Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 8 (1935-1936)

Artikel: Zahlentheorie in rationalen Algebren.
Autor: Speiser, A.
DOI: https://doi.org/10.5169/seals-9304

Zahlentheorie in rationalen Algebren

Von A. Speiser, Zürich

In dieser Arbeit möchte ich an die Methoden meiner Abhandlung „Allgemeine Zahlentheorie“ (Vierteljahrschrift der Naturforschenden Gesellschaft in Zürich, Bd. 71, S. 8, 1926), die in etwas veränderter Form als Kap. 13 in Dickson, Algebren und ihre Zahlentheorie, Zürich 1927, abgedruckt ist, anknüpfen und einige Beweise vereinfachen; ferner soll die Ergänzung, welche durch die grundlegende Entdeckung des Gruppoids durch Herrn Brandt gefordert wird, ausgeführt und die Struktur der Ideale einer Algebra dargestellt werden.

Zur Entdeckungsgeschichte des Gruppoids schreibt mir Herr Brandt folgendes: „Der Gedanke, die Gruppoidarbeit zu schreiben, ergab sich mir gelegentlich der Weierstraßwoche in Münster im Juni 1925 bei einer Unterhaltung mit Herrn Haupt. Ich erzählte ihm von den Verknüpfungsgesetzen der Formenklassen bei der Komposition der quadratischen Formen (die i. a. ein gestörtes Gruppoid bilden) und dabei ergab sich der Wunsch, die Verknüpfungsgesetze in idealisierter Form abstrakt festzulegen.

„Ehe Ihre Arbeit erschien, hatte ich das Gruppoid der Ideale noch nicht, auch nicht bei den Quaternionen. Ich betrachtete aber die ‚Idealprodukte‘ aus Rechts- und Linksidealen einer Ordnung. War die Ordnung auch als ‚Einheitsideal‘ aufzufassen, so zeigte sich, daß unter den ‚Idealprodukten‘ auch ‚Halbeinheiten‘ vorhanden waren. So erhielt ich für ein Rechtsideal $\mathfrak{a}$ durch die Multiplikation mit dem inversen Ideal $\mathfrak{a}^{-1}$ die Halbeinheit $\mathfrak{a}\,\mathfrak{a}^{-1} = \mathfrak{o}'$. Da erhielt ich Ihre Arbeit. Was mir am meisten daraus auffiel, war die darin enthaltene versteckte Multiplikation $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$. Als ich sie bemerkte, durchfuhr mich wie ein Blitz der Gedanke: Einheiten und Halbeinheiten sind gleichberechtigt, und die Idee des Gruppoids der Ideale war geboren zunächst für die Quaternionen.

„Während ich nun mit dem Ausbau der Quaternionenarbeit beschäftigt war, über die ich in Freiburg vortrug, wurde ich auf die Modultheorie geführt, welche sich auf beliebige Dedekindsche Systeme übertragen ließ. Das führte mich auf Grund Ihrer Arbeit zu der klaren Erkenntnis, daß der Gruppoidsatz der Ideale allgemeine Gültigkeit hat für einfache Systeme über algebraischen Zahlkörpern, welche Behauptung ich daher in die Einleitung der Quaternionenarbeit (Math. Ann. 99, S. 1) aufnahm, als ich die Arbeit im Januar 1927 einreichte und im Durchschlag Ihnen zusandte.“

Für die Literatur verweise ich auf das Buch von Deuring „Algebren". Zur Ergänzung sei noch erwähnt: Verhandlungen der Schweiz. Naturforschenden Gesellschaft, Basel 1927, II. Teil, H. Brandt: Zur allgemeinen Idealtheorie, A. Speiser: Über Gruppen und Gruppoide. Dieselben Verhandlungen, Davos 1929, H. Brandt: Primidealzerlegung in einer Dedekindschen Algebra.

I. Aufstellung der Ideale und der Ordnungen

1. Wir legen eine Algebra im Gebiet der rationalen Zahlen zugrunde und beginnen mit dem Fall, daß das Restesystem der ganzen Zahlen einer Ordnung (mod p) eine vollständige Matrixalgebra in einem Galoisfeld bildet. Die Basisgrößen gegenüber dem Galoisfeld seien mit e_{ik} bezeichnet. Sie genügen den bekannten Gleichungen

$$e_{ik} \cdot e_{lm} \equiv 0 \text{ für } k \neq l \text{ und } e_{ik} \cdot e_{km} \equiv e_{im} \pmod{p}.$$

Nun betrachten wir die Algebra (mod p^r) und wählen ein beliebiges System von Größen aus, das (mod p) den e_{ik} kongruent ist und wieder mit e_{ik} bezeichnet werden soll. Wir beweisen nun den

Satz 1: Man kann die Größen e_{ik} (mod p^r) so auswählen, daß sie denselben Gleichungen (mod p^r) genügen, wie (mod p).

Beweis: Wir können zunächst wie in Dickson S. 278 ohne Schwierigkeit zeigen, daß die Größen e_{ii} als Idempotente auch (mod p^r) gewählt werden können. Man bildet zu diesem Zweck die Potenzen; wird nun $e_{ii}^s \equiv e_{ii}^{s+t}$ (mod p^r), so ergibt sich e_{ii}^{st} unmittelbar als ein Idempotent, das an Stelle von e_{ii} verwendet werden kann.

Diese neuen Größen bezeichnen wir wieder mit e_{ii} und ersetzen nun die bisherigen Repräsentanten e_{ik} durch folgende: $e_{ii}\, e_{ik}\, e_{kk}$, die wieder mit e_{ik} bezeichnet werden sollen.

Jetzt mögen die Gleichungen bestehen:

$$e_{ii}\, e_{kk} \equiv pa \pmod{p^2}.$$

Wenn wir links mit e_{ll} multiplizieren und l von i verschieden ist, so erhalten wir eine durch p^2 teilbare Zahl, ebenso rechts, wenn l von k verschieden ist. Daher wird $a \equiv a_{ik}\, e_{ik} \pmod{p}$, wo a_{ik} irgend eine Größe des Galoisfeldes ist. Nun bilden wir die Ausdrücke

$$e_{ii} - p\,(a_{i1}\, e_{i1} + a_{i2}\, e_{i2} + \cdots + a_{i,i-1}\, e_{i,i-1} + a_{i,i+1}\, e_{i,i+1} + \cdots + a_{i,n} e_{i,n}).$$

Wir bezeichnen sie wieder mit e_{ii} und finden durch Ausrechnen, daß sie den Gleichungen genügen

$$e_{ii}^2 \equiv e_{ii} \pmod{p^2} \text{ und } e_{ii}\, e_{kk} \equiv 0 \pmod{p^2} \text{ für } i \neq k\,.$$

In derselben Weise kann man fortfahren und man findet ein System von Idempotenten, die (mod p^r) zu einander orthogonal sind. Mit diesen normiert man die bisherigen e_{ik} durch Multiplikation $e_{ii}\, e_{ik}\, e_{kk}$ und erhält das im Satz geforderte System.

Wir bemerken noch, daß die Größen des Galoisfeldes nicht so normiert werden können, daß sie auch (mod p^r) ein Galoisfeld bilden. Das wird aber im folgenden nicht stören. Die einzige hier in Betracht kommende Tatsache ist, daß wir die 0 sofort auch modulo einer beliebigen Zahl normieren können, nämlich durch die 0 der Algebra.

