

Zur Idealtheorie Dedekindscher Algebren.

Autor(en): **Brandt, H.**

Objektyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **2 (1930)**

PDF erstellt am: **17.07.2024**

Persistenter Link: <https://doi.org/10.5169/seals-3607>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Zur Idealtheorie Dedekindscher Algebren

Von H. BRANDT, in Aachen

Bekanntlich ist es bei einem algebraischen Zahlkörper \mathbb{K} nur in Sonderfällen möglich, allgemeine Aussagen über die Zerlegung einer Primzahl in Primideale zu machen. Man sollte nun meinen, daß eine nicht-kommutative Erweiterung von \mathbb{K} die Schwierigkeiten dieses Problems noch wesentlich erhöhen würde. Doch ist das, wie wir zeigen werden, keineswegs der Fall.

Wir beschränken uns auf Systeme, welche keine eigentlich nilpotenten Elemente enthalten und nicht mehr als direkte Summe einfacherer Systeme darstellbar sind¹⁾. Es liege also eine in \mathbb{K} definierte einfache Dedekindsche Algebra \mathfrak{A} vor²⁾. Unter dem *Grad* einer Algebra verstehen wir den Grad ihrer allgemeinen Gleichung, unter dem *Rang* die Anzahl ihrer linear unabhängigen Zahlen³⁾. Dabei muß noch angegeben werden, auf welchen Körper diese Anzahlen bezogen sind. Wenn man sie bei der Algebra \mathfrak{A} auf das Zentrum \mathfrak{Z} bezieht, so ist der Rang m^2 , wenn der Grad den Wert m hat. Es ist dann bekanntlich möglich, durch geeignete algebraische Erweiterung von \mathfrak{Z} in \mathfrak{A} Isomorphie mit dem System aller Matrizen vom Grade m herzustellen, wobei die Koeffizienten in dem erweiterten Zentrum zu nehmen sind.

Die Schwierigkeiten, welche das Problem der Zerlegung in gleichseitige Primideale⁴⁾ bietet, liegen dann fast allein im Zentrum, während der Schritt von \mathfrak{Z} nach \mathfrak{A} oder genauer von der Hauptordnung in \mathfrak{Z} zu einer Hauptordnung in \mathfrak{A} verhältnismäßig leicht zu erledigen ist⁵⁾. Es ist bekannt, daß ein Primideal \mathfrak{p} des Zentrums i. a. auch in jeder Hauptordnung \mathfrak{o} von \mathfrak{A} Primideal bleibt. Nur in endlich vielen Ausnahmefällen ist überhaupt eine weitere Zerlegung möglich⁶⁾. Wir werden zeigen, daß die Zerlegung nur die Form $\mathfrak{p} = \mathfrak{p}^e$ haben kann, woraus sich dann noch Folgerungen für die Differenten ergeben.

Um das zu beweisen, nehmen wir an, es liege in einer maximalen Ordnung oder Hauptordnung \mathfrak{o} von \mathfrak{A} eine Zerlegung $\mathfrak{p} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$

1) Vgl. hierzu wie zum folgenden: Dickson, Algebren und ihre Zahlentheorie, Zürich 1927.

2) Dedekindsche Algebren sind solche ohne Radikal.

3) Sonst wird der Grad als Rang und der Rang als Ordnung bezeichnet. Da aber das Wort „Ordnung“ noch in mehreren ganz andern Bedeutungen gebraucht wird, scheint es empfehlenswert, es hier zu vermeiden.

4) Zum Unterschiede von ungleichseitigen Primidealen, welche links und rechts zu verschiedenen Ordnungen gehören.

