Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 26 (1952)

Artikel: Über Ringe mit gemeinsamer multiplikativer Halbgruppe.
Autor: Rédei, L. / Steinfeld, O.
DOI: https://doi.org/10.5169/seals-21271

Über Ringe mit gemeinsamer multiplikativer Halbgruppe

Von L. Rédei und O. Steinfeld in Szeged (Ungarn)

§ 1. Unter einer Halbgruppe verstehen wir wie üblich eine multiplikative assoziative Struktur. In einem Ring R bilden die Elemente sowohl eine Halbgruppe $R^\times$ als auch einen Modul R^+, diese nennen wir kurz die Halbgruppe bzw. den Modul von R.

Es ist eine wichtige Frage, wie weit R durch die eine der Strukturen R^+, $R^\times$ bestimmt ist. Genauer gesprochen, es läßt sich bei einem gegebenen Modul M bzw. bei einer gegebenen Halbgruppe H nach allen Ringen R fragen, für die

$$R^+ = M \tag{1}$$

bzw.

$$R^\times = H \tag{2}$$

gilt.

Bei jedem M ist stets mindestens ein Ring R mit (1) vorhanden, nämlich der Zeroring mit dem Modul M. (Unter einem Zeroring versteht man einen Ring, in dem alle Elementenprodukte gleich 0 sind.) Nach Szele[1]) gibt es nur ganz wenige Moduln M, für die (1) nur den Zeroring zur Lösung hat. Man weiß auch, daß im allgemeinen geeignete Unterringe des vollen Endomorphismenringes von M Lösungen von (1) liefern.

Problem (2) scheint schon auf den ersten Blick viel schwieriger zu sein. Vor allem gibt es offenbar sehr viele Halbgruppen H, für die (2) keine Lösungen hat, ferner scheint es, daß bei vielen H (bis auf Isomorphie) nur ein R mit (2) vorhanden ist[2]).

---

[1]) *T. Szele*, Zur Theorie der Zeroringe, Math. Ann. 121 (1949) 242—246.

[2]) Entsprechend dem abstrakt-algebraischen Standpunkt betrachten wir zwei isomorphe Ringe R, S mit $R^\times = S^\times = H$ als *gleiche* Lösungen von (2). Hierüber bemerken wir folgendes. Bezeichne R eine Lösung von (2). Man nehme einen Automorphismus A von H und ersetze die Addition $\alpha + \beta$ in R durch

$$\alpha \oplus \beta = A(A^{-1}\alpha + A^{-1}\beta) .$$

So entsteht ein zu R isomorpher Ring S (dabei wird R auf S durch $\alpha \to A\alpha$ isomorph abgebildet), der ebenfalls eine Lösung von (2) ist, und alle zu R isomorphen Lösungen S von (2) entstehen (eventuell mehrmals) auf diese Weise.

In Paragraph 2 betrachten wir ein interessantes Beispiel für den Fall, daß (2) nur eine Lösung R hat. In Paragraph 3 machen wir einige weitere Bemerkungen über Problem (2).

§ 2. Satz. *Bezeichne R den Restklassenring der ganzen Zahlen mod p^e ($p \neq 2$ Primzahl, $e \geqq 1$). Wenn $e \neq 2$, so gibt es bis auf Isomorphie nur einen Ring S mit $S^\times = R^\times$, nämlich $S = R$. Wenn $e = 2$, so gibt es genau zwei nichtisomorphe Lösungen, nämlich R und einen anderen Ring S.* (Im Beweis werden wir diesen S genau angeben, und so wird sich herausstellen, daß für ihn auch schon R^+, S^+ nichtisomorph sind.)

Wir bemerken, daß die zweite Hälfte des Satzes auch für $p = 2$ richtig ist, und es scheint uns, daß das auch für die erste Hälfte zutrifft, wir haben aber verzichtet, diese Frage genau zu untersuchen, da wir das nur mit sehr vielen Rechnungen machen könnten.

