Werk

Titel: Mathematische Annalen
Ort: Berlin
Jahr: 1933
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235181684_0107
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0107

LOG Id: LOG_0045
LOG Titel: Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. Insbesondere Begründung der Theorie des Normenrestsymbols und Herleitung des Reziprozitätsgesetzes mit nichtkommutative
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN235181684
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235181684

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper.

Insbesondere Begründung der Theorie des Normenrestsymbols und Herleitung des Reziprozitätsgesetzes mit nichtkommutativen Hilfsmitteln.

Emmy Noether zum 50. Geburtstag am 23. März 1932.

Von

Helmut Hasse in Marburg.

Einleitung.

Emmy Noether [4] hat wohl zuerst den Gedanken ausgesprochen, die Theorie der nichtkommutativen Algebren sei von einfacheren Gesetzmäßigkeiten beherrscht als die Theorie der kommutativen Algebren, insbesondere der kommutativen algebraischen Erweiterungskörper, und folgerichtig sei die nichtkommutative Theorie in einem systematischen Aufbau nicht nur rein äußerlich der kommutativen Theorie voranzustellen, sondern auch zu deren Begründung sachlich weitgehend heranzuziehen. Sie hat selbst die Durchführbarkeit dieses Gedankens für verschiedene Einzelabschnitte der Gesamttheorie dargetan, und zwar nicht nur für rein-algebraische Teile (Galoissche Theorie), sondern neuerdings auch für tiefliegende arithmetische Gedankenreihen (Hauptgeschlechtssatz).

Daß die Arithmetik der nichtkommutativen Algebren sich in der Tat vor der Arithmetik der kommutativen Zahlkörper durch besondere Einfachheit auszeichnet, geht aus den an die grundlegende Arbeit von Speiser [1] anknüpfenden Arbeiten von Artin [1], Brandt [1—5] und mir [5] hervor. Es sei etwa nur der Umstand angeführt, daß im Nichtkommutativen bei der Primidealzerlegung stets Restklassengrad gleich Verzweigungsordnung ist, und daß die aus dem Kommutativen bekannten besonderen Schwierigkeiten, die in dem Auftreten höherer Verzweigungen bestehen, im Nichtkommutativen gar nicht auftreten.

Ich will im folgenden aus dieser einfachen Arithmetik der nichtkommutativen Algebren einen neuen Beweis des Reziprozitätsgesetzes entwickeln. Damit erfülle ich einen mir schon vor einiger Zeit von Emmy Noether ausgesprochenen Wunsch; und so hat die dieser Arbeit vorangestellte Widmung ihre innere Berechtigung.

Sie hat sie um so mehr, als auch die Idee, die mich zu diesem Beweis geführt hat, auf eine Anregung von Emmy Noether zurückgeht: In einer kürzlich erschienenen Arbeit [8] hatte ich gezeigt, daß aus den Normenrestsymbolen $\left(\frac{\alpha, Z}{\mathfrak{p}}\right)$ ein volles Invariantensystem für die zyklische Algebra (α, Z, S) entspringt. Der Nachweis der Invarianz dort in Abschnitt III war deshalb nicht ganz einfach, weil man für das Normenrestsymbol $\left(\frac{\alpha, Z}{\mathfrak{p}}\right)$ keine direkte Definition besaß, die sich allein auf das Verhalten von α „im Kleinen", d. h. an der Primstelle $\mathfrak{p}$ des Grundkörpers k stützt. Man war vielmehr zur Definition des Normenrestsymbols auf einen Umweg über andere Primstellen $\mathfrak{q}$ von k angewiesen, und somit im Prinzip auf das Reziprozitätsgesetz, das sich ja als Bindung „im Großen":

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, Z}{\mathfrak{p}}\right) = 1$$

zwischen dem Verhalten an den einzelnen Primstellen darstellt. Emmy Noether bemerkte nun mit Recht, daß ja gerade der von mir bewiesene Invarianzsatz eine direkte, ganz im Kleinen verlaufende Definition des Normenrestsymbols liefert; sie hat damit den Schlußsatz meiner Arbeit [8] in einer nicht vorhergesehenen Weise widerlegt.

Verfolgt man diesen ihren Gedanken durch eine entsprechende Fassung der Definition des Normenrestsymbols, so hört natürlich der Invarianzsatz auf, eine tiefliegende Tatsache zu sein — er wird ja definitorisch erzwungen —; dafür wird aber jetzt das Reziprozitätsgesetz in obiger Produktform, das bei der bisherigen Definition definitorisch erzwungen wurde, eine tiefliegende Tatsache. Überdies wird die Normenresteigenschaft des Normenrestsymbols, die bei der bisherigen Definition eine tiefliegende Tatsache darstellte, durch die neue Definition fast unmittelbar in Evidenz gesetzt. Durch diese Verschiebung zwischen Definition und Sätzen wird somit das Gesicht der Theorie des Normenrestsymbols, d. i. die Klassenkörpertheorie im Kleinen (Hasse [3, 4], F. K. Schmidt [1], Chevalley [1, 2, 4, 5]), von den ihm bisher anhaftenden entstellenden Zügen befreit. Der erste Ansatz in dieser Richtung geht übrigens auf Deuring [1] zurück, der mit den nichtkommutativen Methoden den Vertauschungssatz für das Normenrestsymbol bewies.

Im folgenden will ich all' dies im einzelnen auseinandersetzen.

Im Hinblick auf die gegenwärtig im Fluß befindliche, weitergehende Idee Emmy Noethers, auch die Klassenkörpertheorie im Großen vom Nichtkommutativen her aufzubauen, will ich noch voranschicken, welche Tatsachen aus der Klassenkörpertheorie für das Folgende allein gebraucht werden.

Aus der Klassenkörpertheorie im Kleinen wird gebraucht:

(0. 1) (Sätze der Klassenkörpertheorie im Kleinen für Klasseneinteilungen nach dem Kongruenzwert der Ordnungszahl in $\mathfrak{p}$). *Zu der*

von der Ordnung $m_\mathfrak{p}$ zyklischen Klasseneinteilung in $k_\mathfrak{p}$ nach dem Kongruenzwert mod $m_\mathfrak{p}$ *der Ordnungszahl in* $\mathfrak{p}$ *existiert ein Klassenkörper $W^\mathfrak{p}$, derart also, daß die Zahlnormen aus $W^\mathfrak{p}$ in $k_\mathfrak{p}$ genau die Zahlen mit durch $m_\mathfrak{p}$ teilbarer Ordnungszahl sind, nämlich der Körper der $\mathfrak{N}(\mathfrak{p})^{m_\mathfrak{p}} - 1$-ten Einheitswurzeln über $k_\mathfrak{p}$. Er ist zyklisch vom Grade $m_\mathfrak{p}$ und unverzweigt über $k_\mathfrak{p}$.*

Umgekehrt ist ein über $k_\mathfrak{p}$ unverzweigter Körper vom Grade $m_\mathfrak{p}$ notwendig dieser Körper $W^\mathfrak{p}$.

Hierbei wurde $\mathfrak{p}$ als endlich vorausgesetzt. Den ganz einfachen Beweis siehe in Hasse [5].

Für unendliches $\mathfrak{p}$ ist das Analogon trivial: Ist $\mathfrak{p}$ reell (für komplexes $\mathfrak{p}$ ist nichts zu beweisen), so ist $k_\mathfrak{p}$ der Körper aller reellen Zahlen, und zu der einzigen Klasseneinteilung in $k_\mathfrak{p}$, der nach dem Vorzeichen, also zyklisch von der Ordnung 2, gehört als Klassenkörper der einzige algebraische Erweiterungskörper $W^\mathfrak{p}$ über $k_\mathfrak{p}$, der Körper aller komplexen Zahlen; dieser ist zyklisch vom Grade 2 über $k_\mathfrak{p}$. —

Aus der Klassenkörpertheorie im Großen wird gebraucht:

(0. 2) (Normensatz). *Ist Z ein zyklischer Körper über dem algebraischen Zahlkörper k, so ist eine Zahl α aus k dann und nur dann Norm einer Zahl aus Z, wenn α für jede Primstelle $\mathfrak{p}$ von k Norm einer Zahl aus dem zugehörigen $\mathfrak{p}$-adischen Erweiterungskörper $Z^\mathfrak{p}$ in bezug auf die $\mathfrak{p}$-adische Erweiterung $k_\mathfrak{p}$ ist.*

Dieser Satz braucht sogar nur für Z von Primzahlgrad bekannt zu sein; daraus folgt er mit nichtkommutativen Hilfsmitteln in einfacher Weise für beliebigen Grad. Doch geben ja, im Gegensatz zur bisherigen Klassenkörpertheorie (Hasse [6]), die neuen Vereinfachungen von Chevalley und Herbrand (siehe in Chevalley [4]) den Satz ohne jede Schwierigkeit von Anfang an für beliebigen Grad.

