8. Über ein bewertungstheoretisches Axiomensystem für die Dedekind-Noethersche Idealtheorie.

Von Kameo MATUSITA.

(Eingegangen am 4. Februar, 1944.)

Zwischen Ideal- und Bewertungstheorie⁽¹⁾ besteht bekanntlich ein enger Zusammenhang. Insbesondere lässt sich das Axiomensystem für die Dedekind-Noethersche Idealtheorie bewertungstheoretisch formulieren, wie es u.a. von M. Moriya⁽²⁾ bzw. E. Artin⁽³⁾ angegeben ist. Im folgenden soll gezeigt werden, dass man durch Modifizierung des Axiomensystems von Artin ein etwas leichter handzuhabendes System bekommt, und dass dessen Anwendung auf die „Übergangssätze“ (Sätze 7, 8 w.u.) einfachere Beweise dieser Sätze ergibt, als bisher in der Literatur geschehen ist. Beim Beweis der Äquivalenz unseres Axiomensystems mit dem Bestehen des Fundamentalsatzes der Idealtheorie werden wir sogar etwas mehr zeigen: nämlich die Tatsache, dass aus der Darstellbarkeit jeden Ideals als Produkt der Primideale die Eindeutigkeit dieser Darstellung folgt (§2). Die folgende Darstellung setzt keinerlei Kenntnis der früheren Arbeit voraus.

§ 1.

k sei ein Körper, $W = \{w\}$ ein System der Exponentenbewertungen von k , und $\mathfrak{o}$ ein Ring mit k als Quotientenkörper. Als eine notwendige

---

(1) Für die Bewertungstheorie im allgemeinen siehe ferner: A. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper*, Math. Zeits. 39, 1935.

(2) M. Moriya, *Bewertungstheoretischer Aufbau der multiplikativen Idealtheorie*, Journ. Fac. Sci. Hokkaido Imp. Univ. Ser. 1, vol. 3, 1939.

Moriya stellt als Axiomensystem für die Dedekind-Noethersche Idealtheorie folgendes auf: I, II, III (s. § 1) und

MIV. Zu zwei beliebigen verschiedenen Bewertungen w, w' aus W gibt es zwei Elemente c, c' in $\mathfrak{o}$, für welche $w(c) > 0$, $w'(c) = 0$, und $w(c') = 0$, $w'(c') > 0$ gelten.

MV. Es gibt nur einziges nullwertiges Ideal. Dabei versteht man unter einem nullwertigen Ideal ein solches, dass der kleinste unter den Werten von dessen Elementen für jede Bewertung aus W Null ist.

Dort ist noch die Idealtheorie auch von dem allgemeineren Standpunkt auf Grund von I, II, III und MIV diskutiert.

(3) Dies ist berichtet in der Arbeit: K. Asano und T. Nakayama, *A remark on the arithmetic in a subfield*, Proc. Imp. Acad. Tokyo 1940.

Dort ist die Bedingung III versehentlich ausgelassen, wie mir Herr Nakayama freundlich mitgeteilt hat.

und hinreichende Bedingung dafür, dass in $\mathfrak{o}$ die Dedekind-Noethersche Idealtheorie gilt, d.h. dass jedes ganze Ideal eindeutig darstellbar als Produkt der endlichvielen Primideale ist, hat E. Artin folgendes Axiomensystem aufgestellt:

- I. $\mathfrak{o} = \bigcap_{w \in W} \mathfrak{B}_w$, wo $\mathfrak{B}_w$ der Bewertungsring von w ist, und w alle Bewertungen von W durchläuft,
- II. Jedes w aus W ist diskret,
- III. Jedes Element aus k hat für höchstens endlich viele verschiedene Bewertungen von W eine von Null verschiedenen Wert,
- AIV. Für beliebige, endlichviele Bewertungen aus W $w_1, w_2, \dots, w_r$ und ebensoviele Elemente $a_1, a_2, \dots, a_r$ aus k gibt es ein Element a aus k , so dass

$$w_i(a - a_i) > M \quad (i = 1, 2, \dots, r) \text{ für eine gegebene (reelle) Zahl } M,$$

und

$$w'(a) \geq 0 \text{ für jede von den oben genannten } w_i \text{ verschiedene Bewertung } w' \text{ aus } W$$

gelten.

Nun wollen wir statt dieser Axiome die folgenden zugrundelegen:

- I, II, III und
- IV. Zu zwei beliebigen verschiedenen Bewertungen w, w' aus W gibt es zwei Elemente c_1, c_2 in $\mathfrak{o}$, für welche $w(1 - c_1) > 0$, $w'(c_1) > 0$ und $w(c_2) > 0$, $w'(1 - c_2) > 0$ gelten.

In diesem Paragraphen weisen wir nach, erstens, dass dieses Axiomensystem mit dem Artinschen äquivalent ist, und zweitens, dass aus diesem System die Gültigkeit der Dedekind-Noetherschen Idealtheorie folgt.

Beim Beweis der Äquivalenz unseres Axiomensystems mit dem Artinschen haben wir nur zu zeigen, dass AIV aus I-IV folgt, da offenbar IV ein Spezialfall von AIV ist.

Zunächst wollen wir bemerken, dass aus dem Axiom I unmittelbar folgt der

Satz 1. Das Einselement 1 von k liegt in $\mathfrak{o}$.

Denn es ist ja $w(1) = 0$, und $1 \in \mathfrak{B}_w$ für alle $w \in W$.

Ferner dürfen wir uns wegen II ohne Beschränkung der Allgemeinheit immer so denken, dass jede Bewertung w aus W normiert ist: d.h. dass der kleinste positive Wert für w gleich 1 ist. Das soll also im folgenden stets vorausgesetzt werden.

