Zur Existenz und Homogenität des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen

Von HANNS JOACHIM WEINERT in Potsdam (Deutschland)

Im ersten Teil dieser Note wird ein eigenartiges Verhalten des größten gemeinsamen Linksteilers $(\alpha_1, \ldots, \alpha_n)_l^*$ bzw. des kleinsten gemeinsamen Linksvielfachen $[\alpha_1, \ldots, \alpha_n]_l^*$ in einem nullteilerfreien Ring R mit Einselement 1 behandelt; der Verfasser ist darauf durch ein Versehen in dem Lehrbuch „Algebra" von L. RÉDEI (1. Teil, deutsche Ausg., Leipzig, 1959) aufmerksam geworden und kommt mit der Veröffentlichung einem Wunsche von Herrn Professor RÉDEI nach. Im Zusammenhang damit steht ein notwendiges und hinreichendes Kriterium für die eindeutige Zerlegung in irreduzible Faktoren in einem Integritätsbereich, welches Gegenstand des zweiten Teiles ist.

Existiert in R der größte gemeinsame Linksteiler $\delta' = (\varrho\alpha_1, \ldots, \varrho\alpha_n)_l^*$ der Elemente $\varrho\alpha_1, \ldots, \varrho\alpha_n$, so zeigt man leicht, daß $\delta' = \varrho\delta$ gilt und der Komplementärteiler δ größter gemeinsamer Linksteiler der Elemente $\alpha_1, \ldots, \alpha_n$ ist, also

$$\varrho(\alpha_1, \ldots, \alpha_n)_l^* = (\varrho\alpha_1, \ldots, \varrho\alpha_n)_l^* \tag{1}$$

erfüllt ist. Dagegen kann man nicht umgekehrt von der Existenz von $(\alpha_1, \ldots, \alpha_n)_l^*$ auf die von $(\varrho\alpha_1, \ldots, \varrho\alpha_n)_l^*$ und damit auf (1) schließen (vgl. a. a. O. S. 312, Formel (20)), eine Feststellung, die auch für kommutative Ringe zutrifft. So existiert z. B. in $R = \mathfrak{J}[\sqrt{-5}]$ zu den beiden nichtassoziierten irreduziblen[1]) Elementen 3 und $2 + \sqrt{-5}$ trivialer Weise der größte gemeinsame Teiler $(3, 2 + \sqrt{-5})^* = 1$, während $3 \cdot 3$ und $3 \cdot (2 + \sqrt{-5})$ keinen größten gemeinsamen Teiler besitzen (vgl. etwa a. a. O. S. 318).

Für das kleinste gemeinsame Linksvielfache zieht jedoch gemäß

$$\varrho[\alpha_1, \ldots, \alpha_n]_l^* = [\varrho\alpha_1, \ldots, \varrho\alpha_n]_l^* \tag{2}$$

die Existenz von $[\varrho\alpha_1, \ldots, \varrho\alpha_n]_l^*$ die von $[\alpha_1, \ldots, \alpha_n]_l^*$ und auch umgekehrt die Existenz von $[\alpha_1, \ldots, \alpha_n]_l^*$ die von $[\varrho\alpha_1, \ldots, \varrho\alpha_n]_l^*$ nach sich.

---

[1]) Wie RÉDEI nennen wir Nichteinheiten ($\neq 0$) ohne echte Faktorzerlegung irreduzibel.

Dieses unterschiedliche Verhalten wirkt sich nun auch auf die a. a. O. auf S. 313 angegebene Regel

$$(3) \qquad (\alpha_1, \ldots, \alpha_n)^* [\beta_1, \ldots, \beta_n]^* = \gamma \quad \text{mit} \quad \alpha_1\beta_1 = \cdots = \alpha_n\beta_n = \gamma \neq 0$$

aus, die nur für einen Integritätsbereich R diskutierbar ist. Hier kann unter Verwendung der zweiten Existenzsaussage zu (2) gezeigt werden, daß mit $[\beta_1, \ldots, \beta_n]^*$ auch $(\alpha_1, \ldots, \alpha_n)^*$ existiert und dann (3) erfüllt ist. Die Umkehrung ist dagegen falsch; wählt man nämlich wieder in $R = \mathfrak{J}[\sqrt{-5}]$

$$\alpha_1 = \beta_1 = 3, \quad \alpha_2 = 2 + \sqrt{-5}, \quad \beta_2 = 2 - \sqrt{-5},$$

so gilt $\gamma = \alpha_1\beta_1 = \alpha_2\beta_2 = 9$ und der größte gemeinsame Teiler $(\alpha_1, \alpha_2)^* = 1$ existiert, während es kein kleinstes gemeinsames Vielfaches von β_1 und β_2 gibt. In der Tat verwendet auch der a. a. O. angegebene Beweis die Existenz von $(\varrho\alpha_1, \ldots, \varrho\alpha_n)$, die nach der obigen Feststellung bei (1) eben nicht aus der Existenz von $(\alpha_1, \ldots, \alpha_n)^*$ gefolgert werden kann.

