32. *Eine hinreichende Bedingung für die eindeutige Primfaktorzerlegung der Ideale in einem kommutativen Ring.*

Von Yosi KOBAYASI und Mikao MORIYA.

Mathematisches Institut der Kaiserlichen Hokkaido Universität, Sapporo.

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

In einem kommutativen Ring $\mathfrak{o}$ seien die folgenden Axiome erfüllt:

1) In $\mathfrak{o}$ existiert das Einselement.
2) Für jedes Ideal aus $\mathfrak{o}$ gilt der Teilerkettensatz.
3) Zu jedem Primideal[1] $\mathfrak{p}$ aus $\mathfrak{o}$ existiert stets kein echtes Zwischenideal zwischen $\mathfrak{p}$ und $\mathfrak{p}^2$.
4) Nur ein nilpotentes Ideal kann das von Null verschiedene annullierende Ideal[2] besitzen.

Unter den obigen Axiomen beweisen wir folgenden

Hauptsatz. *Jedes vom Null- und Einheitsideal verschiedene Ideal aus* $\mathfrak{o}$, *wenn es überhaupt existiert, läßt sich als Produkt aus endlich vielen, vom Null- und Einheitsideal verschiedenen Primidealen darstellen. Ferner sind diese Produktdarstellungen bis auf die Reihenfolge der Primfaktoren*[3] *eindeutig bestimmt.*

1. Satz 1. *Es sei* $\mathfrak{c}$ *ein von Null verschiedenes Ideal und* $\mathfrak{p}$ *ein Primideal aus* $\mathfrak{o}$. *Gilt dann für ein Ideal* $\mathfrak{q} \geqq \mathfrak{p}$ *die Gleichung* $\mathfrak{cp}=\mathfrak{cq}$, *so ist stets* $\mathfrak{p}=\mathfrak{q}$.

Beweis. Da für das Ideal $\mathfrak{c}$ der Teilerkettensatz gilt, so besitzt $\mathfrak{c}$ bekanntlich eine Idealbasis $\gamma_1, \cdots, \gamma_n$. Für ein beliebiges Element τ aus $\mathfrak{q}$ gilt nun:

$$\tau\gamma_i = p_{i1}\gamma_1 + \cdots + p_{in}\gamma_n \qquad (i=1, \ldots, n),$$

wo die p_{ij} Elemente aus $\mathfrak{p}$ bezeichnen. Hieraus folgt ohne weiteres:

$$\gamma_i \begin{vmatrix} p_{11}-\tau & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{n1} & & p_{nn}-\tau \end{vmatrix} = 0 \qquad (i=1, \ldots, n).$$

Bezeichnet man nun mit Δ die Determinante $\begin{vmatrix} p_{11}-\tau & \cdots & p_{1n} \\ \vdots & & \\ p_{n1} & \cdots & p_{nn}-\tau \end{vmatrix}$, so erhält man die Kongruenz

---

1) Wir rechnen $\mathfrak{o}$ unter die Primideale und ebenso auch (0), falls es die Primidealeigenschaft besitzt.

2) Für die Definition des annullierenden Ideales vergleiche man unsere vorangehende Note: Mikao Moriya und Yosi Kobayasi, Eine notwendige Bedingung für die Primfaktorzerlegung der Ideale in einem kommutativen Ring.

3) Unter einem Primfaktor eines Ideales verstehen wir stets ein vom Null- und Einheitsideal verschiedenes Primideal.

$$\tau^n \equiv 0 \mod \mathfrak{p},$$

wenn $\Delta = 0$ ist. Hieraus folgt sofort $\tau \equiv 0 \mod \mathfrak{p}$.

Ist aber $\Delta \neq 0$, so ist nach Axiom 4) das Hauptideal (Δ) aus $\mathfrak{o}$ nilpotent; es existier also ein Exponent $\nu (> 1)$, für den $\Delta^\nu = 0$ wird. Dann besteht offenbar die Kongruenz

$$\tau^{n\nu} \equiv 0 \mod \mathfrak{p},$$

woraus wieder $\tau \equiv 0 \mod \mathfrak{p}$ folgt. Auf jeden Fall ist ein beliebiges Element aus $\mathfrak{q}$ in $\mathfrak{p}$ enthalten. Weil anderseits $\mathfrak{q} \geqq \mathfrak{p}$ ist, so gilt offenbar $\mathfrak{p} = \mathfrak{q}$.