Des weiteren wird ein Existenztheorem gebraucht, das aber viel schwächer ist als der allgemeine Existenzsatz der Klassenkörpertheorie und der allgemeine Satz von der arithmetischen Progression:

(0. 3) (Existenztheorem). *Sind $p_1, \ldots, p_r$ verschiedene Primzahlen und $k_1, \ldots, k_r$ natürliche Zahlen, so gibt es stets eine zyklische Kongruenzklasseneinteilung der rationalen Zahlen, bei der die Exponenten von $p_1, \ldots, p_r$ jeweils Multipla von $k_1, \ldots, k_r$ sind und -1 den Exponenten 2 hat.*

Indem man die Kongruenzklasseneinteilung durch einen Primzahlmodul zu realisieren sucht, kann man diesen Satz unmittelbar dem Frobeniusschen Dichtigkeitssatz (oder auch nur Existenzsatz) für einen geeigneten absolutmetabelschen Körper vom Typus $R(\zeta, \sqrt[k]{-1}, \sqrt[k]{p_1}, \ldots, \sqrt[k]{p_r})$ (ζ k-te Einheitswurzel) unterordnen*). Ich möchte jedoch glauben, daß man den Beweis auch

*) Zusatz bei der Korrektur. Es genügt für alle Fälle, k als kleinstes gemeinsames Vielfaches der Zahlen $2k_i$, p_i und 8 zu wählen.

durchaus elementar erbringen kann, indem man die Klasseneinteilung durch einen zusammengesetzten Modul zu realisieren sucht.

Übrigens ist dieser Existenzsatz auch noch etwas einfacher als das ursprünglich von Artin [2] zum Beweis seines Reziprozitätsgesetzes herangezogene ähnliche Lemma, weil hier keine Bedingung der Gleichheit zweier Klassen auftritt; doch kann Artin neuerdings auch seinen Beweis auf den obigen einfacheren Existenzsatz, ja sogar auf dessen Spezialfall $r = 1$ (und ohne -1) stützen. —

Schließlich wird gebraucht:

(0. 4) (Existenzsatz der Klassenkörpertheorie und Artinsches Reziprozitätsgesetz für (zyklische) Klasseneinteilungen nach dem Kongruenzwert der absoluten Idealnormen.) *Zu jeder (zyklischen) Klasseneinteilung nach dem Kongruenzwert der absoluten Idealnormen in einem algebraischen Zahlkörper k existiert ein (zyklischer) Kreiskörper W als Klassenkörper, derart also, daß die Kongruenzwerte der Idealnormen aus W in k genau die Hauptklasse ausmachen.*

Die zugehörigen Frobenius-Artin-Automorphismen $F_\mathfrak{p} = \left(\frac{W}{\mathfrak{p}}\right)$ liefern eine isomorphe Abbildung jener Kongruenzklassengruppe auf die galoissche Gruppe von W.

Diese Tatsachen sind bekanntlich unmittelbare Folgerungen aus dem bekannten Beweis des Zerlegungsgesetzes im Kreiskörper. —

Wie gesagt, werde ich für das eigentliche Ziel dieser Arbeit, die Begründung der Theorie des Normenrestsymbols und Herleitung des Reziprozitätsgesetzes mit nichtkommutativen Hilfsmitteln, nur von den hier zusammengestellten speziellen Tatsachen aus der Klassenkörpertheorie Gebrauch machen. Das soll jedoch nicht ausschließen, daß ich an einigen Stellen zur Abrundung der gewonnenen Strukturresultate auch weitere Tatsachen aus der Klassenkörpertheorie heranziehe. Ich werde das dann jedesmal ausdrücklich hervorheben. —

Nach Fertigstellung dieser Arbeit ist eine Note von Chevalley [3] erschienen, in der auf anderem Wege, ohne Heranziehung nichtkommutativer Hilfsmittel, ähnliche Strukturzusammenhänge zwischen den Sätzen der Klassenkörpertheorie wie hier entwickelt werden. Ferner hat, wie ich während der Drucklegung erfahre, Chevalley [5] auch seinerseits, angeregt durch Einsichtnahme in die Ausarbeitung einer Vorlesung von E. Noether [4], die Klassenkörpertheorie im Kleinen unter Verwendung derselben Gedanken und Methoden wie hier vollständig entwickelt. Da jedoch bei mir hier das Hauptgewicht auf dem Übergang zur Klassenkörpertheorie im Großen liegt, so überschneiden sich unsere Arbeiten nur geringfügig.

I. Abschnitt.

Algebraische Theorie.

Es handelt sich um eine Theorie, die im Anschluß an die grundlegende Wedderburnsche Theorie (Wedderburn [1], Dickson [1, 3]) einerseits von R. Brauer [1–5, 7, 8], Emmy Noether [1, 2, 4, 5] und v. d. Waerden [1], andererseits in den Grundzügen auch von Wedderburn [2], Dickson [1—5] und Albert [1—10] entwickelt wurde. Siehe außerdem die Darstellung in Abschnitt II meiner Arbeit [8].

Der Kürze und Übersichtlichkeit halber bringe ich hier die Tatsachen in etwas anderer Reihenfolge, als sie sich bei systematischem Aufbau naturgemäß ergeben würden. Beweise führe ich nicht aus, mit Ausnahme der Tatsache (2. 5), für die ich einen modifizierten Beweis bringe.

1. Einfache normale Algebren.

Es sei k ein beliebiger Körper. Wir betrachten *einfache* Algebren A über k als Koeffizientenkörper.

(1. 1) Der Wedderburnsche Struktursatz. Zu den einfachen Algebren gehören speziell die *Divisionsalgebren* D und die vollständigen Matrixalgebren D_r über ihnen (charakterisiert allein durch ihre Reihenzahl r). Hiermit ist bereits der allgemeinste Typus gegeben. Jede einfache Algebra A ist also vom Typus D_r. Hierbei ist D durch A abstrakt eindeutig bestimmt (und sogar innerhalb A eindeutig bis auf Transformation).

Das Zentrum Z von A ist gleich dem Zentrum von D, und ist ein algebraischer Erweiterungskörper von k. Will man nur das typisch Nichtkommutative untersuchen, so hat man den Schritt von k nach Z von der Betrachtung auszuschließen und nur A über Z als erweitertem Koeffizientenkörper zu betrachten. Demgemäß setzt man zweckmäßig gleich voraus, der Koeffizientenkörper k sei das Zentrum von A. Dann heißt A *normal*.

Der Rang von A ist dann eine Quadratzahl n^2. Dabei heißt n der *Grad* von A; er ist der Grad des allgemeinen Elementes von A.

(1. 2) Die R. Brauersche Algebrenklassengruppe. Zwei einfache normale Algebren A und $\overline{A}$ heißen *ähnlich*, $A \sim \overline{A}$, wenn ihnen dieselbe Divisionsalgebra D im Sinne von (1. 1) zugeordnet ist.

Diese Ähnlichkeitsbeziehung führt zu einer *Klasseneinteilung* im Bereich aller einfachen normalen Algebren über dem festen Koeffizientenkörper k; jede solche Klasse $\mathfrak{A}$ ist durch die in ihr enthaltene Divisionsalgebra D eindeutig charakteristiert und besteht aus der Gesamtheit aller vollen Matrixalgebren $A = D_r$ $(r = 1, 2, \ldots)$ über D.

Der Grad m von D heißt der *Index* von $\mathfrak{A}$. Er ist Teiler der Grade $n = mr$ aller Elemente $A = D_r$ aus $\mathfrak{A}$.

Das *direkte Produkt* $A \times B$ zweier einfacher normaler Algebren A und B ist wieder eine einfache normale Algebra.

Aus $A \sim \overline{A}$, $B \sim \overline{B}$ folgt $A \times B \sim \overline{A} \times \overline{B}$. Hiernach führt die direkte Multiplikation zu einer elementweisen *Klassenmultiplikation*.

In bezug auf diese Multiplikation bilden die Klassen $\mathfrak{A}$ eine abelsche *Gruppe* $\mathfrak{G}$, die also allein durch den Koeffizientenkörper k bestimmt ist. *Einselement* 1 ist die Klasse, die zu k selbst als Divisionsalgebra gehört und also aus allen vollen Matrixalgebren k_r $(r = 1, 2, \ldots)$ über k besteht. *Reziprok* zu $\mathfrak{A}$ ist die Klasse $\mathfrak{A}'$, deren Algebren A' zu den Algebren A aus $\mathfrak{A}$ reziprok-isomorph sind.