2. Die Gesamtheit der Reste (mod p^r) einer Ordnung $\mathfrak{J}$ kann in folgender Weise dargestellt werden:

$$R + p\,R' + p^2\,R'' + \cdots + p^{r-1}\,R^{(r-1)}\,.$$

Hierbei bedeuten die R jeweils die Gesamtheit der Matrizen mit n Zeilen und Kolonnen, deren Koeffizienten unabhängig von einander die Größen des Galoisfeldes, irgendwie (mod p^r) normiert, durchlaufen. Jedoch ist zu bemerken, daß die Größen von $R^{(j)}$ nur (mod p^{r-j}) festgelegt zu sein brauchen. Die Gesamtheit aller Zahlen der Ordnung $\mathfrak{J}$, von der wir ausgegangen sind, kann dargestellt werden in der Gestalt

$$R + p\,R' + \cdots + p^{r-1}\,R^{(r-1)} + p^r\,\mathfrak{J}\,,$$

wo $\mathfrak{J}$ alle Zahlen der Ordnung durchläuft.

3. Wir bilden jetzt ein in p^r enthaltenes Rechtsideal $\mathfrak{a}$ von folgendem Typus: S möge die Gesamtheit der Matrizen bezeichnen, deren n_0 erste Zeilen beliebig sind, während die übrigen lauter Nullen enthalten. S' bedeute entsprechend die Matrizen, deren n_1 erste Zeilen beliebig sind, während die übrigen Zeilen nur Null enthalten, ebenso $S^{(j)}$ die Matrizen, deren n_j erste Zeilen beliebig sind, während die übrigen verschwinden. Dann bilden wir das Rechtsideal

$$\mathfrak{a} = S + pS' + \cdots + p^{r-1}\,S^{(r-1)} + p^r\,\mathfrak{J}\,.$$

Weil mit dem Restesystem S auch pS in $\mathfrak{a}$ vorkommt, muß pS in S' enthalten sein und wir haben daher die Ungleichungen

$$0 < n_0 \leqq n_1 \leqq \cdots \leqq n_{r-1} < n .$$

Zu diesem Rechtsideal bilden wir ein Linksideal und führen folgende Bezeichnung ein:

$$n - n_0 = m_{r-1}, \ldots, n - n_{r-1} = m_0 .$$

Dann verstehen wir unter $T^{(j)}$ die Matrix, deren m_j letzte Spalten beliebig mit Resten des Galoisfeldes ausgefüllt sind, während die vorherigen Spalten sämtlich 0 sind. Offenbar gilt

$$0 < m_0 \leqq m_1 \leqq \cdots \leqq m_{r-1} < n .$$

Die Gesamtheit der Reste in

$$\mathfrak{b} = T + pT' + \cdots + p^{r-1} T^{(r-1)} \pmod{p^r}$$

bildet ein Linksideal, das ich früher (Dickson, S. 294) als das zu $\mathfrak{a}$ komplementäre Ideal bezeichnet habe.

4. Nun bilden wir das Produkt $\mathfrak{b}\mathfrak{a}$ der beiden Ideale, indem wir in der üblichen Weise darunter das Produkt einer beliebigen Zahl aus $\mathfrak{b}$ mit einer beliebigen Zahl aus $\mathfrak{a}$ und die Summen solcher Produkte verstehen. Indem man

$$(T + pT' + \cdots + p^{r-1} T^{(r-1)} + p^r \mathfrak{J})\,(S + \cdots + p^{r-1} S^{(r-1)} + p^r \mathfrak{J})$$

nach dem Distributivgesetz ausmultipliziert, findet man, daß alle Größen durch p^r teilbar sind. Denn es ist $p^i T^{(i)} p^k S^{(k)} = p^{i+k} T^{(i)} S^{(k)}$. Falls nun $i + k < r$ ist, so wird das Produkt der beiden Matrizen $= 0$. Dagegen kommt im Produkt jedes Vielfache von p^r vor. Denn es ist ein zweiseitiges Ideal, welches insbesondere $T\, p^r\, \mathfrak{J}$ enthält. Wir können den Faktor p^r weglassen und $T\,\mathfrak{J}$ untersuchen. Weil wir ein zweiseitiges Ideal vor uns haben, kommt auch $\mathfrak{J} T \mathfrak{J}$ darin vor. Dies reduzieren wir (mod p) und erhalten $R\,T\,R$. Bedenken wir nun, daß T nicht die Nullmatrix ist, sondern daß mindestens eines der e_{ik} mit einem von Null verschiedenen Faktor auftritt, so sehen wir, daß $R\,T\,R$ die vollständige Matrixalgebra (mod p) ist. Daher ist das zugehörige Ideal das Ideal (1), also die Ordnung $\mathfrak{J}$ selber.

Wir bekommen daher die Gleichung

$$\mathfrak{b}\,\mathfrak{a} = p^r \mathfrak{J};$$

indem man setzt $\mathfrak{b}/p^r = \mathfrak{a}^{-1}$, erhält man das zu $\mathfrak{a}$ inverse Ideal, das die Gleichung erfüllt:

$$\mathfrak{a}^{-1}\,\mathfrak{a} = (1)$$

5. Um das Weitere übersehen zu können, ist es bequem, die Matrixdarstellung des Restesystems (mod p^r), die durch den Satz 1 gegeben ist, zu verwenden. Die Ordnung besteht (mod p^r) aus den Matrizen von n Zeilen und Kolonnen, deren Koeffizienten unabhängig voneinander die numerischen Reste (mod p^r), welche das Zentrum (mod p^r) bilden, durchlaufen. Das Ideal $\mathfrak{a}$ besteht aus denjenigen Matrizen, deren n_0 erste Zeilen beliebig sind, während die nächsten n_1—n_0 Zeilen sämtliche durch p teilbaren numerischen Reste enthalten usw. Bezeichnen wir das System aller Reste mit M, das System, aus welchem in der soeben angegebenen Weise das Ideal $\mathfrak{a}$ gebildet wird, mit A, so sieht man ohne weiteres, daß $A = PM$ ist, wo P eine Matrix ist, welche außerhalb der Hauptdiagonalen mit 0 ausgefüllt ist, während in der Hauptdiagonalen zuerst n_0-mal 1 steht, hierauf $(n_1 - n_0)$-mal p usw.; am Schluß steht $(n - n_{r-1})$-mal 0. Entsprechend wird das Linksideal $\mathfrak{b}$ von den Matrizen MQ gebildet, wo Q wieder eine Diagonalmatrix ist, deren n_0 erste Diagonalstellen mit 0, die nächsten n_1—n_0 Stellen mit p^{r-1} usw. ausgefüllt sind, so daß $PQ = p^r E$ ist, wo E die Einheitsmatrix bedeutet. Schließlich wird das Ideal $\mathfrak{a}^{-1}$ zu MP^{-1}.