Es folgt dann weiter

Hilfssatz 1.1. Für zwei verschiedene Bewertungen w, w' und eine beliebige Zahl M gibt es ein Element c in $\mathfrak{o}$, so dass

$$w(1-c) > M, \quad w'(c) > M$$

gilt.

Beweis. Nach IV gibt es ein Element c' in $\mathfrak{o}$, so dass

$$w(1-c') > 0, \quad w'(c') > 0$$

gilt. Ist ν eine natürliche Zahl $> M$, dann ist offenbar für $c = (1-(1-c')^\nu)^\nu$

$$w(1-c) \geq w(1-c')^\nu \geq \nu > M,$$

$$w'(c) \geq \nu w'(c') > M,$$

$$c \in \mathfrak{o}.$$

Hilfssatz 1.2. Sind $w, w_1, \dots, w_r$ von einander verschiedene Bewertungen und M eine beliebige Zahl, dann gibt es ein Element c in $\mathfrak{o}$, so dass

$$w(1-c) > M, \quad w_i(c) > M \quad (i = 1, 2, \dots, r)$$

gilt.

Beweis. Nach dem Hilfssatz 1.1 gibt es ein Element c_i in $\mathfrak{o}$ für jedes w_i , für welches $w(1-c_i) > M, w_i(c_i) > M$ besteht. Dann hat $c = c_1 c_2 \dots c_r$ offenbar die verlangte Eigenschaft.

Hilfssatz 1.3. Sind $w_1, w_2, \dots, w_{r+s}$ voneinander verschiedene Bewertungen und M eine beliebige Zahl, dann gibt es ein Element c in $\mathfrak{o}$, so dass

$$w_i(1-c) > M \quad (i = 1, 2, \dots, r),$$

$$w_j(c) > M \quad (j = r+1, r+2, \dots, r+s)$$

gilt.

Beweis. Für jedes w_i existiert nach dem Hilfssatz 1.2 ein Element c_i in $\mathfrak{o}$, für das

$$w_i(1-c_i) > M, \quad w_k(c_i) > M \quad \text{für } k \neq i$$

besteht. Dann genügt $c = c_1 + c_2 + \dots + c_r$ offenbar den aufgestellten Bedingungen.

Hilfssatz 1.4. Es seien eine Bewertung w aus W , ein Element a aus k und eine Zahl M gegeben. Dann existiert ein Element α aus k , für welches

$$w(\alpha - a) > M \quad \text{und} \quad w'(a) \geq 0 \quad \text{für jedes } w' \neq w$$

gilt.

Beweis. $w_1, w_2, \dots, w_r$ seien die von w verschiedenen Bewertungen, für welche das Element a negativwertig ist. Nach dem Hilfssatz 1.2 gibt es dann in $\mathfrak{o}$ ein Element c mit $w(1-c) > M - w(a)$ und $w_i(c) > -w_i(a)$ ($i = 1, 2, \dots, r$), $\alpha = ac$ ist dann ein gesuchtes Element.

Hilfssatz 1.5. Aus I-IV folgt AIV.

Beweis. Nach dem Hilfssatz 1.4 gibt es für jedes w_i ein Element a_i mit $w_i(a_i - a_i) > M$ und $w'(a_i) \geq 0$ für jedes $w' \neq w_i$. Andererseits gibt es nach dem Hilfssatz 1.2 ein Element c_i in $\mathfrak{o}$ mit $w_i(1-c_i) > M - w_i(a_i)$, $w_j(c_i) > M$ für $j \neq i$. Dann haben wir für $\alpha = \sum_{i=1}^r a_i c_i$

$$\begin{aligned} w_i(\alpha - a_i) &= w_i(a_1 c_1 + \dots + a_r c_r - a_i) \\ &\geq \text{Min}(w_i(a_1 c_1), \dots, w_i(a_{i-1} c_{i-1}), w_i(a_i c_i - a_i), \\ &\quad w_i(a_{i+1} c_{i+1}), \dots, w_i(a_r c_r)) \\ &> M \quad (i = 1, 2, \dots, r), \end{aligned}$$

weil $w_i(a_i c_i - a_i) = w_i(a_i c_i - a_i + a_i - a_i) \geq \text{Min}(w_i(a_i c_i - a_i), w_i(a_i - a_i)) > M$ ist, und $w'(a) \geq 0$ für $w' \neq w_i$ ($i = 1, 2, \dots, r$), w.z.b.w.

Die Äquivalenz unseres Systems mit dem Artinschen ist somit festgestellt.

Beim Beweis des Fundamentalsatzes, dass jedes ganze Ideal eindeutig darstellbar als Primidealprodukt ist, machen wir jedoch nicht von dem Hilfssatz 1.5 Gebrauch, sondern nur von dem Hilfssatz 1.4 mit $M = 0$, also von einem Spezialfall von jenen.

Im folgenden verstehen wir unter einem einer Bewertung w zugehörigen Primideal das Ideal aller Elemente aus $\mathfrak{o}$, die für w positivwertig sind.

$\mathfrak{p}$ sei ein einer Bewertung w zugehöriges Primideal, und a ein nicht in $\mathfrak{p}$ enthaltenes Element aus $\mathfrak{o}$. Nach dem Hilfssatz 1.4 gibt es dann ein Element b , so dass

$$w(a^{-1} - b) > 0 \quad \text{und} \quad w'(b) \geq 0 \quad \text{für} \quad w' \neq w$$

bestehen. Da $w(a) = 0$, also $w(a^{-1}) = 0$ ist, ist $w(b) = 0$, b gehört also zu $\mathfrak{o}$ nach I. Wir haben auch $w(1 - ab) > 0$, d.h. $ab \equiv 1 \pmod{\mathfrak{p}}$, was bedeutet, dass der Restklassenring $\mathfrak{o} \pmod{\mathfrak{p}}$ ein Körper ist. Somit haben wir den