Jede Klasse $\mathfrak{A}$ hat als Element der Gruppe $\mathfrak{G}$ endlichen *Exponenten* l. Dieser Exponent l ist Teiler des Index m von $\mathfrak{A}$. Andererseits ist das Produkt m_0 der einfachen Primfaktoren von m Teiler von l. Also $m_0 | l | m$.

(1. 3) Erweiterung des Koeffizientenkörpers. Ist K ein beliebiger Erweiterungskörper von k, so entsteht durch Erweiterung des Koeffizientenkörpers k auf K als neuen Koeffizientenkörper die *Erweiterung* A_K von A. Sie ist einfach und normal über K.

Aus $A \sim \overline{A}$ folgt $A_K \sim \overline{A}_K$, und es ist $(A \times B)_K = A_K \times B_K$. Daher bewirkt die Erweiterung auf K eine elementweise *Erweiterung der Klasse* $\mathfrak{A}$ auf eine Klasse $\mathfrak{A}_K$, und eine *Reduktion der Gruppe* $\mathfrak{G}$ auf eine Faktorgruppe $\mathfrak{G}_K = \mathfrak{G}/\mathfrak{U}_K$. Dabei ist $\mathfrak{U}_K$ die Untergruppe derjenigen Klassen $\mathfrak{A}$ aus $\mathfrak{G}$, die bei der Erweiterung auf K in die Einsklasse übergehen: $\mathfrak{A}_K = 1$ (d. h. $A_K = K_n$). $\mathfrak{G}_K$ ist eine gewisse Untergruppe der Brauerschen Algebrenklassengruppe über K.

Die Reduktion von $\mathfrak{G}$ auf $\mathfrak{G}_K$ hat eine *Reduktion des Index* m von $\mathfrak{A}$ auf einen Teiler m_K als Index von $\mathfrak{A}_K$ *und des Exponenten* l von $\mathfrak{A}$ auf einen Teiler l_K als Exponent von $\mathfrak{A}_K$ zur Folge.

(1. 4) Zerfällungskörper. Kehrt man die der Definition von $\mathfrak{U}_K$ zugrunde liegende Fragestellung um, indem man jetzt bei gegebenem $\mathfrak{A}$ nach denjenigen Erweiterungskörpern K fragt, für die $\mathfrak{A}_K = 1$ wird, so hat man den Begriff des *Zerfällungskörpers* K von $\mathfrak{A}$. Zur Anpassung an diesen Ausdruck sage ich für die Relationen $A \sim k$, $\mathfrak{A} = 1$ gelegentlich auch A bzw. $\mathfrak{A}$ *zerfällt*.

Die Zerfällungskörper K von $\mathfrak{A}$ von endlichem Grade über k haben als Grade stets Multipla $n = mr$ des Index m von $\mathfrak{A}$ und sind identisch mit den Teilkörpern vom Maximalgrad $n = mr$ der Algebren $A = D_r$ aus $\mathfrak{A}$.

Ob es solche Zerfällungskörper für jedes vorgeschriebene Vielfache $n = mr$ wirklich gibt, hängt von der Natur des Koeffizientenkörpers k ab (es ist z. B. sicher der Fall für algebraische Zahlkörper k). Jedenfalls gibt es stets Zerfällungskörper vom Minimalgrad m, d. h. Teilkörper von D selbst vom Maximalgrad m, nämlich die maximalen Teilkörper von D.

Die obige Untergruppe $\mathfrak{U}_K$ kann jetzt auch charakterisiert werden als die Untergruppe der von K zerfällten Klassen $\mathfrak{A}$ aus $\mathfrak{G}$.

2. Zyklische Algebren.

Ohne auf die allgemeine Emmy Noethersche Theorie der verschränkten Produkte einzugehen, die ich in Abschnitt II meiner Arbeit [8] ausführlich dargelegt habe, will ich hier nur die auf den zyklischen Spezialfall bezüglichen Tatsachen zusammenstellen, die übrigens auch einer einfachen, von der allgemeinen Theorie unabhängigen Begründung fähig sind.

(2. 1) Zyklische Erzeugung einer Algebra. Eine einfache normale Algebra A über k vom Grade n heißt *zyklisch*, wenn sie einen über k zyklischen Teilkörper Z vom Maximalgrade n besitzt. A hat dann die folgende Struktur:

$$A = Z + uZ + \ldots + u^{n-1}Z$$

mit

$zu = uz^S$ für jedes z aus Z, wo S ein erzeugender Automorphismus der zyklischen galoisschen Gruppe von Z ist,

$u^n = \alpha$, wo $\alpha \neq 0$ aus k.

Ich bezeichne das kurz durch $A = (\alpha, Z, S)$,

und nenne es eine *zyklische Erzeugung* von A.

Umgekehrt wird so für beliebige α, Z, S mit den angegebenen Eigenschaften eine einfache normale Algebra A mit Z als Teilkörper vom Maximalgrad erzeugt.

(2. 2) Zyklische Darstellung einer Algebrenklasse. Hat eine Algebrenklasse $\mathfrak{A}$ vom Index m einen zyklischen Zerfällungskörper Z vom Grade $n = mr$, so gibt es in ihr eine zyklische Algebra $A = (\alpha, Z, S)$, nämlich $A = D_r$. $\mathfrak{A}$ heißt dann *zyklisch darstellbar* und $A = (\alpha, Z, S)$ eine *zyklische Darstellung* von $\mathfrak{A}$.

Es gilt:

$(\alpha, Z, S) \sim$ und daher $= (\bar{\alpha}, Z, S)$ dann und nur dann, wenn $\alpha = \bar{\alpha} N(c)$ mit c aus Z,

ferner $(1, Z, S) \sim k$,

also speziell

$(\alpha_1, Z, S) \sim k$ dann und nur dann, wenn $\alpha_1 = N(c)$ mit c aus Z;

ferner $(\alpha, Z, S)\,(\beta, Z, S) \sim (\alpha\beta, Z, S)$.

Hiernach besteht eine isomorphe Abbildung der zum Körper Z gehörigen Untergruppe $\mathfrak{U}_Z$ (der von Z zerfällten Klassen $\mathfrak{A}$) auf die *Normklassengruppe* von Z in k, d. h. die Faktorgruppe in der Gruppe aller $\alpha \neq 0$ aus k nach der Untergruppe aller Zahlnormen $\alpha_1 = N(c)$ mit c aus Z.

Insbesondere ist dann der Exponent l von $\mathfrak{A}$ die früheste Potenz des zugeordneten α, die Norm einer Zahl aus Z ist.

(2. 3) Übergang zu einer anderen Erzeugenden. Geht man von S zu einer anderen Erzeugenden S^ν $[(\nu, n) = 1]$ der galoisschen Gruppe von Z über, so transformiert sich die zyklische Erzeugung so:

$$(\alpha, Z, S) = (\alpha^\nu, Z, S^\nu).$$

Hiernach hat man allgemein:

$(\alpha, Z, S) \sim$ und daher $= (\bar{\alpha}, Z, \bar{S})$ dann und nur dann,

$$\text{wenn gleichzeitig } \begin{cases} \bar{S} = S^{\nu} \text{ mit } (\nu, n) = 1, \\ \bar{\alpha} = \alpha^{\nu} N(c) \text{ mit } c \text{ aus } Z. \end{cases}$$

(2. 4) Übergang zu einer Erweiterungsklasse. Jede Erweiterungsklasse $\mathfrak{A}_K$ einer zyklisch darstellbaren Klasse $\mathfrak{A}$ ist wieder zyklisch darstellbar, nämlich

$$(\alpha, Z, S)_K \sim (\alpha, Z^K, S_K).$$

Hier bezeichnet Z^K das gewöhnliche Kompositum von Z und K (einen der untereinander isomorphen Kernkörper der Erweiterung Z_K von Z auf K) und S_K die früheste Potenz von S, die in der galoisschen Gruppe von Z^K über K liegt (Reduktion der galoisschen Gruppe von Z durch Erweiterung auf K).

(2. 5) Übergang zu einem Teilkörper oder zyklischen Erweiterungskörper. Ist Z_0 ein Teilkörper von Z, und Z vom Grade s über Z_0, so gilt:

$$(\alpha^s, Z, S) \sim (\alpha, Z_0, S_0),$$

wo S_0 rechts den durch S im Teilkörper Z_0 bewirkten Automorphismus bezeichnet.

