Über Semiringe mit multiplikativer Kürzungsregel

Von O. STEINFELD in Budapest

Herrn Professor Béla Szőkefalvi-Nagy zum 50. Geburtstag gewidmet

§ 1

Unter einem *Semiring* verstehen wir eine (nichtleere) Menge $S=\{\alpha, \beta, \gamma, \ldots\}$, in der eine Addition und eine Multiplikation mit den folgenden Eigenschaften definiert sind: (i) S ist eine additive Halbgruppe, (ii) S ist eine multiplikative Halbgruppe, (iii) die links- und rechtsseitigen Distributivitätsregeln $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$ und $(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$ sind auch gültig.

Das Element 0 von S heißt *Nullelement*, wenn

$$0+\xi=\xi+0=\xi \quad \text{und} \quad 0\xi=\xi 0=0$$

für jedes $\xi(\in S)$ gelten.

Ein Semiring enthält höchstens ein Nullelement. Offenbar kann man zu jedem Semiring ein Nullelement adjungieren.

Ist die Addition in einem Semiring S kommutativ, und besitzt S ein Nullelement, so nennen wir S einen *Halbring*.

Wir sagen, daß in einem Semiring S die *linksseitige multiplikative Kürzungsregel* gilt, wenn

$$\sigma\alpha=\sigma\beta \Rightarrow \alpha=\beta \qquad (\alpha, \beta, \sigma \in S;\ \sigma \neq 0) \tag{1}$$

für jedes $\sigma(\neq 0, \sigma \in S)$ gilt.

Ähnlich definiert man die *rechtsseitige multiplikative Kürzungsregel* in einem Semiring.

Wir sagen, daß in einem *Semiring die multiplikative Kürzungsregel* gilt, wenn in ihm die linksseitige und rechtsseitige multiplikative Kürzungsregel gleichzeitig gelten.

Ein Semiring mit multiplikativer Kürzungsregel ist offenbar nullteilerfrei. Die Umkehrung dieser Behauptung ist dagegen ungültig, siehe z. B. BOURNE [1], Beispiele 2 und 3.

Es ist bekannt, daß die Charakteristik eines nullteilerfreien Ringes mit mindestens zwei Elementen 0 oder eine Primzahl ist. (Siehe z. B. RÉDEI [2], Satz 38.)

Wir wollen in dieser Arbeit ein Analogon dieses Resultates für Semiringe mit linksseitiger (rechtsseitiger) multiplikativer Kürzungsregel beweisen. (S. Satz 1.)

J. SZENDREI hat in seiner Arbeit [4] bewiesen, daß es zu jedem nullteilerfreien Ring einen ebensolchen „minimalen" Oberring mit Einselement gibt.

In Satz 2 werden wir beweisen, daß ein ähnliches Ergebnis über Halbringe mit multiplikativer Kürzungsregel gilt.

§ 2

Zur Vorbereitung betrachten wir nun eine multiplikative Halbgruppe $H=\{\alpha, \beta, \gamma, \ldots\}$.

Wir sagen, daß ein Element $\alpha(\in H)$ von *endlicher Ordnung* bzw. *unendlicher Ordnung* ist, je nachdem unter den Potenzen $\alpha, \alpha^2, \ldots$ nur endlich viele oder unendlich viele verschiedene Elemente vorkommen. Im ersten Fall bezeichnen wir mit $o(\alpha)$ die Anzahl der verschiedenen Elemente unter den Potenzen $\alpha, \alpha^2, \ldots$. Es ist bekannt (s. z. B. RÉDEI [2], § 20):

Ist α von unendlicher Ordnung, so besteht die Folge $\alpha, \alpha^2, \ldots$ aus lauter verschiedenen Gliedern. Im Falle $o(\alpha)=n$ ist die Folge $\alpha, \alpha^2, \ldots$ stets von der Form

$$\alpha, \alpha^2, \ldots, \alpha^{k-1}, \alpha^k, \ldots, a^n;\ \alpha^{n+1}=\alpha^k, \ldots, \alpha^{2n}=\alpha^{n+k-1} \qquad (1 \leqq k \leqq n), \tag{2}$$

wobei $\alpha, \ldots, \alpha^n$ verschieden sind. Die Elemente $\alpha^k, \alpha^{k+1}, \ldots, \alpha^n$ bilden eine zyklische Gruppe $\langle\alpha\rangle$ von der Ordnung $n-k+1$.