Man findet jetzt, daß dem Produkt $\mathfrak{a}\mathfrak{b}$ das folgende Matrixsystem entspricht: $PMMQ = PMQ$. Hier genügt die Betrachtung (mod p^r) nicht, sondern wir müssen zunächst zu den Idealen selber übergehen. $\mathfrak{a}$ besteht aus den Zahlen von $PM + p^r \mathfrak{J}$ und $\mathfrak{b}$ aus den Zahlen $MQ + p^r \mathfrak{J}$. Es wird $\mathfrak{a}\mathfrak{b} = (PM + p^r \mathfrak{J})\,(MQ + p^r \mathfrak{J})$. Multipliziert man aus, so findet man, daß in $\mathfrak{a}\mathfrak{b}$ jedenfalls $p^{2r}\,\mathfrak{J}$ enthalten ist, so daß dieses Produkt aus Restklassen (mod p^{2r}) besteht. Verstehen wir nun wieder unter M das System aller Matrizen, deren Koeffizienten die Zentrumsreste (mod p^{2r}) durchlaufen, so wird

$$\mathfrak{a}\mathfrak{b} \equiv PMQ \pmod{p^{2r}}.$$

6. Es ist nützlich, sich von dem System PMQ eine deutliche Vorstellung zu machen. Zu dem Zweck teile man das Quadrat von n Zeilen und Kolonnen in Teilrechtecke ein, indem man nach der $n_k$ten Zeile und Kolonne $(k = 0,1, \ldots, r-1)$ einen Teilungsstrich durch das ganze Quadrat zieht. Man erhält so r^2 rechteckige Felder. Die Einteilung ist symmetrisch zur

Hauptdiagonalen, so daß die Felder, welche von ihr durchschnitten werden, quadratisch sind. Numerieren wir die Felder nach dieser Einteilung, so daß sie durch zwei Zahlen (i, k) bezeichnet sind, deren erste sich auf die vertikale Einteilung nach r horizontalen Streifen, die zweite auf die horizontale Einteilung nach r vertikalen Streifen bezieht, so wird das Feld mit der Nummer (i, k) von allen Resten des Zentrums (mod p^{2r}) ausgefüllt sein, die durch p^{i+r-k} teilbar sind. Hierbei soll die Numerierung in i und k von 0 bis r—1 gehen. In der Tat wird der Faktor P den $i$ten Horizontalstreifen mit p^i multiplizieren und der Rechtsfaktor Q den $k$ten Vertikalstreifen mit p^{r-k}. Spiegelt man die Matrix an der Hauptdiagonalen, so bedeutet das die Vertauschung von i und k und man sieht, daß Felder, die spiegelbildlich zur Hauptdiagonalen stehen, mit Potenzen von p multipliziert sind, deren Produkt p^{2r} ergibt.

7. Das Produkt $\mathfrak{a}\mathfrak{b}$ besteht aus allen Zahlen der Gestalt $PMQ + p^{2r}\mathfrak{J}$. Wir dividieren sie nun durch p^r und erhalten damit $\mathfrak{a}\mathfrak{a}^{-1} = PMP^{-1} + p^r\mathfrak{J}$. Dieses System, das gegenüber $\mathfrak{J}$ auch gebrochene Zahlen enthält, bezeichnen wir mit $\mathfrak{K}$. Es enthält die Haupteinheit, denn die Hauptdiagonale ist mit beliebigen ganzen Zahlen zu besetzen, da sie vorher genau durch p^r teilbar sein mußte. $\mathfrak{K}$ ist eine Ordnung, denn es wird $\mathfrak{K}\mathfrak{K} = PMP^{-1}PMP^{-1} = PMP^{-1}$.

Für PMP^{-1} gelten entsprechende Sätze, wie früher für PMQ. Felder, welche spiegelbildlich zur Hauptdiagonalen liegen, sind mit Potenzen von p multipliziert, deren Produkt 1 ist. Die Anzahl der Reste (mod p^r) ist in M und PMP^{-1} dieselbe.

Die Diskriminante der Ordnung $\mathfrak{K}$ ist gleich derjenigen von $\mathfrak{J}$. Denn die Substitutionsmatrix, welche eine Basis von $\mathfrak{J}$ in eine solche von $\mathfrak{K}$ überführt, hat die Determinante 1, weil die Anzahl der Reste (mod p^r) in beiden Ordnungen dieselbe ist. Was an ganzen Zahlen von $\mathfrak{J}$ verloren geht, wird an gebrochenen Zahlen wieder gewonnen. Wenn daher $\mathfrak{J}$ eine maximale Ordnung ist, deren Diskriminante ein Minimum ist, so ist auch $\mathfrak{K}$ eine maximale Ordnung.

$\mathfrak{K} = \mathfrak{a}\mathfrak{a}^{-1}$ ist die Linksordnung des Ideales $\mathfrak{a}$. Denn es gilt $\mathfrak{K}\mathfrak{a} = \mathfrak{a}\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{a}$. Hieraus ergibt sich der Satz von Brandt für unseren Spezialfall:

Satz 2: Ein Rechtsideal $\mathfrak{a}$ der Ordnung $\mathfrak{J}$ ist stets auch Linksideal der Ordnung $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{K}$.

8. Um einen beliebigen Rechtsidealteiler von p^r zu bestimmen, benützt man wieder die Matrizendarstellung. Wir suchen in dem Rechtsideal

Matrizen, deren Rang $n_0 \pmod p$ möglichst groß ist; es gibt also in jenen Matrizen genau n_0 Zeilen, welche $\pmod p$ unabhängig sind. Unter allen Matrizen mit diesem maximalen Rang $\pmod p$ wählen wir diejenigen aus, deren Rang $\pmod{p^2}$ maximal ist. Dieser Rang sei $n_0 + n_1$. In dieser Weise fahren wir fort und wir erhalten eine Matrix von höchstem Gesamtrang. Nun führen wir diese Matrix in eine Normalform über. Wir bringen n_0 Zeilen, die $\pmod p$ unabhängig sind, in der Matrix nach oben an die Stelle der n_0 ersten Zeilen. Alsdann fügen wir lineare Kombinationen dieser Zeilen zu den übrigen hinzu so, daß sie alle durch p teilbar werden. Unter diesen durch p teilbaren Zeilen suchen wir $n_1 \pmod{p^2}$ unabhängige aus und setzen sie unterhalb der vorigen, also an die Stelle der $(n_0 + 1)$ten bis zur $(n_0 + n_1)$ten Zeile. Am Ende bekommen wir n_{r-1} Zeilen, welche durch p^{r-1} teilbar sind und schließlich n_r Zeilen, welche mit 0 ausgefüllt sind. Die Operationen, welche mit der Matrix M vorgenommen worden sind, nämlich die Vertauschung von Zeilen und die Hinzufügung linearer Kombinationen gewisser Zeilen zu andern Zeilen, sind Zusammensetzungen von links her mit Matrizen, deren Determinante von 0 verschieden ist. Unser Resultat ist also folgendes: man kann eine Matrix A angeben, deren Determinante zu p prim ist und für welche AM die normale Gestalt hat, daß die n_0 ersten Zeilen $\pmod p$ linear unabhängig sind, die n_1 darauf folgenden durch p teilbar, aber $\pmod{p^2}$ linear unabhängig usw. Ich bezeichne diese Zeilen mit

$$Z_1, \ldots, Z_{n_0}, pZ_{n_0+1}, \ldots, pZ_{n_0+n_1}, \ldots .$$

Nun behaupte ich, daß die von den Potenzen von p befreiten Zeilen $Z_1, \ldots, Z_{n_0+1}, \ldots$ ebenfalls linear unabhängig sind $\pmod p$. Denn bestände eine Beziehung

$$Z_{n_0+1} \equiv a_1 Z_1 + \cdots + a_{n_0} Z_{n_0} \pmod p ,$$

so ergäbe sich durch Multiplikation dieser Kongruenz mit p eine Beziehung zwischen den $n_0 + 1$ ersten Zeilen der Matrix $\pmod{p^2}$, was nach der Voraussetzung nicht der Fall ist. In derselben Weise kommt man zu einem Widerspruch, wenn die Beziehung zwischen andern Zeilen besteht.

