

Teilerfremde und relativ prime Ideale

Von

Shinjiro MORI

(Eingegangen am 30. Mai 1950)

廣島市東千田町
廣島文理科大学数学教室

Abgesehen davon, ob der kommutative Ring $\mathfrak{R}$ das Einselement besitzt, oder nicht, heissen zwei Ideale a und b in $\mathfrak{R}$ *teilerfremd*, wenn ihr grösster gemeinsamer Teiler gleich $\mathfrak{R}$ ist, nämlich $(a, b) = \mathfrak{R}$ ist. Andererseits nennen wir b *relativ prim* zu a ($\neq (0)$), wenn $a = a : b$ ist. Bekanntlich ist aber das Prädikat "relativ prim" nicht symmetrisch, und in allgemeineren Fällen sind auch die beiden Prädikate "teilerfremd" und "relativ prim" nicht gleichwertig.

Es ist das Ziel der vorliegenden Arbeit die Eigenschaften der Ringe, in welchen die beiden Prädikate "teilerfremd" und "relativ prim" gleichbedeutend sind, aufzudecken. Um Missverständnisse zu vermeiden stellen wir wieder die Hauptaufgabe unserer späteren Ausführungen als folgendes Problem zusammen:

Von welcher Art ist der kommutative Ring, in welchem die Beziehung $(a, b) = \mathfrak{R}$ aus $a = a : b$, oder $b = b : a$ folgt, und umgekehrt aus $(a, b) = \mathfrak{R}$ die Beziehung $a = a : b$, oder $b = b : a$ folgt?

Endlich ist noch eine Bemerkung zuzufügen:

Können wir vermuten, dass im idempotenten kommutativen Ring kein Totalnullteiler existiert, lassen sich die Eigenschaften des in Frage stehenden Ringes in noch einfacherer Form darstellen.

I. Fall. Kommutativer Ring mit Einselement.

Um den Zusammenhang der Prädikate "teilerfremd" und "relativ prim" zu erkennen, stellen wir den folgenden Satz an die Spitze.

Satz 1. *Im kommutativen Ring $\mathfrak{R}$ mit Einselement finden die beiden Prädikate "teilerfremd" und "relativ prim" dann und nur dann dieselbe Deutung, wenn dem Ring $\mathfrak{R}$ folgende Eigenschaft zukommt:*

Für jedes Halbprimideal $\mathfrak{h}$ ($\neq \mathfrak{R}$), welches ein echter Teiler eines Ideals a ($\neq (0)$) ist, lässt sich ein Element r , so wählen, dass $r\mathfrak{h} \subseteq a$, $r \notin a$ ist.

Es gelte jetzt die Annahme, dass beide Definitionen in $\mathfrak{R}$ gleichwertig sind. Dann, aus $\mathfrak{R} \supset \mathfrak{h} \supset a$, $\mathfrak{R} = \mathfrak{h} : a$ folgt $a + a : \mathfrak{h}$; also ist die Eigenschaft notwendig.

Umgekehrt setzen wir die Eigenschaft voraus. Es sei $a = a : b$ für zwei von $\mathfrak{R}$ und (0) verschiedene Ideale a und b , und ferner sei $\mathfrak{h}$ das zu $c = (a, b)$ gehörige Halbprimideal. Dann muss $\mathfrak{R} = \mathfrak{h}$, also nach der Existenz des Einselements $c = (a, b) = \mathfrak{R}$ sein. Denn, wäre $\mathfrak{R} \neq \mathfrak{h}$, so gäbe es ein solches Element r , dass $r\mathfrak{h} \subseteq a$, $r \notin a$ ist, und folglich wäre $r\mathfrak{b} \subseteq a$, $r \notin a$. Daraus würde folgen der Annahme entgegen $a \neq a : b$.

Ist endlich $(a, b) = \mathfrak{R}$, so folgt $a = a : b$ aus $a : b = a : (a, b) = a : \mathfrak{R}$.

Zufolge des Satzes führt die Annahme der Endlichkeit der Teilerkette zum Satze.