Satz 2. *Das einer Bewertung zugehörige Primideal ist teilerlos.*

Nun sei p ein Primelement von w aus $\mathfrak{o}$, d.h. ein Element aus $\mathfrak{o}$ mit $w(p) = 1$. Nach dem Hilfssatz 1.4 haben wir dann ein Element q

mit $w(p^{-1} - q) > 0$ und $w'(q) \geq 0$ für $w' \neq w$. Wegen $w(p^{-1}) = -1$ ist $w(q) = -1$. Bezeichnen wir nun allgemein mit $w(a)$ den kleinsten unter den Werten für w , die von den Elementen aus einem Ideal a genommen sind, dann haben wir $w(qp) = 0$ und $w'(qp) \geq 0$ für $w' \neq w$. Wegen I ist qp also in $\mathfrak{o}$ enthalten. Nun sei p^{-1} wie gewöhnlich die Menge aller Elemente in k , deren Produkte mit p ganz ausfallen, d.h. in $\mathfrak{o}$ enthalten sind. p^{-1} enthält dann offenbar $\mathfrak{o}$ und q . Daher haben wir $\mathfrak{o} \supseteq pp^{-1} \supseteq p$ und $w(pp^{-1}) = 0$, also $pp^{-1} > p$, was $pp^{-1} = \mathfrak{o}$ zur Folge hat, weil p teilerlos ist. Falls $pp^{-1} = \mathfrak{o}$ gilt, sagen wir, dass p umkehrbar ist. Also haben wir den

Satz 3. *Das einer Bewertung zugehörige Primideal ist umkehrbar.*

Dieser Satz hat, wie leicht ersichtlich, folgendes zur Folge:

Die e -te Potenz p^e von einer Bewertung w zugehörigen Primideal p besteht aus allen Elementen in $\mathfrak{o}$, deren Werte für w gleich oder grösser als e sind.

Nun sei a ein Element aus $\mathfrak{o}$, und $w_1, \dots, w_r$ alle Bewertungen mit $w_i(a) = e_i > 0$. Dann ist $a \in p_i^{e_i}$, wo p_i das w_i zugehörige Primideal ist, mithin

$$(a) \subseteq p_1^{e_1} \cap \dots \cap p_r^{e_r} = p_1^{e_1} \dots p_r^{e_r},$$

da $p_1, \dots, p_r$ teilerlos, mithin zueinander teilerfremd sind. Ist umgekehrt c ein Element aus $p_1^{e_1} \dots p_r^{e_r}$, dann gilt offenbar $w\left(\frac{c}{a}\right) \geq 0$ für $w = w_1, \dots, w_r$, und sogar auch für andere beliebige Bewertung w' , da $w'(a) = 0$, $w'(c) \geq 0$ ist. Nach I gehört also $\frac{c}{a}$ zu $\mathfrak{o}$, was

$$(a) = p_1^{e_1} \dots p_r^{e_r}$$

zu Folge hat. Diese Zerlegung ist nach Satz 3 offenbar eindeutig. Mithin:

Jedes ganze Hauptideal in $\mathfrak{o}$ lässt sich eindeutig als das Produkt der endlichvielen Bewertungen aus W zugehörigen Primideale darstellen.

Es sei nun $\mathfrak{a}$ ein ganzes Ideal, und a ein Element aus $\mathfrak{a}$. Dann haben wir nach dem oben gewonnenen Resultat

$$\mathfrak{a} \supseteq (a) = p_1^{f_1} \dots p_s^{f_s}.$$

Nun lassen wir die Primideale aus diesem Produkt $p_1^{f_1} \dots p_s^{f_s}$ insofern weg, als das gebliebene Produkt noch in $\mathfrak{a}$ enthalten ist; ein in solcher Weise zuletzt gebliebenes Produkt nennen wir ein unverkürzbares Produkt von $\mathfrak{a}$. Es seien nun $p_1^{e'_1} \dots p_r^{e'_r}$ und $p_1^{e''_1} \dots p_r^{e''_r}$ ($e'_i, e''_i \geq 0$, $i = 1, 2, \dots, r$) zwei unverkürzbare Produkte von $\mathfrak{a}$. Da die Primideale p_i zu

einander teilerfremd sind, haben wir dann

$$a \geq (p_1^{e'_1} \cdots p_r^{e'_r}, p_1^{e''_1} \cdots p_r^{e''_r}) = p_1^{e_1} \cdots p_r^{e_r},$$

wo $e_i = \min(e'_i, e''_i)$ ($i = 1, 2, \dots, r$). Infolge $a \geq p_1^{e'_1} \cdots p_r^{e'_r} \geq p_1^{e'_1} \cdots p_r^{e''_r}$ und der Unverkürzbarkeit von $p_1^{e'_1} \cdots p_r^{e'_r}$ erhalten wir $p_1^{e'_1} \cdots p_r^{e'_r} = p_1^{e'_1} \cdots p_r^{e''_r}$, was bedeutet, dass nur einziges unverkürzbares Produkt von a existieren kann. Nach der Konstruktion des unverkürzbaren Produktes ist ersichtlich jedes Element aus a in einem unverkürzbaren Produkt enthalten. Mithin besteht

$$a = p_1^{e_1} \cdots p_r^{e_r}.$$

Die so gewonnene Darstellung ist offenbar eindeutig. Somit ist bewiesen der

Satz 4. (Fundamentalsatz der Idealtheorie.) *Jedes ganze von dem Einheits- und dem Nullideal verschiedene Ideal in $\mathfrak{o}$ lässt sich eindeutig als das Produkt der endlichvielen, den Bewertungen aus W zugehörigen Primideale darstellen.*

Zusatz: *Existiert ein System W der Bewertungen von k , das die Axiome I bis IV erfüllt, so ist eine beliebige nicht triviale, nicht archimedische, diskrete Bewertung von k , dessen Bewertungsring $\mathfrak{o}$ umfasst, äquivalent einer und nur einer Bewertung aus W .*

Denn einer solchen Bewertung gehört ein Primideal $\mathfrak{p}$, und dieses $\mathfrak{p}$ ist nach unserem Satz einer Bewertung aus W zugehörig.