Zusatz. Es sei $\mathfrak{p}^\nu (\nu \geqq 0)$ eine Potenz eines von $\mathfrak{a}$ verschiedenen Primideals $\mathfrak{p}$ aus $\mathfrak{o}$, und $\mathfrak{p}^\nu$ kein Nullideal. Dann ist für eine natürliche Zahl $\mu > \nu$ stets $\mathfrak{p}^\mu \neq \mathfrak{p}^\nu$.

Beweis. Da $\mu \geqq \nu + 1$ ist, so folgt aus $\mathfrak{p}^\mu = \mathfrak{p}^\nu$ die Gleichung $\mathfrak{p}^{\nu+1} = \mathfrak{p}^\nu = \mathfrak{p}^\nu \mathfrak{o}$. Weil $\mathfrak{p}^\nu$ kein Nullideal ist, so gilt nach Satz 1:

$$\mathfrak{p} = \mathfrak{o},$$

was aber ein Widerspruch ist.

Satz 2. *Jedes von Null verschiedene Primideal ist teilerlos.*

Beweis. Existiert zwischen einem von (0) verschiedenen Primideal $\mathfrak{p}$ und $\mathfrak{o}$ ein echtes Zwischenideal, so beweist man mit Hilfe des Axioms 1) aus den Wohlordnungsschlüssen, daß es zwischen $\mathfrak{p}$ und $\mathfrak{o}$ ein von $\mathfrak{p}$ und $\mathfrak{o}$ verschiedenes Primideal $\mathfrak{m}$ gibt. Dann gilt offenbar:

$$\mathfrak{p}^2 \subseteqq \mathfrak{p}\mathfrak{m} \subseteqq \mathfrak{p}\mathfrak{o} = \mathfrak{p}.$$

Nach Axiom 3) sind nur die beiden Fälle möglich:

$$\text{i)}\ \mathfrak{p}^2 = \mathfrak{p}\mathfrak{m} \quad \text{und} \quad \text{ii)}\ \mathfrak{p}\mathfrak{m} = \mathfrak{p}\mathfrak{o}.$$

i) $\mathfrak{p}^2 = \mathfrak{p}\mathfrak{m}$. Nach Satz 1 muß dann $\mathfrak{p} = \mathfrak{m}$ sein entgegen der Annahme über $\mathfrak{m}$.

ii) $\mathfrak{p}\mathfrak{m} = \mathfrak{p}\mathfrak{o}$. Aus Satz 1 folgt in diesem Fall $\mathfrak{m} = \mathfrak{o}$, was ein Widerspruch ist.

Daher ist $\mathfrak{p}$ teilerlos.

Satz 3. *Jede Primidealpotenz ist primär.*

Beweis. Es sei $\mathfrak{p}^e (e \geqq 1)$ eine Potenz eines Primideals $\mathfrak{p}$ aus $\mathfrak{o}$. Dann gilt der Satz in trivialer Weise, wenn $\mathfrak{p} = (0)$ oder $\mathfrak{p} = \mathfrak{o}$ ist. Wir wollen also im folgenden $\mathfrak{p} \neq (0)$ und $\mathfrak{p} \neq \mathfrak{o}$ annehmen.

Ist nun $ab \equiv 0 \mod \mathfrak{p}^e$ und $a \not\equiv 0 \mod \mathfrak{p}^e$, so genügt es, $b \equiv 0 \mod \mathfrak{p}$ zu beweisen. Wäre also $b \not\equiv 0 \mod \mathfrak{p}$, so gälte nach Satz 2 $(\mathfrak{p}, b) = \mathfrak{o}$; daraus folgte $\mathfrak{o} = (\mathfrak{p}, b)^e \subseteqq (\mathfrak{p}^e, b)$. Durch Multiplikation von $\mathfrak{o} = (\mathfrak{p}^e, b)$ mit (a) erhielte man:

$$\big((a)\mathfrak{p}^e, ba\big) = (a);$$

dies ist aber ein Widerspruch, weil $(a) = \big((a)\mathfrak{p}^e, ab\big) \subseteqq \mathfrak{p}^e$ ist, w. z. b. w.

