(7) *Hardy, G. H.* and *Wright, E. M.* Introduction to the Theory of Numbers, Third Edition (O. U. P. 1954), Chapter XXIV.

(8) *Robinson, R. M.* The approximation of irrational numbers by fractions with odd or even terms. Duke Math. J. 7 (1940), 354—359.

(9) *Segre, B.* Lattice points in infinite domains and asymmetric diophantine approximations. Duke Math. J. 12 (1945), 337—365.

Über die homomorphen Bilder des Ringes der ganzen Zahlen und über eine verwandte Ringfamilie[1]

Von

F. A. Szász, Debrecen (Ungarn)

(Eingegangen am 25. Juni 1956)

Wir behandeln in dieser Note zwei spezielle ringtheoretische Probleme. Professor *L. Rédei* hat in dem Artikel [7] alle Ringe (die sog. „Vollidealringe") bestimmt, deren sämtliche additive Untergruppen zweiseitige Ideale im Ringe sind. Wir haben in einer Note [10] alle Ringe gekennzeichnet, deren sämtliche Unterringe die Form $n\,R$ haben, wo R der besprochene Ring und n eine geeignete ganze Zahl ist.

Ein Ring R wird Ring mit der Eigenschaft E_1 genannt, wenn sämtliche Unterringe in der Gestalt $R\,r$ darstellbar sind ($r \in R$).

Ein Ring R wird Ring mit der Eigenschaft E_2 genannt, wenn sämtliche echte additive Untergruppen von endlich vielen Erzeugenden in der Gestalt $R\,r$ darstellbar sind ($r \in R$).

Der Ring J der ganzen Zahlen hat sowohl die Eigenschaft E_1 als auch die Eigenschaft E_2. In einem Ringe mit der Eigenschaft E_2 deckt sich die gruppentheoretische Erzeugung mit der ringtheoretischen Erzeugung, da sämtliche Untergruppen gleichzeitig Linksideale sind. Die kommutativen Ringe mit der Eigenschaft E_1 sind (nach der Terminologie von *L. Rédei*) „Vollidealringe im weiteren Sinn" (d. h. sämtliche Unterringe erweisen sich als zweiseitige Ideale) [8]. Es gibt auch nicht kommutative Ringe mit der Eigenschaft E_2. Z. B. $R(p)=\{x, y\}$, p Primzahl, $p\,x = p\,y = y\,x - x = y^2 - y = 0$, wo der Unterring $\{M\}$ von der Teilmenge M von R erzeugt ist. Man wird hingegen sehen, daß nur ein kommutativer Ring die Eigenschaft E_1 haben kann. Die Grundbegriffe der modernen Algebra sind z. B. in den Büchern [1], [4], [5] und [6] zu finden, daher machen wir keine terminologische Bemerkung, aber man soll betonen, daß ein zyklischer Ring (d. h. Ring mit

[1] Dem Andenken meines verehrten Meisters *T. Szele.*

zyklischer additiver Gruppe) immer in der Gestalt $R(m, d) = \{a\}$ darstellbar ist, wo $O(a) = m$ und $a^2 = d \cdot a$, $d \mid m$. Die Elemente $f_1, f_2, \ldots$ werden linearunabhängig genannt, wenn aus $\sum\limits_{j} n_j f_j = 0$ immer $n_j f_j = 0$ folgt (n_j eine Zahl, und die Summe „endlich"). Nach dem Lemma von Zorn gibt es in R^+ eine maximale linearunabhängige Menge M der Elemente von R^+ und (während zu der Menge M nur Elemente von 0- und Primzahlpotenz-Ordnung) wird die Mannigfaltigkeit von M (der s. g. Rang) invariant für R^+. Wir bezeichnen den Primkörper von der Ordnung p mit K_p und die ringtheoretische direkte Summe mit $R = \sum\limits_{\alpha} S_\alpha$.

Es gilt der folgende

Satz 1. Ein beliebiger Ring R hat die Eigenschaft E_1 dann und nur dann, wenn $R \simeq J/(m)$, $(m = 0, 1, 2, \ldots)$.

Beweis. Es ist hinreichend zu zeigen, daß ein Ring mit der Eigenschaft E_1 das homomorphe Bild von J ist. Nach der Eigenschaft E_1 ist klar, daß $S = R\,r \subseteq R\{r\} \subseteq \{r\}$ gilt, dementsprechend im Falle $R = R.a$ offenbar folgt $R = \{a\}$. Aber $R = R.a$ bedeutet die Existenz eines Elements $b \neq 0$ mit $a = b\,a$, und so wird das Linksideal $L = \{b\}\,a$ zyklisch.

Es gilt $R = \{a\} = \{b\,a\} \subseteq \{b\}\,a = L$, also ist R selbst zyklisch und $R(m, d) = \{a\}$. Wenn $m = 0$ (d. h. $O(a) = 0$), ist $R = R(l\,a)$ und deswegen $a = k\,a \cdot l\,a$, wo $k, l \in J$. So gilt nach $a^2 = d\,a$ offenbar $1 = k\,l \cdot d$ und $d \mid 1$, also $R \simeq J$. Aber im Falle $m > 0$ und $d \mid m$ besteht gleichfalls $1 \equiv k\,l\,d \pmod{m}$ und hieraus $1 \equiv 0 \pmod{d}$, d. h. $d = 1$ und $R \simeq T/(m)$, womit der Satz 1 bewiesen ist.