§ 2.

Nun soll umgekehrt bewiesen werden, dass aus dem Fundamentalsatz der Idealtheorie die Existenz eines Systems der Bewertungen folgt, das die Axiome I-IV erfüllt. Zuvor bemerken wir aber, dass dies eine fast triviale Angelegenheit ist, wenn man die Existenz des Eins in $\mathfrak{o}$ und das Bestehen des Fundamentalsatzes in folgender stärkerer Fassung voraussetzt:

A: *Jedes ganze Ideal in $\mathfrak{o}$ ($\neq 0, \mathfrak{o}$) lässt sich eindeutig als (nicht leeres, endliches) Produkt der teilerlosen Primideale darstellen.*

Dann genügt nämlich das System W aller $\mathfrak{p}$ -adischen Bewertungen unseren Axiomen. II, III sind ja offensichtlich erfüllt. I folgt aus der Existenz des Eins in $\mathfrak{o}$. Denn aus $a \in \bigcap_{w \in W} \mathfrak{B}_w$ folgt $aw = p_1^{e_1} \cdots p_r^{e_r}$ mit $e_i \geq 0$, also $aw \leq \mathfrak{o}$, woraus $a \in \mathfrak{o}$ wegen der Existenz des Eins in $\mathfrak{o}$ erhalten wird.

Da offenbar $\mathfrak{o} \subseteq \bigcap_{w \in W} \mathfrak{B}_w$ gilt, folgt also I. Nach A ist ferner jedes Primideal teilerlos. Aus $(\mathfrak{p}, \mathfrak{q}) = \mathfrak{o} \ni 1$ folgert man dann in bekannter Weise auch IV.

Wir wollen aber hier etwas mehr beweisen, nämlich den folgenden

Satz 5. *Ist in einem Integritätsbereich $\mathfrak{o}$ jedes ganze Ideal ($\neq 0, \mathfrak{o}$) darstellbar als Produkt der endlichvielen Primideale, so ist $\mathfrak{o}$ ganz abgeschlossen im Quotientenkörper k von $\mathfrak{o}$, und jedes Primideal ist teilerlos und umkehrbar.⁽⁴⁾*

Hieraus folgt offenbar die Existenz des Eins in $\mathfrak{o}$, und die Eindeutigkeit der Darstellung als Primidealprodukt der Ideale.⁽⁵⁾ (Im folgenden beweisen wir aber die Existenz des Eins in $\mathfrak{o}$ früher als die Ganz-abgeschlossenheit von $\mathfrak{o}$ in k .) Das System der p -adischen Bewertungen erfüllt also auch hier unsere Axiome. Mit dem Satz 5 wird also die Äquivalenz unseres Axiomensystems mit der folgenden schwächeren Fassung des Fundamentalsatzes bewiesen seien:

A': In $\mathfrak{o}$ ist jedes ganze Ideal ($\neq 0, \mathfrak{o}$) darstellbar als Produkt der endlichvielen Primideale.

Dem Beweis des Satzes 5 schicken wir einige Hilfssätze voraus.

Hilfssatz 2.1. Es ist $\mathfrak{o}\mathfrak{o} = \mathfrak{o}$.

Denn, wäre $\mathfrak{o}\mathfrak{o} < \mathfrak{o}$, so hätte man wegen der Nullteilerfreiheit von $\mathfrak{o}$

$$\mathfrak{o}\mathfrak{o} = \mathfrak{p}_1 \cdots \mathfrak{p}_r, \quad (r \geq 1)$$

folglich

$$\mathfrak{o} < \mathfrak{p}_1$$

was mit $\mathfrak{p}_1 < \mathfrak{o}$ im Widerspruch steht.

Hilfssatz 2.2. Ist für $a \in \mathfrak{o}$ $a\mathfrak{o} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, so ist jedes $\mathfrak{p}_i$ umkehrbar.

Denn es gilt ersichtlich

$$\mathfrak{p}_i^{-1} \supseteq \frac{1}{a} \mathfrak{p}_1 \cdots \mathfrak{p}_{i-1} \mathfrak{p}_{i+1} \cdots \mathfrak{p}_r,$$

mithin $\mathfrak{p}_i \mathfrak{p}_i^{-1} = \mathfrak{o}$, d.h. $\mathfrak{p}_i$ ist umkehrbar.

Hilfssatz 2.3. $\mathfrak{o}$ enthält das Einselement; also $\mathfrak{o}^{-1} = \mathfrak{o}$, und $a\mathfrak{o} = a$ für beliebiges Ideal a .

Bezeichnet man mit $\mathfrak{o}_0$ den von $\mathfrak{o}$ und dem Einselement erzeugten Ring in k , so ist $a\mathfrak{o}_0$ offenbar für $a \in \mathfrak{o}$ ein ganzes Ideal und lässt sich

(4) 東大代數談話會(河田敬義)全國紙上數學談話會, 談話 992.

M. Moriya und Y. Kobayasi, Eine notwendige Bedingung für die eindeutige Primfaktorzerlegung der Ideale in einem kommutativen Ring, Proc. Imp. Acad. Tokyo 1941.

