen $\mathfrak{P}$, $\mathfrak{P}'$ äquivalent, wenn sie bis auf endlichviele Elemente übereinstimmen. Bildet man ein volles System nichtäquivalenter $\mathfrak{P}$, so representieren die $\frac{1}{\mathfrak{P}}$ nach Satz 1a alle nichtisomorphen Untergruppen von $\mathfrak{R}^+$. Diese, die Gruppen $\mathfrak{Z}(p^\infty)$ und die zyklischen p-Gruppen erschöpfen dann alle möglichen verschiedenen Gruppentypen ersten Ranges.

Nunmehr wollen wir die Ringe ersten Ranges angeben. Es sind also die Ringe zu bestimmen, die sich auf den eben aufgezählten additiven Gruppen „aufbauen“ lassen[11]). Wir beweisen den folgenden:

Satz 2. *Die Unterringe des rationalen Zahlkörpers $\mathfrak{R}$, die Unterringe der Restklassenringe* mod p^e, *außerdem diejenigen Zeroringe, deren additive Gruppe eine Untergruppe von* $\mathfrak{R}^+$ *oder eine Gruppe* $\mathfrak{Z}(p^\infty)$ *ist, sind gerade die Ringe ersten Ranges.*

Bemerkung. Hiervon sind die endlichen p-Ringe ersten Ranges (d. h. die Unterringe der Restklassenringe mod p^e) schon wegen ihrer großen zahlentheoretischen Wichtigkeit wohlbekannt, und es sind auch die nichtisomorphen Ringe unter ihnen leicht anzugeben. Letztere stimmen nämlich offenbar mit allen verschiedenen Typen der „zyklischen“ p-Ringe[12]) überein und sind die folgenden Ringe $Z(p^e, p^k)$ $(0 \leq k \leq e)$: Die Elemente von $Z(p^e, p^k)$ sind $0, \beta, 2\beta, \ldots, (p^e-1)\beta$ mit $\beta^2 = p^k\beta$.[13]) Zu jeder Potenz p^e gibt es also ins-

[10]) Die p-Gruppen ersten Ranges sind identisch mit den lokal-zyklischen p-Gruppen, da im Falle einer Abelschen p-Gruppe E_3 ebenso wie E^* gleichwertig damit ist, daß die Gruppe *nur eine* Untergruppe p-ter Ordnung enthält.

[11]) Im allgemeinen nennen wir einen Ring R mit $R^+ = \mathfrak{G}$ einen auf $\mathfrak{G}$ aufgebauten Ring.

[12]) So nennen wir die Ringe R, für die R^+ eine zyklische p-Gruppe ist.

[13]) Insbesondere ist $Z(p^e, p^e)$ offenbar der Zeroring mit der additiven Gruppe $\mathfrak{Z}(p^e)$.

gesamt $e+1$ zyklische p-Ringe mit p^e Elementen. Den Zeroring mit der additiven Gruppe $\mathfrak{Z}(p^\infty)$ bezeichnen wir im folgenden mit $Z(p^\infty)$.

Um also auf Grund von Satz 2 alle verschiedenen Ringtypen ersten Ranges vollständig aufzählen zu können, ist es nur noch nötig einen Überblick über die Unterringe von $\mathfrak{R}$ zu verschaffen. Das geschieht im folgenden

Satz 2a. *Die Unterringe des rationalen Zahlkörpers* $\mathfrak{R}$ *lassen sich so angeben:*

Bezeichne $\mathfrak{M}$ *eine beliebige endliche (eventuell leere) oder unendliche Menge von verschiedenen Primzahlen* $p_1, p_2, \ldots$ *und* n *eine zu allen* p_i *prime natürliche Zahl. Die Zahlen von der Form* $\frac{na}{b}$ *(*a *ganz,* b *ein Potenzprodukt aus den* p_i*) bilden einen Unterring von* $\mathfrak{R}$*, den wir mit*

$$nR\left(\frac{1}{p_1}, \frac{1}{p_2}, \ldots\right) \tag{4}$$

bezeichnen[14]*). Diese sind die sämtlichen Unterringe von* $\mathfrak{R}$ *und es gibt unter ihnen keine isomorphen. (Enthält* $\mathfrak{M}$ *alle Primzahlen, so ist nur* $n=1$ *zuzulassen, und dann geht* (4) *in* $\mathfrak{R}$ *über; in jedem anderen Falle gehören zu* $\mathfrak{M}$ *unendlichviele* n *und somit Ringe* (4).)

