JOURNAL OF SCIENCE OF THE HIROSHIMA UNIVERSITY, SER. A, VOL. 17, NO. 1, AUG., 1953

Über die Kürzeste Darstellung der Ideale im Unendlichen Algebraischen Zahlkörper

Von

Noboru NAKANO

(Eingegangen am 31, Januar 1953)

Im allgemeinen unendlichen algebraischen Zahlkörper $\mathfrak{K}$ erhalten wir den folgenden Fundamentalsatz[1]: *Jedes ganze Ideal* $\mathfrak{a}$ *aus* $\mathfrak{K}$ *lässt sich als Durchschnitt von seinen sämtlichen isolierten Primärkomponenten darstellen;* $\mathfrak{a}=\bigwedge_{\iota}\mathfrak{q}_{(\iota)}$. Wenn dabei $\mathfrak{q}_{(\iota)}\not\supseteq\bigwedge_{\tau\neq\iota}\mathfrak{q}_{(\tau)}$ für alle ι gilt, so nennen wir diese Darstellung $\mathfrak{a}=\bigwedge_{\iota}\mathfrak{q}_{(\iota)}$ die *„kürzest"*. Wenn zum Beispiel $\mathfrak{a}$ ein Ideal ist, welches nur endlich viele Primidealteiler $\mathfrak{p}_{(1)}, \mathfrak{p}_{(2)},\cdots, \mathfrak{p}_{(n)}$ besitzt, so lässt sich $\mathfrak{a}$ als kürzester Durchschnitt von den zu jedem $\mathfrak{p}_{(i)}$ gehörigen isolierten Primärkomponenten $\mathfrak{q}_{(i)}$ von $\mathfrak{a}$ darstellen; $\mathfrak{a}=\mathfrak{q}_{(1)}\wedge\mathfrak{q}_{(2)}\wedge\cdots\wedge\mathfrak{q}_{(n)}$.[2] Wenn umgekehrt $\mathfrak{a}$ unendlich viele Primidealteiler besitzt, so erhebt sich die Frage, ob ein Ideal $\mathfrak{a}$ als kürzester Durchschnitt darstellbar ist oder nicht. Um auf diese Frage zu antworten wollen wir in dieser Note den folgenden Hauptsatz beweisen; *Dafür dass ein Ideal* $\mathfrak{a}$ *als der kürzeste Durchschnitt von seinen sämtlichen isolierten Primärkomponenten darstellbar ist, ist es notwendig und hinreichend, dass irgendeine von den zwei Bedingungen erfüllt ist,*

(1) $\mathfrak{a}$ *besitzt nur endlich viele Primidealteiler.*

(2) *Es gibt für alle isolierten Primärkomponenten* $\mathfrak{q}_{(\iota)}$ *von* $\mathfrak{a}$ *ein Element* r_ι *von der Art, dass* $\mathfrak{a}:(r_\iota)=\mathfrak{q}_{(\iota)}$ *ist.*

§ 1. Vorbereitende Untersuchungen

In Zukunft bedeutet $\mathfrak{K}$ einen unendlichen algebraischen Zahlkörper und $\mathfrak{O}$ die menge aller ganzen algebraischen Zahlen aus $\mathfrak{K}$. Ist $\mathfrak{a}$ ein gegebenes

1) W. Krull, „Idealtheorie in unendlichen algebraischen Zahlkörpern." Math. Zeit. 29 (1929), zitiert mit „Krull (1)".

N. Nakano, „Über den Fundamentalsatz der Idealtheorie in unendlichen algebraischen Zahlkörpern." Jour. of Sci. of the Hiroshima Univ. Vol. 15. No. 3, zitiert mit „Nakano (1)".

2) In seiner Arbeit hat Herr W. Krull *„Stiemkesche Körper"* einen unendlichen algebraischen Zahlkörper genannt, in denen jedes Ideal nur endlich viele Primidealteiler besitzt. Im Stiemkeschen Körper ist jedes Ideal als der kürzester Durchschnitt darstellbar. Siehe „Krull (1)".