(5) Vgl. v. d. Waerden, Moderne Algebra II.

nach unserer Voraussetzung als ein Primidealprodukt darstellen. Es sei also

$$a_0 = p_1 \cdots p_r.$$

Ist andererseits

$$a_0 = q_1 \cdots q_s,$$

dann gilt

$$a_0 = p_1 \cdots p_r \cdot v = q_1 \cdots q_s.$$

Ist p_1 ein minimales Primideal unter $p_1, \dots, p_r$, und enthält p_1 etwa q_1 , so folgt $p_1 = q_1$, da q_1 v nicht enthält, also eines unter $p_1, \dots, p_r$ enthalten muss. Man hat also nach Hilfssatz 2.2

$$p_1^{-1} p_1 \cdots p_r v = p_1^{-1} q_1 \cdots q_s$$

$$= p_2 \cdots p_r v = q_2 \cdots q_s v.$$

Durch Fortsetzung dieses Verfahrens sieht man ein, dass die Menge $\{p_1, \dots, p_r\}$ mit $\{q_1, \dots, q_s\}$ übereinstimmt. Es gilt also

$$a_0 = p_1 \cdots p_r = q_1 \cdots q_s = a_0 v.$$

Hieraus folgt $v = 1$, d.h. das Einselement liegt in v .

Aus Hilfssätze 2.3 und 2.2 folgt weiter

Hilfssatz 2.4. Sind $p_1, \dots, p_r$ umkehrbare Primideale, und $a = p_1 \cdots p_r$, so ist $p_1 \cdots p_r$ die einzige Darstellung von a als Produkt der Primideale. Insbesondere gilt also die Eindeutigkeit der Primidealproduktendarstellung für die Ideale von der Form $a_0 v$.

Hilfssatz 2.5. Jedes minimale Primideal ist umkehrbar.

Jedes Primideal p enthält ein Ideal von der Form $p_0 v = p_1 \cdots p_r$ mit $p \in p_i$, also ein Umkehrbares Primideal (Hilfssatz 2.2). Ist aber p ein minimales Primideal, so muss p mit einem in p enthaltenen umkehrbaren Primideal zusammenfallen.

Hilfssatz 2.6. Ist q ein echter Teiler von einem umkehrbaren Primideal p , so ist $q^{-1} = 0$.

Aus $p \subset q$ folgt nämlich $p^{-1} \supseteq q^{-1}$, $p q^{-1}$ ist also ein ganzes Ideal. Dann ist

$$(p q^{-1}) q = p (q^{-1} q) \subseteq p_0 v = p,$$

woraus folgt $p q^{-1} \subseteq p$ wegen $q \not\subseteq p$, da p Primideal ist. Hieraus folgt weiter $q^{-1} = 0 q^{-1} = (p^{-1} p) q^{-1} = p^{-1} (p q^{-1}) \subseteq p^{-1} p = 0$. Offenbar ist nun $q^{-1} \geq 0$. Also hat man $q^{-1} = 0$.

Aus Hilfssätze 2.5 und 2.6 folgert man leicht den

Hilfssatz 2.7. Ist q ein nicht umkehrbares Primideal, so ist $q^{-1} = 0$.

Ist nun $a^{-1} = b^{-1}$ und c ein beliebiges Ideal, so ist $(ac)^{-1} = (bc)^{-1}$, denn $a \in (ac)^{-1}$ bedeutet ja $ac \leq a^{-1} = b^{-1}$. Daraus folgt:

Hilfssatz 2.8. Sind $p_1, \dots, p_r$ umkehrbar, und $q_1, \dots, q_s$ nicht umkehrbar, so ist $(p_1 \cdots p_r q_1 \cdots q_s)^{-1} = p_1^{-1} \cdots p_r^{-1}$.

Denn, $(p_1 \cdots p_r q_1 \cdots q_s)^{-1} = (p_1 \cdots p_r q_1 \cdots q_{s-1} o)^{-1} = \cdots = (p_1 \cdots p_r)^{-1} = p_1^{-1} \cdots p_r^{-1}$, indem man Hilfssatz 2.7 benutzt.

Beweis des Satzes. 1) o ist ganz abgeschlossen. a sei ein ganzes Ideal, und

$$a = p_1 \cdots p_r q_1 \cdots q_s$$

eine Darstellung von a als Produkt der Primideale, wobei $p_1, \dots, p_r$ umkehrbar, $q_1, \dots, q_s$ dagegen nicht umkehrbar sind. Dann haben wir nach dem Hilfssatz 2.8

$$a^{-1} = (p_1 \cdots p_r q_1 \cdots q_s)^{-1} = p_1^{-1} \cdots p_r^{-1},$$

mithin

$$aa^{-1} = q_1 \cdots q_s,$$

$$((aa^{-1})^{-1})^{-1} = ((q_1 \cdots q_s)^{-1})^{-1} = o^{-1} = o.$$

womit gezeigt ist, dass in o der v -Gruppensatz gilt. o ist also ganz abgeschlossen im Quotientenkörper k .

2. *Jedes umkehrbare Primideal ist teilerlos.* Es sei p ein umkehrbares Primideal, und a ein Element in o mit $a \notin p$. Die Annahme $(a, p) < o$ soll nun zu einem Widerspruch geführt werden. Dann hätte man nämlich die Zerlegungen

$$(a, p) = q_1 q_2 \cdots q_r,$$

$$(a^2, p) = q'_1 q'_2 \cdots q'_s.$$

Geht man zum Restklassenring $\bar{o} = o/p$ über, so gilt

$$(\bar{a}) = \bar{q}_1 \bar{q}_2 \cdots \bar{q}_r,$$

$$(\bar{a}^2) = \bar{q}'_1 \bar{q}'_2 \cdots \bar{q}'_s,$$

wobei $\bar{a}$, $\bar{q}_i$ bzw. $\bar{q}'_i$ die Bilder von a , q_i bzw. q'_i beim Homomorphismus $o \sim \bar{o} = o/p$ bedeuten. Es ist offenbar $\bar{o} > \bar{q}_i$, $\bar{q}'_i$, da $o > q_i$, $q'_i > p$ ist. $\bar{q}_i$, $\bar{q}'_i$ sind nun als Teiler der Hauptideale nach dem Hilfssatz 2.2 umkehrbar. Nach dem Hilfssatz 2.4 folgt dann aus