Auf Grund der vorigen lassen sich nunmehr auch die lokal-zyklischen Gruppen bzw. Ringe leicht angeben. Wie wir schon erwähnt haben, ist die Gruppe $\mathfrak{Z}=\mathfrak{R}^+/\{1\}$ lokal-zyklisch. Dann sind auch ihre Untergruppen von dieser Eigenschaft, die als Torsionsgruppen in eine direkte Summe von (zu verschiedenen Primzahlen p gehörenden) p-Gruppen zerfallen. Sie lassen sich also explizit als

$$\sum_{i=1}^{\infty} \mathfrak{Z}(q_i^{e_i}) \tag{5}$$

angeben, wobei $q_1, q_2, \ldots$ die (zunehmende) Folge aller Primzahlen ist und jedes e_i entweder eine nichtnegative ganze Zahl oder ∞ bezeichnet. (Im Fall $e_i=0$ fällt der entsprechende Summand $\mathfrak{Z}(1)$ heraus.) Nun gilt der

Satz 3. *Die Untergruppen von* $\mathfrak{R}^+$ *und* $\mathfrak{Z}=\mathfrak{R}^+/\{1\}$ *sind gerade alle lokal-zyklischen Gruppen*[15]*). Man erhält also sämtliche lokal-zyklische Gruppentypen durch Hinzunahme derjenigen Gruppen* (5) *zu den Gruppen ersten Ranges, die keine p-Gruppen sind.*

---

[14]) Speziell bezeichnet $R\left(\frac{1}{p_1}, \frac{1}{p_2}, \ldots\right)$ den Ring derjenigen rationalen Zahlen, die nur Primfaktoren $p_1, p_2, \ldots$ im Nenner enthalten. Dann läßt sich (4) als ein Produkt auffassen, wobei man den zweiten Faktor elementweise mit n zu multiplizieren hat. Ist $\mathfrak{M}=0$ die leere Menge, so schreibe man für (4) entsprechen $n.R(0)$; es ist $R(0)$ der Ring der ganzen Zahlen, $n.R(0)$ der Ring der Vielfachen von n.

[15]) Vgl. Prüfer [3] (wobei man unter einen „Modul" offenbar eine Untergruppe von $\mathfrak{R}+$ zu verstehen hat).

Die Unterringe von $\mathfrak{R}$ und die direkten Summen von (endlich- oder unendlichvielen) zu verschiedenen Primzahlen p gehörenden p-Ringen ersten Ranges (die oben schon angegeben wurden) erschöpfen alle lokal-zyklischen Ringtypen. Letztere sind eben die Ringe, die sich auf den Gruppen (5) *aufbauen lassen, d. h. die direkten Summen*

$$(6) \qquad \sum_{i=1}^{\infty} Z(q_i^{e_i}, q_i^{k_i}),$$

mit $0 \leqq k_i \leqq e_i$ *für ein endliches* e_i, *dagegen soll das Symbol* $Z(q^{\infty}, q_i^{k_i})$ *(für ein* $e_i = \infty$*) durch* $Z(q^{\infty})$ *ersetzt werden.*

Zusammenfassende Bemerkungen. Nach Satz 3 sind alle lokal-zyklischen Ringe (insbesondere also alle Ringe ersten Ranges) kommutativ. Auch sieht man, daß unter den unendlichen Ringen ersten Ranges nach Satz 2 nur die zwei extremen Fälle, nämlich Zeroringe und Integritätsbereiche (d. h. kommutative Ringe ohne Nullteiler) vorkommen.

Wie stark im allgemeinen die Ringe ersten Ranges durch ihre additive Gruppe determiniert sind, das wird uns so noch klarer, daß wir folgende interessante Fragen beantworten: *Welche und wieviele Ringtypen lassen sich auf einer festen Gruppe $\mathfrak{G}$ vom ersten Range aufbauen, die keine Zeroringe sind?* Diese Ringe und ihre Anzahl bezeichnen wir mit $R(\mathfrak{G})$ bzw. $[\mathfrak{G}]$. Wir bemerken gleich, daß sehr wohl auch $[\mathfrak{G}] = \infty$ sein kann, denn z. B. haben alle Ringe (4) bei festen $p_1, p_2, \ldots$ isomorphe additive Gruppen. Nach Satz 1 unterscheiden wir die Fälle $\mathfrak{G} = \mathfrak{Z}(p^{\infty})$, $\mathfrak{G} \subset \mathfrak{Z}(p^{\infty})$, $\mathfrak{G} = \mathfrak{R}^+$, $\mathfrak{G} \subset \mathfrak{R}^+$, wovon sich der letzte in zwei weitere Fälle spalten wird.