Es folgt aus den obigen, daß man zu jedem Element $\alpha(\in H)$ von endlicher Ordnung zwei eindeutig bestimmte natürliche Zahlen $o(\alpha)=n$ und $s(\alpha)=k$ zuordnen kann, wobei $o(\alpha)=n$ die Ordnung von α und $s(\alpha)=k$ die *Sprungstelle* von α d. h. die kleinste natürliche Zahl k mit $\alpha^{n+1}=\alpha^k$ $(1 \leqq k \leqq n)$ bezeichnen.

Das folgende Ergebnis ist unseres Wissens neu und es stammt im wesentlichen von A. RÉNYI.

Hilfssatz. *Hat das Element α einer Halbgruppe H die Ordnung $o(\alpha)=n$H und die Sprungstelle $s(\alpha)=k$, so gilt*

$$o(\alpha^r) = m + \frac{n-k+1}{(n-k+1, r)} \quad \text{und} \quad s(\alpha^r) = m+1 \qquad (1 \leqq r \leqq n), \tag{3}$$

wobei $k = mr+j$ $(0 \leqq m;\ 1 \leqq j \leqq r)$ besteht.

Beweis. Nach der Voraussetzung ist $m+1$ die kleinste natürliche Zahl mit $(m+1)r \geqq k$, deshalb ist $\alpha^{(m+1)r}=\alpha^{k+u}$ $(0 \leqq u \leqq n-k)$ ein Element der Gruppe $\langle\alpha\rangle$. Wir haben die kleinste natürliche Zahl x mit $\alpha^{k+u+xr}=\alpha^{k+u}$ zu bestimmen. Da $\alpha^{k+u+xr}=\alpha^{k+u} \Leftrightarrow k+u+xr \equiv k+u \pmod{n-k+1}$ gilt, besteht $x=\dfrac{n-k+1}{(n-k+1, r)}$.

Damit ist der Hilfssatz bewiesen.

§ 3

In einem Semiring kann man über die *additive Ordnung* $o^+(\alpha)$ und über die *multiplikative Ordnung* $o^\times(\alpha)$ ferner über die *additive Sprungstelle* $s^+(\alpha)$ und über die *multiplikative Sprungstelle* $s^\times(\alpha)$ eines Elementes sprechen.

Gilt $o^+(\alpha)=\infty$ in einem Semiring S für alle $\alpha(\neq 0)$, so verstehen wir unter der *Charakteristik* von S die Zahl 0. Gibt es dagegen eine natürliche Zahl n, so daß stets $o^+(\alpha)=m$ und $m|n$ gelten, dann nennen wir die kleinste solche Zahl n die Charakteristik von S. In jedem anderen Fall habe S die Charakteristik ∞.

Satz 1. *Die Charakteristik eines Semiringes mit linksseitiger (rechtsseitiger) multiplikativer Kürzungsregel ist entweder* 0 *oder* 1, *oder aber eine Primzahl* p. *Im letzteren Falle hat jedes Element* $\alpha(\neq 0)$ *die additive Sprungstelle* 1, *d. h. die Elemente* $\alpha, 2\alpha, \ldots, p\alpha$ *bilden eine p-Gruppe.*

Beweis. Ist die additive Ordnung jedes Elementes $\alpha(\neq 0)$ von S unendlich, so ist nichts zu beweisen.

Es sei $\alpha(\neq 0)$ ein Element von der endlichen, additiven Ordnung $o^+(\alpha)=n$ und von der additiven Sprungstelle $s^+(\alpha)=k$. Wir zeigen, daß jedes Element $\beta(\neq 0)$ von S dieselbe additive Ordnung n und dieselbe additive Sprungstelle k hat.

Betrachten wir die Elemente $\beta, 2\beta, \ldots, n\beta$. Wäre

$$m\beta = l\beta \qquad (1 \leqq l < m \leqq n)$$

gültig, so bestände

$$m\beta\alpha = l\beta\alpha = \beta m\alpha = \beta l\alpha \Rightarrow m\alpha = l\alpha \qquad (1 \leqq l < m \leqq n),$$

was der Annahme $o^+(\alpha)=n$ widerspricht. So gilt $o^+(\alpha) \leqq o^+(\beta)$. Wir werden einsehen, daß der Fall $o^+(\alpha) < o^+(\beta)$ unmöglich ist. Wären nämlich die Elemente $\beta, 2\beta, \ldots, n\beta, \ldots, r\beta (r > n)$ alle verschieden, so wäre wegen $o^+(\alpha)=n$

$$r\alpha = s\alpha \qquad (1 \leqq s \leqq n < r)$$

gültig, woraus wegen $r\alpha\beta = s\alpha\beta = \alpha r\beta = \alpha s\beta$ der Widerspruch $r\beta = s\beta$ $(1 \leqq s < r)$ folgte.