$$(\bar{a}^2) = \bar{q}_1^2 \bar{q}_2^2 \cdots \bar{q}_r^2 = \bar{q}'_1 \bar{q}'_2 \cdots \bar{q}'_s,$$

dass $\bar{q}_1$, $\bar{q}_1$, $\bar{q}_2$, $\bar{q}_2$, $\dots$, $\bar{q}_r$, $\bar{q}_r$ im ganzen mit $\bar{q}'_1$, $\bar{q}'_2$, $\dots$, $\bar{q}'_s$ zusammenfallen müssen. Also können wir setzen

$$\bar{q}_1 = \bar{q}'_1 = \bar{q}'_2.$$

Dann haben wir

$$q_1 = q'_1 = q'_2,$$

da $q_1, q'_1, q'_2 > p$ ist. Mithin gilt

$$p < (a^2, p) = q_1^2 q'_3 \cdots q'_s \leq q_1^2. \quad (*)$$

Es sei nun

$$(a) = p_1 p_2 \cdots p_t.$$

Aus $(a) < q_1$ folgt etwa $p_1 < q_1$. Dann hat man

$$(p, p_1) \leq q_1,$$

was bedeutet in $\bar{o} = o/p$

$$(\bar{0} <) \bar{p}_1 \leq \bar{q}_1.$$

Da $\bar{q}_1$ ein minimales Primideal in $\bar{o}$ ist, so hat man

$$\bar{p}_1 = \bar{q}_1,$$

mithin

$$(p, p_1) = q_1.$$

Nach (*) gilt also

$$p < (p, p_1)^2.$$

Geht man nun zum Restklassenring $\bar{o} = o/p_1$ über, und bezeichnet man mit $\bar{p}$ das Bild von p beim Homomorphismus $o \sim \bar{o}$, so besteht

$$\bar{p} = \bar{p}^2,$$

folglich

$$\bar{p} = \bar{0},$$

denn $\bar{p}$ ist offenbar ein minimales Primideal in $\bar{o}$, mithin umkehrbar. Man hat also

$$(p, p_1) = o,$$

was mit $(p, p_1) = q_1 < o$ im Widerspruch steht. Daher muss $(a, p) = o$ sein, d.h. p ist teilerlos.

3. *Jedes Primideal ist umkehrbar und teilerlos.* Nach dem eben Bewiesenen haben wir nur noch zu zeigen, dass jedes Primideal umkehrbar ist. Es sei p ein Primideal. Ist p nicht umkehrbar, so ist p nach dem Hilfssatz 2.5 nicht minimal, enthält also ein minimales Primideal p' , das seinerseits umkehrbar, also teilerlos ist. Dann müsste p mit p' zusammenfallen, was nicht geht.

Somit ist unser Satz 5 bewiesen.

§ 3.

Satz 6. *Es sei $\mathfrak{o}$ ein Integritätsbereich, k sein Quotientenkörper. K sei ein endlicher Erweiterungskörper von k , und $\mathfrak{D}$ der Ring aller Elemente aus K , die in bezug auf $\mathfrak{o}$ ganz sind. Dann folgt die Gültigkeit des Fundamentalsatzes der Idealtheorie in $\mathfrak{D}$ aus der in $\mathfrak{o}$.*

Beweis.⁽⁶⁾ $\{w\}$ sei das System der Bewertungen von k , das I bis IV erfüllt, und $\{\bar{w}\}$ das System von allen Fortsetzungen der Bewertungen aus $\{w\}$ zu K . Aus der Definition der Fortsetzung folgt sofort, dass dann das System $\{\bar{w}\}$ die Axiome I bis III erfüllt. Dass auch IV erfüllt ist, zeigen wir folgendermassen. Dabei dürfen wir uns offenbar auf den Fall beschränken, wo K eine einfache Erweiterung von k ist. Nun seien $\bar{w}, \bar{w}'$, zwei voneinander verschiedene Bewertungen aus $\{\bar{w}\}$. Sind w, w' , nicht äquivalent, d.h. beide nicht Fortsetzungen von einer und derselben Bewertung aus $\{w\}$, so gilt IV offenbar für $\bar{w}, \bar{w}'$, da $\{w\}$ in k IV genügt. $\bar{w}, \bar{w}'$ seien also zwei Fortsetzungen von einer Bewertung w aus $\{w\}$. Dann setzen wir:

$K = k(\xi)$, wo ξ , ohne Einschränkung der Allgemeinheit, als ganz in bezug auf $\mathfrak{o}$ angenommen wird;

$f(x)$: ein irreduzibles Polynom aus $\mathfrak{o}[x]$, sodass $f(\xi) = 0$ in K gilt;

k_w : die perfekte Hülle von k in bezug auf w ;

$\mathfrak{Q}$: eine galoissche Erweiterung von k_w , in der $f(x)$ in lineare Faktoren zerfällt.

In k_w zerfällt $f(x)$ in die irreduzible Polynome, etwa in der Gestalt

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r},$$

wo $f_i(x)$ und $f_j(x)$ teilerfremd für $i \neq j$ sind. Dabei können wir annehmen, dass $f_i(x)$ ($i = 1, \dots, r$) ganze Koeffizienten in bezug auf w , d.h. für w nicht negativwertige Koeffizienten hat. Ferner setzen wir $K_1 = k_w(\xi_1), \dots, K_r = k_w(\xi_r)$, wobei $\xi_1, \dots, \xi_r$ bzw. Wurzeln von $f_1(x), \dots, f_r(x)$ in $\mathfrak{Q}$ sind. Dann gewinnt man $\bar{w}, \bar{w}'$ nach der bekannten Konstruktion der Fortsetzungen, indem man K etwa in K_i bzw. K_j einbettet.⁽⁷⁾ Nun besthet (in k_w) die Gleichung

$$f_i(x)g(x) + f_j(x)h(x) = 1$$

mit passenden $g(x)$ und $h(x)$ aus $k_w[x]$. Alsdann sei $h'(x)$ ein solches Polynom aus $k[x]$, dass alle Koeffizienten von $h(x) - h'(x)$ positivwertig in

⁽⁶⁾ Diesen Beweis verdanke ich Herrn T. Nakayama.