Fall 1: $\mathfrak{G} = \mathfrak{Z}(p^{\infty})$. Nach Satz 2 gibt es jetzt kein $R(\mathfrak{G})$, und so ist $[\mathfrak{G}] = 0$.

Fall 2: $\mathfrak{G} \subset \mathfrak{Z}(p^{\infty})$ d. h. $\mathfrak{G} = \mathfrak{Z}(p^e)$ $(e = 1, 2, \ldots)$. Dann sind die $R(\mathfrak{G})$ die $Z(p^e, p^k)$ $(0 \leqq k < e)$, und so ist $[\mathfrak{G}] = e$.

Fall 3: $\mathfrak{G} = \mathfrak{R}^+$. Nach Satz 2a ist jetzt $\mathfrak{R}$ offenbar der einzige Ring $R(\mathfrak{G})$, und so ist $[\mathfrak{G}] = 1$.

Fall 4: $\mathfrak{G} \subset \mathfrak{R}^+$. Nach Satz 1a läßt sich $\mathfrak{G} = \frac{1}{\mathfrak{P}}$ setzen, wobei $\mathfrak{P}$ nicht aus allen Primzahlpotenzen besteht (dann läge nämlich Fall 3 vor). Wir unterscheiden die weiteren zwei Fälle:

Fall 4a: *$\mathfrak{P}$ enthält nur endlich viele solche Primzahlen p, für die nicht zugleich auch alle Potenzen $p, p^2, \ldots$ in $\mathfrak{P}$ liegen.* Diese p und ihre (insgesamt endlich vielen) Potenzen lassen sich aus $\mathfrak{P}$ streichen, denn dabei bleibt $\mathfrak{G} \cong \frac{1}{\mathfrak{P}}$ nach Satz 1a immer noch aufrechterhalten. Bezeichne $p_1, p_2, \ldots$ alle Primzahlelemente von $\mathfrak{P}$, so sind sämtliche $R(\mathfrak{G})$ offenbar durch (4) angegeben, und so ist $[\mathfrak{G}] = \infty$.

Fall 4b: *$\mathfrak{P}$ enthält unendlich viele solche Primzahlen p, für die nicht zugleich alle Potenzen $p, p^2, \ldots$ in $\mathfrak{P}$ liegen.* Da die additive Gruppe des

Ringes (4) offenbar $\frac{n}{\mathfrak{P}'}$ ist, wobei $\mathfrak{P}'$ genau aus allen Potenzen der p_i besteht, und nach Satz 1a $\frac{1}{\mathfrak{P}}$ gewiß nicht-isomorph zu $\frac{n}{\mathfrak{P}'}$ ist, so gibt es jetzt nach Satz 2a kein $R(\mathfrak{G})$ und es ist $[\mathfrak{G}]=0$.

Wir sehen also, daß alle Fälle $[\mathfrak{G}]=0, 1, 2, \ldots, \infty$ möglich sind. Zwei besonders interessante Fälle geben uns Anlass zu den folgenden Bemerkungen.

$[\mathfrak{G}]=1$ gilt nur für $\mathfrak{G}=\mathfrak{Z}(p)$, $\mathfrak{R}^+$ (Fälle 2, 3). Entsprechend ist $R(\mathfrak{G})=Z(p, 1)$, d. h. der endliche Körper von p Elementen bzw. $R(\mathfrak{G})=\mathfrak{R}$; beide machen eben alle Primkörper aus. Also gilt: *Unter allen Ringen ersten Ranges sind die Primkörper (von jeder Charakteristik) dadurch ausgezeichnet, daß sich auf ihrer additiven Gruppe keine weiteren Nicht-Zeroringe aufbauen lassen.*