Umgekehrt also: Läßt Z eine über k zyklische Erweiterung Z_1 vom Grade s über Z zu, so ist die s-reihige volle Matrixalgebra über (α, Z, S) wieder zyklisch, nämlich

$$(\alpha, Z, S)_s = (\alpha^s, Z_1, S_1),$$

wo S_1 rechts einen durch Fortsetzung von S auf Z_1 entstehenden Automorphismus bezeichnet.

Dieser Satz wurde kürzlich von Albert [10] bewiesen. Ich gebe anschließend einen auf ähnlicher Grundlage beruhenden Beweis.

Sei $\mathfrak{b}$ eine Z_0-Basis von Z, als Zeilenvektor gedacht, und

$$z\mathfrak{b} = \mathfrak{b} M_z$$

die zugehörige Matrizendarstellung von Z in Z_0. Sei ferner P diejenige Matrix aus Z_0, die die Anwendung von S auf $\mathfrak{b}$ rückgängig macht:

$$\mathfrak{b}^S P = \mathfrak{b}, \quad \mathfrak{b}^S = \mathfrak{b} P^{-1}.$$

Hiermit werde die Matrix

$$M_u = u_0 P$$

aus (α, Z_0, S_0) gebildet, wo u_0 das S_0 in dieser zyklischen Erzeugung zugeordnete Element ist:

$$z_0 u_0 = u_0 z_0^{S_0} \text{ für jedes } z_0 \text{ aus } Z_0,$$

$$u_0^{n_0} = \alpha, \quad \text{wo} \quad n_0 = \frac{n}{s} \text{ der Grad von } Z_0.$$

Aus

$$\mathfrak{b}\, M_z S = z^S \mathfrak{b} = z^S \mathfrak{b}^S P = \mathfrak{b}^S M_{z_0} P = \mathfrak{b}\, P^{-1} u_0^{-1} M_z^{\cdot} u_0 P = \mathfrak{b}\, M_u^{-1} M_z M_u$$

folgt dann

$$M_z M_u = M_u M_z S.$$

Ferner folgt

$$M_u^{n_0} = (u_0 P)^{n_0} = \alpha P^{S_0^{n_0-1}+\ldots+S_0+1},$$

wegen $P^{S_0^{n_0}} = P$ weiter

$$M_u^n = \alpha^s P^{S_0^{n-1}+\ldots+S_0+1},$$

und, weil aus $\mathfrak{b}^{S^n} = \mathfrak{b}$ folgt $P^{S_0^{n-1}+\ldots+S_0+1} = 1$, somit

$$M_u^n = \alpha^s.$$

Hiernach erzeugen die M_z mit M_u zusammen eine zur zyklischen Algebra (α^s, Z, S) homomorphe, also wegen der Einfachheit der letzteren sicher isomorphe Algebra und lassen somit (α^s, Z, S) als Teilalgebra der s-reihigen Matrixalgebra $(\alpha, Z_0, S_0)_s$ erkennen. Wegen der Gleichheit der Grade ergibt sich die Behauptung. —

Wie die ganze Theorie der zyklischen Algebren, so ist auch der Satz (2. 5) Spezialfall einer allgemeineren Tatsache über verschränkte Produkte. In der Ausdrucksweise der Gruppen linearer Substitutionen wurde diese allgemeine Tatsache bereits von R. Brauer in § 3 seiner Arbeit [2] hergeleitet. Sie lautet:

Ist Z galoissch mit der Gruppe $\mathfrak{G}$, Z_0 ein galoisscher Teilkörper von Z, $\mathfrak{G}_0$ der zugehörige Normalteiler von $\mathfrak{G}$, und hängt ein Faktorensystem $a_{S,T}$ zu Z nur von den Klassen S_0, T_0 der S, T nach $\mathfrak{G}_0$ ab: $a_{S,T} = a_{S_0,T_0}$, so gilt:

$$(a_{S,T}, Z) \sim (a_{S_0,T_0}, Z_0).$$

Der obige Beweis für (2. 5) kann dann durch ohne weiteres ersichtliche geringfügige Modifikationen zu einem Beweis dieser allgemeineren Tatsache ausgestaltet werden. Auch läßt sich diese wieder, entsprechend zu der obigen zweiten Formulierung von (2. 5), umkehren.

II. Abschnitt.

Arithmetische Theorie.

Es handelt sich um Anwendung arithmetischer Methoden zur Untersuchung der algebraischen Struktur der einfachen normalen Algebren über einem algebraischen Zahlkörper k.

Der Grundgedanke dieser Untersuchung ist folgender: Man erweitere zunächst die zu untersuchenden Algebren über k auf die zu den Primstellen p von k gehörigen p-adischen Erweiterungskörper k_p, untersuche dann die viel einfachere Struktur der entstehenden p-adischen Erweiterungen, und setze

schließlich die gewonnenen Resultate über die Struktur im Kleinen zu Resultaten über die Struktur im Großen zusammen.

Als fundamentales Hilfsmittel für den Hauptpunkt bei dieser Untersuchung, den Übergang vom Kleinen zum Großen, dient dabei der Normensatz (0. 2).

Es ist derselbe Grundgedanke, den zuerst Minkowski in seiner Theorie der quadratischen Formen konzipiert hat, der weiter der Henselschen Theorie der algebraischen Zahlen und der Henselschen arithmetischen Theorie der algebraischen Funktionen zugrunde liegt, der im Anschluß an Minkowski und Hensel in meinen Arbeiten über quadratische Formen [1, 2] systematisch durchgeführt ist, der weiterhin im Anschluß an Speiser [1] von mir [5] schon für die Begründung der arithmetischen Idealtheorie in Algebren erfolgreich angewendet werden konnte, und der schließlich, in Verwirklichung der in meiner Arbeit [4] über die Klassenkörpertheorie im Kleinen ausgesprochenen Gedanken, sich neuerdings durch die Untersuchungen von Chevalley und Herbrand (siehe in Chevalley [4]) auch für die Begründung der Klassenkörpertheorie als beherrschender Gesichtspunkt erweist.

3. Übergang ins Kleine (p-adische Erweiterung).

(3. 1) Verhalten der Algebren und Algebrenklassen. Durch p-adische Erweiterung des Grundkörpers k auf $k_\mathfrak{p}$ erweitern sich die einfachen normalen Algebren A über k auf einfache normale Algebren $A_{k_\mathfrak{p}} = A_\mathfrak{p}$ über $k_\mathfrak{p}$, die Klassen $\mathfrak{A}$ auf Klassen $\mathfrak{A}_{k_\mathfrak{p}} = \mathfrak{A}_\mathfrak{p}$, und ihre Gruppe $\mathfrak{G}$ reduziert sich auf eine Faktorgruppe $\mathfrak{G}_{k_\mathfrak{p}} = \mathfrak{G}_\mathfrak{p} = \mathfrak{G}/\mathfrak{U}_\mathfrak{p}$, wo $\mathfrak{U}_{k_\mathfrak{p}} = \mathfrak{U}_\mathfrak{p}$ die Untergruppe derjenigen Klassen $\mathfrak{A}$ aus $\mathfrak{G}$ ist, die von $k_\mathfrak{p}$ zerfällt werden: $\mathfrak{A}_\mathfrak{p} = 1$. $\mathfrak{G}_\mathfrak{p}$ ist (wie sich nachträglich leicht ergibt) die volle Brauersche Algebrenklassengruppe über $k_\mathfrak{p}$; doch ist das für das Folgende unwesentlich.

Index m und Exponent l einer Klasse $\mathfrak{A}$ reduzieren sich auf Index $m_\mathfrak{p}$ und Exponent $l_\mathfrak{p}$ von $\mathfrak{A}_\mathfrak{p}$; das sind gewisse Teiler von m bzw. l, die ich auch p-*Index* und p-*Exponent* von $\mathfrak{A}$ nenne.

Ist $A_\mathfrak{p} \sim k_\mathfrak{p}$, d. h. $\mathfrak{A}_\mathfrak{p} = 1$, für alle Primstellen $\mathfrak{p}$ von k, so sage ich, A oder $\mathfrak{A}$ *zerfällt überall*. Trivialerweise gilt:

(3. 11) *Zerfällt* $\mathfrak{A}$ *schlechthin, so zerfällt* $\mathfrak{A}$ *überall*:

$$\textit{Aus } \mathfrak{A} = 1 \text{ folgt } \mathfrak{A}_\mathfrak{p} = 1 \textit{ für alle } \mathfrak{p}.$$

Allgemeiner:

(3. 12) *Aus* $\mathfrak{A} = \overline{\mathfrak{A}}$ *folgt* $\mathfrak{A}_\mathfrak{p} = \overline{\mathfrak{A}}_\mathfrak{p}$ *für alle* $\mathfrak{p}$.