Satz 4. *Jedes Primärideal aus $\mathfrak{o}$ ist eine Primidealpotenz.*

Beweis. Es sei $\mathfrak{q}$ ein Primärideal aus $\mathfrak{o}$ und $\mathfrak{p}$ das zu $\mathfrak{q}$ gehörige Primideal. Im Falle, wo $\mathfrak{p} = (0)$ oder $\mathfrak{p} = \mathfrak{o}$ ist, ist offenbar $\mathfrak{q} = (0)$ oder

$\mathfrak{q}=\mathfrak{p}$. Wir wollen also annehmen, daß $\mathfrak{p}$ von (0) und $\mathfrak{o}$ verschieden ist. Da in diesem Falle nach Zusatz zu Satz 1 stets $\mathfrak{p}^2 \neq \mathfrak{p}$ ist, so gibt es ein genau durch $\mathfrak{p}$ teilbares Element π, für das $(\pi, \mathfrak{p}^2)=\mathfrak{p}$ gilt, weil $\mathfrak{p} \geqq (\pi, \mathfrak{p}^2) \supset \mathfrak{p}^2$ ist. Daraus schließt man durch vollständige Induktion $\mathfrak{p}^\nu=(\pi^\nu, \mathfrak{p}^{\nu+1})$. Nun existiert ein Exponent μ derart, daß $\mathfrak{p}^\mu \leqq \mathfrak{q}$, aber nicht mehr $\mathfrak{p}^{\mu-1} \leqq \mathfrak{q}$ ist. Ebenso gibt es einen Exponenten ν derart, daß $\mathfrak{q} \leqq \mathfrak{p}^\nu$, aber nicht mehr $\mathfrak{q} \leqq \mathfrak{p}^{\nu+1}$ ist.

Ist nun q ein Element aus $\mathfrak{q}$, welches nicht durch $\mathfrak{p}^{\nu+1}$ teilbar ist, so gilt wegen $\mathfrak{q} \leqq \mathfrak{p}^\nu=(\pi^\nu, \mathfrak{p}^{\nu+1})$ die Kongruenz:

$$q \equiv c\pi^\nu \mod \mathfrak{p}^{\nu+1};$$

dabei ist offenbar $c \not\equiv 0 \mod \mathfrak{p}$. Da nach Satz 3 $(\mathfrak{p}^{\nu+1}, \mathfrak{q})$ ein zu $\mathfrak{p}$ gehöriges Primärideal ist, so folgt ohne weiteres

$$\pi^\nu \equiv 0 \mod (\mathfrak{p}^{\nu+1}, \mathfrak{q})^{1)}.$$

Wenn also $\nu \neq \mu$ ist, so ergibt sich wegen $\nu < \mu$ durch Multiplikation von $\pi^{\mu-\nu-1}$ mit der obligen Kongruenz:

$$\pi^{\mu-1} \equiv 0 \mod (\mathfrak{p}^\mu, \mathfrak{q}).$$

Da $\mathfrak{q} \geqq \mathfrak{p}^\mu$ ist, so ist sicher $\pi^{\mu-1} \equiv 0 \mod \mathfrak{q}$, woraus entgegen der Annahme über μ $\mathfrak{q} \geqq (\pi^{\mu-1}, \mathfrak{p}^\mu)=\mathfrak{p}^{\mu-1}$ folgt. Es ist also $\mu=\nu$; d. h. $\mathfrak{q}$ ist eine Potenz von $\mathfrak{p}$.

Beweis des Hauptsatzes. Es sei $\mathfrak{a}$ ein vom Null- und Einheitsideal verschiedenes Ideal aus $\mathfrak{o}$. Dann läßt sich $\mathfrak{a}$ als Durchschnitt der endlich vielen Primärideale, welche bzw. zu verschiedenen Primidealen aus $\mathfrak{o}$ gehören, darstellen[2]. Nach Satz 4 ist also $\mathfrak{a}$ als Durchschnitt von endlich vielen Primidealpotenzen darstellbar, von denen je zwei nach Satz 2 einander teilerfremd sind. Wir können daher in geläufiger Weise schließen, daß $\mathfrak{a}$ als ein Produkt aus den Potenzen von endlich vielen, verschliedenen Primidealen aus $\mathfrak{o}$ darstellbar ist, wo insbesondere alle Primteiler von $\mathfrak{a}$ von (0) und $\mathfrak{o}$ verschieden sind.