$[\mathfrak{G}]=0$ gilt für die $\mathfrak{G}=\mathfrak{Z}(p^\infty)$ (Fall 1) und für die $\mathfrak{G}=\frac{1}{\mathfrak{P}}$ im Fall 4b. *Auf diesen Gruppen lassen sich somit überhaupt keine Nicht-Zeroringe aufbauen.* Unseres Wissens ist in der Literatur bisher noch nicht bemerkt worden, daß es additive Gruppen gibt, in denen sich ein nicht identisch verschwindendes (kommutatives oder nichtkommutatives) Produkt der Elemente in keiner Weise so definieren läßt, daß dabei ein Ring entsteht[16]). Das lautet überraschend, denn auf den endlichen additiven Gruppen läßt sich immer mindestens ein Nicht-Zeroring aufbauen[17]), und so hätte man von den unendlichen Gruppen ähnliches erwartet.

Vollständigkeitshalber werden wir uns beim Beweis unserer Sätze nicht auf die erwähnten Resultate von Baer und Prüfer stützen.

§ 3. Beweis der Sätze 1, 2, 3.

Wir beweisen die Sätze 1, 2 zusammen. Es ist vor allem klar, daß die in diesen Sätzen aufgezählten Gruppen bzw. Ringe vom ersten Range sind. Bezeichne umgekehrt R einen beliebigen Ring ersten Ranges, also $R^+=\mathfrak{G}$ eine ebenfalls beliebige Gruppe ersten Ranges.

Ist R (und $\mathfrak{G}$) endlich, so muß $\mathfrak{G}$ ein $\mathfrak{Z}(p^e)$ $(e=1, 2, \ldots)$ sein, denn sonst zerfällt $\mathfrak{G}$ nach dem Fundamentalsatze der endlichen Abelschen Gruppen in eine direkte Summe, was wegen E_1 nicht sein kann. Dies beweist schon

16) Inzwischen ist einem von uns gelungen, die Struktur dieser Gruppen weitgehend aufzudecken. Vgl. T. Szele, Zur Theorie der Zeroringe, *Math. Annalen*, **121** (1949), S. 242–246.

17) Das folgt unmittelbar aus dem Fundamentalsatz der endlichen Abelschen Gruppen, nach dem nämlich jede solche Gruppe in eine direkte Summe von zyklischen Gruppen zerlegbar ist. Dann ist die direkte Summe der Restklassenringe (gebildet im Ring der ganzen Zahlen), die sich auf den einzelnen zyklischen Komponenten dieser Zerlegung aufbauen lassen, offenbar kein Zeroring (sogar ist ein Ring mit Einselement).

Satz 1 und Satz 2 für endliche Gruppen bzw. für endliche Ringe. (Vgl. hierzu die Bemerkung nach Satz 2.)

Es sind nur noch die unendlichen R (und $\mathfrak{G}$) übrig. Offenbar schließt E_3 aus, daß von α und β das eine von endlicher das andere von unendlicher Ordnung ist, und so ist $\mathfrak{G}$ entweder eine (unendliche) Torsionsgruppe oder eine torsionsfreie Gruppe. Beide Fälle betrachten wir getrennt als Fall 1 bzw. 2.

Fall 1: *$\mathfrak{G}$ ist eine unendliche Torsionsgruppe.* Die endlichen Untergruppen von $\mathfrak{G}$ müssen nach obigem lauter Gruppen $\mathfrak{Z}(p^e)$ sein, und so sind alle Elemente von einer Ordnung $1, p, p^2, \ldots$, wobei p eine feste Primzahl ist. Mit anderen Worten ist dann $\mathfrak{G}$ eine p-Gruppe. Würden die Gleichung