(3. 2) Verhalten der Differente. Weil die zweiseitigen Ideale einer Maximalordnung von D sich eineindeutig mit den zweiseitigen Idealen jeder Maximalordnung jedes Elementes $A = D_r$ aus $\mathfrak{A}$ entsprechen, und weil sich dabei insbesondere die (reduzierten) Differenten der A aus $\mathfrak{A}$ einander

entsprechen, so kann ohne Mißverständnis von der *Differente ∂ der Klasse* $\mathfrak{A}$ gesprochen werden.

Diese reduziert sich bei der Erweiterung zu $\mathfrak{A}_\mathfrak{p}$ auf ihren p-Beitrag, die Differente $\partial_\mathfrak{p}$ von $\mathfrak{A}_\mathfrak{p}$, die ich auch die p-*Differente* von $\mathfrak{A}$ nenne (p endlich).

(3. 3) Verhalten der Erweiterungskörper endlichen Grades. Ist K ein Erweiterungskörper von endlichem Grade n über k, so wird (Hensel [1]) die p-adische Erweiterung $K_\mathfrak{p}$ direkte Summe von $\mathfrak{P}$-adischen Körpern $K_\mathfrak{P}$, entsprechend den verschiedenen Primteilern $\mathfrak{P}$ von p in K. Die $K_\mathfrak{P}$ sind algebraische Erweiterungskörper von Graden $n_\mathfrak{P}$ über $k_\mathfrak{p}$, den $\mathfrak{P}$-*Graden* von K; für diese gilt:

$$\sum_{\mathfrak{P}|\mathfrak{p}} n_\mathfrak{P} = n.$$

$n_\mathfrak{P}$ ist das Produkt aus Grad $f_\mathfrak{P}$ und Ordnung $e_\mathfrak{P}$ des Primteilers $\mathfrak{P}$ in bezug auf p. — Falls p unendlich reell ist, sind alle $f_\mathfrak{P} = 1$ und $e_\mathfrak{P} = 1$ oder 2, je nachdem $\mathfrak{P}$ reell oder komplex ist, falls p unendlich komplex ist, sind alle $f_\mathfrak{p} = 1$ und alle $e_\mathfrak{P} = 1$. (Ich schließe mich damit, entgegen meiner bisherigen Gepflogenheit $f_\mathfrak{P} = 1$ oder 2, $e_\mathfrak{P} = 1$, einem zweckmäßigen Vorschlag von Artin an.)

Ist speziell K galoissch über k, so sind alle p entsprechenden $K_\mathfrak{P}$ einander isomorph; ihr gemeinsamer Typus sei dann mit $K^\mathfrak{p}$ bezeichnet, sein Grad mit $n_\mathfrak{p}$. Dieser p-*Grad* von K ist dann ein Teiler des Grades n von K; der komplementäre Teiler ist die Anzahl der verschiedenen Primteiler $\mathfrak{P}$ von p in K. $n_\mathfrak{p}$ selbst ist das Produkt aus Grad $f_\mathfrak{p}$ und Ordnung $e_\mathfrak{p}$ der Primteiler $\mathfrak{P}$ in bezug auf p.

Für galoissches K reduziert sich ferner die galoissche Gruppe bei Übergang zu einem der $K_\mathfrak{P}$ auf die Zerlegungsgruppe zu $\mathfrak{P}$. Ist (für endliches p) insbesondere $e_\mathfrak{p} = 1$, d. h. ist $K^\mathfrak{p}$ unverzweigt über $k_\mathfrak{p}$, so ist diese Zerlegungsgruppe zyklisch [siehe (0. 1)], und eine eindeutig normierte Erzeugende ist der durch die Kongruenzeigenschaft

$$w_\mathfrak{P}^{F_\mathfrak{P}} \equiv w_\mathfrak{P}^{\mathfrak{N}(\mathfrak{p})} \bmod \mathfrak{P}$$

für alle ganzen $w_\mathfrak{P}$ aus $K_\mathfrak{P}$ charakterisierte Frobenius-Artin-Automorphismus $F_\mathfrak{P} = \left(\frac{K}{\mathfrak{P}}\right)$. Kommt es auf die Unterscheidung der konjugierten Primteiler und Zerlegungsgruppen nicht an (also z. B. von selbst immer bei abelschem K), so schreibe ich $F_\mathfrak{p} = \left(\frac{K}{\mathfrak{p}}\right) = \left(\frac{K^\mathfrak{p}}{\mathfrak{p}}\right)$.

(3. 4) Verhalten der Zerfällungskörper. Ist (K sei galoissch oder nicht) $K_\mathfrak{P}$ Zerfällungskörper von $\mathfrak{A}_\mathfrak{p}$, also $(\mathfrak{A}_\mathfrak{p})_{K_\mathfrak{P}} = 1$, so sage ich, K ist *Zerfällungskörper für* $\mathfrak{P}$ von $\mathfrak{A}$. Ist dies gleichzeitig für alle $\mathfrak{P}|\mathfrak{p}$ der Fall (also z. B. von selbst immer bei galoisschem Körper K), so sage ich, K ist *Zerfällungskörper für* p von $\mathfrak{A}$.

Aus der Relation

$$(\mathfrak{A}_\mathfrak{p})_{K_\mathfrak{P}} = \mathfrak{A}_{K_\mathfrak{P}} = (\mathfrak{A}_K)_\mathfrak{P}$$

ergibt sich:

(3. 41) *Ist K Zerfällungskörper schlechthin von $\mathfrak{A}$, so ist K Zerfällungskörper von $\mathfrak{A}$ für alle Primstellen $\mathfrak{P}$ von K:*

Aus $\mathfrak{A}_K = 1$ *folgt* $(\mathfrak{A}_\mathfrak{p})_{K_\mathfrak{P}} = 1$ *für alle* $\mathfrak{P}$.

(3. 5) Verhalten der zyklischen Darstellungen. Ist $\mathfrak{A}$ zyklisch darstellbar, so ist auch $\mathfrak{A}_\mathfrak{p}$ zyklisch darstellbar, nämlich

$$(\alpha, Z, S)_\mathfrak{p} \sim (\alpha, Z^\mathfrak{p}, S_\mathfrak{p});$$

dabei ist $Z^\mathfrak{p}$ der $\mathfrak{p}$ entsprechende p-adische Erweiterungskörper von Z im Sinne von (3. 3), und $S_\mathfrak{p}$ die früheste Potenz von S, die in dessen galoisscher Gruppe, der Zerlegungsgruppe zu $\mathfrak{p}$ von Z, liegt.

4. Die Struktur im Kleinen I (frühere Resultate).

Ich stelle hier die Resultate meiner früheren Arbeit [5] unter Benutzung der im vorhergehenden eingeführten Terminologie zusammen. Es kommt für diese Resultate an sich nicht auf die Entstehung der p-adischen Algebren $A_\mathfrak{p}$ durch p-adische Erweiterung von Algebren A an; sie beziehen sich also auf beliebige einfache normale Algebren über $k_\mathfrak{p}$. Ich behalte hier gleichwohl, der beabsichtigten Anwendung auf die Strukturuntersuchung im Großen zuliebe, den Gesichtspunkt der Entstehung durch p-adische Erweiterung in der Bezeichnung bei. Sachlich bedeutet das übrigens nach der Bemerkung in (3. 1) keinen Unterschied.

(4. 1) Zyklische Darstellung von $\mathfrak{A}_\mathfrak{p}$. $\mathfrak{A}_\mathfrak{p}$ ist stets zyklisch darstellbar, und besitzt sogar stets einen zyklischen Zerfällungskörper vom Minimalgrade $m_\mathfrak{p}$, nämlich den Körper $W^\mathfrak{p}$ aus (0. 1).

Die in $\mathfrak{A}_\mathfrak{p}$ liegende p-adische Divisionsalgebra $D^\mathfrak{p}$ (die i. a. natürlich nicht mit der p-adischen Erweiterung $D_\mathfrak{p}$ der in $\mathfrak{A}$ liegenden Divisionsalgebra D übereinstimmt) besitzt also eine zyklische Erzeugung:

$$D^\mathfrak{p} = (\alpha_\mathfrak{p}, W^\mathfrak{p}, F_\mathfrak{p}).$$

Dabei kann für endliches $\mathfrak{p}$ als Erzeugende $F_\mathfrak{p}$ der zyklischen galoisschen Gruppe von $W^\mathfrak{p}$ der Frobenius-Artin-Automorphismus von $W^\mathfrak{p}$ gewählt werden.