Offenbar treten in jeder Darstellung von $\mathfrak{a}$ als Primidealpotenzenprodukt genau dieselben Primteiler auf. Es seien also $\mathfrak{a}=\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ und $\mathfrak{a}=\mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'}$ die Primfaktorzerlegungen von $\mathfrak{a}$. Ferner sei für einen Index i, also etwa $i=1$, $e_1 > e_1'$. Dann ist $(\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r})=\mathfrak{o}$, weil $\mathfrak{p}_1^{e_1}$, $\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$ einander teilerfremd sind. Multipliziert man die obige Gleichung mit $\mathfrak{p}_1^{e_1}$, so ergibt sich:

$$(\mathfrak{p}_1^{2e_1}, \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r})=(\mathfrak{p}_1^{2e_1}, \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'})=\mathfrak{p}_1^{e_1}.$$

Setzt man dabei $e^*=\mathrm{Min}(2e_1, e_1')$, so ist sicher $\mathfrak{p}_1^{e_1}$ in $\mathfrak{p}_1^{e^*}$ enthalten; wegen $\mathfrak{p}_1^{e_1^*} \leqq \mathfrak{p}_1^{e_1}$ muß dann $\mathfrak{p}_1^{e_1^*}=\mathfrak{p}_1^{e_1}$ sein, was aber mit dem in Zusatz zu Satz 1 Bewiesenen im Widerspruch steht.

---

1) Van der Waerden, Moderne Algebra, II. Teil (1940), S. 28.
2) Van der Waerden, loc. cit., S. 30-34.

2. Unabhängigkeit der Axiome. Im folgenden wollen wir durch Beispiele zeigen, daß die im Anfang aufgestellten Axiome voneinander unabhängig sind.

1. Es sei k ein Körper von der Charakteristik 2 und $P(x)$ der Körper der Potenzreihen von x, deren Koeffizienten Elemente aus k sind. Dann ist ein von Null verschiedenes Element $\varphi(x)$ aus $P(x)$ von der Form: $\varphi(x)=x^{\nu}+c_{\nu+1}x^{\nu+1}+\cdots\cdots$, wo ν eine ganze rationale Zahl und $c_{\nu+1}, \cdots$ Elemente aus k bezeichnen. Wir wollen nun den Grad ν des Anfangsgliedes von $\varphi(x)$ kurz den Grad von $\varphi(x)$ nennen. Im Körper $P(x)$ bildet die Gesamtheit aller Flemente, deren Grade positiv sind, mit dem Nullelement zusammen einen Teilring $\mathfrak{o}$ von $P(x)$. Der Ring $\mathfrak{o}$ besitzt offenbar kein Einselement. In $\mathfrak{o}$ ist jedes Ideal stets Hauptideal. Dazu genügt es nur zu zeigen, daß ein von (0) verschiedenens Ideal $\mathfrak{a}$ aus $\mathfrak{o}$ Hauptideal ist. In $\mathfrak{a}$ existiert ein solches Element $a(x)\neq 0$, dessen Grad minimal ist. Es sei $a'(x)$ ein von Null verschiedenes Element aus $\mathfrak{a}$. Ist dann der Grad von $a'(x)$ größer als der von $a(x)$, so gibt es ein Element $q(x)$ aus $\mathfrak{o}$ derart, daß $a'(x)=q(x)a(x)$ ist. It aber der Grad von $a'(x)$ gleich dem von $a(x)$, so ist $b(x)=a'(x)-a(x)$ entweder gleich Null oder ein Element aus $\mathfrak{o}$, dessen Grad größer ist als der von $a(x)$. Jedenfalls gibt es ein Element $q(x)$ aus $\mathfrak{o}$ derart, daß $b(x)=q(x)a(x)$ ist. Somit ist gezeigt, daß $\mathfrak{a}$ das von $a(x)$ erzeugte Hauptideal ist.