Zum Beweis des Satzes bezeichne S einen zu R nichtisomorphen Ring mit

$$S^\times = R^\times \ . \tag{3}$$

Wir haben zu zeigen, daß S nur im Fall $e = 2$ existiert und dann bis auf Isomorphie eindeutig bestimmt ist. Der Fall $e = 1$ ist trivial, weshalb wir

$$e \geqq 2$$

annehmen. Die Elemente von R bezeichnen wir mit kleinen griechischen Buchstaben; diese sind dann wegen (3) auch die Elemente von S. Kleine lateinische Buchstaben bezeichnen ganze Zahlen. Die Summe von α und β bezeichnen wir in S mit $\alpha + \beta$, das Produkt dürfen wir wegen (3) in beiden Ringen mit $\alpha\beta$ bezeichnen. Wenn wir $a\alpha$ schreiben, so soll das stets in S gedeutet werden (in R hätte $a\alpha$ einen anderen Sinn). Bezeichne ε das gemeinsame Einselement.

Die regulären Elemente von R bilden eine zyklische Gruppe von der Ordnung $p^e - p^{e-1}$. Deshalb gibt es ein Element α mit

$$\alpha^{p^{e-2}} \neq \varepsilon \ , \qquad \alpha^{p^{e-1}} = \varepsilon \ . \ , \tag{5}$$

In einem beliebigen kommutativen Ring T bilden die nilpotenten Elemente einen Unterring, der mit T_0 bezeichnet werden soll. Offenbar gilt $O(R_0) = p^{e-1}$. Wegen (3) ist auch S kommutativ, deshalb existiert der Ring S_0. Dieser besteht wieder wegen (3) aus denselben Elementen wie R_0, folglich gilt

$$O(S_0) = p^{e-1} \ . \tag{6}$$

Wir bezeichnen mit $\omega_1, \ldots, \omega_s$ eine unabhängige Basis des Moduls S_0^+ und setzen

$$o^+(\omega_i) = p^{e_i} \qquad (i = 1, \ldots, s) \ , \tag{7}$$

wobei o^+ die additive Ordnung der Elemente in S bezeichnet. Dann gilt wegen (6)

$$e_1 + \cdots + e_s = e - 1 \ . \tag{8}$$

Dabei dürfen wir

$$e_1 \geqq \cdots \geqq e_s (\geqq 1) \tag{9}$$

annehmen.

Wegen (6) hat S_0^+ den Index p in S^+, deshalb gilt $p\varepsilon \in S_0$. Andererseits nimmt $o^+(\varrho)(\varrho \in S)$ sein Maximum für $\varrho = \varepsilon$ an, folglich läßt sich nach (7), (9)

$$o^+(\varepsilon) = p^{\bar{e}} \ , \qquad e_1 \leqq \bar{e} \leqq e_1 + 1 \tag{10}$$

setzen.

Da S_0 nilpotent ist, gibt es ein n mit $S_0 \supset S_0^2 \supset \cdots \supset S_0^n = 0$. (Es ließe sich $n = e-1$ zeigen.) Dies und (6) ergeben $O(S_0^k) \leqq p^{e-k}$ $(k = 1, \ldots, e)$. Wegen $\omega_i^k \in S_0^k$ folgt hieraus

$$o^+(\omega_i^k) \leqq p^{e-k} \qquad (i = 1, \ldots, s; \ k = 1, \ldots, e) \ . \tag{11}$$

Wegen (5) ist α kein Element von S_0, folglich läßt sich nach obigem

$$\alpha \equiv a\varepsilon \ (\mathrm{mod}\ \omega_1, \omega_2, \ldots) \qquad (p \nmid a) \tag{12}$$

setzen (dabei dürfte man sogar $0 < a < p$ vorschreiben). Wir behaupten für $k = 0, 1, \ldots$

$$\alpha^{p^k} \equiv a^{p^k}\varepsilon \ (\mathrm{mod} \ldots, p^t \omega_i^{p^{k-t}}, \ldots) \ (i = 1, \ldots, s; \ t = 0, \ldots, k) \ , \tag{13}$$

wobei man für i und t voneinander unabhängig alle angeschriebenen Werte einzusetzen hat. Für $k = 0$ stimmt (13) mit (12) überein. Man nehme (13) für ein k an. Das bedeutet

$$\alpha^{p^k} = a^{p^k}\varepsilon + \sum p^t \omega_i^{p^{k-t}} \alpha_{it}$$

mit irgendwelchen Elementen $\alpha_{it} (\in S)$. Erhebt man diese Gleichung zur p-ten Potenz, so folgt aus dem Polynomialsatz sofort die Richtigkeit von (13) für $k + 1$, also auch allgemein.