(4. 2) Invariante Kennzeichnung von $\mathfrak{A}_\mathfrak{p}$. Nach (2. 2) und (0. 1) kommt es bei der Zahl $\alpha_\mathfrak{p}$ aus $k_\mathfrak{p}$ nur auf die Restklasse mod $m_\mathfrak{p}$ der Ordnungszahl $\mu_\mathfrak{p}$ in $\mathfrak{p}$ an; für unendliches (reelles) $\mathfrak{p}$ ist $\mu_\mathfrak{p}$ als Exponent des Vorzeichens von $\alpha_\mathfrak{p}$ zu verstehen.

Diese Restklasse $\mu_\mathfrak{p}$ mod $m_\mathfrak{p}$ ist stets prim zu $m_\mathfrak{p}$.

Es sind also $\varphi(m_\mathfrak{p})$ Typen p-adischer Divisionsalgebren $D^\mathfrak{p}$ vom Grade $m_\mathfrak{p}$ und somit $\varphi(m_\mathfrak{p})$ Klassen $\mathfrak{A}_\mathfrak{p}$ p-adischer Algebren vom Index $m_\mathfrak{p}$ vorhanden; diese sind auch wirklich voneinander verschieden, weil sich umgekehrt $\mu_\mathfrak{p}$

invariant durch $D^{\mathfrak{p}}$ kennzeichnen läßt: Ist für endliches $\mathfrak{p}$ (für unendliches $\mathfrak{p}$ ist nichts zu beweisen) $\wp$ das (einzige) zweiseitige Primideal der (einzigen) Maximalordnung von $D^{\mathfrak{p}}$, so erfährt der Restklassenkörper mod $\wp$ bei Transformation mit irgendeinem genau durch $\wp^1$ teilbaren Element aus $D^{\mathfrak{p}}$ die $\mu_{\mathfrak{p}}^{-1}$-te Potenz des Frobenius-Artin-Automorphismus, d. h. potenziert sich mit $\mathfrak{N}(\mathfrak{p})^{\mu_{\mathfrak{p}}^{-1}}$ ($\mu_{\mathfrak{p}}^{-1}$ mod $m_{\mathfrak{p}}$ verstanden).

(4. 3) Die Differente von $\mathfrak{A}_{\mathfrak{p}}$. Die Differente von $D^{\mathfrak{p}}$, und somit in entsprechendem Sinne wie in (3. 2) die Differente der Klasse $\mathfrak{A}_{\mathfrak{p}}$, ist $\partial_{\mathfrak{p}} = \wp^{m_{\mathfrak{p}}-1}$ ($\mathfrak{p}$ endlich).

(4. 4) Die Gruppe $\mathfrak{U}_{W^{\mathfrak{p}}}$. Die Gruppe $\mathfrak{U}_{W^{\mathfrak{p}}}$ der von $W^{\mathfrak{p}}$ zerfällten $\mathfrak{p}$-adischen Algebrenklassen ist zyklisch von der Ordnung $m_{\mathfrak{p}}$. Denn sie ist nach (2. 2) isomorph zur Normklassengruppe von $W^{\mathfrak{p}}$ in $k_{\mathfrak{p}}$, und diese ist nach (0. 1) zyklisch von der Ordnung $m_{\mathfrak{p}}$, repräsentiert durch die Restklassen mod $m_{\mathfrak{p}}$ der Ordnungszahlen (Vorzeichenexponenten) in $\mathfrak{p}$.

Insbesondere bedeutet hiernach die in (4. 2) erwähnte Tatsache $(\mu_{\mathfrak{p}}, m_{\mathfrak{p}}) = 1$, daß jede Klasse $\mathfrak{A}_{\mathfrak{p}}$ vom Index $m_{\mathfrak{p}}$ erzeugendes Element der zyklischen Gruppe $\mathfrak{U}_{W^{\mathfrak{p}}}$ ist. Das hat zur Folge:

Der Exponent $l_{\mathfrak{p}}$ jeder Klasse $\mathfrak{A}_{\mathfrak{p}}$ ist gleich ihrem Index $m_{\mathfrak{p}}$.

Die sämtlichen Elemente der Gruppe $\mathfrak{U}_{W^{\mathfrak{p}}}$ werden geliefert als die Potenzen eines erzeugenden Elementes, werden also nach (2, 2) in der Form

$$(\alpha_{\mathfrak{p}}^{\nu},\ W^{\mathfrak{p}},\ F_{\mathfrak{p}}) \qquad (\nu = 0,1,\ldots,m_{\mathfrak{p}}-1)$$

zyklisch dargestellt.

5. Die Struktur im Kleinen II (weitere Ausführungen).

(5. 1) Die Struktur der Gesamtgruppe $\mathfrak{G}_{\mathfrak{p}}$. Es sei

$$\mathfrak{A}_{\mathfrak{p}}^{\circ} = \mathfrak{A}_{\mathfrak{p}}^{\nu}$$

eine beliebige Klasse aus $\mathfrak{U}_{W^{\mathfrak{p}}}$. Nach (4. 4) besitzt sie die zyklische Darstellung

$$A_{\mathfrak{p}}^{\circ} = (\alpha_{\mathfrak{p}}^{\nu},\ W^{\mathfrak{p}},\ F_{\mathfrak{p}}).$$

Wenn $\mathfrak{A}_{\mathfrak{p}}^{\circ}$ kein erzeugendes Element der Gruppe $\mathfrak{U}_{W^{\mathfrak{p}}}$ (d. h. ν nicht prim zu $m_{\mathfrak{p}}$) ist, so ist dies noch nicht die ausgezeichnete zyklische Darstellung von $\mathfrak{A}_{\mathfrak{p}}^{\circ}$ gemäß (4. 1). Diese ist vielmehr mit dem Körper $W_{\circ}^{\mathfrak{p}}$ des in (0. 1) genannten Typus vom Grade $m_{\mathfrak{p}}^{\circ}$ zu bilden; da $m_{\mathfrak{p}}^{\circ}$ nach (4. 4) Teiler von $m_{\mathfrak{p}}$ ist, so ist $W_{\circ}^{\mathfrak{p}}$ Teilkörper von $W^{\mathfrak{p}}$. Die zyklische Darstellung von $\mathfrak{A}_{\mathfrak{p}}^{\circ}$ im Sinne von (4. 1) möge dann

$$D_{\circ}^{\mathfrak{p}} = (\alpha_{\mathfrak{p}}^{\circ},\ W_{\circ}^{\mathfrak{p}},\ F_{\mathfrak{p}}^{\circ})$$

lauten und die gemäß (4. 2) zugeordnete invariante prime Restklasse $\mu_{\mathfrak{p}}^{\circ}$ mod $m_{\mathfrak{p}}^{\circ}$ sein.

Nun ist

$$A_{\mathfrak{p}}^{\circ} = (D_{\circ}^{\mathfrak{p}})_{s}, \quad \text{wo} \quad s = \frac{m_{\mathfrak{p}}}{m_{\mathfrak{p}}^{\circ}}.$$

Nach dem Satz (2. 5) ist aber

$$(D_\circ^{\mathfrak{p}})_s = (\alpha_{\mathfrak{p}}^{\circ s},\ W^{\mathfrak{p}},\ F_{\mathfrak{p}}).$$

Somit ergibt sich zwischen den beiden zyklischen Darstellungen

$$A_{\mathfrak{p}}^\circ = (\alpha_{\mathfrak{p}}^{\nu},\ W^{\mathfrak{p}},\ F_{\mathfrak{p}}) \quad \text{und} \quad D_\circ^{\mathfrak{p}} = (\alpha_{\mathfrak{p}}^\circ,\ W_\circ^{\mathfrak{p}},\ F_{\mathfrak{p}}^\circ)$$

von $\mathfrak{A}_{\mathfrak{p}}^\circ$ der Zusammenhang:

$$(\alpha_{\mathfrak{p}}^{\nu},\ W^{\mathfrak{p}},\ F_{\mathfrak{p}}) = (\alpha_{\mathfrak{p}}^{\circ s},\ W^{\mathfrak{p}},\ F_{\mathfrak{p}}).$$

Daraus folgt nach (2. 2) und (0. 1) für die $\mathfrak{A}_{\mathfrak{p}}$ und $\mathfrak{A}_{\mathfrak{p}}^\circ$ zugeordneten invarianten Restklassen der Zusammenhang

$$\bar{\mu}_{\mathfrak{p}} \equiv \nu\mu_{\mathfrak{p}} \equiv s\mu_{\mathfrak{p}}^\circ \bmod m_{\mathfrak{p}},$$

übersichtlicher geschrieben:

$$\frac{\bar{\mu}_{\mathfrak{p}}}{m_{\mathfrak{p}}} \equiv \frac{\nu\mu_{\mathfrak{p}}}{m_{\mathfrak{p}}} \equiv \frac{\mu_{\mathfrak{p}}^\circ}{m_{\mathfrak{p}}^\circ} \bmod 1,$$

wo jetzt links und rechts im Zähler jeweils die Ordnungszahl (der Vorzeichenexponent) aus der betreffenden zyklischen Darstellung von $\mathfrak{A}_{\mathfrak{p}}^\circ$ steht.