Wie man sich leicht überzeugt, besitzen alle erzeugenden Elemente von $\mathfrak{a}$ einen und denselben Grad; wir nennen also den Grad eines erzeugenden Elementes schlechthin den Grad von $\mathfrak{a}$. Ist nun der Grad von $\mathfrak{a}$ gleich $\nu(>0)$, so bestätigt man leicht, daß $\mathfrak{a}=(x^{\nu})=(x)^{\nu}=\mathfrak{o}^{\nu}$ ist. In $\mathfrak{o}$ wird also jedes von Null verschiedene Ideal stets eine Potenz von $\mathfrak{o}$. Daher gelten in $\mathfrak{o}$ die Axiome 2) und 3). Da $\mathfrak{o}$ keinen Nullteiler besitzt, so ist das Axiom 4) in trivialer Weise erfüllt.

2. Wir bezeichenen mit l eine ungerade Primzahl und mit ζ_{ν} eine primitive l^{ν}-te Einheitswurzel. Im Körper $R(\zeta_{\nu})$, welcher aus dem rationalen Zahlkörper R durch Adjunktion von ζ_{ν} entsteht, gilt bekanntlich folgende Primidealzerlegung: $(l)=(1-\zeta_{\nu})^{l^{\nu-1}(l-1)}$. Hieraus schließt man leicht, daß im Körper $R(\zeta_{\nu+1})$ die Gleichung $(1-\zeta_{\nu})=(1-\zeta_{\nu+1})^{l}$ gilt. Bildet man nun den Vereinigungskörper k von den Körpern $R(\zeta_1), \cdots, R(\zeta_{\nu}), \cdots$, so besitzt im Ring $\mathfrak{o}$ aller ganzen algebraischen Zahlen aus k das Hauptideal (l) nur einen einzigen Primteiler $\mathfrak{l}$. Ferner sind die Hauptideale $(1-\zeta_1), \cdots, (1-\zeta_{\nu}), \cdots$ aus $\mathfrak{o}$ alle echte Teiler von (l), und für $\nu\geqq 1$ ist stets $(1-\zeta_{\nu+1})$ echter Teiler von $(1-\zeta_{\nu})$. Im Ring $\mathfrak{o}$ gilt also für das Ideal (l) der Teilerkettensatz nicht mehr, aber die Axiome 1) und 4) sind offenbar erfüllt. Für die Primideale (0), $\mathfrak{l}$, $\mathfrak{o}$ sind bekanntlich $(0)^2=(0)$ $\mathfrak{l}^2=\mathfrak{l}$, $\mathfrak{o}^2=\mathfrak{o}$, aber für ein anderes Primideal $\mathfrak{p}$ aus $\mathfrak{o}$ ist stets $\mathfrak{p}^2\neq\mathfrak{p}$. Auf jeden Fall beweist man ohne Schwierigkeit, daß zwischen $\mathfrak{p}$ und $\mathfrak{p}^2$ kein echtes Zwischenideal existiert. Das Axiom 3) ist also auch in $\mathfrak{o}$ erfüllt.

3. Es sei k ein Körper und $\mathfrak{o}=k[x, y]$ ein Integritätsbereich von Polynomen zweier Unbestimmten x, y mit Koeffizienten aus k. Dann ist offenbar das Ideal (x, y) aus $\mathfrak{o}$ ein Primideal. Da zwischen

(x, y) und $(x, y)^2$ ein echtes Zwischenideal (x^2, y) existiert, so ist in $\mathfrak{o}$ das Axiom 3) nicht erfüllt, aber die übrigen Axiome sind sicher erfüllt.

4. In einem kommutativen Ring $\mathfrak{o}$, welcher als die direkte Summe der Körper K_1 und K_2 definiert ist, existieren nur folgende Ideale: (0), K_1, K_2, $\mathfrak{o}$. Ferner sind $\mathfrak{o}$, K_1 und K_2 alle Primideale. Hieraus sehen wir leicht ein, daß in $\mathfrak{o}$ die Axiome 1), 2), 3) erfüllt sind, aber das letzte Axiom nicht mehr, weil $K_1 \neq (0)$ den Körper K_2 als das annullierende Ideal besitzt.