5) Ein Ideal, welches im Zentrum liegt, wird hier nicht von dem Ideal unterschieden, das daraus nach Multiplikation mit allen Zahlen einer Hauptordnung der ganzen Algebra entsteht.

vor, wo p_1, \dots, p_r gleichseitige Primideale von \mathfrak{o} bezeichnen. Wir werden dann aus der Annahme, daß die Anzahl r dieser Primideale größer als 1 ist, allein durch Abzählen der Rang- und Gradzahlen im Restesystem von \mathfrak{o} nach \mathfrak{P} , einen Widerspruch herleiten, womit dann die ausgesprochene Behauptung bewiesen ist.

Das Restesystem der Hauptordnung des Zentrums nach \mathfrak{P} ist ein Galoisfeld \mathfrak{G}_0 , dessen Grad durch g_0 bezeichnet werden möge. Das Restesystem von \mathfrak{o} nach \mathfrak{P} ist dann eine Algebra in \mathfrak{G}_0 , deren Rang in bezug auf \mathfrak{G}_0 den Wert m^2 hat, während der Grad höchstens den Wert m hat⁶⁾.

In dieser Algebra entspricht der Zerlegung von \mathfrak{P} in Primidealpotenzen eine Darstellung als direkte Summe. Dabei ergeben die Summen der Rang- und Gradzahlen in den Teilsystemen wieder den Rang und den Grad in dem ganzen System. Ist \mathfrak{p} eins der Primideale p_1, \dots, p_r und e der zugehörige Exponent, so wird das entsprechende Teilsystem durch das Restesystem von \mathfrak{o} nach \mathfrak{p}^e gegeben.

Das Restesystem von \mathfrak{o} nach \mathfrak{p} ist eine Matrixalgebra in einem Galoisfeld \mathfrak{G} ⁷⁾. Der Grad der Matrizen sei k , der des Galoisfeldes g . Weil \mathfrak{G} eine Erweiterung von \mathfrak{G}_0 ist, so gilt $g = g_0 f$, wo f eine ganze rationale Zahl ist, die wir den Relativgrad von \mathfrak{G} nennen können.

Das Restesystem von \mathfrak{o} nach \mathfrak{p}^e wird nach Herrn Speiser⁷⁾ durch Matrizen desselben Grades k gegeben, deren Elemente einen Ring \mathfrak{G}^* durchlaufen, nämlich von der Gestalt

$$\alpha_0 + \alpha_1 \pi + \dots + \alpha_{e-1} \pi^{e-1}$$

sind, wo die α_i in \mathfrak{G} liegen, während π eine durch \mathfrak{p} , aber nicht durch \mathfrak{p}^2 teilbare Zahl ist. Der Kürze wegen möge \mathfrak{G}^* als *Galoisring* bezeichnet werden, e heiße seine *Länge*.

In diesem Restesystem haben wir nun den Rang und den Grad abzuzählen. Der Rang ist offenbar efk^2 , weil der Rang von \mathfrak{G}^* gleich ef ist. Der Grad kann zunächst nicht genau bestimmt, aber abgeschätzt werden. Einerseits gibt es in \mathfrak{G}^* Elemente, deren Grad in bezug auf \mathfrak{G}_0 den Wert f hat (denn solche Elemente sind schon in \mathfrak{G} vorhanden), andererseits hat π in bezug auf \mathfrak{G}_0 den Grad e . Der Grad im Galoisring, bezogen auf \mathfrak{G}_0 , ist also mindestens so groß wie die größere der

⁶⁾ E. Artin, Zur Arithmetik hyperkomplexer Zahlen, Abhandlungen des mathematischen Seminars Hamburg 1927, S. 278.

⁷⁾ A. Speiser, Allgemeine Zahlentheorie, Vierteljahrsschrift der Naturforschenden Gesellschaft Zürich 1926 = Dickson letztes Kapitel.

beiden Zahlen e und f , also auch mindestens so groß wie \sqrt{ef} . Geht man aber in einer Algebra mit Haupteinheit zu Matrizen eines bestimmten Grades über, so multipliziert sich der Grad der Algebra mit dem Grad der Matrizen. Der Grad im Restesystem von \mathfrak{o} nach \mathfrak{p}^e ist also größer oder gleich $\sqrt{ef} \cdot k$.

