Ein hinreichendes und notwendiges Kriterium für die ZPE-Eigenschaft in kommutativen, regulären Halbgruppen

Von H. J. WEINERT in Potsdam (DDR)

In Verallgemeinerung des ZERMELOschen Beweises für den Fundamentalsatz der elementaren Zahlentheorie hat HASSE in [1] ein hinreichendes Kriterium dafür angegeben, daß in einem Integritätsbereich $\mathfrak{R}$ jede Nichteinheit ($\neq o$) als Produkt von Primelementen[1]) geschrieben werden kann, welches von KRULL in [2] zu einem hinreichenden und notwendigen Kriterium verschärft wird. Beide Kriterien (vgl. auch KRULL [3], § 5) arbeiten mit einer Art reellwertigen Bewertung und beruhen auf der Existenz gewisser Linearkombinationen, womit sie von der Ringeigenschaft von $\mathfrak{R}$ wesentlichen Gebrauch machen. In der vorliegenden Note wird gezeigt, daß sich der ZERMELOsche Beweisgedanke sogar zu einem allgemeinen Kriterium für eine Zerlegung in Primelemente (ZPE) in Halbgruppen ausbauen läßt, welches die oben genannten Kriterien als Spezialfälle enthält. Die allgemeinere Formulierung des Kriteriums macht dabei seinen Beweis einfacher und beeinträchtigt auch nicht die Handlichkeit seiner Anwendung, wofür wir abschließend einige Beispiele geben.

Für eine (kommutative und reguläre) Halbgruppe $\mathfrak{H}$ mit Einselement e[2]) lassen sich die Begriffe Teiler, Einheit, assoziierte Elemente usw. wie üblich erklären. Insbesondere verstehen wir unter einer echten Zerlegung

$$a = a_1 a_2 \ldots a_n$$

von $a \in \mathfrak{H}$ eine solche, für die $n \geqq 2$ gilt und kein $a_i \in \mathfrak{H}$ eine Einheit ist; eine Nichteinheit $r \in \mathfrak{H}$ ohne echte Zerlegungen heißt irreduzibel und sogar prim, wenn aus $r|ab$ stets $r|a$ oder $r|b$ folgt. Die Eindeutigkeit jeder Zerlegung in irreduzible Elemente (bis auf assoziierte Faktoren) ist gleichwertig damit, daß auch umgekehrt jedes irreduzible Element von $\mathfrak{H}$ prim ist. Damit läuft die Möglichkeit, jede Nichteinheit von $\mathfrak{H}$ in ein Produkt von Primelementen zu zerlegen, auf das gleiche hinaus wie die Existenz und Eindeutigkeit der Zerlegung aller Nichteinheiten von $\mathfrak{H}$ in irreduzible Elemente. Wir sagen dann, daß $\mathfrak{H}$ eine ZPE-Halbgruppe ist und zeigen, daß für diese Eigenschaft von $\mathfrak{H}$ das folgende Kriterium hinreichend und notwendig ist:

---

[1]) Entsprechend der nachstehenden Festlegung der Begriffe „irreduzibel" und „prim" (im Einklang mit KRULL [2], [3] bzw. RÉDEI [4], § 79) sind die Faktoren einer solchen Zerlegung bis auf assoziierte Elemente eindeutig bestimmt.

[2]) Übrigens gelten alle Überlegungen auch für Halbgruppen ohne Einselement, wenn man einfach alle sich auf Einheiten bzw. Assoziiertheit beziehenden Formulierungen wegfallen läßt.

Für die Elemente von $\mathfrak{H}$ läßt sich eine irreflexive, asymmetrische und transitive Relation $a \prec b$ erklären, die den nachstehenden Bedingungen genügt:

(1) *In jeder Teilmenge von $\mathfrak{H}$ existiert ein in bezug auf diese Relation minimales Element.*
(2) *Ist b keine Einheit, so gilt $a \prec ab$ für alle $a \in \mathfrak{H}$.*
(3) *Aus $a \prec b$ folgt $ac \prec bc$ für alle $c \in \mathfrak{H}$.*
(4) *Zu je zwei nicht assoziierten irreduziblen Elementen r und s von $\mathfrak{H}$ gibt es ein Element $z \in \mathfrak{H}$, welches*

$$\alpha)\ z \prec r, \quad \beta)\ s \nmid z, \quad \gamma)\ \text{aus } s \mid ra \text{ folgt } s \mid za,$$

oder die gleichen Bedingungen mit Vertauschung von r und s erfüllt.