Satz 2. *Es sei im Ring $\mathfrak{R}$ mit Einselement die Endlichkeit der Teilerkette der Ideale erfüllt. Die beiden Definitionen sind dann und nur dann gleichgültig, wenn jedes Primideal $(\neq (0))$ in $\mathfrak{R}$ ein maximales Ideal ist.*

In diesem Ring $\mathfrak{R}$ gilt nach der Bedingung des Satzes I, dass jeder Primideal $(\neq (0))$ ein maximales Ideal ist.

Wenn umgekehrt jedes Primideal $(\neq (0))$ maximal ist, und wenn a ein beliebiges von Null verschiedenes Ideal ist, so gibt es nur endlich viele Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n$, welche a enthalten, und der Durchschnitt $\mathfrak{h}$ von $\mathfrak{p}_i (i=1, 2 \dots n)$ ist das zu a gehörige Halbprimideal, und ferner ist $\mathfrak{h} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \dots \mathfrak{p}_n$, da in $\mathfrak{R}$ das Einselement existiert und $\mathfrak{p}_i$ maximal sind. Andererseits ist nach dem Teilerkettensatz eine endliche Potenz von $\mathfrak{h}$ durch a teilbar. Daraus ergibt sich die Existenz eines Elements r_i von der Art, dass $r_i \mathfrak{p}_i \subseteq a$, $r_i \notin a$ ist. Wir können demnach unseren Satz als erwiesen ansehen.

Zum Schlusse soll noch ein Satz hinzugefügt werden,

Satz 3. *Im Ring mit Einselement sind die beiden Definitionen dann und nur dann gleichwertig, wenn das Prädikat "relativ prim" symmetrisch ist.*

Denn, aus der Existenz des Einselements ziehen wir leicht den Schluss, dass zwei Ideale in beiden Richtungen relativ prim sind, wenn sie teilerfremd sind, und dass die Symmetrie des Prädikates "relativ prim" notwendig ist. Die Umkehrung ist auch leicht beweisbar ⁽¹⁾.

II. Fall. Kommutativer Ring ohne Einselement.

Es sei b ein echter Teiler eines Ideals a und r ein Element von der Art, dass $r\mathfrak{b} \subseteq a$, $r \notin a$ ist. Dann nennen wir ein solches Element r einen *Total-*

(1) Weiteres, hierüber siehe bei van der Waerden, *Moderne Algebra*, II. S. 39, und S. Mori, Über die Symmetrie des Prädikates "relativ prim", *Journ. of the Hiroshima University* 14 (1950), S. 102.

nullteiler von b in bezug auf a . Hierbei können wir zwei verschiedene Fälle betrachten, je nachdem wenigstens ein Totalnullteiler r in b liegt, oder gar kein r in b . Der erste heisst ein *Teiler von zweiter Art in bezug auf a* und der andere ein *Teiler von erster Art in bezug auf a* .

Aus der Benutzung dieser Definition ergibt sich nun folgendes Resultat:

Satz 4. 1. Alle von $\mathfrak{R}$ verschiedenen echten Teiler jedes Ideals $a (\neq (0))$ sind von erster, oder zweiter Art in bezug auf a .

2. Wenn a einen Teiler $b (\neq \mathfrak{R})$ von erster Art besitzt, so gibt es ein solches Ideal b_1 , dass $(b, b_1) = \mathfrak{R}$, $b \wedge b_1 = a$ ist.

3. Wenn b ein Teiler von zweiter Art in bezug auf a , so gibt es kein Ideal b_1 von zweiter Art, für welches $(b, b_1) = \mathfrak{R}$, $b \wedge b_1 = a$ ist.

Diese Forderungen sind notwendig und hinreichend dafür, dass die beiden Prädikate "relativ prim" und "teilerfremd" gleichbedeutend sind.

Wenn in $\mathfrak{R}$ die beiden Prädikate gleichwertig sind, und wenn $b (\neq \mathfrak{R})$ ein Teiler eines Ideals a , so soll $a \neq a : b$ sein, denn sonst würde $(a, b) = b = \mathfrak{R}$ unserer Annahme entgegen. Folglich ist die erste Forderung notwendig.