9. Die Matrix AM ist normal und kann in ein Produkt PZ zerlegt werden, wobei P eine Matrix ist, welche außerhalb der Hauptdiagonalen mit 0 ausgefüllt ist, während in der Hauptdiagonalen von oben an zuerst n_0-mal 1 steht, hierauf n_1-mal p, dann n_2-mal p^2 usw. Am Schluß steht

n_r-mal 0. Die Matrix Z besitzt die Zeilen $Z_1, Z_2, \ldots$ in dieser Reihenfolge, die n_r letzten Zeilen können ganz beliebig ausgefüllt werden, weil sie mit 0 multipliziert werden. Wir können daher annehmen, daß die Determinante von Z zu p prim ist.

Nun sei S eine ganz beliebige Matrix (mod p^r). Die Gleichung

$$ZX \equiv S \pmod{p^r}$$

besitzt als Lösung $X \equiv Z^{-1}S$, ist also stets auf eine Weise lösbar. Daher durchläuft ZX mit X das ganze System der Matrizen (mod p^r).

Weil das vorgegebene Rechtsideal die Matrix $A^{-1}PZ$ enthält, so enthält es sämtliche Matrizen $A^{-1}PM$. Nun muß noch gezeigt werden, daß damit schon das ganze Ideal erfaßt ist. Nehmen wir an, es gebe im Ideal noch eine weitere Matrix, etwa T, so bilden wir AT und erhalten eine Matrix U, welche nicht die Gestalt PX hat. Das heißt aber, irgend ein Koeffizient wird nicht durch diejenige Potenz von p teilbar sein, welche seine Zeile erfordert. Wieder genügt es, ein Beispiel zu behandeln. Es möge also etwa in der $(n_0 + 1)$ten Zeile ein zu p primer Koeffizient vorkommen. Weil wir ein Ideal vor uns haben, so dürfen wir zu B eine beliebige Matrix von PX addieren, ohne aus dem Ideal herauszukommen. Wir dürfen also insbesondere annehmen, daß die n_0 ersten Zeilen ganz beliebige Reste (mod p) enthalten, während der Koeffizient in der $(n_0 + 1)$ten Zeile sich (mod p) nicht geändert hat, denn die addierten Matrizen sind ja in jener Zeile sämtlich durch p teilbar. Damit können wir aber eine Matrix herstellen, deren Rang (mod p) größer als n_0 ist und die trotzdem zum Ideal gehört, was einen Widerspruch ergibt. Damit erhalten wir den

Satz 3: Ein beliebiger Rechtsidealteiler von p^r entsteht stets aus einem normalen Rechtsteiler durch Linksmultiplikation mit einem zu p primen Rest.

Bedenken wir weiter, daß auch die normalen Ideale entstehen, indem man das Gesamtsystem aller Matrizen (mod p^r) links mit dem durch P repräsentierten Rest multipliziert, so erhalten wir für unseren Fall den

Satz 4: Sämtliche Rechtsidealteiler von p^r sind Hauptideale (mod p^r), d. h. sie lassen sich in der Gestalt $a\,\mathfrak{J}$ (mod p^r) darstellen, wo a ein Rest ist. Umgekehrt sind sämtliche Systeme $a\,\mathfrak{J}$ (mod p^r) Idealteiler von p^r.

Korollar: Mit denselben Mitteln beweist man, daß sämtliche Ideale der vollständigen Matrixalgebra im Gebiet der rationalen Zahlen Haupt-

ideale sind. Denn die Reduktionen welche wir vorgenommen haben, nämlich die Vertauschung von Zeilen und die Hinzufügung von Zeilen zu andern, nachdem man sie mit ganzen Zahlen multipliziert hat, entsprechen ja der Zusammensetzung von links her mit Matrizen, welche ganzzahlig sind und eine Determinante ± 1 haben.

10. Der Satz 4 läßt sich nun ohne Mühe auf irgendwelche zur Diskriminante prime Rechtsideale ausdehnen. Betrachten wir zunächst den Fall, daß das Restesystem (mod p) eine direkte Summe von vollständigen Matrixalgebren ist, so zeigt man ohne weiteres, daß auch das System (mod p^r) in eine direkte Summe zerfällt. Man hat bloß die Haupteinheiten $e_1, e_2, \ldots, e_l$ durch Potenzierung zu orthogonalen Einheiten (mod p^r) zu machen, dann ist die Zerlegung bereits ausgeführt (vgl. Dickson, Kap. 13, Satz 10, pg. 278 und pg. 279). Jeder der Summanden in der direkten Summe bildet eines der bereits behandelten Systeme und der allgemeine Rechtsteiler von p^r ist direkte Summe von Rechtsidealen in den einzelnen Summanden. Diese letzteren sind aber Hauptideale von der Gestalt $a_k Q_k$, wo Q_k den $k$ten Summanden, a_k irgend einen Rest desselben darstellt. Bildet man $a = a_1 e_1 + a_2 e_2 + \cdots + a_l e_l$, so ist das ganze Rechtsideal offenbar identisch mit dem Hauptideal $a\mathfrak{J}$ (mod p^r).

Nun seien f und g zwei ganze, zu einander prime Zahlen und $\mathfrak{q}$ ein Rechtsidealteiler von fg. Bilden wir das Rechtsideal $\mathfrak{q} + g\mathfrak{J}$, d. h. addieren wir sämtliche Vielfachen von g, so erhalten wir einen Rechtsidealteiler $\mathfrak{a}$ von f. Entsprechend wird $\mathfrak{q} + f\mathfrak{J} = \mathfrak{b}$ ein Rechtsteiler von g. Wir setzen voraus, daß Satz 4 für die Teiler von f und die Teiler von g bewiesen ist und beweisen ihn für den Teiler von fg. Es sei $\mathfrak{a} \equiv a\mathfrak{J}$ (mod f) und $\mathfrak{b} \equiv b\mathfrak{J}$ (mod g), dann wird $\mathfrak{q} \equiv (ga + fb)\mathfrak{J}$ (mod fg), also ein Hauptideal.

11. Wir behandeln nun die Diskriminantenteiler. Ist p ein solcher, so besitzt das System der Reste (mod p), das mit $\mathfrak{R}$ bezeichnet sei, ein von 0 verschiedenes Radikal $\mathfrak{N}$. Wieder nehmen wir zunächst den Fall, daß die Differenzalgebra $\mathfrak{R} - \mathfrak{N}$ einfach, also eine vollständige Matrixalgebra in einem Galoisfeld ist. Im folgenden bezeichnen wir Repräsentanten der Reste (mod $\mathfrak{N}$), stets mit $\mathfrak{P}$, gleichgültig nach welchem Modul sie reduziert werden; ihre Zahl ist gleich der Zahl der Reste von $\mathfrak{R} - \mathfrak{N}$, da sie eben diese Algebra repräsentieren.