Wir zeigen, daß es ein Paar i, t mit

$$p^t \omega_i^{p^{e-2-t}} \neq 0 \qquad (i = 1, \ldots, s; \ t = 0, \ldots, e-2) \tag{14}$$

gibt. Sonst wäre nämlich nach (13)

$$\alpha^{p^{e-2}} = a^{p^{e-2}} \varepsilon \ .$$

Dies und (5_1), (10_1) ergeben

$$a^{p^{e-2}} \not\equiv 1 \pmod{p^{\bar{e}}} \ .$$

Andererseits folgt aus voriger Gleichung und aus (5_2), (10_1)

$$a^{p^{e-1}} \equiv 1 \pmod{p^{\bar{e}}} \ .$$

Beide ergeben $\bar{e} \geqq e$. Wegen $O(S) = p^e$ muß $\bar{e} \leqq e$ gelten, somit haben wir $\bar{e} = e$. Das bedeutet nach (10), daß S^+ zyklisch ist mit dem Erzeugenden ε. Dann ist aber S isomorph zu R, mit diesem Widerspruch wurde die Behauptung über (14) bewiesen.

Aus (14) folgt

$$o^+(\omega_i^{p^{e-2-t}}) \geqq p^{t+1} \ , \tag{15}$$

also nach (11)

$$e - p^{e-2-t} \geqq t + 1 \ .$$

Schreibt man dies in der Form

$$1 + (e - 2 - t) \geqq p^{e-2-t} \ ,$$

so sieht man, daß wegen $p \geqq 3$ nur $e - 2 - t = 0$, das heißt $t = e - 2$, möglich ist. Dies in (15) eingesetzt besagt

$$o^+(\omega_i) \geqq p^{e-1} \ .$$

Wegen (6) muß hier $=$ gelten. Mit (7), (8) zusammen ergibt dies $s = 1$, $e_1 = e - 1$ [3]), ferner muß nach (10)

$$o^+(\varepsilon) = p^{e-1} \tag{16}$$

gelten, da $o^+(\varepsilon) = p^e$ wie schon bemerkt unmöglich ist. Man schreibe einfacher $\omega_1 = \omega$, so haben wir nach vorigem

$$o^+(\omega) = p^{e-1} \ , \tag{17}$$

dabei ist S_0^+ der durch ω erzeugte zyklische Modul.

Wegen $p\varepsilon \in S_0$ gilt

$$p\varepsilon = c\omega \ .$$

---

[3]) Wäre $p = 2$, so könnte man auf ähnlichem Wege nur auf $e - 4 \leqq e_1 \leqq e - 1$ schließen, und dann müßte man wegen (8) noch eine Anzahl Fallunterscheidungen machen.

Hieraus und aus (16), (17) folgt $p \mid c$, also $c = pd$, $p(\varepsilon - d\omega) = 0$,

$$o^+(\varepsilon - d\omega) \leqq p \ .$$

Nun ist aber $\varepsilon - d\omega$ ein reguläres Element von S, und alle regulären Elemente haben dieselbe additive Ordnung wie ε, folglich gilt $o^+(\varepsilon) \leqq p$. Dies mit (4), (16) zusammen besagt

$$e = 2 \ , \tag{18}$$

$$o^+(\varepsilon) = p \ , \tag{19}$$

ferner gilt nach (17) auch

$$o^+(\omega) = p \ . \tag{20}$$

Außerdem folgt noch aus (11) für $k = 2$

$$\omega^2 = 0 \ . \tag{21}$$

Endlich ist durch die Bedingungen (19) bis (21) der Ring S mit den Basiselementen ε, ω und dem Einselement ε bis auf Isomorphie vollständig charakterisiert. Seine Elemente sind die