Damit ist

$$o^+(\alpha) = o^+(\beta) = n \qquad \text{(für jedes } \beta \neq 0, \in S) \tag{4}$$

bewiesen.

Da man die Äquivalenz $(n+1)\alpha = k\alpha \Leftrightarrow (n+1)\beta = k\beta$ leicht einsehen kann, ist auch $s^+(\alpha) = s^+(\beta)$ richtig.

Es wird gezeigt, daß $o^+(\alpha)=n$ entweder 1 oder eine Primzahl p sein muß. Im entgegengesetzten Falle wäre $p|n$ ($p < n$, p eine Primzahl) gültig. Man bekommt aus dem Hilfssatz

$$o^+(p\alpha) \leqq n-1 \qquad \text{für jede Sprungstelle } s^+(\alpha). \tag{5}$$

Da wegen $o^+(\alpha) = n > p$ das Element $p\alpha$ von Null verschieden ist, steht (5) im Widerspruch mit (4).

Wir haben noch zu beweisen, daß im Falle $o^+(\alpha)=p$ die Behauptung $s^+(\alpha)=1$ besteht. Wäre nämlich $s^+(\alpha) = k \geqq 2$, so folgte aus dem Hilfssatz $s^+(k\alpha) = 1 \neq k$, was nach den Vorigen unmöglich ist.

Damit ist der Beweis von Satz 1 beendet.

§ 4

Wir schicken einige Begriffe voraus.

Eine additive Teilhalbgruppe $\mathfrak{a}$ eines Semiringes S wird ein *Ideal* von S genannt, wenn für alle Elemente $\alpha \in \mathfrak{a}$ und $\sigma \in S$

$$\alpha\sigma,\ \sigma\alpha \in \mathfrak{a}$$

gilt.

Wir sagen, daß eine Klasseneinteilung C eines Semiringes S *kompatibel* ist, wenn die der Klasseneinteilung C zugehörige Äquivalenzrelation $\equiv$ eine *Kongruenzrelation* ist, d. h. wenn für die Elemente $\varkappa, \lambda, \sigma \in S$ die Regeln

$$\varkappa \equiv \lambda \pmod{C} \Rightarrow \varkappa + \sigma \equiv \lambda + \sigma \pmod{C},\quad \sigma + \varkappa \equiv \sigma + \lambda \pmod{C} \tag{6}$$

und

$$\varkappa \equiv \lambda \pmod{C} \Rightarrow \varkappa\sigma \equiv \lambda\sigma \pmod{C},\quad \sigma\varkappa \equiv \sigma\lambda \pmod{C} \tag{7}$$

gelten. (S. z. B. RÉDEI [2], §§ 30 und 46.)

Wir betrachten eine kompatible Klasseneinteilung C eines Semiringes S. Die durch das Element $\alpha (\in S)$ repräsentierte Klasse und die Menge der Klassen bezeichnen wir mit $\bar{\alpha}$ bzw. $\bar{S}$. Definiert man in $\bar{S}$ die Verknüpfungen

$$\bar{\alpha} + \bar{\beta} = \overline{\alpha + \beta} \quad \text{und} \quad \bar{\alpha}\bar{\beta} = \overline{\alpha\beta} \qquad (\alpha, \beta \in S), \tag{8}$$

so wird $\bar{S}$ ein Semiring, den wir einen *Faktorsemiring* nennen.

Wir bezeichnen mit N den Halbring der nichtnegativen ganzen Zahlen.

Satz 2 (Vgl. SZENDREI [4] und RÉDEI [2], Satz 201). *Jeder Halbring*[1]) $R = \{\alpha, \beta, \gamma, \ldots\}$ *mit multiplikativer Kürzungsregel hat ebensolche Erweiterungshalbringe mit Einselement. Unter ihnen gibt es einen, der mit S bezeichnet werde, derart, daß die übrigen einen mit S isomorphen Teilhalbring enthalten. Dabei ist R ein Ideal von S.*

Beweis. Es bezeichne ω das Nullelement von R. Wir betrachten die Menge R_1 aller Elementenpaare (a, α), wo a bzw. α die Elemente von N bzw. von R durchlaufen. Definiert man in R_1 die Verknüpfungen

$$(a, \alpha) + (b, \beta) = (a + b, \alpha + \beta) \qquad (a, b \in \mathsf{N};\ \alpha, \beta \in R), \tag{9}$$

$$(a, \alpha)(b, \beta) = (ab, a\beta + b\alpha + \alpha\beta) \qquad (a, b \in \mathsf{N};\ \alpha, \beta \in R), \tag{10}$$

so ist es leicht einzusehen, daß R_1 ein Halbring mit dem Einselement $(1, \omega)$ ist und die Elemente der Form $(0, \xi)$ ein Ideal von R_1 bilden, welches mit dem Halbring R isomorph ist[2]).

