

31. Eine notwendige Bedingung für die eindeutige Primfaktorzerlegung der Ideale in einem kommutativen Ring.

Von Mikao MORIYA und Yosi KOBAYASI.

Mathematisches Institut der Kaiserlichen Hokkaido Universität, Sapporo.

(Comm. by T. TAKAGI, M.I.A., May 12, 1941.)

Herr K. Kubo¹⁾ hat neuerlich eine notwendige und hinreichende Bedingung dafür aufgestellt, daß sich in einem kommutativen Ring \mathfrak{o} jedes vom Einheits- und Nullideal verschiedene Ideal eindeutig als Produkt aus endlich vielen, vom Einheits- und Nullideal verschiedenen Primidealen darstellen läßt. Da die in der Kuboschen Arbeit angeführte Literatur uns nicht so leicht zugänglich ist, so wollen wir in der vorliegenden Note zu zeigen versuchen, wie man mit möglichst elementaren idealtheoretischen Vorkenntnissen seine Resultate erhalten kann. Inzwischen wollen wir auch die von Herrn K. Kubo aufgestellte Bedingung durch die folgende, ihr äquivalente ersetzen, weil die neue Bedingung uns als eine hinreichende Bedingung zweckmäßiger erscheint:

- 1) Es gibt in \mathfrak{o} das Einselement.
- 2) Nur ein nilpotentes Ideal kann das von Null verschiedene annullierende Ideal²⁾ besitzen.
- 3) In \mathfrak{o} gilt der Teilerkettensatz für Ideale.
- 4) Für jedes Primideal³⁾ \mathfrak{p} gibt es zwischen \mathfrak{p} und \mathfrak{p}^2 kein echtes Zwischenideal.

Voraussetzung.

Ein kommutativer Ring \mathfrak{o} besitze ein vom Einheitsideal \mathfrak{o} und Nullideal (0) verschiedenes Ideal. Ferner sei in \mathfrak{o} jedes von \mathfrak{o} und (0) verschiedene Ideal eindeutig als Produkt von endlich vielen, von \mathfrak{o} und (0) verschiedenen Primidealen darstellbar.

Unter dieser Voraussetzung beweisen wir dann folgenden

Hilfssatz. $\mathfrak{o}^2 = \mathfrak{o}$.

Beweis. Nach Voraussetzung existiert in \mathfrak{o} ein von \mathfrak{o} und (0) verschiedenes Ideal; dieses Ideal besitzt einen von \mathfrak{o} und (0) verschiedenen Primteiler \mathfrak{p} . Da für ein Element $a \in \mathfrak{p}$ stets $a^2 \notin \mathfrak{p}$ ist, so gilt offenbar:

$$(0) \not\subseteq \mathfrak{o}^2 \subseteq \mathfrak{o}.$$

Wäre nun \mathfrak{o} ein echter Teiler von \mathfrak{o}^2 , so bestände nach Voraussetzung folgende Primfaktorzerlegung⁴⁾: $\mathfrak{o}^2 = \mathfrak{p}_1 \dots \mathfrak{p}_r$. Hieraus folgte für ein

1) Über die Noetherschen fünf Axiome in kommutativen Ringen. Journal of Science of the Hiroshima Univ., **10** (1940), 77.

2) Unter dem annullierenden Ideal eines Ideals \mathfrak{a} aus \mathfrak{o} verstehen wir die Gesamtheit der Elemente γ von \mathfrak{o} , für die $\mathfrak{a}(\gamma)$ das Nullideal wird.

3) Wir rechnen \mathfrak{o} unter die Primideale und ebenso das Nullideal, falls es die Primidealeigenschaft besitzt.

4) Unter einem Primfaktor eines Ideals aus \mathfrak{o} verstehen wir stets ein von \mathfrak{o} und (0) verschiedenes Primideal aus \mathfrak{o} .

$p_i \not\supseteq 0$, was aber ein Widerspruch ist.

