Ein Satz über die Struktur der endlichen Ringe.

Von T. SZELE in Szeged.

Es ist bekannt, daß sich jeder endliche Ring[1]) $\mathfrak{R}$ in eine direkte Summe von eindeutig bestimmten p-Ringen[2]) $\mathfrak{R}_1, \ldots, \mathfrak{R}_m$ zerlegen läßt, die zu verschiedenen $p_1, \ldots, p_m$ gehören, und einander (beiderseits) annulieren[3]). Durch diesen Satz wird das Problem der Struktur der endlichen Ringe auf das von p-Ringen zurückgeführt.

Leider weiß man über die Struktur der p-Ringe nur sehr wenig. Bekannte wichtige Beispiele sind: die endlichen (kommutativen) Körper, ferner die p-Ringe $\mathfrak{R}$ mit zyklischer additiver Gruppe $\mathfrak{R}^+$; letztere sind sämtliche Unterringe der Restklassenringe mod p^e (im Ring der ganzen Zahlen)[4]). Als weitere Beispiele sind noch alle $\mathfrak{R}$ mit p^2 Elementen und nichtzyklischem $\mathfrak{R}^+$ bekannt[5]). Darunter gibt es 6 kommutative und 2 nichtkommutative Ringe[6]). Wir erwähnen noch die Untersuchungen von VANDIVER[7]) über die endlichen kommutativen Ringe mit mindestens einem Nicht-nullteiler.

---

[1]) Wir lassen durchwegs auch nichtkommutative Ringe zu.

[2]) Als Analogon von p-Gruppen verstehen wir unter einem p-Ring einen Ring mit p^e Elementen (p Primzahl).

[3]) Die $\mathfrak{R}_1, \ldots, \mathfrak{R}_m$ entstehen einfach so, daß man in der additiven Gruppe $\mathfrak{R}^+$ (der Elemente) von $\mathfrak{R}$ die Menge aller Elemente bildet, deren Ordnungen Potenzen eines festen Primfaktors der Ordnung von $\mathfrak{R}^+$ sind.

[4]) Bezeichne man mit $\mathfrak{R}(p^e, p^f)$ den Ring derjenigen Restklassen mod p^e, die aus lauter durch p^f teilbaren Zahlen gebildet sind ($e \geqq f \geqq 0$). Dann sieht man leicht ein, daß alle Ringe mit p^n Elementen und zyklischer additiver Gruppe die folgenden sind: $\mathfrak{R}(p^n, 1)$, $\mathfrak{R}(p^{n+1}, p), \ldots, \mathfrak{R}(p^{2n}, p^n)$. Ihre Anzahl ist $n+1$. Vgl. R. BALLIEU, Anneaux finis; systèmes hypercomplexes de rang deux sur un corps, *Annales de la Société Scientifique de Bruxelles*, (1) **61** (1947), S. 117—126. Diese Arbeit war mir bisher nicht zugänglich.

[5]) Siehe die am Ende von [4]) zitierte Arbeit von R. BALLIEU und außerdem die Arbeit von CAYLEY, On double algebra, *Proceedings London Math. Society*, (1) 15 (1883), S. 185—197. CAYLEY beschäftigt sich dabei mit allgemeineren Strukturfragen, welche als Spezialfall auch die obigen endlichen Ringe (ausgenommen den endlichen Körper) umfassen.

[6]) Folglich ist die Gesamtzahl der Ringe mit p^2 Elementen 11.

[7]) H. S. VANDIVER, Theory of finite algebras, *Transaction American Math. Society*, **13** (1912), S. 293—304.

In dieser Arbeit geben wir gewisse leicht konstruierbare endliche Matrizenringe von ganzzahligen Matrizen (mit aber nur nach gewissen Moduln p^e in Betracht kommenden Elementen) an, deren Unterringe alle denkbaren p-Ringe sind. Um den diesbezüglichen Satz aussprechen zu können, schicken wir Folgendes voran.