Hiernach ist es zweckmäßig, die Klasse $\mathfrak{A}_{\mathfrak{p}}$ an Stelle durch die Restklasse $\mu_{\mathfrak{p}} \bmod m_{\mathfrak{p}}$ lieber durch die Restklasse

$$\varrho_{\mathfrak{p}} \equiv \frac{\mu_{\mathfrak{p}}}{m_{\mathfrak{p}}} \bmod 1$$

zu charakterisieren. Die hergeleitete Tatsache, etwas anderes gewendet, besagt nämlich, daß man diese Restklasse mod 1 nicht nur aus der zyklischen Darstellung $(\alpha_{\mathfrak{p}}, W^{\mathfrak{p}}, F_{\mathfrak{p}})$, die zum Zerfällungskörper $W^{\mathfrak{p}}$ vom Minimalgrad $m_{\mathfrak{p}}$ gehört, ablesen kann, sondern in derselben Weise auch aus jeder zyklischen Darstellung $(\bar{\alpha}_{\mathfrak{p}}, \overline{W}^{\mathfrak{p}}, \overline{F}_{\mathfrak{p}})$ mit irgendeinem Zerfällungskörper $\overline{W}^{\mathfrak{p}}$ des in (0. 1) genannten Typus. Dessen Grad $\bar{m}_{\mathfrak{p}}$ ist ja dann nach (1. 4) ein Multiplum von $m_{\mathfrak{p}}$, also $\overline{W}^{\mathfrak{p}}$ selbst ein Erweiterungskörper von $W^{\mathfrak{p}}$; und nach dem eben Gezeigten gilt

$$\frac{\bar{\mu}_{\mathfrak{p}}}{\bar{m}_{\mathfrak{p}}} \equiv \frac{\mu_{\mathfrak{p}}}{m_{\mathfrak{p}}} \bmod 1,$$

wenn $\bar{\mu}_{\mathfrak{p}}$ die Ordnungszahl (den Vorzeichenexponenten) von $\bar{\alpha}_{\mathfrak{p}}$ in $\mathfrak{p}$ bezeichnet.

Ich nenne $\varrho_{\mathfrak{p}}$ die *Invariante von* $\mathfrak{A}_{\mathfrak{p}}$ und bezeichne sie mit $\left(\frac{\mathfrak{A}_{\mathfrak{p}}}{\mathfrak{p}}\right)$. Wenn es auf die Entstehung von $\mathfrak{A}_{\mathfrak{p}}$ durch p-adische Erweiterung von $\mathfrak{A}$ ankommt, nenne ich sie auch die p-*Invariante von* $\mathfrak{A}$ und bezeichne sie mit $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$.

Indem man zu einem gemeinsamen Zerfällungskörper von dem in (0. 1) genannten Typus übergeht, erhält man jetzt nach (4. 4) ohne weiteres:

(5. 11) *Es ist*

$$\left(\frac{\mathfrak{A}_{\mathfrak{p}}\mathfrak{B}_{\mathfrak{p}}}{\mathfrak{p}}\right) \equiv \left(\frac{\mathfrak{A}_{\mathfrak{p}}}{\mathfrak{p}}\right) + \left(\frac{\mathfrak{B}_{\mathfrak{p}}}{\mathfrak{p}}\right) \bmod 1.$$

Hiernach gilt:

(5. 12) *Durch die Invarianten* $\left(\frac{\mathfrak{A}_\mathfrak{p}}{\mathfrak{p}}\right)$ *wird (für endliches* $\mathfrak{p}$*) die Gesamtgruppe* $\mathfrak{G}_\mathfrak{p}$ *isomorph auf die additive Restklassengruppe aller rationalen Zahlen* mod 1 *abgebildet.*

Für unendliches (reelles) $\mathfrak{p}$ wird $\mathfrak{G}_\mathfrak{p}$ nur auf die additive Gruppe aus 0 und $\frac{1}{2}$ mod 1 isomorph abgebildet, entsprechend der Tatsache, daß es dann für $W^\mathfrak{p}$ nur zwei Möglichkeiten, den Körper $k_\mathfrak{p}$ selbst aller reellen Zahlen und den Körper aller komplexen Zahlen, gibt.

(5. 2) Kriterium für Zerfällungskörper von $\mathfrak{A}_\mathfrak{p}$. *Damit ein algebraischer Körper* $K_\mathfrak{P}$ *vom Grade* $n_\mathfrak{P}$ *über* $k_\mathfrak{p}$ *Zerfällungskörper der Klasse* $\mathfrak{A}_\mathfrak{p}$ *vom Index* $m_\mathfrak{p}$ *ist, ist die notwendige Gradbedingung* $m_\mathfrak{p} | n_\mathfrak{P}$ *auch hinreichend.*

Den Beweis siehe in Hasse [9] oder besser in Köthe [1], wo mit demselben Beweisansatz gleich allgemeiner das Verhalten der Invariante $\varrho_\mathfrak{p}$ von $\mathfrak{A}_\mathfrak{p}$ bei Übergang zu einem algebraischen Erweiterungskörper $K_\mathfrak{P}$ ausgedrückt wird: sie multipliziert sich einfach mit dem Grade $n_\mathfrak{P}$.

(5. 3) Theorie des Normenrestsymbols (Klassenkörpertheorie im Kleinen). Sei ein zyklischer Körper $Z^\mathfrak{p}$ vom Grade $n_\mathfrak{p}$ über $k_\mathfrak{p}$ gegeben. Um zu einer ganz im Kleinen verlaufenden Definition des Normenrestsymbols $\left(\frac{\alpha_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right)$ zu gelangen, betrachte ich die zyklische Algebra

$$A_\mathfrak{p} = (\alpha_\mathfrak{p}, Z^\mathfrak{p}, S_\mathfrak{p}),$$

wo $S_\mathfrak{p}$ irgendein erzeugender Automorphismus von $Z^\mathfrak{p}$ ist, und ihre Klasse $\mathfrak{A}_\mathfrak{p}$. Sei

$$\left(\frac{\mathfrak{A}_\mathfrak{p}}{\mathfrak{p}}\right) \equiv \frac{\nu_\mathfrak{p}}{n_\mathfrak{p}} \text{ mod. } 1$$

die Darstellung ihrer Invariante als Bruch vom Nenner $n_\mathfrak{p}$. Dann definiere ich:

$$\left(\frac{\alpha_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right) = S_\mathfrak{p}^{-\nu_\mathfrak{p}}.$$

Wenn $Z^\mathfrak{p}$ durch $\mathfrak{p}$-adische Erweiterung eines zyklischen Körpers Z über k entsteht und $\alpha_\mathfrak{p}$ eine Zahl α aus k ist, schreibe ich dafür auch $\left(\frac{\alpha, Z}{\mathfrak{p}}\right)$.

Diese Definition hängt nach (2. 3), (2. 2) und (5. 12) nicht von der Auswahl der Erzeugenden $S_\mathfrak{p}$ ab.

Sie hat folgende Bedeutung: Durchläuft $\alpha_\mathfrak{p}$ die Gruppe aller Zahlen $\neq 0$ aus $k_\mathfrak{p}$, so durchläuft $\mathfrak{A}_\mathfrak{p}$ die Untergruppe $\mathfrak{U}_{Z^\mathfrak{p}}$ aller von $Z^\mathfrak{p}$ zerfällten Klassen aus $\mathfrak{G}_\mathfrak{p}$. Nach (5. 2) ist das die Gruppe aller derjenigen Klassen $\mathfrak{A}_\mathfrak{p}$, deren Index $m_\mathfrak{p}$ ein Teiler von $n_\mathfrak{p}$ ist. Nach (5. 1) liefert $\left(\frac{\mathfrak{A}_\mathfrak{p}}{\mathfrak{p}}\right)$ eine isomorphe Abbildung dieser Gruppe $\mathfrak{U}_{Z^\mathfrak{p}}$ auf die additive Gruppe aller rationalen Zahlen vom Nenner $n_\mathfrak{p}$ mod 1. Folglich liefert das Symbol $\left(\frac{\alpha_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right)$ eine isomorphe Abbildung der Gruppe $\mathfrak{U}_{Z^\mathfrak{p}}$ auf die galoissche Gruppe von $Z^\mathfrak{p}$ über $k_\mathfrak{p}$.