⁽⁷⁾ A. Ostrowski a. a. O.

bezug auf w sind, und $f'_j(x)$ ein solches (aus $\mathfrak{o}[x]$), dass alle Koeffizienten von $(f_j(x) - f'_j(x))h(x)$ positivwertig in bezug auf w sind. Da in K_i $f_i(\xi)g(\xi) = 1 - f_j(\xi)h(\xi) = 0$, in K_j $f_j(\xi)h(\xi) = 0$ und $\bar{w}_i(\xi) \geq 0$, $\bar{w}_j(\xi) \geq 0$ sind, so haben wir

$$\bar{w}_i(1 - f_j(\xi)h(\xi)) = \infty, \quad \bar{w}_j(f_j(\xi)h(\xi)) = \infty, \quad \bar{w}_l(f_j(\xi)h(\xi)) \geq 0 \quad (l \neq i, j),$$

wo $\bar{w}_l$ die durch Einbettung von K in K_l gewonnene Bewertung bedeutet. Also besteht

$$\bar{w}_i(1 - f'_j(\xi)h'(\xi)) > 0, \quad \bar{w}_j(f'_j(\xi)h'(\xi)) > 0, \quad \bar{w}_l(f'_j(\xi)h'(\xi)) \geq 0.$$

Denn es ist

$$\begin{aligned} \bar{w}_i(1 - f'_j(\xi)h'(\xi)) &= \bar{w}_i(1 - f_j(\xi)h(\xi) + f_j(\xi)h(\xi) - f'_j(\xi)h(\xi) \\ &\quad + f'_j(\xi)h(\xi) - f'_j(\xi)h'(\xi)) \\ &\geq \text{Min} \left(\bar{w}_i(1 - f_j(\xi)h(\xi)), \quad \bar{w}_i((f_j(\xi) - f'_j(\xi))h(\xi)), \right. \\ &\quad \left. \bar{w}_i(f'_j(\xi)(h(\xi) - h'(\xi))) \right) > 0, \end{aligned}$$

$$\begin{aligned} \bar{w}_j(f'_j(\xi)h'(\xi)) &= \bar{w}_j(f'_j(\xi)h'(\xi) - f'_j(\xi)h(\xi) + f'_j(\xi)h(\xi) - f(\xi)h(\xi) + f(\xi)h(\xi)) \\ &\geq \text{Min} \left(\bar{w}_j(f'_j(\xi)(h'(\xi) - h(\xi))), \quad \bar{w}_j((f'_j(\xi) - f_j(\xi))h(\xi)), \right. \\ &\quad \left. \bar{w}_j(f_j(\xi)h(\xi)) \right) > 0, \end{aligned}$$

$$\begin{aligned} \bar{w}_l(f'_j(\xi)h'(\xi)) &\geq \text{Min} \left(\bar{w}_l(f'_j(\xi)(h'(\xi) - h(\xi))), \quad \bar{w}_l((f'_j(\xi) - f_j(\xi))h(\xi)), \right. \\ &\quad \left. \bar{w}_l(f_j(\xi)h(\xi)) \right) \geq 0. \end{aligned}$$

$f'_i(\xi)h'(\xi)$ kann nur für endlichviele, nicht zu $\bar{w}_i$ äquivalente Bewertungen, etwa für $\bar{w}'_1, \dots, \bar{w}'_s$ negativwertig sein. Sind $w'_1, \dots, w'_t$ alle voneinander verschiedene Bewertungen, die $\bar{w}'_1, \dots, \bar{w}'_s$ in k induzieren, dann sind $w, w'_1, \dots, w'_t$ voneinander verschieden, also gibt es nach dem Hilfssatz 2 ein Element c_1 in $\mathfrak{o}$, sodass

$$w(1 - c_1) > 0$$

$$w'_l(c_1) > \text{Max} \left(-\bar{w}'_1(f'_j(\xi)h'(\xi)), \dots, -\bar{w}'_s(f'_j(\xi)h'(\xi)) \right) \quad (l = 1, 2, \dots, t)$$

gelten. $c = c_1 f'_i(\xi)h'(\xi)$ ist dann ersichtlich in $\mathfrak{O}$ enthalten, und es besteht

$$\bar{w}(1 - c) > 0, \quad \bar{w}'(c) > 0,$$

w.z.b.w.

Satz 7. *K sei ein endlicher galoisscher Erweiterungskörper von k , $\mathfrak{D}$ ein Integritätsbereich mit K als Quotientenkörper, in dem der Fundamentalsatz der Idealtheorie gilt, $\mathfrak{D}$ falle ferner mit seinen Konjugierten in bezug auf k zusammen. Dann gilt auch in $\mathfrak{o} = \mathfrak{D} \cap k$ derselbe Fundamentalsatz.⁽⁸⁾*

