Zur Teilbarkeit in Ringen

Autor(en): **Hering, Hermann**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **30 (1975)**

Heft 2

PDF erstellt am: **19.03.2024**

Persistenter Link: https://doi.org/10.5169/seals-30645

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

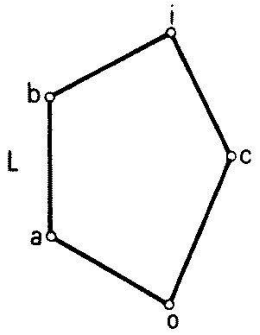
Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

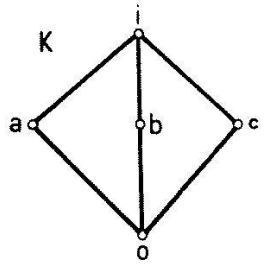
Fall I: V besitzt einen Teilverband L', der zu dem Verband L isomorph ist. Wir schränken nicht die Allgemeinheit des Beweises ein, wenn wir die Elemente von L' so bezeichnen wie die Elemente von L. Dann ist zweifellos $p(x) = \big((c \vee x) \wedge b\big) \vee a$ ein Polynom des Verbandes V. Es gilt nun:



$$p(o) = \big((c \vee o) \wedge b\big) \vee a = a$$
$$p(a) = \big((c \vee a) \wedge b\big) \vee a = b$$
$$p\big(p(o)\big) = p(a) = b \neq p(o);\ \text{d.h. } p$$

ist keine idempotente Polynomfunktion.

Fall II: V besitzt einen Teilverband K', der zu K isomorph ist. Wie oben bezeichnen wir die Elemente von K' ebenso wie die von K. Dann ist $p(x) = \big((a \vee x) \wedge b\big) \vee c$ ein Polynom von V.



$$p(o) = \big((a \vee o) \wedge b\big) \vee c = c$$
$$p(c) = \big((a \vee c) \wedge b\big) \vee c = i$$
$$p\big(p(o)\big) \neq p(o)\ \text{d.h. } p$$

ist keine idempotente Polynomfunktion von V.

D. Schweigert, Universität Trier–Kaiserslautern

LITERATURVERZEICHNIS

[1] Birkhoff-Bartee, *Modern Applied Algebra*, New York 1970.
[2] Hermes, *Einführung in die Verbandstheorie*, Berlin–Heidelberg–New York 1967.
[3] Lausch-Nöbauer, *Algebra of Polynomials*, Amsterdam 1973.
[4] Mitsch, H., *Über Polynome und Polynomfunktionen auf Verbänden*, Mh. Math. *74*, 239–243 (1970).

Elementarmathematik und Didaktik

Zur Teilbarkeit in Ringen

1. Algebraische Strukturen durchdringen mit Recht zunehmend den Mathematikunterricht des Gymnasiums [4], beginnen auch schon den der anderen weiterführenden Schulen zu beeinflussen und machen auch vor der Grundschule nicht halt, wie ein Blick in moderne Lehrbücher der verschiedenen Schultypen zeigt. Dasselbe lässt sich bei der Zahlentheorie nicht einmal fürs Gymnasium feststellen (vgl. dazu [2], Seite 252 und [4], wo Zahlentheorie wenigstens unter die wahlfreien Gebiete aufgenommen worden ist), was wohl mit der – wegen des gewohnten Umgangs mit den

elementaren Sätzen der multiplikativen Zahlentheorie in $\boldsymbol{Z}$ – schwieriger zu motivierenden strengen Begründung zusammenhängt.

Hat man sich aber dazu entschlossen – etwa in einer Arbeitsgemeinschaft – ein Teilgebiet der multiplikativen Zahlentheorie, z.B. elementare Teilbarkeitslehre der ganzen Zahlen, zu betreiben, so *erscheinen* Sätze wie die folgenden wegen der Gewöhnung an die Rechenregeln in diesem speziellen Bereich leicht als trivial.