In der Tat ist dieses Kriterium hinreichend für die ZPE-Eigenschaft von $\mathfrak{H}$. Wir gehen indirekt vor und betrachten zunächst die Menge aller Nichteinheiten von $\mathfrak{H}$, für die keine Zerlegung in irreduzible Elemente existieren sollte. In dieser Menge gibt es nach (1) ein minimales Element c, welches also nicht irreduzibel ist. Aus $c = ab$ folgt aber gemäß (2) $a \prec c$ und $b \prec c$, so daß es nach Wahl von c für a und b und damit für c Zerlegungen in irreduzible Elemente gibt. Entsprechend sei nun c ein minimales Element mit zwei wesentlich verschiedenen Zerlegungen

$$c = r_1 r_2 \ldots r_n = s_1 s_2 \ldots s_m .$$

Dabei kann kein r_i zu einem der s_j assoziiert sein, da sonst nach (2) und Wahl von c beide Zerlegungen bis auf assoziierte Elemente übereinstimmten. Wir können also etwa auf r_1 und s_1 (4) anwenden. Mit $z \prec r_1$ gilt nach (3)

$$za = zr_2 \ldots r_n \prec r_1 r_2 \ldots r_n = r_1 a = c$$

und wir erhalten

$$s_1 \mid zr_2 \ldots r_n, \quad s_1 \nmid z, \quad s_1 \nmid r_2, \ \ldots, \ s_1 \nmid r_n$$

im Widerspruch dazu, daß die Zerlegung von $zr_2 \ldots r_n \prec c$ in irreduzible Elemente nach der Wahl von c eindeutig ist.

Ist umgekehrt $\mathfrak{H}$ eine ZPE-Halbgruppe, so ist durch die Anzahl der in den Zerlegungen auftretenden Primelemente (worunter für Einheiten die Zahl 0 zu verstehen ist) eine Halbordnungsrelation gegeben, die ersichtlich die Bedingungen (1), (2) und (3) unseres Kriteriums erfüllt. Für (4) stellen wir sogleich allgemeiner fest:

Ist für eine ZPE-Halbgruppe $\mathfrak{H}$ irgendeine Halbordnungsrelation erklärt, die den Bedingungen (1), (2) *und* (3) *genügt, so ist auch* (4) *erfüllt, und zwar sogar für beliebige Elemente r und s aus $\mathfrak{H}$ mit $r \nmid s$ und $s \nmid r$.*

Wir brauchen nämlich für z nur den größten gemeinsamen Teiler von r und s zu nehmen, für den man leicht die Aussagen $\alpha)$, $\beta)$ und $\gamma)$ nachprüft.

Abschließend wenden wir unser Kriterium zum Beweis einiger wichtigen, bekannten ZPE-Aussagen an. Für den Halbring N der natürlichen Zahlen ist es ersichtlich mit der üblichen Ordnungsrelation und $z = r - s$ für $r > s$ erfüllt. Ist $\mathfrak{R}$ ein euklidischer Ring mit der Zuordnung $a \to g(a)$, so bedeute $a \prec b$ einfach $g(a) < g(b)$, und man wählt $z = r - sq$ mit $g(z) < g(s) \leqq g(r)$; zum Nachweis von

(3) benötigt man allerdings, daß $g(ac) < g(bc)$ aus $g(a) < g(b)$ folgt.[3]) Für einen Hauptidealring $\mathfrak{R}$ setzt man $a \prec b$ genau dann, wenn für die zugehörigen Ideale $(a) \supset (b)$ gilt; mit z aus $(r, s) = (z)$ ergeben sich sofort die Bedingungen unseres Kriteriums.

Weiterhin sei $\mathfrak{R}$ der Halbring[4]) aller Ideale eines Ringes $\mathfrak{R}$, dessen Ideale dem Oberkettensatz und dem Faktorsatz genügen. Letzterer besagt also, daß jedes Oberideal $\mathfrak{a}$ eines Ideals $\mathfrak{b}$ auch Faktor von $\mathfrak{b}$, und damit in unserem Sinne Teiler von $\mathfrak{b}$ ist[5]). Mit $\mathfrak{a} \prec \mathfrak{b}$ genau dann, wenn $\mathfrak{a} \supset \mathfrak{b}$ gilt, erhält man eine Halbordnungsrelation, die auch den Forderungen (1), (2) und (3) unseres Kriteriums genügt; (1) ist nämlich die dem Oberkettensatz entsprechende Maximalbedingung, (3) ist gleichwertig mit der Regularität der Idealmultiplikation, die sich aus dem Faktorsatz ergibt, und (2) folgt aus (3) und $\mathfrak{R} \prec \mathfrak{b}$ für jedes $\mathfrak{b} \neq \mathfrak{R}$. Zum Beweis von (4) setzt man $\mathfrak{z} = \mathfrak{r} + \mathfrak{s}$: Wegen des Faktorsatzes gilt mit $\mathfrak{r} \nmid \mathfrak{s}$ und $\mathfrak{s} \nmid \mathfrak{r}$ auch $\mathfrak{r} \nparallel \mathfrak{s}$ und $\mathfrak{s} \nparallel \mathfrak{r}$, also $\mathfrak{z} \supset \mathfrak{r}$ und $\mathfrak{z} \supset \mathfrak{s}$ und damit bereits $\alpha)$ und $\beta)$, während sich $\gamma)$ sofort aus $\mathfrak{z}\mathfrak{a} = \mathfrak{r}\mathfrak{a} + \mathfrak{s}\mathfrak{a}$ ergibt.