Satz 1. *Es gibt in \mathfrak{o} das Einselement.*

Beweis. Wir greifen aus \mathfrak{o} ein von \mathfrak{o} verschiedenes Primideal \mathfrak{p} und ein beliebiges, nicht zu \mathfrak{p} gehöriges Element a aus \mathfrak{o} heraus. Da für jedes n $a^n \not\equiv 0 \pmod{\mathfrak{p}}$ ist, so ist stets $a^n \not\equiv 0$. Wir betrachten zunächst den Fall, wo $(a) \not\equiv 0$ ist. Dann gilt ersichtlich $(a)\mathfrak{o} \subseteq (a)$. Da $(a)\mathfrak{o} \not\equiv (0)$ ist, weil $a^2 \not\equiv 0$ zu $(a)\mathfrak{o}$ gehört, so erhält man die Primfaktorzerlegungen $(a)\mathfrak{o} = p_1 \dots p_r$, $(a) = p'_1 \dots p'_s$. Aus $(a)\mathfrak{o}^2 = (a)\mathfrak{o}$ folgt $p_1 \dots p_r \mathfrak{o} = p'_1 \dots p'_s \mathfrak{o}$. Unter den Primfaktoren $p_1, \dots, p_r, p'_1, \dots, p'_s$ gibt es sicher einen minimalen, d. h. einen solchen, welcher keinen der übrigen als echte Teilmenge enthält. Es sei etwa p_1 ein derartiger Primfaktor. Dann muß $p'_1 \dots p'_s \mathfrak{o}$ durch p_1 teilbar sein, und da p_1 ein Primideal ist, so gibt es unter $p'_1 \dots p'_s$ ein Primideal, also etwa p'_1 , welches in p_1 enthalten ist. Wegen der Minimaleigenschaft von p_1 muß daher $p_1 = p'_1$ sein; dann ist $(p_1\mathfrak{o}) p_2 \dots p_r = (p_1\mathfrak{o}) p'_2 \dots p'_s$. Nach Voraussetzung müssen p_2, \dots, p_r und p'_2, \dots, p'_s bis auf die Reihenfolge übereinstimmen. Also ist $(a)\mathfrak{o} = (a)$. Folglich gibt es ein Element μ derart, daß $a\mu = a$. Hieraus folgt ohne weiteres $(\mu) = \mathfrak{o}$, weil sonst das Ideal $(a) (\mu) = (a)$ zwei verschiedene Primfaktorzerlegungen besitzen müßte. Wenn $(a) = \mathfrak{o}$ ist, dann können wir uns a selbst als μ denken. Da $(\mu^2) = \mathfrak{o}^2 = \mathfrak{o} = (\mu)$ ist, so gilt: $\mu = \mu^2\xi + n\mu^2 = \mu(\mu\xi + n\mu)$, wo ξ ein Element aus a und n eine ganze rationale Zahl bezeichnet. Setzt man hierbei $\eta = \mu\xi + n\mu$, so gilt für ein beliebiges Element $r = \mu\zeta = m\mu$ aus \mathfrak{o} , $\eta = (\mu\eta)\zeta + m(\mu\eta) = \mu\zeta + m\mu = r$; d. h. η ist das Einselement von \mathfrak{o} .

Satz 2. *Jedes vom Nullideal verschiedene Primideal aus \mathfrak{o} ist teilerlos.*

Beweis. Für das Primideal \mathfrak{o} bleibt nichts zu beweisen. Es sei also \mathfrak{p} ein beliebiges, von \mathfrak{o} verschiedenes Primideal, und a ein nicht zu \mathfrak{p} gehöriges Element aus \mathfrak{o} . Dann ist offenbar $(a, \mathfrak{p})^2 = (a^2, a\mathfrak{p}, \mathfrak{p}^2) \subseteq (a^2, \mathfrak{p})$. Wir zeigen zunächst $(a, \mathfrak{p})^2 = (a^2, \mathfrak{p})$.