Ist ein Teiler b von a von erster Art, so setzen wir $b_1 = a : b$, $b = b_1 \wedge b$. Dann ist $b \supseteq a$. Wenn $b \supset a$ wäre, so würde für ein Element d aus b $db \subseteq a$, $d \in b$ und unserer Annahme entgegen wäre b von zweiter Art. Damit ist $a = b_1 \wedge b$. Wenn $xb \subseteq b_1$ ist, so folgt $xb \subseteq b_1 b \subseteq a$. Da aber b von erster Art ist, so muss dabei $xb \subseteq a$ und folglich $b_1 = b_1 : b$ sein. Also ist nach unserer Annahme $(b_1, b) = \mathfrak{R}$.

Schliesslich sei $a = b_1 \wedge b$, wobei b_1 und b von zweiter Art sind. Dann können wir ein solches Element r in b finden, dass $rb \subseteq a$, $r \notin a$ ist. Nach $a = b_1 \wedge b$ folgt daraus $r \notin b_1$ und danach ist $b_1 \neq b_1 : b$. In gleicher Weise gilt auch $b \neq b : b_1$. Danach ist $(b, b_1) \neq \mathfrak{R}$.

Nehmen wir umgekehrt an, dass in $\mathfrak{R}$ die drei Bedingungen erfüllt sind, so gilt zunächst $b_1 = a : b$ für die in zweiter Bedingung ausgesprochenen Ideale b_1 und b . Denn, nach $(b, b_1) = \mathfrak{R}$ ist jedes durch a unteilbare Element r in der Form $r = b + b_1$, $b \in b$, $b_1 \in b$ darstellbar. Aus $rb \subseteq a$, $r \notin a$ folgt danach $rb = (b + b_1)b \subseteq a$. Da aber $b_1 b \subseteq b_1 \wedge b = a$ ist, so erhalten wir $bb \subseteq a$. Nach der Eigenschaft von b soll damit $b \in a$, folglich $r \in b_1$ sein. Wir haben also $b_1 = a : b$.

Wenn $b_1 = b_1 : b$ für zwei von $\mathfrak{R}$ verschiedene Ideale b_1 und b ist, so ist $b = b_1 \wedge b \neq b$ und wegen erster Bedingung muss b von erster, oder zweiter Art in bezug auf b sein. Wäre b von zweiter Art in bezug auf b , so wäre $bb \subseteq b \subset b_1$, $b \notin b$ für ein Element b von b und danach $b \in b_1$, $b \in b$, was

unserer Annahme $b \notin \mathfrak{d}$ widerspricht. Demnach ist b von erster Art und ferner muss $b_1 = \mathfrak{d} : b$ sein. Andererseits können wir nach zweiter Bedingung ein Ideal b_1' auswählen, so dass $(b, b_1') = \mathfrak{R}$, $\mathfrak{d} = b \wedge b_1'$ ist, und dann nach dem obig gewonnenen Resultat gilt $b_1' = \mathfrak{d} : b$. Daraus folgt $b_1 = b_1'$, und dass also b_1 und b teilerfremd sind.

Es sei endlich $(b, b_1) = \mathfrak{R}$, $b \wedge b_1 = \mathfrak{d}$ für zwei von $\mathfrak{R}$ verschiedene ideale b und b_1 . Fügen wir noch die Annahme hinzu, dass b und b_1 beide von zweiter Art in bezug auf $\mathfrak{d}$ sind, so ergibt sich nach Bedingung 3 ein Widerspruch. Damit können wir behaupten, dass b von erster Art in bezug auf $\mathfrak{d}$ ist, und daher folgt, wie oben, $b_1 = \mathfrak{d} : b$, $b_1 = b_1 : b$. Also ist b relativ prim zu b_1 . Wir haben hiermit unseren Satz bewiesen.

Wir schliessen noch eine Bemerkung über einen speziellen Ring an.