$$(7) \qquad p^e \xi = 0$$

mehr als p^e Elemente ξ von $\mathfrak{G}$ befriedigen, so nehme man p^e+1 solche Elemente; diese erzeugen eine endliche nichtzyklische Gruppe, und das ist ein Widerspruch. Da also (7) höchstens p^e Lösungen in $\mathfrak{G}$ hat, so gibt es in $\mathfrak{G}$ Elemente von beliebig hoher Ordnung, d. h. von jeder Ordnung $1, p, p^2, \ldots$. Folglich hat $\mathfrak{G}$ genau p^e Elemente ξ, für die (7) gilt. Wir zeigen nun, daß sich in $\mathfrak{G}$ Elemente $\alpha_1, \alpha_2, \ldots (\neq 0)$ angeben lassen, die die Gleichungen (1) befriedigen. Hierzu wählen wir für α_1 ein beliebiges Element p-ter Ordnung in $\mathfrak{G}$, wofür also die erste Gleichung (1) gilt, und nehmen an, daß wir schon Elemente $\alpha_1, \ldots, \alpha_e$ $(e \geqq 1)$ gefunden haben, für die die ersten e Gleichungen (1) (einschließlich bis $p\alpha_e = \alpha_{e-1}$) erfüllt sind. Einerseits bilden dann die $k\alpha_e (k = 0, 1, \ldots, p^e - 1)$ alle Lösungen von (7), andererseits gibt es in $\mathfrak{G}$ ein Element α von der Ordnung p^{e+1}, wofür dann notwendig $p\alpha = k\alpha_e$ mit einem geeigneten k $(p \nmid k)$ gilt. Wir bestimmen k' mit $kk' \equiv 1 \pmod{p^e}$ und setzen $\alpha_{e+1} = k'\alpha$. Dann gilt $p\alpha_{e+1} (= kk'\alpha_e) = \alpha_e$, und so haben wir die Behauptung durch Induktion bewiesen. Die angegebenen Elemente $\alpha_1, \alpha_2, \ldots$ von $\mathfrak{G}$ erzeugen eine Gruppe $\mathfrak{Z}(p^\infty) \subseteqq \mathfrak{G}$. Da es schon in $\mathfrak{Z}(p^\infty)$ p^e Lösungen von (7) gibt und jedes Element von $\mathfrak{G}$ eine Gleichung (7) befriedigt, so können in $\mathfrak{G}$ außerhalb $\mathfrak{Z}(p^\infty)$ keine Elemente vorhanden sein, d. h. es ist $\mathfrak{G} = \mathfrak{Z}(p^\infty)$. Satz 1 ist für diesen Fall bewiesen.

Auch folgt aus $R^+ = \mathfrak{G} = \mathfrak{Z}(p\ \ )$, daß R nur ein Zeroring sein kann. Nach (1) lassen nämlich irgendzwei Elemente von R in der Form $c\alpha_k$, $d\alpha_l$ annehmen mit ganzen rationalen c, d. Wieder nach (1) gilt aber

$$c\alpha_k \cdot d\alpha_l = c\alpha_k \cdot dp^k \alpha_{k+l} = p^k \alpha_k \cdot c d\alpha_{k+l} = 0,$$

(es ist nämlich $p^k\alpha_k = 0$) und so ist R in der Tat ein Zeroring, wie es im Satz 2 behauptet wurde.

Fall 2: *$\mathfrak{G}$ ist eine torsionsfreie Gruppe.* Wir geben eine isomorphe Abbildung von $\mathfrak{G}$ in $\mathfrak{R}^+$ an, womit wir insbesondere den Beweis von Satz 1 vollendet werden haben. Hierzu wählen wir ein beliebiges Elementenpaar $\alpha \in \mathfrak{G}$, $a \in \mathfrak{R}^+ (\alpha, a \neq 0)$ fest und betrachten ein weiteres Element ξ von $\mathfrak{G}$.

Nach E_3 gibt es ganze Zahlen r, s mit

(8) $$s\xi = r\alpha \qquad (s \neq 0).$$

(Dies ist auch für $\xi = 0$ richtig mit $r = 0$.) Wir ordnen ξ die rationale Zahl $a \cdot \frac{r}{s}$ als Bild zu:

(9) $$\xi \rightarrow a \cdot \frac{r}{s}.$$

Diese Abbildung ist eindeutig, denn gilt auch $\xi \rightarrow a \cdot \frac{r'}{s'}$, d. h. $s'\xi = r'\alpha$, so folgt aus (8): $(rs' - r's)\xi = 0$. Da $\mathfrak{G}$ torsionsfrei ist, muß der erste Faktor verschwinden; also ist $\frac{r}{s} = \frac{r'}{s'}$, und so sind beide Bilder $a \cdot \frac{r}{s}$, $a \cdot \frac{r'}{s'}$ gleich. Verschiedenen Elementen gehören auch verschiedene Bilder zu. Denn nehmen wir ein weiteres Element ξ' von $\mathfrak{G}$ an, wofür dann entsprechend (8) und (9)