Nun betrachten wir die sukzessiven Potenzen von $\mathfrak{N}$ (mod p^2). Es sei $\mathfrak{N}^{\lambda+1}$ die erste durch p teilbare Potenz, also enthalte $\mathfrak{N}^{\lambda}$ noch Reste (mod p^2), die nicht durch p teilbar sind. Setzen wir $\mathfrak{N}^{\lambda+1} \equiv p\mathfrak{M}$ (mod p^2),

so ist $\mathfrak{M}$ (mod p) betrachtet ein zweiseitiges Ideal. Wenn daher irgend ein Rest in $\mathfrak{M}$ vorkommt, der nicht in $\mathfrak{N}$ enthalten ist, so muß $\mathfrak{M} \equiv \mathfrak{N}$ (mod p) sein, denn $\mathfrak{N}$ enthält außer sich selbst nur solche zweiseitigen Teiler, die in $\mathfrak{N}$ liegen. Es bestehen also nur die beiden Möglichkeiten: entweder es ist $\mathfrak{N}^{\lambda+1} \equiv p\mathfrak{N}$ (mod p^2) oder es ist $\mathfrak{N}^{\lambda+1}$ in $p\mathfrak{N}$ enthalten. Im zweiten Fall wird $\mathfrak{N}^{2\lambda}$ in $p\mathfrak{N}^{\lambda}$ enthalten sein und ich habe gezeigt (Dickson, pg. 283), daß man hier den Integritätsbereich erweitern kann durch Hinzufügung von $\mathfrak{N}^{\lambda}/p$. Wenn wir also von vorneherein einen maximalen Integritätsbereich voraussetzen, so wird stets $\mathfrak{N}^{\lambda+1} \equiv p\mathfrak{N}$ (mod p^2).

12. Wir gehen wieder zu den Resten (mod p) zurück und nehmen einen Rest ν aus $\mathfrak{N}$, der nicht in $\mathfrak{N}^2$ liegt. Jetzt bilden wir das System $\nu\mathfrak{P}$. Die Anzahl der Reste in $\mathfrak{P}$ sei v. Diese Zahl ist gleich $k^2 p^f$, wo k den Grad der Matrixalgebra $\mathfrak{P}$ bedeutet (die sogenannte Kapazität) und p^f die Ordnung des Galoisfeldes. Ich behaupte, daß $\nu\mathfrak{P}$ ebenfalls v Reste enthält, die sämtlich (mod $\mathfrak{N}^2$) verschieden sind. Denn im andern Fall läge eine Verbindung $\nu(a_{11}e_{11} + a_{12}e_{12} + \cdots + a_{kk}e_{kk})$ in $\mathfrak{N}^2$. Multipliziert man links mit e_{ii} und rechts mit e_{kk}, so folgt, daß der generelle Summand $a_{ik}e_{ik}$ schon in $\mathfrak{N}^2$ liegt, also auch $\nu(e_{11} + e_{22} + \cdots + e_{kk})$, was der Voraussetzung widerspricht, da $e_{11} + e_{22} + \cdots + e_{kk} = 1$ die Haupteinheit ist.

In derselben Weise zeigt man, daß $\mathfrak{P}\nu$ (mod $\mathfrak{N}^2$) genau v Reste enthält. Nehmen wir nun an, daß $\mathfrak{N}$ (mod $\mathfrak{N}^2$) selber nur v Reste enthält, so können diese sowohl durch $\nu\mathfrak{P}$, als durch $\mathfrak{P}\nu$ repräsentiert werden und wir erhalten $\nu\mathfrak{P} \equiv \mathfrak{P}\nu \equiv \mathfrak{N}$ (mod $\mathfrak{N}^2$). Das heißt aber, daß $\mathfrak{N}$ (mod $\mathfrak{N}^2$) ein Hauptideal ist. Ich beweise nun, daß unter dieser Voraussetzung auch $\mathfrak{N}$ (mod p) das Hauptideal $\nu\mathfrak{N}$ ist. Was wir bis jetzt gezeigt haben, ist, daß $\mathfrak{N} \equiv \nu\mathfrak{P} + \mathfrak{N}^2$ (mod p) ist, denn nach Voraussetzung wird eine beliebige Größe von $\mathfrak{N}$ (mod $\mathfrak{N}^2$) einer Größe νa kongruent, wo a in $\mathfrak{P}$ liegt, dies ist aber gerade obige Formel. $\mathfrak{N}^2$ besteht aus allen Produkten von zwei Größen aus $\mathfrak{N}$ und aus den Summen solcher Produkte. Betrachten wir also ein solches Produkt $\nu(a+\mu)\,\nu(a'+\mu')$, wo μ und μ' in $\mathfrak{N}$ liegen. Es liefert $\nu a\,\nu a' + \varrho$, wo ϱ in $\mathfrak{N}^3$ liegt, weil jeder seiner Summanden mindestens drei Größen aus $\mathfrak{N}$ als Faktor besitzt. Nun können wir aber nach oben $a\nu \equiv \nu a''$ (mod $\mathfrak{N}^2$) setzen, d. h. $a\nu = \nu a'' + \sigma$, wo σ in $\mathfrak{N}^2$ liegt. Es wird nun $\nu a\,\nu a' \equiv \nu\nu a''\,a'$ (mod $\mathfrak{N}^2$) und wir haben das Resultat, daß jede Größe von $\mathfrak{N}^2$ einer Größe der Gestalt $\nu^2\mathfrak{P}$ kongruent ist (mod $\mathfrak{N}^3$). In derselben Weise zeigt man für jeden Exponenten j, daß $\mathfrak{N}^j$ einer Größe $\nu^j\mathfrak{P}$ kongruent ist (mod N^{j+1}), daß also alle Differenzalgebren $\mathfrak{N}^j - \mathfrak{N}^{j+1}$ zweiseitige Hauptideale sind. Nehmen wir nun irgend eine

Zahl v' aus $\mathfrak{N}$, so können wir eine Zahl aus $v\mathfrak{P}$ subtrahieren so, daß die Differenz in $\mathfrak{N}^2$ liegt, hierauf eine Zahl aus $v^2\mathfrak{P}$ subtrahieren, so daß die Differenz in $\mathfrak{N}^3$ liegt usw., und es ergibt sich

$$v' \equiv va_1 + v^2a_2 + \cdots + v^\lambda a_\lambda \pmod{p}$$

d. h. das Ideal $\mathfrak{N}$ ist (mod p) ein Hauptideal $v\mathfrak{N}$, ferner ist $\mathfrak{N}^2 = v^2\mathfrak{N}$ usw. Dasselbe gilt auch (mod p^r).

13. Die ganze Schwierigkeit ist nun darauf zurückgeführt, zu beweisen, daß die Differenzalgebra $\mathfrak{N} - \mathfrak{N}^2$ die Ordnung v hat, dieselbe wie die Algebra $\mathfrak{P}$.

Um diesen Satz zu beweisen, müssen wir das obige Verfahren etwas verfeinern. Es sei wieder v eine Zahl aus $\mathfrak{N}$, welche nicht in $\mathfrak{N}^2$ liegt. Wir bilden die sämtlichen Produkte $e_{ii}\, v\, e_{jj}$ (mod $\mathfrak{N}^2$). Mindestens eines derselben liegt außerhalb von $\mathfrak{N}^2$, denn die Summe aller ist v. Es sei etwa $e_{11}\, v\, e_{11} = v_{11}$ außerhalb $\mathfrak{N}^2$. Dann setzen wir $e_{i1}\, v_{11}\, e_{1j} = v_{ij}$. Diese k^2 Größen sind linear unabhängig (mod $\mathfrak{N}^2$), was wie oben bewiesen wird, sie liefern ein System von v Größen und dieses bildet ein zweiseitiges Ideal $\mathfrak{U}$ (mod $\mathfrak{N}^2$). Denn $\mathfrak{P}\mathfrak{U}\mathfrak{P} \equiv \mathfrak{U}$ (mod $\mathfrak{N}^2$), weil allgemein gilt

$$e_{lm}\, v_{ij} \equiv 0 \text{ falls } m \neq i, \quad e_{li}\, v_{ij} \equiv v_{lj} \pmod{\mathfrak{N}^2}$$

Falls $\mathfrak{N}$ mit $\mathfrak{U}$ nicht identisch ist, so gibt es einen weiteren Rest μ in $\mathfrak{N}$, der nicht in $\mathfrak{U}$ enthalten ist. Wir behandeln ihn wie vorher v, nehmen an, daß $\mu_{11} = e_{11}\mu e_{11}$ außerhalb von $\mathfrak{U}$ liegt und bilden das System μ_{ij} nebst sämtlichen linearen Verbindungen im Galoisfeld. Wir erhalten wieder v Reste, welche verschieden sind und mit den Resten aus $\mathfrak{U}$ keinen gemeinsamen haben. Dieses neue System sei mit $\mathfrak{V}$ bezeichnet. Nun nehmen wir an, daß alle Reste erschöpft sind, daß also $\mathfrak{N} = \mathfrak{U} + \mathfrak{V}$ ist.