Angenommen, es wäre $(a, \mathfrak{p})^2 \not\equiv (a^2, \mathfrak{p})$. Dann existieren die Ideale a, b, c , derart, daß $(a, \mathfrak{p})^2 = ac$, $(a^2, \mathfrak{p}) = bc$ sind, und a, b keinen Primfaktor gemeinsam haben. Dabei können b, c eventuell gleich \mathfrak{o} sein, aber a ist sicher von \mathfrak{o} verschieden, weil sonst $(a, \mathfrak{p})^2 \supseteq (a^2, \mathfrak{p})$ sein würde. Ist nun $a = p_1 \dots p_r$ die Primfaktorzerlegung von a , so sind alle Primfaktoren von a Primteiler von \mathfrak{p} , weil sie Primteiler von $(a, \mathfrak{p}) \supseteq \mathfrak{p}$ sind. Bezeichnet man mit \bar{p}_i ($1 \leq i \leq r$) das Ideal p_i/\mathfrak{p} aus dem Restklassenring $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{p}$, so ist \bar{p}_i , wie man leicht bestätigt, ein von $\bar{\mathfrak{o}}$ und Null verschiedenes Primideal aus $\bar{\mathfrak{o}}$. Wenn man mit \bar{a} das Ideal aus $\bar{\mathfrak{o}}$ bezeichnet, welches aus den die Elemente aus a enthaltenden Restklassen aus $\bar{\mathfrak{o}}$ besteht, so gilt:

$$\bar{a} = \bar{p}_1 \dots \bar{p}_r.$$

Ebenso entstehen aus $(a, \mathfrak{p})^2$, (a^2, \mathfrak{p}) , b, c bzw. die Ideale $(\bar{a}, \bar{\mathfrak{p}})^2 = (\bar{a}^2)$, $(\bar{a}^2, \bar{\mathfrak{p}}) = (\bar{a}^2)$, b, c , wo \bar{a} die a enthaltende Restklasse aus $\bar{\mathfrak{o}}$ bedeutet. Ferner gilt

$$(\bar{a}, \bar{\mathfrak{p}})^2 = (\bar{a}^2) = \bar{a}\bar{c}, \quad (\bar{a}^2, \bar{\mathfrak{p}}) = (\bar{a}^2) = \bar{b}\bar{c},$$

woraus $(\bar{a}^2)\bar{b} = \bar{a}\bar{b}\bar{c} = (\bar{a}^2)\bar{a}$ folgt. Weil aber $\bar{\mathfrak{o}}$ keinen Nullteiler enthält,

so ist $\bar{a} = \bar{b}$. Das Ideal \bar{b} ist daher von \mathfrak{o} verschieden. Ist nun $\bar{b} = \mathfrak{p}'_1 \dots \mathfrak{p}'_s$ die Primfaktorzerlegung von \bar{b} , so gilt im Restklassenring $\bar{\mathfrak{o}}$:

$$\bar{\mathfrak{p}}_1 \dots \bar{\mathfrak{p}}_r = \bar{a} = \bar{b} = \bar{\mathfrak{p}}'_1 \dots \bar{\mathfrak{p}}'_s.$$

Es sei etwa $\bar{\mathfrak{p}}_1$ ein minimales Ideal unter $\bar{\mathfrak{p}}_1, \dots, \bar{\mathfrak{p}}_r, \bar{\mathfrak{p}}'_1, \dots, \bar{\mathfrak{p}}'_s$. Dann muß unter $\bar{\mathfrak{p}}'_1, \dots, \bar{\mathfrak{p}}'_s$ ein Ideal, etwa $\bar{\mathfrak{p}}'_1$ vorhanden sein, welches in $\bar{\mathfrak{p}}_1$ enthalten ist, woraus $\bar{\mathfrak{p}}_1 = \bar{\mathfrak{p}}'_1$ folgt. Da $\mathfrak{p}_1, \mathfrak{p}'_1$ beide \mathfrak{p} enthalten, so ist sicher $\mathfrak{p}_1 = \mathfrak{p}'_1$; dies ist aber ein Widerspruch. Es muß daher $(a, \mathfrak{p})^2 = (a^2, \mathfrak{p})$ sein.