(10) $$s'\xi' = r'\alpha,$$

(11) $$\xi' \rightarrow a \cdot \frac{r'}{s'}$$

gilt. Sind nun die rechten Seiten von (9) und (11) gleich, d. h. $rs' - r's = 0$, so folgt aus (8), (10): $ss'(\xi - \xi') = (rs' - r's)\alpha = 0$, $\xi = \xi'$, wie behauptet wurde. Endlich betrachten wir ein beliebiges Elementenpaar ξ, ξ' in $\mathfrak{G}$, wofür wir wieder (8)—(11) annehmen. Ähnlich wie vorher folgt $ss'(\xi + \xi') = (rs' + r's)\alpha$, also $\xi + \xi' \rightarrow a \cdot \frac{r}{s} + a \cdot \frac{r'}{s'}$, d. h. die angegebene eindeutige Abbildung ist ein Isomorphismus.

Um auch noch den Beweis von Satz 2 zu beenden, genügt es folgendes zu zeigen. Ist R kein Zeroring, so läßt sich das obige (bisher willkürliche) a so wählen, daß R durch (9) *ringisomorph* in $\mathfrak{R}$ abgebildet wird. Hierzu braucht nur noch gezeigt zu werden, daß für ein passendes (festes) a aus (9) und (11) immer

(12) $$\xi\xi' \rightarrow a \frac{r}{s} \cdot a \frac{r'}{s'}$$

folgt.

Zuerst zeigen wir $\alpha^2 \neq 0$ $(\alpha \in R, \alpha \neq 0)$. Denn nehmen wir $\alpha^2 = 0$ an. Für ein beliebiges Elementenpaar β_1, β_2 $(\neq 0)$ von R gibt es nach E_3 ganze Zahlen r_1, s_1, r_2, s_2 mit

$$r_1\beta_1 = s_1\alpha \neq 0, \quad r_2\beta_2 = s_2\alpha \neq 0.$$

Es folgt $r_1 r_2 \beta_1 \beta_2 = s_1 s_2 \alpha^2 = 0$. Da $r_1 r_2 \neq 0$ und $\mathfrak{G}$ torsionsfrei ist, so folgt weiter, daß $\beta_1\beta_2 = 0$ d. h. R ein Zeroring ist. Dieser Widerspruch beweist unsere Behauptung.

Da α, α^2 von 0 verschiedene Elemente von $\mathfrak{G}$ sind, so gibt es nach E_3 ganze Zahlen c, d mit

$$c\alpha = d\alpha^2 \neq 0. \tag{13}$$

Wir wählen

$$a = \frac{c}{d} \tag{14}$$

und zeigen, daß dann aus (9), (11) in der Tat (12) folgt. Wegen (9), (11) dürfen (8), (10) angenommen werden. Nach Multiplikation haben wir $ss'\xi\xi' = rr'\alpha^2$ also nach (13) und (14):

$$dss'\xi\xi' = crr'\alpha = adrr'\alpha.$$

Nach der Definition der Abbildung (9) folgt hieraus

$$\xi\xi' \to a^2 \cdot \frac{rr'}{ss'}.$$

Dies stimmt mit (12) überein, womit wir Satz 2 bewiesen haben.

Wir wollen noch Satz 3 in diesem § beweisen. Ist $\mathfrak{G}$ eine lokal-zyklische Gruppe (d. h. eine Gruppe mit der Eigenschaft E^*), so ist vor allem klar, daß auch jetzt gilt: $\mathfrak{G}$ ist entweder eine torsionsfreie Gruppe oder eine Torsionsgruppe.

Ist $\mathfrak{G}$ torsionsfrei, so folgt aus der Existenz eines δ mit $\alpha = a\delta$, $\beta = b\delta$, daß $ab\delta$ ein gemeinsames Multiplum von α und β ist (und zwar gilt $ab\delta \neq 0$, falls $\alpha, \beta \neq 0$ sind), mithin hat $\mathfrak{G}$ die Eigenschaft E_3. Damit sind alle Behauptungen von Satz 3 bewiesen, die sich auf $\mathfrak{R}^+$ bzw. $\mathfrak{R}$ beziehen.