Sind nun mehrere Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ vorhanden und unterscheidet man die Anzahlen e, f, k entsprechend durch Indizes, so gibt die doppelte Abzählung der Rang- und Gradzahlen die beiden Beziehungen

$$m^2 = e_1 f_1 k_1^2 + \dots + e_r f_r k_r^2$$

$$m \geq \sqrt{e_1 f_1} \cdot k_1 + \dots + \sqrt{e_r f_r} \cdot k_r$$

welche, wie man durch Quadrieren der zweiten erkennt, nur zusammen bestehen können, wenn $r = 1$, auf den rechten Seiten also nur ein Glied auftritt.

Man hat daher

$$m^2 = e f k^2, \quad m \geq e k, \quad m \geq f k,$$

woraus noch $e = f$ folgt, so daß $m = e k$.

Aus der Isomorphie der von den gleichseitigen Idealen in den verschiedenen Hauptordnungen gebildeten Gruppen schließt man noch, daß e von der ausgewählten Ordnung \mathfrak{o} unabhängig ist.

Daher ist ein Primideal \mathfrak{P} des Zentrums entweder in allen Hauptordnungen unzerlegbar oder in jeder als e -te Potenz darstellbar.

Durch unsere Betrachtungen wird die Struktur des Restesystems von \mathfrak{o} nach \mathfrak{P} vollkommen aufgeklärt. Das Restesystem wird durch Matrizen vom Grade $k = \frac{m}{e}$ gegeben, deren Elemente einen Galoisring \mathfrak{G}^* durchlaufen, welcher aus einem Galoisfeld \mathfrak{G} vom Relativgrad e gebildet ist und selbst die Länge und übrigens auch denselben Relativgrad e hat. In dem gewöhnlichen Fall $e = 1$ ist $k = m$ und $\mathfrak{G}^* = \mathfrak{G} = \mathfrak{G}_0$.

Wir zeigen noch, daß in der Ordnung \mathfrak{o} die in bezug auf \mathfrak{J} genommenen Spuren der Zahlen nach dem Modul \mathfrak{P} jeden beliebigen Wert haben können. Bildet man die Spuren im Restesystem nach \mathfrak{P} , so hat man zunächst die Diagonalglieder in den Matrizen vom Grade k zu addieren und hat damit, wenn $k = m$, also $e = 1$, bereits die Spuren, welche, wie man sieht, beliebige Reste aus \mathfrak{G}_0 sein können. Ist $e > 1$,

so erhält man zunächst Reste aus \mathfrak{G}^* , für welche die Spur in bezug auf \mathfrak{G}_0 zu bilden ist. Da \mathfrak{G}^* eine hyperkomplexe Erweiterung von \mathfrak{G} ist, aber in bezug auf \mathfrak{G}_0 denselben Grad e besitzt, und schon, wie man leicht erkennt, die Spuren der Zahlen aus \mathfrak{G} in \mathfrak{G}_0 jeden beliebigen Wert haben können, so gilt das umsomehr von \mathfrak{G}^* . Damit ist die Behauptung über die Spuren bewiesen.