Wir schicken die folgende *Bemerkung* voraus:

Gilt für die Elemente (m, μ), (n, ν) und $(0, \alpha)$ $(\alpha \neq \omega)$ eine der Bedingungen

$$(m, \mu)(0, \alpha) = (n, \nu)(0, \alpha);\quad (0, \alpha)(m, \mu) = (0, \alpha)(n, \nu), \tag{11}$$

[1]) Die Existenz des Nullelementes ist nur der Einfachheit halber vorausgesetzt.

[2]) Diese Erweiterung ist das Analogon der Dorrohschen Ringerweiterung.

so gelten

$$(12) \qquad (m, \mu)(0, \xi) = (n, \nu)(0, \xi) \text{ und } (0, \xi)(m, \mu) = (0, \xi)(n, \nu)$$

für jedes Element $(0, \xi)$ $(\xi \in R)$.

Aus (10) und (11) folgt nämlich $(0, m\xi + \xi\mu)(0, \alpha) = \big((0, \xi)(m, \mu)\big)(0, \alpha) = \big((0, \xi)(n, \nu)\big)(0, \alpha) = (0, n\xi + \xi\nu)(0, \alpha)$. Daraus bekommt man nach Kürzung mit dem Element $(0, \alpha)$ die Behauptung (12_2). Ähnlicherweise ist (12_1) einzusehen.

Wir betrachten die folgende Klasseneinteilung C des Halbringes R_1

$$(13) \qquad \begin{cases} (r, \varrho) \equiv (s, \sigma) \pmod{C} \leftrightarrow (r, \varrho)(0, \alpha) = (s, \sigma)(0, \alpha) \\ \text{für ein gegebenes Element } (0, \alpha) \text{ mit } \alpha \neq \omega. \end{cases}$$

Um zu zeigen, daß C eine kompatible Klasseneinteilung von R_1 ist, haben wir die Erfüllung der Regeln (6), (7) einzusehen.

Ist $(r, \varrho) \equiv (s, \sigma) \pmod{C}$, so gilt für ein beliebiges $(b, \beta) \in R_1$ die Regel $\big((r, \varrho) + (b, \beta)\big)(0, \alpha) = (r, \varrho)(0, \alpha) + (b, \beta)(0, \alpha) = (s, \sigma)(0, \alpha) + (b, \beta)(0, \alpha) = \big((s, \sigma) + (b, \beta)\big)(0, \alpha)$ d. h.

$$(r, \varrho) + (b, \beta) \equiv (s, \sigma) + (b, \beta) \pmod{C}.$$

Da ferner auch

$$(b, \beta)(r, \varrho)(0, \alpha) = (b, \beta)(s, \sigma)(0, \alpha) \Rightarrow (b, \beta)(r, \varrho) \equiv (b, \beta)(s, \sigma) \pmod{C}$$

und nach der vorausgeschickten Bemerkung

$$\big((r, \varrho)(b, \beta)\big)(0, \alpha) = (r, \varrho)\big((b, \beta)(0, \alpha)\big) = (s, \sigma)\big((b, \beta)(0, \alpha)\big) =$$

$$= \big((s, \sigma)(b, \beta)\big)(0, \alpha) \Rightarrow (r, \varrho)(b, \beta) \equiv (s, \sigma)(b, \beta) \pmod{C}$$

gelten, sind (6) und (7) für C bewiesen. Es bezeichne $\overline{(r, \varrho)}$ bzw. $\overline{R_1} = S$ die durch das Element (r, ϱ) $(\in R_1)$ repräsentierte Klasse bzw. den Faktorhalbring.

Offenbar ist $\overline{(1, \omega)}$ das Einselement von S.

Da die Elemente der Form $(0, \xi)$ $(\xi \in R)$ einen mit R isomorphen Halbring, also einen Halbring mit multiplikativer Kürzungsregel bilden, gilt nach (13)

$$(14) \qquad (0, \xi) \equiv (0, \tau) \pmod{C} \Leftrightarrow (0, \xi) = (0, \tau).$$

So bilden die Klassen der Form $\overline{(0, \xi)}$ einen mit R isomorphen Teilhalbring, sogar ein Ideal S^* von S.