Wir bilden jetzt

$$\mathfrak{N}^\lambda\mathfrak{N} \equiv \mathfrak{N}^\lambda\mathfrak{U} + \mathfrak{N}^\lambda\mathfrak{V} \pmod{\mathfrak{N}^{\lambda+2}}$$

Bedenken wir, daß $\mathfrak{U}$ und $\mathfrak{V}$ in $\mathfrak{N}$ enthalten sind, dagegen $\mathfrak{N}^2$ enthalten, so müssen $\mathfrak{N}^\lambda\mathfrak{U}$ und $\mathfrak{N}^\lambda\mathfrak{V}$ zweiseitige Ideale sein, welche durch p teilbar, dagegen in $p\mathfrak{N}$ enthalten sind. Solcher Ideale gibt es aber nur zwei, nämlich (p) und $p\mathfrak{N}$. Wäre nun $\mathfrak{N}^\lambda\mathfrak{U} \equiv p\mathfrak{N}$ (mod p^2), so ergäbe sich durch Linksmultiplikation mit $\mathfrak{N}$ die Gleichung $\mathfrak{N}^{\lambda+1}\mathfrak{U} \equiv p\mathfrak{N}^2$ (mod p^2). Nun ist aber $\mathfrak{N}^{\lambda+1} \equiv (p)$, also erhalten wir den Widerspruch $p\mathfrak{U} \equiv p\mathfrak{N}^2$ (mod p^2). Daher wird $\mathfrak{N}^\lambda\mathfrak{U} \equiv \mathfrak{N}^\lambda\mathfrak{V} \equiv (p)$ (mod p^2). Multiplizieren wir

links mit $\mathfrak{N}$, so bekommen wir $\mathfrak{N}^{\lambda+1}\mathfrak{U} \equiv \mathfrak{N}^{\lambda+1}\mathfrak{V}$. Nun ist aber $\mathfrak{N}^{\lambda+1}\mathfrak{U} \equiv p\mathfrak{U}$ und $\mathfrak{N}^{\lambda+1}\mathfrak{V} \equiv p\mathfrak{V}$. Wir bekommen daher $p\mathfrak{U} \equiv p\mathfrak{V} \pmod{p^2}$ und daraus den Widerspruch $\mathfrak{U} \equiv \mathfrak{V} \pmod{p}$.

14. Nun kann man fortfahren wie im vorigen Fall. Ich will es für die Teiler von $\mathfrak{N}^2$ kurz ausführen. Die folgenden Gleichungen sind stets als Kongruenzen (mod $\mathfrak{N}^2$) aufzufassen.

Man kann zunächst die e_{ii} als Idempotente (mod $\mathfrak{N}^2$) annehmen durch Potenzierung. Mit diesen bildet man $e_{ii} v e_{jj} = v_{ij}$. Nun wird $e_{ii} e_{jj} = a_{ij} v_{ij}$. Jetzt bildet man die neuen Größen:

$$e_{ii} - a_{i1} v_{i1} - a_{i2} v_{i2} - \cdots - a_{i,i-1} v_{i,i-1} - a_{i,i+1} v_{i,i+1} - \cdots - a_{ik} v_{ik}$$

und findet, daß sie orthogonale Idempotente (mod $\mathfrak{N}^2$) sind. Mit diesen bildet man nun aufs Neue $e_{ii} v e_{jj} = v_{ij}$. Aus diesen Größen kann man v ausklammern, weil $\mathfrak{N}$ Hauptideal ist und man kann sie etwa mit $v b_{ik}$ bezeichnen. Hierauf kann man das ganze Restesystem in eine Matrix von k Zeilen und Kolonnen bringen und wie früher weiterfahren. Man hat nur p durch v zu ersetzen.

Hiermit sind auch diese Ideale als Hauptideale nachgewiesen. Für den Fall, daß das System $\mathfrak{R} - \mathfrak{N}$ halbeinfach aber nicht einfach ist, verweise ich auf die „Erste Reduktion" in Dickson § 147, S. 287. Wir erhalten so den

Satz 5: Ist m eine beliebige ganze rationale Zahl, so ist jeder Idealteiler von m ein Hauptideal im System der Reste (mod m).

Mit den gewonnenen Resultaten läßt sich nun der Kristallbau der Ordnungen und Ideale einer Algebra völlig überblicken; er ist von großer Schönheit. Dies soll den Inhalt des zweiten Abschnittes bilden.

II. Die Struktur aller Ordnungen und Ideale einer Algebra.

15. Nachdem die Gesamtheit der Rechtsideale einer Ordnung aufgestellt ist, können wir die Rechts- und Linksideale sämtlicher Ordnungen in ihrer Beziehung untersuchen. Wir denken uns die Ordnungen numeriert und mit 1_i die $i$te unter ihnen bezeichnet. Ferner bedeute $\mathfrak{u}_{ik}$ ein Ideal, das links zu 1_i, rechts zu 1_k gehört, so daß also $1_i \mathfrak{u}_{ik} 1_k = \mathfrak{u}_{ik}$ ist. Die Rechtsideale von 1_1 gehören zu verschiedenen Linksordnungen und es gilt $\mathfrak{a}_{i1} \mathfrak{a}_{1i}^{-1} = 1_i$. Wenn das Ideal $\mathfrak{b}_{k1}$ im Ideal $\mathfrak{a}_{i1}$ enthalten ist, d.h.

wenn alle Zahlen des ersten Ideales auch Zahlen des zweiten sind, so ist $\mathfrak{b}_{k1}\,\mathfrak{a}_{1i}^{-1} = \mathfrak{c}_{ki}$ ein ganzes Ideal. Denn ist $\mathfrak{a}_{i1} > \mathfrak{b}_{k1}$, so wird

$$\mathfrak{a}_{i1}\,\mathfrak{a}_{1i}^{-1} = 1_i > \mathfrak{b}_{k1}\,\mathfrak{a}_{1i}^{-1} = \mathfrak{c}_{ki}$$

Weiter folgt aus derselben Bedingung $\mathfrak{a}_{1i}^{-1} < \mathfrak{b}_{1k}^{-1}$, also

$$\mathfrak{b}_{k1}\,\mathfrak{a}_{1i}^{-1} = \mathfrak{c}_{ki} < \mathfrak{b}_{k1}\,\mathfrak{b}_{1k}^{-1} = 1_k$$

Gilt ferner $\mathfrak{a}_{i1} > \mathfrak{d}_{h1} > \mathfrak{b}_{k1}$, so ist $\mathfrak{d}_{h1}\,\mathfrak{a}_{1i}^{-1}$ ein ganzes Ideal, das $\mathfrak{c}_{ki}$ umfaßt, und ist umgekehrt $\mathfrak{f}_{hi}$ ein ganzes Rechtsideal von 1_i, das $\mathfrak{c}_{ki}$ umfaßt, so ist $\mathfrak{f}_{hi}\,\mathfrak{a}_{i1}$ ein Ideal zwischen $\mathfrak{a}_{i1}$ und $\mathfrak{b}_{k1}$.