Ideal in $\mathfrak{O}$ und $\mathfrak{p}$[3] ein Primidealteiler von $\mathfrak{a}$, so können wir die zu $\mathfrak{p}$ gehörige *„isolierte Primärkomponente"* (im folgenden wird sie kurz mit I. P. K. bezeichnet) $\mathfrak{q}$ von $\mathfrak{a}$ folgendermassen definieren[4]; *Die zu $\mathfrak{p}$ gehörige I. P. K. $\mathfrak{q}$ von $\mathfrak{a}$ ist die Gesamtheit aller Elemente, deren Produkt mit einem geeignet gewählten Elemente $s\ (\notin \mathfrak{p})$ durch $\mathfrak{a}$ teilbar ist.* Aus dieser Definition von I. P. K. erhalten wir folgenden

Satz 1. *Ist $\mathfrak{q}$ eine zu $\mathfrak{p}$ gehörige I. P. K. von $\mathfrak{a}$ und existiert ein Element r von der Art, dass $\mathfrak{a}:(r)=\mathfrak{q}$ gilt, so ist $r \notin \mathfrak{p}$.*

Aus $\mathfrak{a}:(r)=\mathfrak{q}$ ergibt sich zunächst $r \notin \mathfrak{q}$, sonst gäbe es ein Element s, derart dass $rs \in \mathfrak{a}$, $s \notin \mathfrak{p}$ ist. Daraus folgte ein Widerspruch, dass $s \in \mathfrak{a}:(r) = \mathfrak{q} \leqq \mathfrak{p}$ wäre. Also muss

(1) $$r \notin \mathfrak{q}$$

sein. Wäre jetzt $r \in \mathfrak{p}$, so gäbe es nach (1) eine passend gewählte natürliche Zahl $k\ (\geqq 2)$ derart, dass

(2) $$r^{k-1} \notin \mathfrak{q}, \qquad r^k \in \mathfrak{q}$$

ist. Wegen $r^k \in \mathfrak{q}$ gäbe es ein Element t von der Art, dass $r^k t \in \mathfrak{a}$, $t \notin \mathfrak{p}$ ist. Damit wäre $r^{k-1} t \in \mathfrak{q}$ nach $\mathfrak{a}:(r)=\mathfrak{q}$ und daraus folgte der Widerspruch $r^{k-1} \in \mathfrak{q}$ zu (2). Damit muss $r \notin \mathfrak{p}$ sein.

Ist $\mathfrak{a}$ ein gegebenes Ideal aus $\mathfrak{O}$, $\mathfrak{p}_{(\iota)}$ ein Primidealteiler von $\mathfrak{a}$, und $\mathfrak{q}_{(\iota)}$ die zu $\mathfrak{p}_{(\iota)}$ gehörige I. P. K. von $\mathfrak{a}$, so lässt sich $\mathfrak{a}$ als Durchschnitt von seinen sämtlichen I. P. K. darstellen: $\mathfrak{a} = \bigcap_{\iota} \mathfrak{q}_{(\iota)}$. Aus diesem Fundamentalsatz erhalten wir folgenden

Satz 2. *Ist $\mathfrak{a} = \bigcap_{\iota} \mathfrak{q}_{(\iota)}$ eine Darstellung durch seinen sämtlichen I. P. K. und $\mathfrak{p}_{(\iota)}$ ein zu $\mathfrak{q}_{(\iota)}$ gehöriges Primideal, so ist dann und nur dann $\mathfrak{p}_{(\iota)} \ngeqq \bigcap_{\tau \neq \iota} \mathfrak{q}_{(\tau)}$, wenn ein Element r_ι von der Art existiert, dass $\mathfrak{a}:(r_\iota)=\mathfrak{q}_{(\iota)}$ gilt.*

Aus $\mathfrak{a}:(r_\iota)=\mathfrak{q}_{(\iota)}$ ergibt sich nach Satz 1

(3) $$r_\iota \notin \mathfrak{p}_{(\iota)}.$$

Ferner können wir beweisen, dass $r_\iota \in \bigcap_{\tau \neq \iota} \mathfrak{q}_{(\tau)}$ ist. Denn aus $\mathfrak{a}:(r_\iota)=\mathfrak{q}_{(\iota)}$ folgt die Tatsache, dass $\mathfrak{a}:(r_\iota)$ keinen Primidealteiler ausser $\mathfrak{p}_{(\iota)}$ haben kann[5].