Es sei gegeben eine (endliche) Folge von natürlichen Zahlen:

$$\alpha_1, \alpha_2, \ldots, \alpha_n \qquad (\alpha_1 \geqq \alpha_2 \geqq \ldots \geqq \alpha_n \geqq 1). \tag{1}$$

Diese Folge läßt sich auch so schreiben:

$$\beta_1\ (n_1\text{-mal}), \ldots, \beta_r\ (n_r\text{-mal}) \qquad (\beta_1 > \ldots > \beta_r \geqq 1), \tag{2}$$

wobei dann $n_1 + \ldots + n_r = n$ ist. Betrachten wir alle ganzzahligen Matrizen (a_{ik}) vom Typ n^2 mit der Nebenbedingung für die Elemente unterhalb der Hauptdiagonale:

$$p^{\alpha_k - \alpha_i} \mid a_{ik} \qquad (i > k).^8) \tag{3}$$

Wir nennen zwei solche Matrizen (a_{ik}), (a'_{ik}) gleich, wenn

$$a_{ik} \equiv a'_{ik} \pmod{p^{\alpha_k}} \qquad (i, k = 1, \ldots, n) \tag{4}$$

gilt. Die Bedingung (3) können wir so veranschaulichen, daß wir die Matrix (a_{ik}) in r^2 rechteckige „Kästchen" (Teilmatrizen) K_{uv} entsprechend der Multiplizitätszahlen n_j in (2) einteilen (wie das das beigelegte Schema für $r = 3$ andeutet), und dann lautet (3) (wegen (2)) so, daß die Elemente im Kästchen K_{uv} $(u > v)$ durch $p^{\beta_v - \beta_u}$ teilbar sind. Die Definition (4) der Gleichheit kommt darauf hinaus, daß die Elemente in der v-ten „Kästchenspalte" einer Matrix nur mod p^{β_v} in Betracht kommen.

	n_1	n_2	n_3
n_1			
n_2	K_{21}		
n_3	K_{31}	K_{32}	

Offenbar bilden die verschiedenen Matrizen (a_{ik}) einen Ring, den wir mit $\mathfrak{M}_p(\alpha_1, \ldots, \alpha_n) = \mathfrak{M}_p$ bezeichnen. Die additive Gruppe $\mathfrak{M}_p^+$ dieses Ringes ist vom Typ $(p^{\alpha_1}, p^{\alpha_2}, p^{\alpha_3}, p^{\alpha_3}, p^{\alpha_3}, p^{\alpha_3}, p^{\alpha_3}, p^{\alpha_3}, p^{\alpha_3}, \ldots)$, woraus man die Anzahl der Elemente von $\mathfrak{M}_p$ unmittelbar entnehmen kann.

Nunmehr können wir den oben angekündigten Satz so aussprechen:

Satz. *Jeder p-Ring ist ein Unterring eines $\mathfrak{M}_p$. Und zwar, wenn $\mathfrak{R}$ ein Ring ohne Rechtsannihilator*[9]) *und dabei $\mathfrak{R}^+$ eine Gruppe vom*

---

[8]) Die Einschränkung „$i > k$" dürfte weggelassen werden, denn im Fall $i \leqq k$ ist der Quotient der rechten und linken Seite von (3) eine ganze Zahl und so ist die Teilbarkeit von selbst erfüllt.

[9]) Wir nennen ein Element A von $\mathfrak{R}$ einen Rechtsannihilator, wenn $XA = 0$ für alle $X \in \mathfrak{R}$ gilt.

Typ $(p^{\alpha_1}, \ldots, p^{\alpha_n})$ *ist*[10]), *so ist* $\mathfrak{R}$ *gewiß ein Unterring von* $\mathfrak{M}_p(\alpha_1, \ldots, \alpha_n)$. *Läßt man dagegen auch die Existenz eines Rechtsannihilators von* $\mathfrak{R}$ *zu, so kommt man mit* $\mathfrak{M}_p(\alpha_1, \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$ *aus*[11]).

Der Beweis des Satzes geschieht mit Hilfe von folgendem

Lemma. *Hat ein Ring* $\mathfrak{R}$ *keinen Rechtsannihilator, so ist* $\mathfrak{R}$ *ein Unterring des Endomorphismenringes der Gruppe* $\mathfrak{R}^+$.[12]) [13])

Ordnen wir nämlich jedem Element A von $\mathfrak{R}$ den Endomorphismus

$$X \to XA \qquad (X \in \mathfrak{R}) \tag{5}$$

der additiven Gruppe $\mathfrak{R}^+$ zu. Diese bilden einen zu $\mathfrak{R}$ isomorphen Unterring des Endomorphismenringes von $\mathfrak{R}^+$. Um dies einzusehen, betrachten wir neben (5) auch den zu B zugeordneten Endomorphismus:

$$X \to XB. \tag{6}$$

Wegen $X(A+B) = XA + XB$, $X(AB) = (XA)B$ ist den Elementen $A+B$, AB die Summe und das Produkt der Endomorphismen (5) (6) zugeordnet, und so ist die Zuordnung homomorph. Sie ist aber auch isomorph, denn sind (5) und (6) gleich, d. h. gilt $XA = XB$, also $X(A-B) = 0$, für jedes $X(\in \mathfrak{R})$, so muß wegen des Fehlens eines Rechtsannihilators in der Tat $A-B=0$, $A=B$ sein. Damit ist das Lemma bewiesen.