In der Struktur $[\boldsymbol{Z}; +, \cdot]$ gilt:

(T_1) Es existieren unzerlegbare Elemente, nämlich alle Zahlen der Menge $\{z \in \boldsymbol{Z} \mid z \text{ ist Primzahl oder } -z \text{ ist Primzahl}\}$.

(T_2) Es gilt der Satz von der Zerlegbarkeit jedes Elements ($\neq 0$) in unzerlegbare Elemente, z.B. $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$.

(T_3) Es ist jede solche Zerlegung bis auf die Reihenfolge der Elemente und bis auf assoziierte Elemente eindeutig,
z.B. $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 2 \cdot 5 \cdot 2 = (-2) \cdot 3 \cdot 2 \cdot (-5) \cdot 2$.

Die Bedeutung solcher Sätze und auch ihre Beweiswürdigkeit werden eher sichtbar, wenn man die Teilbarkeitslehre auf abstrakte algebraische Strukturen (hier zunächst in geeigneten Modellen) zu übertragen versucht, also auf Integritätsbereiche mit Einselement, damit nichttriviale Teilbarkeitslehre überhaupt erst möglich und sinnvoll wird. Dadurch werden die Teilbarkeitsaussagen in $[\boldsymbol{Z}; +, \cdot]$ aus ihrer Isolation befreit, können als algebraische Sätze den ihnen zukommenden Grad an Allgemeinheit gewinnen und geben damit die richtige Perspektive frei für Teilbarkeitsprobleme in $[\boldsymbol{Z}; +, \cdot]$ als einer der möglichen Modellstrukturen.

Als naheliegende exemplarische Modellstruktur bietet sich der Integritätsbereich der Gaußschen Zahlen $\boldsymbol{G}$ an,

$$[\{a + bi \mid a, b \in \boldsymbol{Z}\}; +, \cdot],$$

der z.B. als 2-dimensionaler Vektorraum über dem Ring $[\boldsymbol{Z}; +, \cdot]$ eingeführt werden kann ([6], Seite 54). Die Hauptergebnisse T_1, T_2, T_3 lassen sich bei geeigneter Verallgemeinerung der zugrunde liegenden Begriffe hier wiederfinden. Das trifft bekanntlich keineswegs für jeden Ring zu, nicht einmal für jeden Integritätsbereich mit Einselement.

2. Elementar kann man die Existenz der Sätze T_1, T_2, T_3 verallgemeinerungsfähig zeigen, indem man den zugrunde liegenden Integritätsbereich als Euklidschen Ring verifiziert und diese Eigenschaft als hinreichende Bedingung für das Bestehen der drei Sätze, insbesonders für den Eindeutigkeitssatz, aufweist, wie z.B. in [3] ausführlich dargestellt ist.

Definition: Ein Ring $[\boldsymbol{R}; +, \cdot]$ heisst ein Euklidischer Ring wenn er Integritätsbereich ist und eine Abbildung

$$g: \boldsymbol{R}/\{0\} \to \{z \in \boldsymbol{Z} \mid z \geqq 0\}$$

definiert ist, für die gilt:

(E_1) $g(a \cdot b) \geqq g(a)$ für alle $a, b \in \boldsymbol{R}$, $a \neq 0$, $b \neq 0$.

(E_2) Für alle $a, b \in \boldsymbol{R}$, $b \neq 0$, existieren Elemente $q, r \in \boldsymbol{R}$, so dass stets Gleichungen $a = b \cdot q + r$ mit $r = 0$ oder mit $r \neq 0$, dann aber mit $g(b) > g(r)$, existieren.

Speziell für $[\boldsymbol{Z}, +, \cdot]$ ist $g: \boldsymbol{Z}/\{0\} \to \boldsymbol{Z}^+$, $z \to |z|$, eine solche Abbildung.