3) Im folgenden verstehen wir unter Primideal stets ein von Einheits- und Null-ideal verschiedenes Primideal.

4) „Nakano (1)", Satz 1. s. 172.

5) Für Primärideal aus $\mathfrak{O}$ gilt bekanntlich der folgende grundlegende Satz: *Ein Ideal $\mathfrak{q}$ ist dann und nur dann ein zu $\mathfrak{p}$ gehöriges Primärideal, wenn $\mathfrak{q}$ nur durch ein einziges Primideal $\mathfrak{p}$ teilbar ist.*

Siehe etwa M. Moriya, „Theorie der algebraischen Zahlkörper unendlichen Grades." Jour. of Sci. Hokkaido Imp. Univ. Series I Vol. III, s. 172.

Also ergibt sich $\mathfrak{a}:(r_\iota)\subsetneqq\mathfrak{p}_{(\tau)}$ für alle $\tau\,(\neq\iota)$. Daraus folgt die Existenz eines Elementes s_τ derart, dass $s_\tau\in\mathfrak{a}:(r_\iota)$, $s_\tau\notin\mathfrak{p}_{(\tau)}$ ist. Dann aus $s_\tau r_\iota\in\mathfrak{a}$, $s_\tau\notin\mathfrak{p}_{(\tau)}$ ergibt sich $r_\iota\in\mathfrak{q}_{(\tau)}$ für alle τ, folglich

$$r_\iota\in\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}. \tag{4}$$

Aus (3) und (4) folgt $\mathfrak{p}_{(\iota)}\not\supseteqq\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}$.

Umgekehrt sei es $\mathfrak{p}_{(\iota)}\not\supseteqq\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}$, dann gibt es ein Element r_ι von der Art, dass $r_\iota\in\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}$, $r_\iota\notin\mathfrak{p}_{(\iota)}$ ist. Daraus folgt

$$\begin{aligned}\mathfrak{a}:(r_\iota)&=\{\mathfrak{q}_{(\iota)}\cap(\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)})\}:(r_\iota)\\&=\big(\mathfrak{q}_{(\iota)}:(r_\iota)\big)\cap\{(\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}):(r_\iota)\}=\mathfrak{q}_{(\iota)}:(r_\iota)\end{aligned}$$

Jetzt sei α ein beliebiges Element aus $\mathfrak{q}_{(\iota)}:(r_\iota)$, dann ist $\alpha r_\iota\in\mathfrak{q}_{(\iota)}$. Wegen $r_\iota\notin\mathfrak{p}_{(\iota)}$, erhalten wir nach der zu $\mathfrak{p}_{(\iota)}$ gehörigen Primäridealeigenschaft $\alpha\in\mathfrak{q}_{(\iota)}$. So ist $\mathfrak{q}_{(\iota)}:(r_\iota)=\mathfrak{q}_{(\iota)}$, d. h. $\mathfrak{a}:(r_\iota)=\mathfrak{q}_{(\iota)}$. Der Beweis von Satz 2 ist hiermit abgeschlossen.