Nunmehr sei $\mathfrak{R}$ endlich und $\mathfrak{R}^+$ eine Gruppe vom Typ $(p^{\alpha_1}, \ldots, p^{\alpha_n})$. Wir zeigen, daß $\mathfrak{M}_p(\alpha_1, \ldots, \alpha_n)$ der Endomorphismenring der Gruppe $\mathfrak{R}^+$ ist[14]), woraus nach dem eben bewiesenen Lemma eine Behauptung

---

[10]) Dabei soll $\alpha_1 \geqq \alpha_2 \geqq \ldots \geqq \alpha_n$ angenommen werden.

[11]) Nach (3) und (4) ließen sich die Elemente a_{ik} im Kästchen K_{uv} einer Matrix (a_{ik}) von $\mathfrak{M}_p(\alpha_1, \ldots, \alpha_n^*)$ auch als Elemente von $\mathfrak{R}(p^{\beta_v}, p^{\beta_v - \beta_u})$ (vgl. [4])) betrachten, wobei $p^{\beta_v - \beta_u}$ im Fall eines negativen Exponenten durch 1 zu ersetzen ist. Das bedeutet, daß bei der Konstruktion von $\mathfrak{M}_p(\alpha_1, \ldots, \alpha_n)$ allein mit Verwendung von Unterringen der Restklassenringe auskommen kann. Allerdings wäre dann die Multiplikationsvorschrift in $\mathfrak{M}_p$ schwerfällig.

[12]) Das ist eine Verschärfung des ähnlichen Satzes für Ringe mit Einselement (N. JACOBSON, *The theory of rings* (New York, 1943), S. 54, Theorem 1), denn ein solcher Ring hat keinen Rechtsannihilator, während das Umgekehrte nicht gilt. Beispiele für Ringe ohne Rechtsannihilator und Einselement: der Ring der geraden Zahlen, oder der Ring bestehend aus den vier Elementen $0, A, B, A+B$ mit den definierenden Relationen $A+A = B+B = 0$; $A^2 = A$, $AB = B$, $B^2 = BA = 0$.

[13]) Unter einem Endomorphismus einer Gruppe versteht man eine homomorphe Abbildung der Gruppe in sich. Im Fall einer Abelschen Gruppe bilden die sämtlichen Endomorphismen einen Ring.

[14]) Inzwischen ist mir bekannt geworden, daß den Endomorphismenring der endlichen Abelschen Gruppen auch schon K. SHODA (Über die Automorphismen einer endlichen Abelschen Gruppe, *Math. Annalen*, **100** (1928), S. 674—686) konstruiert und ihn für einen anderen Zweck (nämlich zur Untersuchung der Struktur der Automorphismengruppe) verwertet hat.

des obigen Satzes unmittelbar folgt. Bezeichne $A_1, \ldots, A_n$ eine Basis von $\mathfrak{R}^+$, für welche

$$(A_i) = p^{\alpha_i} \qquad (i = 1, \ldots, n)^{15}) \tag{7}$$

gilt. Jeder Endomorphismus von $\mathfrak{R}^+$ ist durch die Angabe der Bildelemente von $A_1, \ldots, A_n$ eindeutig bestimmt. Denn sind die Zuordnungen

$$A_i \to A_i' = a_{i1}A_1 + \ldots + a_{in}A_n \quad (i = 1, \ldots, n), \tag{8}$$

schon festgestellt, so muß irgendeinem Element

$$X = c_1A_1 + \ldots + c_nA_n \tag{9}$$

von $\mathfrak{R}^+$ bei einem Endomorphismus das Bildelement

$$X' = c_1A_1' + \ldots + c_nA_n' \tag{10}$$

zugeordnet werden. Andererseits ist die durch (8) (9) (10) angegebene Abbildung von $\mathfrak{R}^+$ in sich offenbar dann und nur dann ein Endomorphismus, wenn sie *eindeutig* ist. Eine notwendige Bedingung dafür ist das Bestehen von (3) für die Koeffizientenmatrix in (8), denn im Fall einer durch (8) festgelegten eindeutigen homomorphen Abbildung von $\mathfrak{R}^+$ in sich gilt zwangsläufig