Ist dann $\mathfrak{G}$ eine Torsionsgruppe mit der Eigenschaft E^*, so zerfällt sie in eine direkte Summe von p-Gruppen, die zu verschiedenen Primzahlen p gehören, und von der Eigenschaft E_3 sind. (Vgl. [10]). Folglich ist $\mathfrak{G}$ nach Satz 1 eine Gruppe (5) und somit zugleich auch eine Untergruppe von $\mathfrak{Z} = \mathfrak{R}^+/\{1\} = \sum_{i=1}^{\infty} \mathfrak{Z}(q_i^\infty)$ (wobei $q_1, q_2, \ldots$ die Folge aller Primzahlen bezeichnet). Da endlich auf einer additiven Gruppe (5) bekanntlich nur Ringe vom Typ (6) aufbauen lassen (und zwar auf der Gruppe $\mathfrak{Z}(q_i^\infty)$ nach Satz 2 nur der Zeroring $Z(q_i^\infty)$), so haben wir auch Satz 3 bewiesen.

§ 4. Beweis der Sätze 1a, 2a.

Bezeichne $\mathfrak{A}$ eine Untergruppe von $\mathfrak{R}^+$, insbesondere $\mathfrak{A}_1$ eine Untergruppe, die die Zahl 1 enthält. $\mathfrak{A}$ enthält ganze, darunter auch positive Elemente. Bezeichne n die kleinste natürliche Zahl in $\mathfrak{A}$. Die Gruppe $\frac{1}{n}\mathfrak{A}$[18]) ist

[18]) $\frac{1}{n}\mathfrak{A}$ bezeichnet, daß man die Elemente von $\mathfrak{A}$ mit $\frac{1}{n}$ multipliziert.

ein $\mathfrak{A}_1$, und so gilt

$$\mathfrak{A} = n\mathfrak{A}_1. \tag{15}$$

Wir haben $\mathfrak{A}_1$ näher zu untersuchen. Ist $\frac{c}{d} \in \mathfrak{A}_1$ mit relativ primen ganzen c, d, so gibt es ganze Zahlen r, s mit $r \cdot \frac{c}{d} = s + \frac{1}{d}$; hieraus folgt $\frac{1}{d} \in \mathfrak{A}_1$ und zugleich $\frac{1}{P} \in \mathfrak{A}_1$ für alle Primzahlpotenzfaktoren P von d. Umgekehrt wird $\frac{c}{d}$ durch diese $\frac{1}{P}$ additiv erzeugt, und so haben wir gezeigt, daß $\mathfrak{A}_1$ in der Form $\left\{\frac{1}{P_1}, \frac{1}{P_2}, \ldots\right\}$ erscheint, wobei $P_1, P_2, \ldots$ passende Primzahlpotenzen sind, die dabei offenbar eine Menge $\mathfrak{P}$ bilden (wie in Satz 1a). Zugleich schreibt sich (15) so:

$$\mathfrak{A} = \left\{\frac{n}{P_1}, \frac{n}{P_2}, \ldots\right\}. \tag{16}$$

Hätte n einen Teiler $d (> 1)$ mit einem P_i gemeinsam, so würde aus (16) $\frac{n}{d} \in \mathfrak{A}$ folgen, und das der Definition von n widerspricht. Also ist n prim zu allen P_i, und so ist $\mathfrak{A}$ in der Tat eine der in (3) angegebenen Gruppen $\frac{n}{\mathfrak{P}}$.

Identisch gleich können zwei solche Untergruppen $\frac{n}{\mathfrak{P}}, \frac{n'}{\mathfrak{P}'}$ wegen[9]) nur im Fall $n = n'$ sein, und dann sind auch $\frac{1}{\mathfrak{P}}, \frac{1}{\mathfrak{P}'}$ identisch gleich, woraus offenbar $\mathfrak{P} = \mathfrak{P}'$ folgt. Wir haben also gezeigt, daß in der Form (3) jede Untergruppe von $\mathfrak{R}^+$ genau einmal erscheint.