$$\beta = a\,\varepsilon + b\,\omega \qquad (a, b = 0, \ldots, p-1) \ .$$

Man hat noch zu zeigen, daß $S^\times$ isomorph zu $R^\times$ und S nichtisomorph zu R ist. Die verschiedenen Elemente von S lassen sich auch in der Form

$$(g\,\varepsilon + \omega)^k, \ \ l\,\omega \qquad (k = 1, \ldots, p^2 - p; \ \ l = 0, \ldots, p-1)$$

annehmen, wobei g eine feste primitive Zahl $\bmod p^2$ bezeichnet, die man auch primitiv $\bmod p^2$ annehmen darf. Werden dann diesen Elementen bzw. die Restklassen

$$g^k, \ p\,l \ (\bmod p^2)$$

zugeordnet, so ist das offenbar eine isomorphe Abbildung von $S^\times$ auf $R^\times$. Andererseits ist S^+ nach (19), (20) nichtzyklisch, also nichtisomorph zu R^+. Den Satz haben wir bewiesen.

§ 3. Als eine direkte Folgerung aus dem Satz von Wedderburn über die endlichen Schiefkörper bemerken wir folgendes:

Bezeichne H eine endliche Halbgruppe, die aus einer Gruppe und einem Nullelement besteht. Dann und nur dann hat (2) *eine Lösung R, wenn die genannte Gruppe zyklisch von der Ordnung $p^n - 1$ ist (p Primzahl).*

Wenn das gilt, so hat (2) *zur einzigen Lösung* R *den endlichen Körper mit* p^n *Elementen.*

Wir bemerken noch folgende Tatsachen, von denen 1), 2), 4) trivial sind und sich auch 3) leicht beweisen ließe:

Bezeichne K *einen absolut algebraischen Zahlkörper* n*-ten Grades,* r_1 *und* $2r_2$ *die Anzahl der reellen bzw. komplexen Konjugierten von* K ($r_1 + 2r_2 = n$), e *die Anzahl der Einheitswurzeln in* K, K_g *den Ring der (algebraisch) ganzen Elemente von* K, $\mathfrak{C}$ *die (absolute) Idealklassengruppe von* K_g *und* $J(\mathfrak{C})$ *das Invariantensystem von* $\mathfrak{C}$. *Bis auf Isomorphie ist bzw.*

1) $K^\times$ *durch* e ,
2) K^+ *durch* n ,
3) $K_g^\times$ *durch* e , $r_1 + r_2, J(\mathfrak{C})$,
4) K^+ *durch* n

eindeutig bestimmt. (Bezüglich 2) und 4) gilt noch mehr, und zwar weiß man, daß K^+ und K_g^+ der n-dimensionale Vektorraum über dem Körper der rationalen Zahlen bzw. über dem Ring der ganzen Zahlen ist.)

Da zwei Körper K dann und nur dann isomorph sind, wenn sie konjugiert sind, ferner entsprechendes auch für die Ringe K_g gilt, so bekommt man hieraus eine Fülle von Beispielen für Halbgruppen H, für die (2) mehrere (sogar eventuell unendlich viele) nichtisomorphe Lösungen R hat, darunter auch solche nichtisomorphen Lösungen $R, S, \ldots$, für die $R^+, S^+, \ldots$ isomorph sind. So zum Beispiel sind nach 1), 2) für alle totalreellen K vom n-ten Grad (für diese gilt $e = 2$) sowohl die entsprechenden $K^\times$ als auch die K^+ miteinander isomorph[4]). Die meisten Ringe R scheinen uns aber wie gesagt durch $R^\times$ (bis auf Isomorphie) eindeutig bestimmt zu sein.

(Eingegangen den 28. Juni 1951, umgearbeitet den 6. Februar 1952)

[4]) Darauf hat uns freundlichst Herr Professor de Rham mit dem Beispiel der durch $\sqrt{2}$, $\sqrt{3}$ erzeugten Zahlkörper aufmerksam gemacht.