$$(A_i) \geqq (A_i') \qquad (i = 1, \ldots, n),^{15}) \tag{11}$$

und diese Bedingung ist wegen (7) gleichwertig mit (3). (11) ist aber auch hinreichend für die Eindeutigkeit der betrachteten Abbildung, denn gilt neben (9) auch die Darstellung

$$X = d_1A_1 + \ldots + d_nA_n,$$

d. h.

$$c_i \equiv d_i \pmod{(A_i)} \qquad (i = 1, \ldots, n),$$

so ist wegen (11) auch zugleich

$$c_i \equiv d_i \pmod{(A_i')} \qquad (i = 1, \ldots, n),$$

mithin X' in (10) eindeutig bestimmt. Wir haben also das Ergebnis bekommen, daß sich ein jeder Endomorphismus von $\mathfrak{R}^+$ durch eine solche Matrix (a_{ik}) (in (8)) angeben läßt, die ein Element des Ringes $\mathfrak{M}_p(\alpha_1, \ldots, \alpha_n)$ ist; außerdem sieht man auch, daß die durch (4) definierte Gleichheit zweier Matrizen gleichbedeutend mit der Identität der beiden entsprechenden Endomorphismen ist. Da endlich die Summe und das Produkt zweier Endomorphismen wieder durch die Summe und das Produkt der entsprechenden Matrizen angegeben ist, so erweist sich $\mathfrak{M}_p(\alpha_1, \ldots, \alpha_n)$ isomorph zum Endomorphismenring der Gruppe $\mathfrak{R}^+$, w. z. b. w.

---

15) Durch (C) soll die Ordnung eines Elementes $C \in \mathfrak{R}$ in $\mathfrak{R}^+$ bezeichnet werden.

Die übrigen Behauptungen des Satzes folgen leicht aus den schon bewiesenen und der Tatsache, daß sich jeder Ring $\mathfrak{R}$ in einem Ring $\overline{\mathfrak{R}}$ mit Einselement einbetten läßt. In unserem Fall, wobei $\mathfrak{R}^+$ vom Typ $(p^{\alpha_1}, \ldots, p^{\alpha_n})$ (also $\mathfrak{R}$ wegen $\alpha_1 \geqq \alpha_i$ von der Charakteristik p^{α_1}) ist, können wir diese Einbettung zweckmäßig wie folgt ausführen[16]). Wir definieren $\overline{\mathfrak{R}}$ als die Menge aller Paare (A, a) mit $A \in \mathfrak{R}$ und rationalen ganzen a. Sei $(A, a) = (B, b)$ dann und nur dann, wenn $A = B$ und $a \equiv b \pmod{p^{\alpha_1}}$ ist. Definieren wir noch die Addition und Multiplikation in $\overline{\mathfrak{R}}$ durch

$$(A, a) + (B, b) = (A + B, a + b), \quad (A, a)(B, b) = (AB + aB + bA, ab),$$

so wird $\overline{\mathfrak{R}}$ zu einem Ring mit dem Einselement $(0, 1)$, mithin hat $\overline{\mathfrak{R}}$ keinen Rechtsannihilator. Da andererseits $\overline{\mathfrak{R}^+}$ offenbar vom Typ $(p^{\alpha_1}, p^{\alpha_1}, p^{\alpha_2}, p^{\alpha_3}, \ldots, p^{\alpha_n})$ ist, so enthält $\mathfrak{M}_p(\alpha_1, \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$ nach dem schon bewiesenen Teil des Satzes einen zu $\overline{\mathfrak{R}}$ isomorphen Unterring. Alle Elemente $(A, 0)$ bilden aber einen zu $\mathfrak{R}$ isomorphen Unterring in $\overline{\mathfrak{R}}$, so daß auch $\mathfrak{M}_p(\alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_n)$ einen Unterring von dieser Eigenschaft besitzen muß. Damit ist der Satz bewiesen.

(Eingegangen am 15. Januar 1948.)

[16]) Vgl. A. A. Albert, *Modern higher Algebra* (Chicago, 1937), S. 22, Theorem 5.