Da $(a^2, \mathfrak{p}) = (a^2, a\mathfrak{p}, \mathfrak{p}^2)$ ist, genügt ein beliebiges Element π aus \mathfrak{p} der Kongruenz:

$$\pi \equiv \xi a^2 + a\pi_1 \pmod{\mathfrak{p}^2},$$

wo ξ ein Element aus \mathfrak{o} und π_1 ein Element aus \mathfrak{p} bezeichnet; d. h. $\xi a^2 \equiv 0 \pmod{\mathfrak{p}}$. Da $\mathfrak{p} \ni a$ ist, so muß $\xi \equiv 0 \pmod{\mathfrak{p}}$ sein. Also ist π ein Element aus $(a\mathfrak{p}, \mathfrak{p}^2)$, woraus $\mathfrak{p} \subseteq (a\mathfrak{p}, \mathfrak{p}^2)$ folgt. Da andererseits $\mathfrak{p} \supseteq (a\mathfrak{p}, \mathfrak{p}^2)$, so ist $\mathfrak{p} = (a\mathfrak{p}, \mathfrak{p}^2) = (a, \mathfrak{p})\mathfrak{p}$; nach Voraussetzung muß unbedingt $(a, \mathfrak{p}) = \mathfrak{o}$ sein, w. z. b. w.

Satz 3. *In \mathfrak{o} existiert ein nilpotentes Primideal.*

Beweis. Wenn \mathfrak{o} ein Ring ohne Nullteiler ist, so ist das Nullideal offenbar prim und nilpotent.

Besitzt aber \mathfrak{o} einen Nullteiler a und ist für ein $b \neq 0$ $ab = 0$, so ist wegen $(a)(b) = (ab) = (0)$ das Nullideal (0) als Produkt aus endlich vielen Primidealen darstellbar. Es sei

$$(0) = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

eine solche Darstellung von (0) als Produkt aus Primidealen, daß die Anzahl r der Primfaktoren minimal ist. Dann ist $\mathfrak{p}_1 = \dots = \mathfrak{p}_r$. Denn wären genau $s < r$ Primfaktoren gleich \mathfrak{p}_1 , so könnte man $(0) = \mathfrak{p}_1^s \mathfrak{q}$ setzen, wo \mathfrak{q} das Primideal \mathfrak{p}_1 als Primfaktor nicht enthielte. Nach Satz 2 gälte dann:

$$(\mathfrak{p}_1^s, \mathfrak{q}) = \mathfrak{o},$$

woraus $\mathfrak{p}_1^s = \mathfrak{p}_1^s (\mathfrak{p}_1^s, \mathfrak{q}) = (\mathfrak{p}_1^{2s}, \mathfrak{p}_1^s \mathfrak{q}) = \mathfrak{p}_1^{2s}$ folgte. Wegen $\mathfrak{p}_1^s \neq (0)$ ergibt sich aus $\mathfrak{p}_1^{2s} = \mathfrak{p}_1^s$ ein Widerspruch. \mathfrak{p}_1 ist also ein nilpotentes Primideal.

Zusatz. Das Radikal von \mathfrak{o} ist prim.

Satz 4. *Nur ein nilpotentes Ideal aus \mathfrak{o} kann das von Null verschiedene annullierende Ideal besitzen.*

Beweis. Nach Satz 3 existiert in \mathfrak{o} ein nilpotentes Primideal \mathfrak{p} . Es sei α ein solches Ideal aus \mathfrak{o} , daß sein annullierendes Ideal \mathfrak{m} von Null verschieden ist. Wir beweisen dann $\alpha \subseteq \mathfrak{p}$. Ist nämlich nicht $\alpha \subseteq \mathfrak{p}$, so muß $\mathfrak{m} \subseteq \mathfrak{p}$ sein, weil $\alpha \mathfrak{m} = (0) \subseteq \mathfrak{p}$ und \mathfrak{p} ein Primideal ist. Geht nun \mathfrak{p} mit dem genauen Exponenten e in \mathfrak{m} auf, so kann man $(0) = \alpha \mathfrak{m} = \mathfrak{p}^e \mathfrak{q}$ mit $(\mathfrak{p}, \mathfrak{q}) = \mathfrak{o}$ setzen. Weil $(\mathfrak{p}^e, \mathfrak{q}) = \mathfrak{o}$ ist, so erhält man offenbar:

$$\mathfrak{p}^e = \mathfrak{p}^e (\mathfrak{p}^e, \mathfrak{q}) = (\mathfrak{p}^{2e}, \mathfrak{p}^e \mathfrak{q}) = \mathfrak{p}^{2e};$$

wegen $\mathfrak{p}^e \supseteq \mathfrak{m} \neq (0)$ ergibt die letzte Gleichung einen Widerspruch.