16. Wir ordnen nun (vgl. Brandt [7] bei Deuring) jedem Rechtsideal einer fest vorgegebenen Ordnung einen Punkt eines Punktsystems zu und konstruieren einen Graph in folgender Weise: Wenn das Ideal $\mathfrak{b}$ im Ideal $\mathfrak{a}$ enthalten ist und zwischen $\mathfrak{a}$ und $\mathfrak{b}$ kein weiteres Ideal liegt, so verbinden wir den Punkt $\mathfrak{a}$ mit dem Punkt $\mathfrak{b}$ durch einen Pfeil, der von $\mathfrak{a}$ nach $\mathfrak{b}$ gerichtet ist. Dieses System von Punkten und Pfeilen heißt die Struktur der Rechtsideale in der Ordnung.

Zwei Strukturen heißen identisch, wenn ihre Punkte so aufeinander eineindeutig bezogen werden können, daß auch die Pfeile in gleichgerichtete Pfeile übergeführt werden. Nun gilt der fundamentale

Satz 6: Die Strukturen der Rechtsideale in den verschiedenen Ordnungen sind identisch.

Beweis: Es sei 1_k eine beliebige Ordnung. Wir bilden durch Basismultiplikation $1_k \times 1_1 = \mathfrak{d}_{k1}$. Nun wird $1_k = \mathfrak{d}_{k1}\,\mathfrak{d}_{1k}^{-1}$. Ordnet man dem Ideal $\mathfrak{a}_{hk}$ das Ideal $\mathfrak{a}_{hk}\,\mathfrak{d}_{k1} = \mathfrak{b}_{h1}$ zu, so erhält man eine eineindeutige Zuordnung der Rechtsideale von 1_1 und 1_k. Ist ferner $\mathfrak{c}_{jk}$ in $\mathfrak{a}_{hk}$ enthalten, ohne daß ein Zwischenideal eingeschaltet werden kann, sind also die beiden Punkte durch einen Pfeil verbunden, so wird dasselbe auch von $\mathfrak{a}_{hk}\mathfrak{d}_{k1}$ und $\mathfrak{c}_{jk}\mathfrak{d}_{k1}$ gelten, d. h. Pfeile werden auf Pfeile mit Erhaltung des Richtungssinnes abgebildet. Die verschiedenen Ordnungen unterscheiden sich nur durch die Stellung der Eins, also durch die Perspektive, in der sie die Struktur erblicken. Ist $\mathfrak{d}_{k1}$ ein Ideal, das links zu 1_k gehört, so kann man diesem Punkt die Ordnung 1_k zuordnen, er repräsentiert das Einheitsideal derselben. Man muß nun die Punkte umnennen, indem $\mathfrak{a}_{i1}$ jetzt mit dem Ideal $\mathfrak{a}_{i1}\,\mathfrak{d}_{1k}^{-1}$ bezeichnet wird. Die Pfeile, welche von diesem neuen Einheitspunkt ausgehen, führen nach den Primidealen usw.

17. Die Struktur gestattet Deckoperationen. Denn ist $\mathfrak{q}_{11}$ ein zweiseitiges Ideal, so kann der entsprechende Punkt ebenfalls als Ausgangspunkt für die Ordnung 1_1 angenommen werden, er ist von der Struktur gleich umgeben, wie der Punkt 1_1. Diese Deckoperationen bilden eine abelsche Gruppe, welche mit der multiplikativen Gruppe aller zweiseitigen Ideale einstufig isomorph ist. Bei diesen Deckoperationen geht das Ideal $\mathfrak{a}_{i1}$ über in das Ideal $\mathfrak{a}_{i1}\mathfrak{q}_{11}$ und dies ist das allgemeinste Ideal, welches die Linksordnung 1_i und die Rechtsordnung 1_1 hat, wie man unmittelbar beweist. Die Gesamtheit dieser Punkte liefert daher gerade die Gesamtheit der Ausgangspunkte für die Ordnung 1_i. Das kann man auch direkt beweisen: Nimmt man den Punkt $\mathfrak{a}_{i1}$ als Ausgang für 1_i, so hat man alle Ideale mit $\mathfrak{a}_{1i}^{-1}$ rechts zu multiplizieren, um die neue Zuordnung zu erhalten. Zwei Ideale, welche sich früher nur um ein Ideal $\mathfrak{q}_{11}$ unterschieden, $\mathfrak{b}_{k1}$ und $\mathfrak{b}_{k1}\mathfrak{q}_{11}$, werden jetzt zu $\mathfrak{b}_{k1}\,\mathfrak{a}_{1i}^{-1}$ und $\mathfrak{b}_{k1}\,\mathfrak{q}_{11}\,\mathfrak{a}_{1i}^{-1}$. Nun ist aber $\mathfrak{q}_{11}\,\mathfrak{a}_{1i}^{-1} = \mathfrak{a}_{1i}^{-1}(\mathfrak{a}_{i1}\,\mathfrak{q}_{11}\,\mathfrak{a}_{1i}^{-1})$ und das Ideal in der Klammer ist ein zweiseitiges Ideal $\mathfrak{q}_{ii}$ in 1_i. Es ist also in der Tat $\mathfrak{b}_{k1}\mathfrak{q}_{11}\mathfrak{a}_{1i}^{-1} = \mathfrak{b}_{k1}\,\mathfrak{a}_{1i}^{-1}\,\mathfrak{q}_{ii}$.

Ersetzt man in der Struktur der Rechtsideale jedes Ideal durch die zugehörige Linksordnung, so erhält man eine neue Struktur, die Struktur der Ordnungen. Hier hat man die Gesamtheit der Punkte, welche dieselbe Bezeichnung besitzen, also die Punktgruppe der unter den Deckoperationen in einander übergeführten Punkte, als einen Punkt anzusehen. Diese Struktur weist gegenüber der früheren neue Eigenschaften auf. Früher kam man, wenn man in der Richtung der Pfeile fortlief, stets in neue Punkte, jetzt wird man in den Anfangspunkt zurückkommen, sobald man einen Polygonzug durchlaufen hat, der ein zweiseitiges Ideal liefert.