Ist $\mathfrak{a}=\bigcap_\iota\mathfrak{q}_{(\iota)}$ eine Darstellung von $\mathfrak{a}$ durch seine sämtlichen I. P. K. und gilt $\mathfrak{q}_{(\iota)}\not\supseteqq\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}$ für alle ι, so nennen wir diese Darstellung $\mathfrak{a}=\bigcap_\iota\mathfrak{q}_{(\iota)}$ die kürzeste. Da aus $\mathfrak{p}_{(\iota)}\not\supseteqq\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}$ ohne weiteres $\mathfrak{q}_{(\iota)}\not\supseteqq\bigcap_{\tau\neq\iota}\mathfrak{q}_{(\tau)}$ folgt, so erhalten wir nach Satz 2 folgenden

Satz 3. *Ist* $\mathfrak{a}=\bigcap_\iota\mathfrak{q}_{(\iota)}$ *eine Darstellung von* $\mathfrak{a}$ *durch seine sämtlichen I. P. K. und existiert für alle* $\mathfrak{q}_{(\iota)}$ *ein Element* r_ι *von der Art, dass* $\mathfrak{a}:(r_\iota)=\mathfrak{q}_{(\iota)}$ *gilt, so ist die Darstellung von* $\mathfrak{a}$ *kürzest.*

§ 2. Nachweis des Hauptsatzes

Es sei $\mathfrak{a}$ ein Ideal aus $\mathfrak{O}$ und $\mathfrak{a}$ besitzte unendlich viele Primidealteiler. Ist weiter $\mathfrak{a}_\lambda$ das kleinste gemeinschaftliche Vielfache vom Ideal $\mathfrak{a}$ und einem endlichen algebraischen Zahlkörper $\mathfrak{K}_\lambda$, so besitzt $\mathfrak{a}_\lambda$ im allgemeinen eine Primidealzerlegung

$$\mathfrak{a}_\lambda=\mathfrak{p}_{\lambda1}^{e_{\lambda1}}\,\mathfrak{p}_{\lambda2}^{e_{\lambda2}}\cdots\mathfrak{p}_{\lambda m_\lambda}^{e_{\lambda m_\lambda}} \tag{5}$$

wobei $\mathfrak{p}_{\lambda1}, \mathfrak{p}_{\lambda2},\cdots,\mathfrak{p}_{\lambda m_\lambda}$ die von einander verschiedenen Primideale in $\mathfrak{K}_\lambda$ bedeuten. Somit muss nach unserer Voraussetzung, dass $\mathfrak{a}$ unendlich viele Primidealteiler besitzt, die Anzahl m_λ von verschiedenen Primidealen $\mathfrak{p}_{\lambda i}$ mit steigenden λ

über alle Grenzen zunehmen. Danach können wir annehmen, dass die Anzahl der Primidealteiler, welche im Körper $\mathfrak{K}_\nu\ (\nu > \lambda)$ $\mathfrak{a} \cap \mathfrak{O}_\nu = \mathfrak{a}_\nu$ enthalten und zugleich mindestens eins von den Primidealen $\mathfrak{p}_{\lambda 1}, \mathfrak{p}_{\lambda 2}, \cdots, \mathfrak{p}_{\lambda m_\lambda}$, etwa $\mathfrak{p}_{\lambda 1}$ enthalten, mit ν über alle Grenzen wächst. Damit können wir stets eine unendliche Zahlenfolge $\lambda = \lambda_1 < \lambda_2 < \lambda_3 < \cdots$ so bestimmen, dass ein Gleichungssystem von der folgenden Form gilt;

$$\mathfrak{a} \cap \mathfrak{O}_{\lambda_2} = \mathfrak{a}_{\lambda_2} = \mathfrak{p}_{\lambda 21}^{e_{\lambda 21}} \mathfrak{p}_{\lambda 22}^{e_{\lambda 22}} \mathfrak{b}_{\lambda_2},$$

wo $\mathfrak{p}_{\lambda 21}$, $\mathfrak{p}_{\lambda 22}$ Primidealteiler von $\mathfrak{p}_{\lambda 11}$ sind,

$$\mathfrak{a} \cap \mathfrak{O}_{\lambda_3} = \mathfrak{a}_{\lambda_3} = \mathfrak{p}_{\lambda 31}^{e_{\lambda 31}} \mathfrak{p}_{\lambda 32}^{e_{\lambda 32}} \mathfrak{b}_{\lambda_3},$$

wo $\mathfrak{p}_{\lambda 31}$, $\mathfrak{p}_{\lambda 32}$ Primidealteiler von $\mathfrak{p}_{\lambda 21}$ sind,

....