Bemerkung. Die Ringe $K_2 + K_2$, $R(p)$, $R(p, 0)$ und $R(p^m, p)$ haben nicht die Eigenschaft E_1, aber alle ihre *echten* Unterringe S sind in der Gestalt $R\,r$ darstellbar. Man durchschaut nicht sehr schwer das Problem; zu charakterisieren alle Ringe, deren sämtliche *echten* Unterringe von der Form $R\,r$ sind. Diesmal geben wir nur die Aufzählung der Ringe mit der Eigenschaft E_2.

Satz 2. Ein beliebiger Ring R hat die Eigenschaft E_2 dann und nur dann, wenn er ein Ring von dem Type $R(0, 1)$, $R(p, 0)$, $R(m, 1)$, $R(p^m, p)$, $R(p)$, $K_2 + K_2$ oder $R = \sum\limits_{p \in \Pi} R(p^k, 1)$ ist, wo Π^* eine wenigstens zwei Primzahlen enthaltende Untermenge von der Menge Π aller verschiedenen Primzahlen ist.

Folgerung. *Ein beliebiger Ring R hat die Eigenschaft E_2^* (d. h. daß sämtliche echte Untergruppen in der Gestalt $R\,r$ darstellbar sind* ($r \in K$)) *dann und nur dan, wenn er von dem Type $R(0, 1)$, $R(p, 0)$, $R(m, 1)$, $R(p^n, p)$, $R(p)$ oder $K_2 + K_2$ ist.*

Die Rechtfertigung dieser Folgerung ist nach dem Satz 2 trivial.

Beweis: Es sei R ein Ring mit der Eigenschaft E_2. Nehmen wir an, daß R^+ eine torsionsfreie Gruppe ist. Wenn R^+ nicht von dem Rang 1 wäre, sondern a und b sich linearunabhängig erweisen, dann wäre $R = \{a, b\} = \{2\,a, b\}$, was unmöglich ist. (Wegen $S = R\,r \subseteq R\{r\} \subseteq \{r\}$ ist jede echte additive Untergruppe von endlich vielen Erzeugenden ein zyklisches Linksideal von R. Ähnlich kann man zeigen, daß R^+ nicht eine gemischte Gruppe ist.) Folglich ist R^+ eine Untergruppe der Gruppe der rationalen Zahlen. R ist kein Zeroring, also R hat keinen Nullteiler. Es sei $\{e\} = R\,r \neq 0$, dann ist wegen $R^+ \simeq (R\,r)^+$ auch R zyklisch, d. h. $R = \{e\} = R(0, d)$. Nun enthält $(d + 1)\,R = R(l\,e)$ die Existenz der Zahl $k \in J$, für welche $(d + 1)\,e = (k\,e)\,(l\,e) = k\,l\,d\,e$, d. h. $d \mid 1$ und $R \simeq R(0, 1) \simeq J$.

Es sei nun R ein p-Ring. Wenn R den Rang 1 hat, dann ist R^+ zyklisch, weil er offenbar nicht algebraisch abgeschlossen sein kann [2]. Es ist trivial, daß $R \simeq R(p, 0)$, $R(p^k, 1)$ oder $R \simeq R(p^k, p)$. Wenn aber R^+ nicht von dem Rang 1 ist, soll offenbar $O(R) = p^2$ sein. Nehmen wir an, daß für jedes Element $x \neq 0$ auch $x^2 \neq 0$ besteht. In der Dekomposition $R^+ = \{x\}^+ - \{y\}^+$ kann man x und y so wählen, daß $x^2 = x$ und $y^2 = y$ besteht. Wir zeigen jetzt die Kommutativität von R. Wenn nämlich $x\,y = a\,y \neq y\,x = b\,x$ wäre $(a, b \in J)$, dann ist a oder b durch p nicht teilbar. Aber $b\,x = x(b\,x) = x\,y\,x = (a\,y)\,x = ab\,x$ und $a\,y = y(a\,y) = y\,x\,y = (b\,x)\,y = a\,b\,y$ zeigt, daß $ab \equiv a \equiv b \pmod{p}$ und $p \nmid a$, $p \nmid b$, d. h. $a \equiv b \equiv 1 \pmod{p}$ und $x\,y = y$; $y\,x = x$. Wegen $\{x\} \cap \{y\} = \{0\}$ ist offenbar $z = x - y \neq 0$, wobei $z^2 = (x - y)\,(x - y) = x^2 - xy - yx + y^2 = x - y - x + y = 0$ besteht, was ein Widerspruch ist. Folglich ist R kommutativ. Wegen $(x + 2\,y)^2 \in \{x + 2\,y\}$ gilt $p = 2$ und $R \simeq K_2 + K_2$, wo K_p ein Primkörper ist. Nehmen wir an, daß ein Element $x \neq 0$ mit $x^2 = 0$ existiert. Wir zeigen, daß $R \simeq R(p)$. Wenn $R^+ = \{x\}^+ + \{y\}^+$ und $x\,y = a\,y$, $y\,x = b\,x$, $y^2 \in \{y\}$, $a, b \in J$ besteht $0 = x^2\,y = x(a\,y) = a^2\,y$, d. h. $p \mid a$ und $x\,y = 0$. Wäre $yx = 0$, so sollte $y^2 \neq 0$ sein (da R kein Zeroring ist), folglich wäre bei geeignetem Wählen von y notwendig $y^2 = y$, d. h. mit einem $x\,c + d\,y \in R$ und mit $m\,x + n\,y \in R$ $(c, d, m, n \in J)$ $\{x\} = R(c\,x + d\,y)$ und dementsprechend wäre $x = (m\,x + n\,y) \cdot (c\,x + d\,y) = n\,d\,y^2 = n\,d\,y \in \{y\}$ was ein Widerspruch ist. Also ist $y\,x = b\,x$ mit $p \nmid b$. Nehmen wir an, daß $y^2 = y$, so besteht $y^2 x = y(b x) = b^2 x \neq 0$ und $y^2 \neq 0$. Aber wegen $y^2 x = y x$ folgt $b \equiv 1 \pmod{p}$, d. h. $y x = x$ und $R \simeq R(p)$.