18. Die Zerlegung eines Ideales in Primideale geschieht folgendermaßen. Wir nehmen zunächst an, daß das Ideal ganz ist. Dann kann es von 1_1 aus durch einen Polygonzug verbunden werden, der stets vorwärts weisende Pfeile enthält. Die Ideale, welche wir bei der Durchlaufung treffen, seien $\mathfrak{a}_{r1}$, $\mathfrak{b}_{s1}$, $\mathfrak{c}_{t1}$. Dann erhält man $\mathfrak{c}_{t1} = (\mathfrak{c}_{t1}\mathfrak{b}_{1s}^{-1})\,(\mathfrak{b}_{s1}\mathfrak{a}_{1r}^{-1})\,(\mathfrak{a}_{r1})$. Die Ideale in den Klammern sind lauter Primideale, freilich in verschiedenen Ordnungen. Dies ist die Zerlegung in Primideale. Da die Struktur zusammenhängend ist, so kann man zwei beliebige Rechtsideale $\mathfrak{a}_{i1}$ und $\mathfrak{b}_{k1}$ durch einen Polygonzug verbinden. Man erhält auf diesem Weg den Quotienten $\mathfrak{a}_{i1}\,\mathfrak{b}_{1k}^{-1}$ in Primfaktoren zerlegt, die den Exponenten $+1$ oder -1 haben, je nachdem der Pfeil dieselbe Richtung hat, wie der Weg, oder die entgegengesetzte.

19. Um die Struktur der Linksideale aller Ordnungen zu erhalten, verfährt man einfach so: man ersetzt in der Struktur der Rechtsideale jedes Ideal durch das inverse. Dann erhält man zunächst die Hierarchie der Linksideale in 1_1, aber offenbar ist die Pfeilrichtung umgekehrt. Hieraus ergibt sich der

Satz 7: Die Struktur der Linksideale entsteht aus derjenigen der Rechtsideale durch Umkehrung der Pfeilrichtung; die beiden Strukturen sind zueinander reziprok.

20. Neben den Deckoperationen, welche durch die zweiseitigen Ideale geliefert werden, gibt es eine andersgeartete Gruppe, welche auf dem Begriff des Hauptideales beruht. Ordnen wir dem Ideal $\mathfrak{a}_{i1}$ das Ideal $\mu\mathfrak{a}_{i1}$ zu, wo μ irgend eine Größe der Algebra bedeutet, die eine inverse besitzt, so erhalten wir wieder eine Gruppe von Deckoperationen, welche der multiplikativen Gruppe jener Zahlen i. a. mehrstufig isomorph ist. Wenn nämlich μ eine Einheit des Zentrums ist, so ist die Operation die Identität. Ideale, welche bei jenen Operationen ineinander übergehen, heißen linksäquivalent. Faßt man sie wieder als einen Punkt auf, so erhält man die Struktur der Linksklassen. Sie enthält nur endlich viele Punkte, wie Artin bewiesen hat.

Kombiniert man die beiden Strukturen, so erhält man eine noch kleinere Struktur, die gebildet wird von den äquivalenten Ordnungen, wenn man zwei Ordnungen als äquivalent ansieht, die durch Transformation mit einer Zahl auseinander hervorgehen. Man erhält sie aus der Gesamtstruktur, indem man zwei Ideale als äquivalent ansieht, die sich nur um einen numerischen Linksfaktor und ein zweiseitiges Ideal als Rechtsfaktor unterscheiden. Alle diese Definitionen sind strukturinvariant. Denn nehmen wir zwei äquivalente Ideale $\mathfrak{a}_{i1}$ und $\mu\mathfrak{a}_{i1}\,\mathfrak{q}_{11}$ und betrachten wir sie vom Punkt $\mathfrak{b}_{k1}$ aus, so liefern sie die beiden Ideale $\mathfrak{a}_{i1}\mathfrak{b}_{1k}^{-1}$ und $\mu\,\mathfrak{a}_{i1}\mathfrak{q}_{11}\mathfrak{b}_{1k}^{-1}$. Diese sind aber auch äquivalent als Rechtsideale in 1_k, denn es ist das zweite jener Ideale $= \mu\,\mathfrak{a}_{i1}\mathfrak{b}_{1k}^{-1}\mathfrak{q}_{kk}$, wo $\mathfrak{q}_{kk} = \mathfrak{b}_{k1}\mathfrak{q}_{11}\mathfrak{b}_{1k}^{-1}$ ist.

21. Ist μ eine ganze Zahl der Ordnung 1_1 und $\mathfrak{a}_{i1}$ ein ganzes Rechtsideal derselben Ordnung, so ist $\mu\,\mathfrak{a}_{i1}$ zwar stets ein ganzes Ideal in 1_1, aber es ist im allgemeinen nicht in $\mathfrak{a}_{i1}$ enthalten. Dies trifft nämlich nur dann ein, wenn μ auch eine ganze Zahl der Linksordnung 1_i ist. Die Struktur wird zwar auf sich selber strukturtreu abgebildet, wenn man die Ideale links mit μ multipliziert, denn aus $\mathfrak{a}_{i1} > \mathfrak{b}_{k1}$ folgt $\mu\,\mathfrak{a}_{i1} > \mu\,\mathfrak{b}_{k1}$, aber bei dieser Abbildung darf man nicht an eine Translation im euklidischen

Sinne denken. Denn das Gesetz vom Parallelogramm gilt nicht. Man kann wohl sagen: $\mu\mathfrak{a}$ liegt zu $\mu\mathfrak{b}$, wie $\mathfrak{a}$ zu $\mathfrak{b}$, denn verbindet man $\mathfrak{a}$ und $\mathfrak{b}$ durch irgendein Polygon der Struktur, so erhält man daraus durch Multiplikation mit μ ein isomorphes Polygon zwischen $\mu\mathfrak{a}$ und $\mu\mathfrak{b}$. Aber man kann nicht daraus schließen, daß auch $\mathfrak{a}$ zu $\mu\mathfrak{a}$ liegt, wie $\mathfrak{b}$ zu $\mu\mathfrak{b}$. Die Polygone, welche $\mathfrak{a}$ und $\mu\mathfrak{a}$ verbinden, sind im allgemeinen anders geartet, als die Polygone zwischen $\mathfrak{b}$ und $\mu\mathfrak{b}$.

22. Beschränken wir uns auf die Hauptideale, oder legen wir von vorneherein eine Algebra zugrunde, deren Ideale Hauptideale sind, so erhalten wir die Struktur der Hauptideale. Ihre Punkte liefern im ersten Falle nicht sämtliche Ordnungen, sondern nur diejenigen, welche aus 1_1 durch Transformation mit Zahlen hervorgehen. Gehen wir von 1_1 aus zu einem ganzen Ideal, indem wir stets in der Pfeilrichtung vorgehen, so liefern uns die Zwischenpunkte eine Zerlegung in ganze Primideale. Sie ist aber nicht mit der Zerlegung in ganze Zahlen identisch, da die Faktoren im Innern ganze Zahlen in andern Ordnungen sind, also in 1_1 nicht mehr ganz zu sein brauchen. Um die Zerlegung innerhalb der ganzen Zahlen zu erhalten, muß man die Struktur anders aufstellen. Wir sagen: das Ideal $\mu\mathfrak{a}$ ist Nachfolger des Ideales $\mathfrak{a}$, falls μ eine ganze Zahl von 1_1 ist. Wie schon oben bemerkt, ist ein Nachfolger im allgemeinen nicht im Vorgänger enthalten. Für die Normen gilt freilich der Satz, daß $Nm\,(\mu\mathfrak{a}) = Nm\,(\mu)\,Nm\,(\mathfrak{a})$, gleichgültig was für ein Ideal $\mathfrak{a}$ ist. Der tiefere Grund für diese Möglichkeit einer zweiten Struktur bei Hauptidealen liegt darin, daß $\mu\ 1_k$ stets ein Ideal von derselben Norm ist, wenn es auch in gewissen Ordnungen ganz, in andern gebrochen ist und je nach der Wahl der Ordnung 1_k verschieden ausfällt.

(Eingegangen den 9. März 1936.)