Nunmehr haben wir nun noch zu untersuchen, welche zwei Gruppen (3) isomorph sind. Als Vorbereitung bemerken wir folgendes. Man dividiere alle Elemente einer Gruppe $\frac{1}{\mathfrak{P}}$ durch eine Primzahl p, d. h. bilde $\frac{1}{p} \cdot \frac{1}{\mathfrak{P}}$. Dies ist dann wieder eine Gruppe $\frac{1}{\mathfrak{P}'}$, wobei zwei Fälle zu unterscheiden sind. Und zwar, wenn $\mathfrak{P}$ alle Potenzen $1, p, p^2, \ldots$ enthält, so ist einfach $\mathfrak{P}' = \mathfrak{P}$. Wenn degegen $1, p, \ldots, p^e$ $(e \geqq 0)$ sämtliche, in $\mathfrak{P}$ enthaltene Potenzen von p sind, so entsteht $\mathfrak{P}'$ aus $\mathfrak{P}$ durch Hinzunahme von p^{e+1} (d. h. e wird zu $e+1$ erhöht).

Betrachten wir nunmehr zwei Untergruppen $\mathfrak{A}, \mathfrak{A}'$ von $\mathfrak{R}^+$ in der Form (3) geschrieben:

$$\mathfrak{A} = \frac{n}{\mathfrak{P}}, \quad \mathfrak{A}' = \frac{n'}{\mathfrak{P}'}. \tag{17}$$

Offenbar sind diese dann und nur dann isomorph, wenn es eine rationale

Zahl $u(\neq 0)$ mit $\mathfrak{A}' = u \cdot \mathfrak{A}$ gibt[19]). Dabei darf $u > 0$ angenommen werden, und dann läßt sich $u = \frac{r}{s}$ setzen (r, s natürliche Zahlen). Dann ergibt sich aus (17): $\frac{1}{n's} \cdot \frac{1}{\mathfrak{P}} = \frac{1}{nr} \cdot \frac{1}{\mathfrak{P}'}$. Wir haben gewonnen: $\mathfrak{A}, \mathfrak{A}'$ sind dann und nur dann isomorph, wenn es natürliche Zahlen c, c' gibt, für die die Gruppen $\frac{1}{c} \cdot \frac{1}{\mathfrak{P}}, \frac{1}{c'} \cdot \frac{1}{\mathfrak{P}'}$ identisch gleich sind. Nach der vorangeschickten Bemerkung ist das gleichbedeutend damit, daß die Menge $\mathfrak{P}, \mathfrak{P}'$ nur in endlichvielen Elementen voneinander unterscheiden. Satz 1a ist bewiesen.

Für Satz 2a ist vor allem klar, daß unter (4) lauter Unterringe von $\mathfrak{R}$ angegeben wurden und sie zu zweien nicht-isomorph sind. Es ist nur noch zu zeigen, daß jeder Unterring U von $\mathfrak{R}$ unter den Ringen (4) vorkommt. Da U^+ eine Untergruppe von $\mathfrak{R}^+$ ist, so machen die Elemente von U nach Satz 1a eine Gruppe $\frac{n}{\mathfrak{P}} = \left\{\frac{n}{P_1}, \frac{n}{P_2}, \ldots\right\}$ aus. Andererseits können dieselben Elemente offenbar nur dann einen Unterring von $\mathfrak{R}$ bilden, wenn mit einer Primzahl $p \in \mathfrak{P}$ auch alle Potenzen $p^2, p^3, \ldots$ in $\mathfrak{P}$ enthalten sind. Bei dieser Einschränkung stimmt die Gruppe (3) mit einem Ring (4) überein, womit wir auch Satz 2a bewiesen haben.

Schriftenverzeichnis.

[1] R. Baer, Abelian groups without elements of finite order, *Duke Math. Journal*, **3** (1937), S. 68-122.

[2] H. Prüfer, Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen, *Math. Zeitschrift*, **17** (1923), S. 35–61.

[3] H. Prüfer, Theorie der Abelschen Gruppen. I. Grundeigenschaften, *ebenda*, **20** (1924), S. 165–187.

(Eingegangen am 23. Juli 1949.)

[19]) Hat nämlich $\alpha \in \mathfrak{A}$ $(\alpha \neq 0)$ bei einer isomorphen Abbildung von $\mathfrak{A}$ auf $\mathfrak{A}'$ das Bildelement $\alpha' \in \mathfrak{A}'$, und ist $\alpha' = u\alpha$, so muß wegen der Eigenschaft E_3 jedes Element $\xi \in \mathfrak{A}$ offenbar das Bildelement $\xi' = u\xi$ bekommen.