Wir bilden noch das Komplement \mathfrak{o}' von \mathfrak{o} , d. h. die Gesamtheit der Zahlen ν , für welche, wenn ω jede Zahl aus \mathfrak{o} bedeutet, die auf das Zentrum bezogenen Spuren $s(\nu\omega) = s(\omega\nu)$ ganz sind, d. h. in der Hauptordnung des Zentrums liegen. Das reziproke Ideal $\mathfrak{o}'^{-1} = \mathfrak{d}$, die Differenten von \mathfrak{o} , ist ganz, nämlich eine Teilmenge von \mathfrak{o} . Es besitze die Primidealzerlegung $\mathfrak{d} = \mathfrak{p}_1^{r_1} \dots \mathfrak{p}_s^{r_s}$. Man kann \mathfrak{d} auffassen als kleinstes gemeinsames Vielfaches oder als Durchschnitt der Primidealpotenzen $\mathfrak{p}_i^{r_i}$, und ebenso $\mathfrak{o}' = \mathfrak{d}^{-1}$ als größten gemeinsamen Teiler oder als Vereinigungsmenge der reziproken Primidealpotenzen $\mathfrak{p}_i^{-r_i}$. Man hat also nur zu fragen: Welche reziproken Primidealpotenzen haben die Eigenschaft, daß die Spuren ihrer Zahlen in der Hauptordnung des Zentrums liegen?

Wenn ein Ideal nur Zahlen mit ganzzahligen Spuren besitzt, so werden die Spuren der Zahlen des Ideals, das durch Multiplikation mit einem ganzen Zentrumsideal entsteht, sämtlich durch das betreffende Zentrumsideal teilbar.

Daher ist es nicht möglich, daß für ein Zentrumsprimideal \mathfrak{P} die Spuren aus \mathfrak{P}^{-1} , noch weniger die einer höheren negativen Potenz, ganz werden. Denn durch Multiplikation mit \mathfrak{P} entsteht \mathfrak{o} , und die Spuren der Zahlen aus \mathfrak{o} sind modulo \mathfrak{P} beliebig, also nicht durch \mathfrak{P} teilbar.

Umgekehrt schließt man: Sind die Spuren der Zahlen eines Ideals sämtlich durch \mathfrak{P} teilbar, so sind die Spuren des Ideals, das durch Multiplikation mit \mathfrak{P}^{-1} oder Division mit \mathfrak{P} entsteht, sämtlich ganz.

Gilt nun für das Zentrumsprimideal \mathfrak{P} die Zerlegung $\mathfrak{P} = \mathfrak{p}^e$ und ist e größer als 1, so sieht man leicht, daß die Spuren der Zahlen aus \mathfrak{p} sämtlich durch \mathfrak{P} teilbar sein müssen. Im Restesystem nach \mathfrak{P} wird nämlich das Ideal \mathfrak{p} durch diejenigen Matrizen vom Grade k gegeben, deren Elemente beliebig aus dem Radikal von \mathfrak{G}^* gewählt sind. Bei einer solchen Matrix liegt daher auch die Summe der Elemente der Hauptdiagonale im Radikal, und ihre e -te Potenz und somit auch die Spur ist Null modulo \mathfrak{P} .

Dividiert man durch \mathfrak{P} , so ergibt sich das Ideal $\mathfrak{p}^{-(e-1)}$. Aus dem vorhin Bewiesenen folgt dann, daß die Spuren aller Zahlen dieses Ideals ganz sind. Da nun schon die Spuren aus $\mathfrak{p}^{-e} = \mathfrak{P}^{-1}$ nicht mehr alle ganz sein können, so sind damit die umfassendsten reziproken Primidealepotenzen, deren Zahlen ganzzahlige Spuren besitzen, gefunden⁸⁾, und es gilt der Satz:

Die in bezug auf das Zentrum gebildete Differentiale δ von \mathfrak{o} enthält alle gleichseitigen Primideale \mathfrak{p} von \mathfrak{o} genau in der Potenz \mathfrak{p}^{e-1} , wenn e der kleinste Exponent ist, für den \mathfrak{p}^e Zentrumsideal wird.

⁸⁾ Aehnliche Betrachtungen geben auch die einfachste Herleitung der bisher bekannten Differentensätze bei Zahlkörpern. Vgl. noch die Diskussionsbemerkungen von Fr. E. Noether beim Vortrag von Herrn Grell in Prag (erscheint demnächst in den Jahresberichten der D.M.V.).

(Eingegangen den 16. Dezember 1929)