Aus (13) folgt

$$(15) \qquad \overline{(c, \gamma)} = \overline{(0, \omega)} \leftrightarrow (c, \gamma)(0, \alpha) = (0, \omega).$$

Wir haben noch zu zeigen, daß die multiplikative Kürzungsregel in S gilt. Es sei

$$(16) \qquad \overline{(r, \varrho)}\,\overline{(b, \beta)} = \overline{(s, \sigma)}\,\overline{(b, \beta)} \qquad \big(\overline{(b, \beta)} \neq \overline{(0, \omega)}\big).$$

Nach (8_2), (13) und (15) folgt aus (16)

$$(17) \qquad (r, \varrho)(b, \beta)(0, \alpha) = (s, \sigma)(b, \beta)(0, \alpha) \qquad \big((b, \beta)(0, \alpha) \neq (0, \omega)\big).$$

Dies impliziert $(0, \alpha)(r, \varrho) \cdot (b, \beta)(0, \alpha) = (0, \alpha)(s, \sigma) \cdot (b, \beta)(0, \alpha)$ $\big((0, \alpha)(r, \varrho), (0, \alpha)(s, \sigma), (b, \beta)(0, \alpha) \in S^*\big)$. Da in S^* die multiplikative Kürzungsregel gilt,

besteht $(0, \alpha)(r, \varrho) = (0, \alpha)(s, \sigma)$. Nach der vorausgeschickten Bemerkung und (13) bekommt man daraus

$$\overline{(r, \varrho)} = \overline{(s, \sigma)}. \tag{18}$$

Durch ähnliche Methode wird die Implikation

$$\overline{(b, \beta)}\,\overline{(r, \varrho)} = \overline{(b, \beta)}\,\overline{(s, \sigma)} \Rightarrow \overline{(r, \varrho)} = \overline{(s, \sigma)} \qquad (\overline{(b, \beta)} \neq \overline{(0, \omega)})$$

bewiesen.

Es sei endlich T ein Erweiterungshalbring von R mit dem Einselement ε, in dem auch die multiplikative Kürzungsregel erfüllt ist. Man kann voraussetzen, daß selbst R ein Teilhalbring von T ist. Wir zeigen, daß

$$\overline{(s, \sigma)} \to s\varepsilon + \sigma \qquad (s \in N,\ \sigma \in R) \tag{19}$$

eine isomorphe Abbildung von S in T liefert.

Wegen

$$\overline{(s, \sigma)} + \overline{(t, \tau)} = \overline{(s+t, \sigma+\tau)} \to (s+t)\varepsilon + (\sigma+\tau) = s\varepsilon + \sigma + t\varepsilon + \tau$$

und

$$\overline{(s, \sigma)}\,\overline{(t, \tau)} = \overline{(st, s\tau + t\sigma + \sigma\tau)} \to st\varepsilon + s\tau + t\sigma + \sigma\tau = (s\varepsilon + \sigma)(t\varepsilon + \tau)$$

ist (19) eine homomorphe Abbildung.

Um die Eineindeutigkeit einzusehen, setzen wir voraus, daß $s\varepsilon + \sigma = t\varepsilon + \tau$ gilt. Multipliziert man diese Gleichung von rechts mit dem Element $\alpha \neq \omega$ von R, so entsteht $s\alpha + \sigma\alpha = t\alpha + \tau\alpha$. Dies bedeutet die Gültigkeit der Bedingung $(s, \sigma)(0, \alpha) = (t, \tau)(0, \alpha)$, woraus nach (13)

$$\overline{(s, \sigma)} \doteq \overline{(t, \tau)}$$

folgt[3]).

Damit ist der Beweis beendet.

Literaturverzeichnis

[1] S. Bourne, On multiplicative idempotents of a potent semiring, *Proc. Nat. Acad. Sci. U. S. A.*, **42** (1956), 632–638.
[2] L. Rédei, *Algebra* I (Leipzig, 1959).
[3] L. Rédei, *Algebra* I (Budapest–Oxford, to appear in 1964).
[4] J. Szendrei, On the extension of rings without divisors of zero, *Acta Sci. Math.*, **13** (1949–50), 231–234.

(Eingegangen am 8. September, 1962)

[3]) Vgl. den Beweis des Satzes von Szendrei in Rédei [3].