Beweis. Das System $\{w\}$ der Bewertungen in K erfülle wieder I bis IV. Das System aller Bewertungen von k , die von denen aus $\{w\}$ in k induziert werden, sei mit $\{\bar{w}\}$ bezeichnet. Dann ist klar, dass $\{\bar{w}\}$ I bis III erfüllt. Sind $\bar{w}, \bar{w}'$ zwei verschiedene Bewertungen aus $\{\bar{w}\}$, und $w_1, \dots, w_r$ bzw. $w'_1, \dots, w'_s$ alle Bewertungen aus $\{w\}$, die in k $\bar{w}$ bzw. $\bar{w}'$ induzieren, dann gibt es nach dem Hilfssatz 3 ein Element c in $\mathfrak{D}$, so dass

$$w_i(1-c) > 0 \quad (i = 1, \dots, r), \quad w'_j(c) > 0 \quad (j = 1, \dots, s)$$

gilt. Ist $c^{(h)}$ eine Konjugierte von c in bezug auf k , so sind $w_1(1-c^{(h)})$ bzw. $w'_1(c^{(h)})$ gleich einem unter $w_1(1-c), \dots, w_r(1-c)$ bzw. einem unter $w'_1(c), \dots, w'_s(c)$, da $w_1, \dots, w_r$ bzw. $w'_1, \dots, w'_s$ alle Fortsetzungen von $\bar{w}$ bzw. $\bar{w}'$ zu K sind. Somit haben wir für jede Konjugierte $c^{(h)}$ von c

$$w_1(1-c^{(h)}) > 0, \quad w'_1(c^{(h)}) > 0.$$

Sind $c^{(1)}, \dots, c^{(n)}$ alle Konjugierten von c in bezug auf K , so liegt $c_0 = c^{(1)} \dots c^{(n)} = N(c)$ in $\mathfrak{D}$ und k , weil $c^{(1)}, \dots, c^{(n)}$ alle in $\mathfrak{D}$ enthalten sind, also in $\mathfrak{o}$. Für dieses c_0 gilt dann

$$\bar{w}(1-c_0) > 0, \quad \bar{w}'(c_0) > 0,$$

denn aus $w(1-c) > 0$ und $w(1-c') > 0$ folgt

$$w(1-cc') = w(1-c+c-cc') \geq \text{Min}(w(1-2), w(c(1-c')))$$

$$= \text{Min}(w(1-c), w(1-c')) > 0, \quad \text{w.z.b.w.}$$

Satz 8. *$\mathfrak{o}$ sei ein Integritätsbereich mit k als Quotientenkörper, in dem der Fundamentalsatz der Idealtheorie gilt. Ist $\mathfrak{o}'$ ein Ring mit $\mathfrak{o} \subseteq \mathfrak{o}' \subseteq k$, so gilt auch in $\mathfrak{o}'$ derselbe Fundamentalsatz.⁽⁹⁾*

Beweis. $W = \{w\}$ erfülle I bis IV. Mit W' bezeichnen wir das System derjenigen Bewertungen aus W , deren Bewertungsringe $\mathfrak{o}'$ umfassen. Dann behaupten wir $\mathfrak{o}' = \bigcap_{w \in W'} \mathfrak{B}_w$. (Falls W' leer ist, ist offenbar $\mathfrak{o}' = k$.) Zunächst ist klar $\mathfrak{o}' \subseteq \bigcap_{w \in W'} \mathfrak{B}_w$. Es sei also $a \in \bigcap_{w \in W'} \mathfrak{B}_w$, und $w_1, \dots, w_r$ alle Bewertungen, für die a negativwertig ausfällt. Da jedes

(8) K. Asano und T. Nakayama, a. a. O.

(9) S. MacLane und O. F. G. Schilling, *Infinite number fields with Noether ideal theories*, Amer. Journ. Math. 61, 1939.

w_i dann nicht zu W' gehört, also $\mathfrak{o}' \not\subseteq \mathfrak{B}_{w_i}$ ist, so gibt es in $\mathfrak{o}'$ ein Element a_i mit $w_i(a_i) < 0$. Nach dem Hilfssatz 2 existieren nun die Elemente c_i, c'_i in $\mathfrak{o}$ für jedes w_i , für welche

$$w_i(c_i) = 0, \quad w_j(c_i) > 0, \quad \text{bzw.} \quad w_i(c'_i) > 0, \quad w_j(c'_i) = 0 \\ (j = 1, \dots, i-1, i+1, \dots, r)$$

gilt. Daher hat man

$$w_i(a_i^n c_i^m) \leq w_i(a), \quad w_j(a_i^n c_i^m) > 0 \quad (j = 1, \dots, i-1, i+1, \dots, r)$$

für passend gross gewählte natürliche Zahlen n, m . Es gilt also für $\gamma_i = a_i^n c_i^m + c'_i$

$$w_i(\gamma_i) \leq w_i(a), \quad w_j(\gamma_i) = 0 \quad (j = 1, \dots, i-1, i+1, \dots, r).$$

Für jedes w_i gibt es ein solches Element γ_i . Setzt man also $\gamma = \gamma_1 \dots \gamma_r$, so ist γ offenbar ein Element in $\mathfrak{o}'$, und es besteht $w_i(\gamma) \leq w_i(a)$ ($i = 1, \dots, r$). Nach dem Hilfssatz 5 existiert nun ein Element β , sodass

$$w_i\left(\frac{a}{\gamma} - \beta\right) \geq -w_i(\gamma) \quad (i = 1, \dots, r),$$

$$w(\beta) \geq -w(\gamma) \quad \text{für jedes von } w_1, \dots, w_r \text{ verschiedene } w \text{ mit } w(\gamma) < 0,$$

$$w'(\beta) \geq 0 \quad \text{für alle andere Bewertungen } w' \text{ aus } W$$

gilt. Dann ist β ersichtlich ein Element aus $\mathfrak{o}$, und man hat für alle Bewertungen w aus W

$$w(a - \gamma\beta) \geq 0,$$

also $a - \gamma\beta \in \mathfrak{o} \subseteq \mathfrak{o}'$. Mithin besteht $\mathfrak{o}' = \bigcap_{w \in W'} \mathfrak{B}_w$. Da W' offenbar II bis IV genügt, ist damit der Beweis beendet.

Mathematisches Institut,
Kaiserliche Universität zu Tokyo.