Liegt freilich ein Ring R mit größtem gemeinsamen Linksteiler vor, in dem also zu je zwei und damit zu je endlich vielen Elementen der größte gemeinsame Linksteiler existiert, so gelten die Homogenitätsregel (1) und im kommutativen Falle auch die Regel (3) stets. Letztere zeigt, daß ein Integritätsbereich mit größtem gemeinsamen Teiler auch ein Intergritätsbereich mit kleinstem gemeinsamen Vielfachen ist und umgekehrt, wobei dies wiederum (gerade vermöge (1)) die Eindeutigkeit irreduzibler Faktorzerlegungen nach sich zieht, wie wir im Rahmen des folgenden Kriteriums beweisen werden.

Ein Integritätsbereich R mit Einselement ist genau dann ein Ring mit eindeutiger irreduzibler Faktorzerlegung, d. h. ein Ring, in dem jedes Element $\alpha \neq 0$ bis auf assoziierte Elemente eindeutig als Produkt

$$(4) \qquad \alpha = \varepsilon\omega_1 \ldots \omega_k$$

einer Einheit ε und irreduzibler Elemente ω_i geschrieben werden kann, wenn gilt:

A) *In R ist jede Kette echter Teiler*

$$\alpha_1, \alpha_2, \alpha_3, \ldots \quad (\alpha_{i+1} \textit{ jeweils echter Teiler von } \alpha_i)$$

endlich.

B) *R ist ein Ring mit größtem gemeinsamen Teiler.*

In der Tat sind beide Aussagen in einem Ring mit eindeutiger irreduzibler Faktorzerlegung erfüllt, da dann alle Teiler eines Elementes α Teilprodukte von (4) sind, und der größte gemeinsame Teiler in bekannter Weise aus den Elementzerlegungen konstruiert werden kann. Für die Umkehrung stellen wir sogleich fest, daß sogar unabhängig voneinander A) die Existenz einer irreduziblen Faktorzerlegung für jedes $\alpha \in R$, B) die Eindeutigkeit irreduzibler Faktorzerlegungen (soweit diese existieren) nach sich zieht. Das erste ergibt sich sofort aus den üblichen Existenzbeweisen (etwa für Hauptidealringe oder Euklidische Ringe), die gerade auf dem Abbrechen echter Teilerketten beruhen. Für das zweite genügt es bekanntlich nachzuweisen, daß mit B) die folgende Eigenschaft irreduzibler Elemente ω gilt:

$$\textit{Aus} \quad \omega|\sigma\tau \quad \textit{folgt} \quad \omega|\sigma \quad \textit{oder} \quad \omega|\tau.$$

Dazu verwenden wir die in Ringen mit größtem gemeinsamen Teiler erfüllte Homogenitätsregel (1). Nach ihr folgt aus $\omega \nmid \sigma$ und $\omega \nmid \tau$, also $(\omega, \sigma)^* = = (\omega, \tau)^* = 1$, nämlich

$$1 = (\omega, \sigma)^* \cdot (\omega, \tau)^* = \big((\omega, \sigma)^* \cdot \omega, \ (\omega, \sigma)^* \cdot \tau\big)^* = (1 \cdot \omega, \omega \cdot \tau, \sigma \cdot \tau)^*$$

und damit $(\omega, \sigma\tau)^* = 1$, im Widerspruch zu $\omega|\sigma\tau$.

Abschließend sei bemerkt, daß sich dieses Kriterium bereits für kommutative, reguläre Halbgruppen mit Einselement aussprechen läßt. Ist etwa H die multiplikative Halbgruppe der Ideale eines Ringes R, so laufen Teilerkettensatz (für Ideale) und Faktorsatz (aus $\mathfrak{a} \supseteq \mathfrak{b}$ folgt $\mathfrak{a}\mathfrak{x} = \mathfrak{b}$) gerade auf die Aussagen A) und B) für H hinaus, woraus sich sofort die eindeutige Zerlegung jedes Ideals $(\neq (0), \neq R)$ in ein Produkt multiplikativ irreduzibler (Prim-) Ideale ergibt.

(Eingegangen am 27. Dezember 1960)