α muß also in \mathfrak{p} enthalten sein; d. h. α ist ein nilpotentes Ideal.

Satz 5. Wenn \mathfrak{o} ein Ring mit Nullteiler ist, so gibt es ein einziges Primideal aus \mathfrak{o} , welches sogar nilpotent ist, und jedes vom Einheitsideal verschiedene Ideal ist eine Potenz des nilpotenten Primideales.

Beweis. Nach Satz 3 existiert ein nilpotentes Primideal \mathfrak{p} aus \mathfrak{o} ; dieses Primideal \mathfrak{p} ist sicher von Null verschieden, weil \mathfrak{o} Nullteiler besitzt. Es wäre \mathfrak{p}' ein von \mathfrak{p} verschiedenes Primideal aus \mathfrak{o} . Dann gälte nach Satz 2: $(\mathfrak{p}, \mathfrak{p}') = \mathfrak{o}$. Bezeichnet nun e den kleinsten Exponenten derart, daß $\mathfrak{p}^e = (0)$ ist, so bestände die Gleichung: $(0) \neq \mathfrak{p}^{e-1} = \mathfrak{p}^{e-1}(\mathfrak{p}, \mathfrak{p}') = (\mathfrak{p}^e, \mathfrak{p}'\mathfrak{p}^{e-1}) = \mathfrak{p}'\mathfrak{p}^{e-1}$, was mit der Voraussetzung im Widerspruch steht. \mathfrak{o} besitzt also nur ein einziges Primideal, welches sogar nilpotent ist.

Satz 6. Es sei \mathfrak{a} ein von \mathfrak{o} und (0) verschiedenes Ideal und \mathfrak{b} ein Teiler von \mathfrak{a} . Ist dann $\mathfrak{a} = \mathfrak{p}_1^{\sigma_1} \dots \mathfrak{p}_r^{\sigma_r}$ eine Primfaktorzerlegung von \mathfrak{a} , so ist

$$\mathfrak{b} = \mathfrak{p}_1^{\rho_1} \dots \mathfrak{p}_r^{\rho_r} \quad \text{mit} \quad \rho_i \geq \sigma_i \geq 0.$$

Dabei sind $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ voneinander verschiedene Primideale aus \mathfrak{o} , und für ein Primideal \mathfrak{p}_i ist \mathfrak{p}_i^0 wie üblich gleich \mathfrak{o} gesetzt.

Beweis. Da jeder Primteiler von \mathfrak{b} stets ein Primteiler von \mathfrak{a} ist und jedes Primideal aus \mathfrak{o} nach Satz 2 teilerlos ist, so kann \mathfrak{b} nur $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ als Primfaktoren besitzen; d. h. es gilt: $\mathfrak{b} = \mathfrak{p}_1^{\rho_1} \dots \mathfrak{p}_r^{\rho_r}$. Es bleibt also nur zu zeigen, daß für jedes i $\rho_i \geq \sigma_i$ ist.