Schließlich kann auch die Übertragung der ZPE-Eigenschaft von einem Ring $\mathfrak{R}$ auf den Polynomring $\mathfrak{R}[x]$ mit unserem Kriterium gezeigt werden, wobei nur der sog. Hilfssatz von GAUSS über das Produkt primitiver Polynome als Hilfsmittel verwendet wird. Dazu erweitern wir eine unserem Kriterium genügende Relation für die Elemente des ZPE-Ringes $\mathfrak{R}$ gemäß

$$\sum_{\nu=0}^{n} a_\nu x^\nu \prec \sum_{\mu=0}^{m} b_\mu x^\mu \quad (a_n \neq o,\ b_m \neq o)$$

genau dann, wenn entweder $n < m$

oder $n = m$ und $a_n \prec b_m$,

zu einer Relation für die Elemente von $\mathfrak{R}[x]$, die ersichtlich irreflexiv, asymmetrisch und transitiv ist und auch wieder den Bedingungen (1), (2) und (3) genügt. Den Nachweis von (4) führen wir für irreduzible Elemente und unterscheiden die Fälle:

$r \in \mathfrak{R}$, $s \in \mathfrak{R}$: Hier leistet das schon in $\mathfrak{R}$ existierende Element z auch für $\mathfrak{R}[x]$ das Verlangte.

$r(x) \in \mathfrak{R}[x]$, $s \in \mathfrak{R}$: Für das Einselement $e = z$ ist $e \prec r(x)$, $s \nmid e$ und aus $s \mid r(x)a(x)$ folgt $s \mid a(x)$, da $r(x)$ als irreduzibles Polynom den Inhalt e hat.

$r(x) \in \mathfrak{R}[x]$, $s(x) \in \mathfrak{R}[x]$: Die Division mit Rest liefert in der Form

$$cr(x) = s(x)q(x) + z(x), \quad c \in \mathfrak{R},$$

ein Element $z(x) \in \mathfrak{R}[x]$ mit einem kleineren Grad als dem von $s(x)$ und dem von $r(x)$. Dieses Element $z(x)$ ist ungleich o (sonst wäre c der Inhalt von $q(x)$ und damit $s(x)$ Teiler von $r(x)$) und erfüllt $\alpha)$, $\beta)$ und $\gamma)$.

---

[3]) Für die üblicherweise betrachteten Beispiele euklidischer Ringe ist diese Bedingung ebenso wie die meist nur geforderte Aussage $g(a) \leqq g(ab)$ erfüllt; zum Nachweis der Hauptidealringeigenschaft sind ohnehin beide entbehrlich.

[4]) Für die Begriffsbildung des Halbringes und weitere Literatur vgl. WEINERT [5].

[5]) Man beachte, daß der für beliebige Halbgruppen erklärte Begriff des Teilers sich definitionsgemäß zunächst mit dem idealtheoretischen Begriff des Faktors und nicht mit dem des Oberideals deckt. Auch ist ein irreduzibles Element $\mathfrak{r}$ von $\mathfrak{R}$ hier als multiplikativ unzerlegbares Ideal erklärt, welches aber auf Grund des Faktorsatzes maximal und damit auch Primideal von $\mathfrak{R}$ ist.

Literaturverzeichnis

[1] H. HASSE, Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen, *J. reine angew. Math.*, **159** (1928), 3—12.
[2] W. KRULL, Über die Zerlegung der Hauptideale in allgemeinen Ringen, *Math. Ann.*, **105** (1931), 1—14.
[3] W. KRULL, *Idealtheorie* (Berlin, 1935).
[4] L. RÉDEI, *Algebra*, I. Teil (Leipzig, 1959).
[5] H. J. WEINERT, Über Halbringe und Halbkörper. I, *Acta Math. Acad. Sci. Hung.*, **13** (1962), 365—378.

(Eingegangen am 10. Februar 1962)