Satz 5. *Wenn im kommutativen Ring $\mathfrak{R}$ der Teilerkettensatz vorausgesetzt wird, so sind die folgenden Bedingungen notwendig und hinreichend dafür, dass die beiden Prädikate "relativ prim" und "teilerfremd" in $\mathfrak{R}$ gleichbedeutend sind.*

1 *Primideal $(\neq(0))$ ist ein maximales Ideal.*

2. *Es gibt kein Ideal zwischen $\mathfrak{R}$ und $\mathfrak{R}^2$.*

Denn aus Bedingung I von Satz 4 folgt unmittelbar, dass jedes Primideal $(\neq(0))$ ein maximales Ideal ist. Wenn $\mathfrak{R} : \mathfrak{R}^2$ ist, so lässt sich $\mathfrak{R}$ nach dem Teilerkettensatz in der Form $\mathfrak{R} = (r_1, r_2, \dots, r_k, \mathfrak{R}^2)$ darstellen. Damit folgt aus Bedingung 3 von Satz 4, dass $\mathfrak{R} = (r, \mathfrak{R}^2)$, $pr \in \mathfrak{R}^2$ für eine Primzahl p ist. Danach sind die Bedingungen 1 und 2 unseres Satzes notwendig.

Um die Umkehrung zu beweisen, wollen wir die obig gewonnenen Bedingungen annehmen. Zuerst folgt hieraus nach dem Teilerkettensatz, dass jeder von $\mathfrak{R}$ verschiedene Teiler von $\alpha(\neq(0))$ ein Teiler von erster, oder zweiter Art ist. Um zweitens Bedingungen 2 und 3 in Satz 4 zuführen, ist es jetzt genug, dass wir folgenden Hilfssatz beweisen.

Hilfssatz. *Wenn im kommutativen Ring $\mathfrak{R}$ Bedingungen 1 und 2 von Satz 5 vorausgesetzt werden, so hat $\mathfrak{R}$ die folgende Eigenschaft:*

Der Restklassenring $\bar{\mathfrak{R}} = \mathfrak{R}/\alpha$ nach einem Ideal $\alpha(\neq(0))$ lässt sich in der direkten Summe $\bar{\mathfrak{R}} = \bar{\mathfrak{M}} + \bar{\mathfrak{N}}$ darstellen. Dabei ist $\bar{\mathfrak{M}}$ ein Ring mit Einselement, oder Null, und $\bar{\mathfrak{N}}$ ein nilpotenter Ring, order N_{null} , in welchem jedes Ideal gleich einer Potenz von $\bar{\mathfrak{N}}$ ist.

Wenn jedes Element von $\mathfrak{R}$ nilpotent in bezug auf α ist, so wird nach dem Teilerkettensatz $\mathfrak{R}^n \subseteq \mathfrak{b}$ für einen Teiler $\mathfrak{b}$ von α . Da es nach Bedingung 2 kein Ideal zwischen $\mathfrak{R}$ und $\mathfrak{R}^2$ gibt, so lässt sich $\mathfrak{R}$ in der Form

$\mathfrak{R}=(r, \mathfrak{R}^2)=(r, \mathfrak{R}^3)=\dots=(r, \mathfrak{R}^n)$ darstellen. Dabei ist $rp \in \mathfrak{R}^2$ für eine Primzahl p .

Wir können damit jedes Element b von $\mathfrak{b}$ in der Form

$$b \equiv r^m + c_1 r^{m+1} + \dots + c_{n-m-1} r^{n-1} (\mathfrak{R}^n), \quad (0 \leq c_i < p, \quad m < n)$$

setzen. Daraus folgt $br^{n-m-1} \equiv r^{n-1} (\mathfrak{R}^n)$, $r^{n-1} \in \mathfrak{b}$ und $b_1 = b - c_{n-m-1} r^{n-1} \in \mathfrak{b}$. Durch solche Prozesse erhalten wir endlich $r^n \in \mathfrak{b}$ und folglich $\mathfrak{R}^n \subseteq \mathfrak{b}$. Da wir hierbei m als den kleinsten Exponent unter den Elementen von $\mathfrak{b}$ betrachten können, so wird $\mathfrak{b} \subseteq \mathfrak{R}^n$ und danach $\mathfrak{R}^n = \mathfrak{b}$.