Angenommen, es wäre für ein i $\sigma_i > \rho_i$. Dann kann man ohne Einschränkung $i=1$ annehmen. Betrachten wir den Idealquotienten¹⁾ $\mathfrak{a} : \mathfrak{p}_1^{\sigma_1} = \mathfrak{c}$, so folgt aus $\mathfrak{p}_1^{\sigma_1}(\mathfrak{p}_1^{\sigma_2} \dots \mathfrak{p}_r^{\sigma_r}) = \mathfrak{a}$, daß $\mathfrak{p}_1^{\sigma_2} \dots \mathfrak{p}_r^{\sigma_r} \subseteq \mathfrak{c}$ ist²⁾. Da aber $\mathfrak{a} = \mathfrak{p}_1^{\sigma_1}(\mathfrak{p}_1^{\sigma_2} \dots \mathfrak{p}_r^{\sigma_r}) \subseteq \mathfrak{p}_1^{\sigma_1} \mathfrak{c} \subseteq \mathfrak{a}$ ist, so gilt $\mathfrak{c} = \mathfrak{p}_1^{\sigma_2} \dots \mathfrak{p}_r^{\sigma_r}$. Setzen wir nun $\mathfrak{b} : \mathfrak{p}_1^{\rho_1} = \mathfrak{d}$, so ist $\mathfrak{c} \subseteq \mathfrak{d}$ wegen $\mathfrak{a} \subseteq \mathfrak{b}$. Aus $\mathfrak{b} = \mathfrak{p}_1^{\rho_1}(\mathfrak{p}_1^{\sigma_1 - \rho_1} \mathfrak{p}_1^{\rho_2} \dots \mathfrak{p}_r^{\rho_r}) \subseteq \mathfrak{p}_1^{\rho_1} \mathfrak{d} \subseteq \mathfrak{b}$ folgt ohne weiteres $\mathfrak{p}_1^{\sigma_1 - \rho_1} \mathfrak{p}_1^{\rho_2} \dots \mathfrak{p}_r^{\rho_r} = \mathfrak{d}$; wegen $\mathfrak{c} \subseteq \mathfrak{d}$ muß \mathfrak{p}_1 auch ein Primteiler von \mathfrak{c} sein, was aber nach Satz 2 unmöglich ist. Es ist daher $\rho_1 \geq \sigma_1$.

Zusatz 1. In \mathfrak{o} gilt der Teilerkettensatz.

Zusatz 2. In \mathfrak{o} gilt der abgeschwächte Vielfachenkettensatz.

Satz 7. Ist \mathfrak{p} ein beliebiges Primideal aus \mathfrak{o} , so existiert kein echtes Zwischenideal zwischen \mathfrak{p} und \mathfrak{p}^2 .

Beweis. Wenn $\mathfrak{p} = (0)$ oder $\mathfrak{p} = \mathfrak{o}$ ist, so bleibt nichts zu beweisen. Wir nehmen also $\mathfrak{p} \neq (0)$ und $\mathfrak{p} \neq \mathfrak{o}$ an.

Ist zunächst $\mathfrak{p}^2 \neq (0)$, so ist jeder echte Teiler von \mathfrak{p}^2 nach Satz 6 von der Form \mathfrak{p}^ν mit $0 \leq \nu < 2$. Wenn aber $\mathfrak{p}^2 = (0)$ ist, so ist ein echter Teiler von \mathfrak{p}^2 nach Satz 5 auch von der Form \mathfrak{p}^ν mit $0 \leq \nu < 2$. Jedenfalls existiert zwischen \mathfrak{p} und \mathfrak{p}^2 kein echtes Zwischenideal.

Aus den oben bewiesenen Sätzen folgt unsere im Eingang aufgestellte Bedingung; ebenso erhält man daraus die von Herrn K. Kubo aufgestellte Bedingung:

- 1) In \mathfrak{o} existiert das Einselement.

1) Van der Waerden, Moderne Algebra, II. Teil (1940), S. 24.

2) Wenn $r=1$ ist, so ist $\mathfrak{c} = \mathfrak{o}$.

- 2) In \mathfrak{o} gilt der abgeschwächte Vielfachenkettensatz für Ideale.
- 3) Zwischen \mathfrak{p} und \mathfrak{p}^2 existiert kein echtes Zwischenideal.
- 4) Das Radikal von \mathfrak{o} ist prim.

Bemerkung. Unter der Voraussetzung, daß in einem kommutativen Ring \mathfrak{o} jedes vom Einheits- und Nullideal verschiedene Ideal eindeutig als Produkt aus endlich vielen Primidealen darstellbar ist, ist \mathfrak{o} entweder ein Ring ohne Nullteiler oder nach Satz 5 ein solcher, daß in \mathfrak{o} jedes vom Einheitsideal verschiedene Ideal stets eine Potenz eines einzigen nilpotenten Primideals wird.