Durch passende Wahl der zu $\mathfrak{K}$ gehörigen Körperfolge $\{\mathfrak{K}_\lambda\}$ können wir eine Voraussetzung erreichen, dass $\lambda = \lambda_1 = 1$, $\lambda_2 = 2$, $\lambda_3 = 3, \cdots$ wird. Damit bezeichnen wir mit $\mathfrak{p}$ das Primideal, welches als die Vereinigungsmenge von abzählbar unendlich vielen Primidealfolgen $\mathfrak{p}_1 = \mathfrak{p}_{11}$, $\mathfrak{p}_2 = \mathfrak{p}_{21}$, $\mathfrak{p}_3 = \mathfrak{p}_{31}, \cdots$ definiert wird, und dagegen mit $\mathfrak{p}_{(n)}$ ein Primideal, dessen Primidealenfolge mit $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \mathfrak{p}_n$ beginnt, während des folgende Glied $\mathfrak{p}'_{n+1} = \mathfrak{p}_{n+1,\,2}$ von $\mathfrak{p}_{n+1} = \mathfrak{p}_{n+1,\,1}$ verschieden ist. Hiermit erhalten wir abzählbar unendlich viele Primideale $\mathfrak{p}$, $\mathfrak{p}_{(1)}$, $\mathfrak{p}_{(2)}, \cdots$, $\mathfrak{p}_{(n)}, \cdots$, welche die Teiler von $\mathfrak{a}$ sind. Bedeutet jetzt $\mathfrak{q}$ bzw. $\mathfrak{q}_{(n)}$ das zu $\mathfrak{p}$ bzw. $\mathfrak{p}_{(n)}$ gehörige I. P. K. von $\mathfrak{a}$, so ist offenbar $\mathfrak{q}$ zu sämtlichen $\mathfrak{q}_{(n)}$ teilerfremd und es gilt $\mathfrak{q} \supset \mathfrak{q}_{(1)} \cap \mathfrak{q}_{(2)} \cap \cdots \cap \mathfrak{q}_{(n)} \cap \cdots$. Denn sei α ein Element aus $\bigcap_n \mathfrak{q}_{(n)}$, so ist $\alpha \in \mathfrak{O}_m$ für ein hinreichend grosses $m\ (\geqq N)$. Damit ist $\alpha \in (\bigcap_n \mathfrak{q}_{(n)}) \cap \mathfrak{O}_m = \bigcap_n (\mathfrak{q}_{(n)} \cap \mathfrak{O}_m)$[6] und nach der Struktur von $\mathfrak{p}_{(m)}$ ist $\mathfrak{q}_{(m)} \cap \mathfrak{O}_m = \mathfrak{q}_{(m+1)} \cap \mathfrak{O}_m = \cdots = \mathfrak{q} \cap \mathfrak{O}_m$. Daraus ergibt sich $\alpha \in \mathfrak{q}_{(m)} \cap \mathfrak{O}_m = \cdots = \mathfrak{q} \cap \mathfrak{O}_m$, folglich $\alpha \in \mathfrak{q}$. Also muss $\mathfrak{q} \geqq \bigcap_n \mathfrak{q}_{(n)}$ sein. Dabei können wir offenbar behaupten, dass $\mathfrak{q} \neq \bigcap_n \mathfrak{q}_{(n)}$ ist.[7] Hieraus folgt $\mathfrak{q} \supset \bigcap_n \mathfrak{q}_{(n)}$.