Es ist verhältnismässig einfach, für den Integritätsbereich $[\boldsymbol{G}; +, \cdot]$ die Euklidsche Eigenschaft nachzuweisen, wenn man $g(z) = \text{Norm}\,(z)$ setzt (vgl. [1], [3], [5], [6]). In der zitierten Literatur werden dafür aber sowohl der Körper der komplexen Zahlen mit rationalem Real- und Imaginärteil als auch der Begriff der Norm und ihre Multiplikativität in diesem Bereich benutzt. Das ist natürlich mathematisch korrekt, aber vom Standpunkt der Didaktik unbefriedigend, da einmal der algebraische Bereich, in dem Teilbarkeitsaussagen gemacht werden sollen, in einen Erweiterungsbereich eingebettet werden muss; zum anderen wird für den Lernenden der Blick gerade wieder vom Integritätsbereich zu einem Körper hin abgelenkt, was der Problematik der Teilbarkeit wieder die Nähe zur trivialisierenden Körpereigenschaft suggerieren kann. Zum dritten sollte auch auf den Mangel an Denkökonomie hingewiesen sein, der den oben zitierten Verfahren dann anhaftet, wenn man den Akzent auf Teilbarkeitsüberlegungen in gewissen Bereichen setzt und die Theorie immanent, also ohne algebraische Erweiterungen, aufbauen möchte.

3. Hier sollen zwei Wege aufgezeigt werden, wie man beim Beweis der Euklidschen Eigenschaft mit den Gaußschen Zahlen allein auskommen kann, wobei im ersten Fall zwar noch die gewöhnlichen rationalen Zahlen herangezogen werden, im zweiten aber nur der Ring der ganzen Zahlen $[\boldsymbol{Z}; +, \cdot]$ als Hilfsmittel benutzt wird.

Im folgenden wird der Integritätsbereich $[\boldsymbol{G}; +, \cdot]$ der Gaußschen Zahlen mit der multiplikativen Norm $N\,(u + iv) = u^2 + v^2$ vorausgesetzt und wieder $g(z) = N(z)$ gesetzt.

Führt man nun folgende Bezeichnungen ein:

$$\alpha = a_1 + a_2\, i\,, \quad \beta = b_1 + b_2\, i \neq 0\,, \quad \varkappa = k_1 + k_2\, i\,, \quad \varrho = r_1 + r_2\, i\,, \tag{1}$$

so ist wegen $(a_1^2 + a_2^2)\,(b_1^2 + b_2^2) \geqq a_1^2 + a_2^2\; E_1$ stets erfüllt. Ebenso ist sicher für jedes Paar $\alpha, \beta \in \boldsymbol{G}$

$$\alpha = \varkappa\beta + \varrho \tag{2}$$

mit geeigneten $\varkappa, \varrho \in \boldsymbol{G}$ erfüllbar. Man braucht ja nur $\varkappa \in \boldsymbol{G}$ vorzugeben und $\varrho \in \boldsymbol{G}$ geeignet bestimmen. Die Norm $N(\varrho)$ lässt sich aus (2) berechnen.

$$\left.\begin{aligned} N(\varrho) &= N\,(\alpha - \varkappa\beta) \\ &= N\,\{a_1 + a_2\, i - [k_1\, b_1 - k_2\, b_2 + (k_1\, b_2 + k_2\, b_1)\, i]\} \\ &= N\,\{a_1 - k_1\, b_1 + k_2\, b_2 + i\,(a_2 - k_2\, b_1 - k_1\, b_2)\} \\ &= (b_1\, k_1 - b_2\, k_2 - a_1)^2 + (b_2\, k_1 + b_1\, k_2 - a_2)^2 \\ N(\beta) &= b_1^2 + b_2^2 \end{aligned}\right\} \tag{3}$$

Zu zeigen ist, dass man $\varkappa$ und ϱ als Elemente aus $\boldsymbol{G}$ so wählen kann, dass im Falle $\varrho \neq 0$

$$N(\beta) > N(\varrho) \tag{4}$$

gilt.