Wenn das zu α gehörige Halbprimideal $\mathfrak{h}$ von $\mathfrak{R}$ verschieden ist, so wird nach Bedingung I und Teilerkettensatz $\mathfrak{h} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_n$. Da $\mathfrak{p}_i$ ($i=1, 2, \dots, n$) aber maximal ist, so gibt es ein solches Element e_i , dass $e_i \equiv e_i^2 (\mathfrak{p}_i)$, $(e_i, \mathfrak{p}_i) = \mathfrak{R}$, $e_i \in \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_{i-1} \cap \mathfrak{p}_{i+1} \cap \dots \cap \mathfrak{p}_n$ sind. Aus $e_i - e_i^2 \in \mathfrak{p}_i$, $e_i - e_i^2 \in \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_{i-1} \cap \mathfrak{p}_{i+1} \cap \dots \cap \mathfrak{p}_n$ folgt ferner $e_i \equiv e_i^2 (\mathfrak{h})$, $e_i e_j \equiv 0 (\mathfrak{h})$ ($i \neq j$). Setzen wir nun $\mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{h}_2$, $\mathfrak{h}_2 \cap \mathfrak{p}_3 = \mathfrak{h}_3$, so folgt nach dem obig gewonnenen Resultat

$$\mathfrak{R}=(e_1, \mathfrak{p}_1)=(e_2, \mathfrak{p}_2)=(e_1, e_2, \mathfrak{h}_2) \quad \mathfrak{h}_2=(e_3, \mathfrak{h}_3)$$

Nach einer endlichen Zahl n von Schritten dieser Art kommen wir zu $\mathfrak{R}=(e_1, e_2, \dots, e_n, \mathfrak{h})$. Setzen wir wieder $e_0 = e_1 + e_2 + \dots + e_n$, so folgt daraus nach $e_0 e_i \equiv e_i (\mathfrak{h})$ ($i=1, 2, \dots, n$)

$$\mathfrak{R}=(e_0, \mathfrak{h}), \quad e_0 \equiv e_0^2 \equiv e_0^3 \equiv \dots (\mathfrak{h}), \quad e_0 \not\equiv 0 (\mathfrak{h})$$

Da jedes Element aus $\mathfrak{h}$ nilpotent in bezug auf α ist, so folgt $(e_0 - e_0^3)^k \in \alpha$, $e_0^k \equiv e_0^{2k} \mathfrak{b} (\alpha)$ und dadurch gilt $\mathfrak{R}=(e, \mathfrak{h})$, $e \equiv e^2 (\alpha)$ für $e = e_0^k \mathfrak{b}$.

Bezeichnen wir jetzt die Gesamtheit der Elemente x von $\mathfrak{R}$, für welche $ex \equiv x (\alpha)$ gilt, mit $\mathfrak{M}$ und die Gesamtheit der Elemente y , für welche $ey \equiv 0 (\alpha)$ gilt, mit $\mathfrak{N}$, so folgt aus dem hier Bewiesenen $\overline{\mathfrak{R}} = \mathfrak{M} + \mathfrak{N}$, wobei $\mathfrak{N}$ nilpotent und e Einselement von $\mathfrak{M}$ ist. Auf der anderen Seite ist nach Bedingung 2 klar, dass es kein Ideal zwischen $\mathfrak{R}$ und $\mathfrak{R}^2$ gibt⁽²⁾, dass also jedes Ideal in $\mathfrak{R}$ gleich einer Potenz von $\mathfrak{R}$ ist. Damit ist der Hilfssatz bewiesen.

(2) Hierbei muss $\mathfrak{R} \neq \mathfrak{R}^2$ sein. Denn sonst hätte $\mathfrak{R}$ Einselement. Vergl. S. Mori, Über Produktzerlegung der Ideale, Journ. of the Hiroshima University 2 (1932), S. 1.