Ist $\mathfrak{a} = \bigcap_\iota \mathfrak{q}_{(\iota)}$ eine Darstellung durch seine sämtlichen I. P. K., so können wir etwa $\mathfrak{q} = \mathfrak{q}_{(\tau)}$ setzen. Nach dem obig gewonnenen Resultat erhalten wir $\mathfrak{q}_{(\tau)} \supset \bigcap_n \mathfrak{q}_{(n)} \geqq \bigcap_{\iota \neq \tau} \mathfrak{q}_{(\iota)}$, wobei $\mathfrak{a} = \mathfrak{q}_{(\tau)} \cap (\bigcap_{\iota \neq \tau} \mathfrak{q}_{(\iota)})$ ist. Damit kann die Darstellung

6) N. Nakano, „Idealtheorie in einem spezialen unendlichen algebraischen Zahlkörper", Jour. of Sci. of the Hiroshima Univ. Vol. 16. No. 3 Hilfssatz 1, zitiert mit „Nakano (2)".

7) Bekanntlich gilt in $\mathfrak{O}$ für I. P. K. eines Ideals folgender Satz: *Ist* $\mathfrak{q}$ *die zu* $\mathfrak{p}$ *gehörige I. P. K. von* $\mathfrak{a}$, *so ist* $\mathfrak{q}$ *dann und nur dann gleich* $\mathfrak{a}$, *wenn* $\mathfrak{a}$ *durch ein einziges Primideal* $\mathfrak{p}$ *teilbar ist.* Siehe „Nakano (1)" Satz 2. s. 172.

$\mathfrak{a}=\bigcap_{\iota}\mathfrak{q}_{(\iota)}$ nicht die kürzeste sein. Das gewonnenne Ergebnis möge als Satz folgendermassen formuliert werden;

Satz 4. *Besitzt ein Ideal* $\mathfrak{a}$ *unendlich viele Primidealteiler, so lässt* $\mathfrak{a}$ *keine kürzeste Darstellung als Durchschnitt von seinen sämtlichen I. P. K. zu.*

Ist $\mathfrak{a}=\bigcap_{\iota}\mathfrak{q}_{(\iota)}$ eine kürzeste Darstellung durch seine sämtlichen I. P. K., so besitzt $\mathfrak{a}$ nach diesem Satz 4 nur endlich viele Primidealteiler. Weiter, besitzt ein Ideal $\mathfrak{a}$ nur endlich viele Primidealteiler, so können wir nach dem Fundamentalsatz die Zerlegung;

$$\mathfrak{a}=\mathfrak{q}_{(1)}\mathfrak{q}_{(2)}\cdots\mathfrak{q}_{(m)}$$

erhalten, wobei $\mathfrak{q}_{(i)}$ $(i=1,2,\cdots,m)$ eine zu $\mathfrak{p}_{(i)}$ gehörige I. P. K. von $\mathfrak{a}$ ist. Dann ist offenbar die Existenz eines Elements r_i von der Art, dass $r_i \notin \mathfrak{p}_{(i)}$, $r_i \in \mathfrak{q}_{(1)}\mathfrak{q}_{(2)}\cdots\mathfrak{q}_{(i-1)}\mathfrak{q}_{(i+1)}\cdots\mathfrak{q}_{(m)}$, d. h. $\mathfrak{a}:(r_i)=\mathfrak{q}_{(i)}$ für alle i ist.

Fassen wir unsere Ergebnisse zusammen, so erhalten wir folgenden Hauptsatz.

Satz 5. *Ist* $\mathfrak{a}$ *ein gegebenes Ideal aus* $\mathfrak{O}$ *und* $\mathfrak{a}=\bigcap_{\iota}\mathfrak{q}_{(\iota)}$ *eine Darstellung durch sämtliche I. P. K. von* $\mathfrak{a}$, *so sind die folgenden Bedingungen zueinander äquivalent:*

(1) $\mathfrak{a}=\bigcap_{\iota}\mathfrak{q}_{(\iota)}$ *ist die kürzeste Darstellung.*

(2) $\mathfrak{a}$ *besitzt nur endlich viele Primidealteiler.*

(3) *Es gibt für alle* $\mathfrak{q}_{(\iota)}$ *ein Element* r_{ι} *von der Art, dass* $\mathfrak{a}:(r_{\iota})=\mathfrak{q}_{(\iota)}$ *ist.*