1. *Weg:* Das Gleichungssystem für k_1^*, k_2^*

$$b_1\, k_1^* - b_2\, k_2^* = a_1\,, \quad b_2\, k_1^* + b_1\, k_2^* = a_2$$

ist wegen (1) und $N(\beta) \neq 0 \leftrightarrow \beta \neq 0$ immer, und zwar mit Elementen aus $\boldsymbol{Q}$, lösbar. Wählt man dann $k_i \in \boldsymbol{Z}$ $(i = 1, 2)$ mit $| k_i - k_i^* | \leqq 1/2$, so erhält man mit (3)

$$\begin{aligned} N(\varrho) &= (b_1 k_1 - b_2 k_2 - a_1)^2 + (b_2 k_1 + b_1 k_2 - a_2)^2 \\ &= (b_1 [k_1 - k_1^*] - b_2 [k_2 - k_2^*])^2 + (b_2 [k_1 - k_1^*] + b_1 [k_2 - k_2^*])^2 \\ &= N(\beta) [k_1 - k_1^*]^2 + N(\beta) [k_2 - k_2^*]^2 \\ &\leqq N(\beta) \cdot 1/2 < N(\beta) . \end{aligned}$$

2. *Weg:* Drückt man (4) mit Hilfe von (3) aus und multipliziert beiderseits mit $N^2(\beta)$, so erhält man die Ungleichung

$$(b_1 k_1 N(\beta) - b_2 k_2 N(\beta) - a_1 N(\beta))^2 + (b_2 k_1 N(\beta) + b_1 k_2 N(\beta) - a_2 N(\beta))^2 < N^3(\beta) . \tag{5}$$

Die an dieser Ungleichung orientierte Ungleichung für k_1^{**}, k_2^{**}

$$(b_1 k_1^{**} - b_2 k_2^{**} - a_1 N(\beta))^2 + (b_2 k_1^{**} + b_1 k_2^{**} - a_2 N(\beta))^2 < N^3(\beta)$$

ist (vgl. 1. Weg) sogar mit Elementen k_1^{**}, $k_2^{**} \in \boldsymbol{Z}$ derart lösbar, dass die beiden Klammerterme links Null sind. Zu k_i^{**} $(i = 1, 2)$ gibt es bekanntlich $k_i, r_i \in \boldsymbol{Z}$, so dass gilt:

$$k_i^{**} = k_i N(\beta) + r_i \quad \text{mit} \quad 2 | r_i | \leq N(\beta) . \tag{6}$$

Damit erhält man (vgl. (5) und Lösungseigenschaft von k_i^{**}):

$$\begin{aligned} &(b_1 k_1 N(\beta) - b_2 k_2 N(\beta) - a_1 N(\beta))^2 + (b_2 k_1 N(\beta) + b_1 k_2 N(\beta) - a_2 N(\beta))^2 \\ &= (b_1 r_1 - b_2 r_2)^2 + (b_2 r_1 + b_1 r_2)^2 \\ &= b_1^2 r_1^2 + b_2^2 r_2^2 + b_2^2 r_1^2 + b_1^2 r_2^2 \\ &= N(\beta) (r_1^2 + r_2^2) . \end{aligned}$$

Für $r_1 = r_2 = 0$ folgt wegen $N(\beta) > 0$ die Behauptung (5) sofort; anderenfalls lässt sich weiter abschätzen:

$$\begin{aligned} &\leqq N(\beta) \cdot 2 \cdot \max^2 (| r_1 | , | r_2 |) \\ &< N(\beta) \cdot (2 \max (| r_1 | , | r_2 |)^2 \\ &\leqq N^3(\beta) \quad \text{(vgl. (6))}. \end{aligned}$$

Die Ungleichung (5) ist wiederum bestätigt.