Wenn aber R kein p-Ring ist, hat jede p-Kompomemte R_p, als ein endomorphes Bild von R (im ringtheoretischen Sinn), die Eigenschaft E_2. Dann ist höchstens $R_p = R(p)$, $R(p, 0)$, $R(p^k, p)$ oder $R(p^k, 1)$. $R(p)$ sollte ein zyklischer Unterring von R sein $(R(p) \subset R)$, was unmöglich ist, d. h. $R_p \neq R(p)$. Wegen Definition der Eigenschaft E_2 besteht notwendig auch $R_p \neq R(p, 0)$. Wir zeigen nun, daß $R_p \neq R(p^k, p)$. Wenn $R_{p_1} = R(p_1^{k_1}, p_1) = \{a_1\} \subset R$ wäre, dann bekämen wir für $R = \sum_{p_\nu \varepsilon \Pi^*} \{a_\nu\}$ (Π^* eine wenigstens zwei Primzahlen erhaltende Teilmenge der Menge Π aller Primzahlen) notwendig:

$$S = \{a_1\} + \sum_{p_1 \neq p_\nu \varepsilon \Pi^{**}} \{p_\nu a_\nu\} = R r$$

wo Π^{**} eine endliche Teilmenge von Π^*.

Nehmen wir an, daß $r = m(a_1 + \sum_{p_1 \neq p_\nu \varepsilon \Pi^{**}} a_\nu)$ mit $m \in J$. Es sei $a_\nu^2 = \delta_\nu a_\nu$ und $\delta_\nu \mid p_\nu$. Dann existierte eine Zahl $n \in J$, für welche

$$a_1 + \sum_{p_1 \neq p_\nu \varepsilon \Pi^{**}} p_\nu a_\nu = m\, n(p_1 a_1 + \sum_{p_1 \neq p_\nu \varepsilon \Pi^{**}} \delta_\nu a_\nu)$$

bestände, d. h. $m n p_1 \equiv 1 \pmod{p_1^{k_1}}$ und $p_1 \mid 1$, was unmöglich ist. Folglich ist $R = \sum_{p \varepsilon \Pi^*} R(p^k, 1)$. Der andere Teil des Beweises des Satzes 2 ist trivial, womit der Satz bewiesen ist.

Literatur

[1] *N. Jacobson*: Lectures in abstract algebra, *New-York* (1951).

[2] *A. Kertész*: On fully decomposable abelian torsion groups, *Acta Math. Acad. Sci. Hungar* 3 (1952) 225—232.

[3] *A. Kertész* and *T. Szele*: Abelian groups every finitely generated subgroup of which is an endomorphie image *Acta. Sci. Math. Szeged* 15 (1953) 70—76.

[4] *A. G. Kurosch*: Gruppentheorie, 2-te Edition, *Moskau* (1953).

[5] *G. Pickert*: Einführung in die höhere Algebra, *Göttingen* (1951).

[6] *L. Rédei*: Algebra I., *Budapest* (1954).

[7] *L. Rédei*: Die Vollidealringe, *Monatshefte f. Math. Wien.* 56 (1952), 89—95.

[8] *L. Redéi:* Die Vollidealringe im weiteren Sinn, *Acta Math. Acad. Sci. Hungar* 3 (1952), 243—268.

[9] *F. Szász*: On groups every subgroup of which is a power of the group, *Acta Math. Acad. Sci. Hungar* 6 (1955) 475—477.

[10] *F. Szász*: On rings every subring of which is a multiple of the ring, *Publ. Math. Debrecen* 4 (1956) 237—238.