Für beide Wege sei abschliessend ein Beispiel angegeben. Mit $\alpha = 3 + 4\,i$ und $\beta = 2 - i$ wird (2) jetzt

$$\left.\begin{aligned} 3 + 4\,i &= (k_1 + k_2\,i) \cdot (2 - i) + r_1 + r_2\,i \\ &= 2\,k_1 + k_2 + r_1 + (2\,k_2 - k_1 + r_2)\,i . \end{aligned}\right\} \tag{7}$$

Das Hilfssystem ist beim 1. Weg

$$2\,k_1^* + k_2^* = 3 , \quad - k_1^* + 2\,k_2^* = 4 ,$$

beim 2. Weg

$$2\,k_1^{**} + k_2^{**} = 15 , \quad - k_1^{**} + 2\,k_2^{**} = 20 ,$$

da die Determinante des 1. Systems $N(\beta) = 5$ ist und (7) nach Multiplikation mit $N(\beta)$ lautet:

$$(3 + 4\,i).\,5 = (2\,k_1 + k_2).\,5 + 5\,r_1 + (\langle 2\,k_2 - k_1\rangle.\,5 + 5\,r_2)\,i\,.$$

Die Hilfssysteme haben wegen $k_i^{**} = N(\beta) \cdot k_i^{*}$ die Lösungen

$$k_1^{**} = 5\,k_1^{*} = 2\,, \quad k_2^{**} = 5\,k_2^{*} = 11\,.$$

Auf beiden Wegen erhält man wegen der Äquivalenz der Bedingungen $|\,k_i - k_i^{*}\,| \leqq 1/2$, $k_i \in \boldsymbol{Z}$, und (6): $k_1 = 0$, $k_2 = 2$. Aus (7) folgt nun $r_1 = 1$, $r_2 = 0$, so dass abschliessend gilt:

$$N(\beta) = 5 > N(\varrho) = 1\,.$$

Überblickt man zusammenfassend die Beweismittel, so sind es über die Voraussetzungen bezüglich des Integritätsbereichs **G** hinaus nur die Bedingung für nicht leere Lösungsmenge eines linearen Gleichungssystems im Falle $m = n = 2$ und die Kenntnis der Lösungsterme sowie etwas elementare Zahlentheorie in $\boldsymbol{Z}$.

Hermann Hering, Frechen (Bundesrepublik)

LITERATURVERZEICHNIS

[1] G. H. Hardy und E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford 1960.
[2] H. Lenné, *Analyse der Mathematikdidaktik in Deutschland*. Stuttgart 1969.
[3] H. Lugowski und H.-J. Weinert, *Grundzüge der Algebra*, Bd. II. Leipzig 1958.
[4] Nürnberger Lehrpläne des Deutschen Vereins zur Förderung des mathematischen und naturwissenschaftlichen Unterrichts. MNU Bd. 18, Heft 1/2, S. 1–8, 1965.
[5] H. J. Reiffen, G. Scheja und U. Vetter, *Algebra*. Mannheim 1969.
[6] B. L. v. d. Waerden, *Algebra*, Bd. 1. Berlin 1960.

Über einige einfache Folgen und Reihen im Schulunterricht

Es sollen hier einige Folgen und Reihen mit einfachen Mitteln behandelt werden, die vielleicht nicht allgemein bekannt sind.

Ein einfacher Beweis für die Monotonie der Folgen mit dem allgemeinen Glied $\left(1 + \frac{1}{n}\right)^n$ bzw. $\left(1 + \frac{1}{n}\right)^{n+1}$ benützt nur die Formel[1])

$$a^n - b^n = (a - b)\,(a^{n-1} + a^{n-2}\,b + \cdots + b^{n-1})\,. \tag{1}$$

Man hat

$$\left(1 + \frac{1}{n}\right)^n - \left(1 + \frac{1}{n-1}\right)^{n-1}$$

$$= \left(1 + \frac{1}{n}\right)^n - \left(1 + \frac{1}{n-1}\right)^n + \frac{1}{n-1}\left(1 + \frac{1}{n-1}\right)^{n-1}.$$

[1]) Herr Professor Hlawka machte mich freundlicherweise darauf aufmerksam, dass dieser Beweis von Yzeren (1970) stammt, der in derselben Weise auch $(1 + z/n)^n$ für komplexes z untersuchte.