Auf der anderen Seite ist $\mathfrak{U}_{Z^\mathfrak{p}}$ nach (2. 2) isomorph zur Normklassengruppe von $Z^\mathfrak{p}$ in $k_\mathfrak{p}$.

Zusammengenommen haben wir also:

(5. 31) *Das Symbol* $\left(\frac{\alpha_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right)$ *vermittelt eine isomorphe Abbildung der Normklassengruppe von* $Z^\mathfrak{p}$ *in* $k_\mathfrak{p}$ *auf die galoissche Gruppe von* $Z^\mathfrak{p}$ *über* $k_\mathfrak{p}$.

Im einzelnen:

(5. 311) *Es ist* $\left(\frac{\alpha_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right) = 1$ *dann und nur dann, wenn* $\alpha_\mathfrak{p}$ *Norm einer Zahl aus* $Z^\mathfrak{p}$ *ist.*

(5. 312) *Es ist*

$$\left(\frac{\alpha_\mathfrak{p}\beta_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right) = \left(\frac{\alpha_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right)\left(\frac{\beta_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right).$$

Insbesondere ergibt sich unmittelbar aus der Definition des Normenrestsymbols und der in (5. 1) entwickelten Berechnungsregel für die Invariante $\left(\frac{\mathfrak{A}_\mathfrak{p}}{\mathfrak{p}}\right)$ bei unverzweigtem Zerfällungskörper:

(5. 32) *Ist (für endliches* $\mathfrak{p}$*)* $W^\mathfrak{p}$ *unverzweigt über* $k_\mathfrak{p}$, *so drückt sich das Normenrestsymbol durch den Frobenius-Artin-Automorphismus so aus:*

$$\left(\frac{\alpha_\mathfrak{p}, W^\mathfrak{p}}{\mathfrak{p}}\right) = \left(\frac{W^\mathfrak{p}}{\mathfrak{p}}\right)^{-\nu_\mathfrak{p}};$$

dabei bezeichnet $\nu_\mathfrak{p}$ *die Ordnungszahl von* $\alpha_\mathfrak{p}$ *in* $\mathfrak{p}$.

Die in (5. 31) auftretende Normklassengruppe von $Z^\mathfrak{p}$ kann auch noch etwas anders charakterisiert werden: Weil jede Zahl aus $k_\mathfrak{p}$, die nach einer festen hinreichend hohen Potenz von $\mathfrak{p}$ kongruent 1 ist, sogar $n_\mathfrak{p}$-te Potenz in $k_\mathfrak{p}$, also sicher Norm einer Zahl aus $Z^\mathfrak{p}$ ist, existiert eine früheste Potenz $\mathfrak{f}_\mathfrak{p}$ dieser Art, der *Führer von* $Z^\mathfrak{p}$, oder, wenn $Z^\mathfrak{p}$ durch $\mathfrak{p}$-adische Erweiterung eines zyklischen Körpers Z über k entsteht, der $\mathfrak{p}$-*Führer von* Z. Die Normklassengruppe von $Z^\mathfrak{p}$ in $k_\mathfrak{p}$ ist identisch mit der *Normenrestklassengruppe* mod $\mathfrak{f}_\mathfrak{p}$ von $Z^\mathfrak{p}$ in $k_\mathfrak{p}$.

Insbesondere besagt (5. 32), daß $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^\varrho$ ist, wenn $Z^\mathfrak{p}$ unverzweigt über $k_\mathfrak{p}$ ist [$\mathfrak{p}$ endlich oder auch unendlich — siehe die Bemerkung über den letzteren Fall in (3. 3)].

Mit (5. 31) ist der *Isomorphiesatz der Klassenkörpertheorie im Kleinen* herausgestellt. Natürlich ist die in (5. 32) liegende Teilaussage dieses Isomorphiesatzes nichts anderes als die von Anfang an vorausgesetzte Tatsache (0. 1) aus der Klassenkörpertheorie im Kleinen. Die Bedeutung von (5. 32) liegt vielmehr darin, daß damit eine bestimmte Normierung des durch (5. 311), (5. 312) nur bis auf einen willkürlichen zu $n_\mathfrak{p}$ primen Exponenten festgelegten Normenrestsymbols ausgedrückt wird. —

Es ist nicht schwer, von der geschaffenen Grundlage aus auch die weiteren Sätze der Klassenkörpertheorie im Kleinen aufzubauen. Was insbesondere den Existenzsatz anbetrifft, so ist, wie ich erfahre, kürzlich von Chevalley [5] ein auf dieser Grundlage beruhender Beweis entwickelt worden. Ich möchte hier den Chevalleyschen Untersuchungen nicht vorgreifen und will daher nur noch den Beweis für die folgende Tatsache entwickeln:

(5. 33) *Ist* $Z_\circ^\mathfrak{p}$ *Teilkörper von* $Z^\mathfrak{p}$, *so ist* $\left(\frac{\alpha_\mathfrak{p}, Z_\circ^\mathfrak{p}}{\mathfrak{p}}\right)$ *derjenige Automorphismus von* $Z_\circ^\mathfrak{p}$, *der durch den Automorphismus* $\left(\frac{\alpha_\mathfrak{p}, Z^\mathfrak{p}}{\mathfrak{p}}\right)$ *von* $Z^\mathfrak{p}$ *geliefert wird.*

Beweis. Sei $n_\mathfrak{p}^\circ = \frac{n_\mathfrak{p}}{s}$ der Grad von $Z_\circ^\mathfrak{p}$ über $k_\mathfrak{p}$. Sei ferner

$$A_\mathfrak{p}^\circ = (\alpha_\mathfrak{p}, Z_\circ^\mathfrak{p}, S_\mathfrak{p}^\circ), \quad A_\mathfrak{p} = (\alpha_\mathfrak{p}, Z^\mathfrak{p}, S_\mathfrak{p}).$$

Nach (2. 5) gilt dann für die entsprechenden Klassen:

$$\mathfrak{A}_\mathfrak{p}^\circ = \mathfrak{A}_\mathfrak{p}^s,$$

also nach (5. 11)

$$\left(\frac{\mathfrak{A}_\mathfrak{p}^\circ}{\mathfrak{p}}\right) \equiv s \cdot \left(\frac{\mathfrak{A}_\mathfrak{p}}{\mathfrak{p}}\right) \bmod 1,$$

und somit

$$\left(\frac{\mathfrak{A}_\mathfrak{p}^\circ}{\mathfrak{p}}\right) \equiv \frac{\nu_\mathfrak{p}^\circ}{n_\mathfrak{p}^\circ}, \quad \left(\frac{\mathfrak{A}_\mathfrak{p}}{\mathfrak{p}}\right) \equiv \frac{\nu_\mathfrak{p}^\circ}{n_\mathfrak{p}} \bmod 1$$

mit demselben $\nu_\mathfrak{p}^\circ$. Das liefert die Behauptung nach der Definition des Normenretssymbols.

6. Zusammensetzung der Struktur im Kleinen zur Struktur im Großen.

Ich wiederhole hier zunächst den Beweis des Hauptsatzes von R. Brauer, Emmy Noether und mir, der in unserer gemeinsamen Arbeit (Hasse [9]) in der etwas umständlichen Form seiner historischen Entstehung mitgeteilt wurde; ich gebe diesen Beweis nunmehr in systematischer Weise. Siehe dazu auch die in gleicher Richtung liegenden Bearbeitungen dieses Beweises von Albert und mir (Albert [11]).

(6. 1) Überall zerfallende Algebrenklassen $\mathfrak{A}$. Eine unmittelbare Folge des Normensatzes (0. 2) ist:

(6. 11) *Besitzt* $\mathfrak{A}$ *einen zyklischen Zerfällungskörper* Z, *und zerfällt* $\mathfrak{A}$ *überall, so zerfällt* $\mathfrak{A}$ *schlechthin*:

Aus $\mathfrak{A}_Z = 1$ *und* $\mathfrak{A}_\mathfrak{p} = 1$ *für alle* $\mathfrak{p}$ *folgt* $\mathfrak{A} = 1$.

Beweis. Ist $A = (\alpha, Z, S)$ die Z entsprechende zyklische Darstellung von $\mathfrak{A}$, so bedeutet $\mathfrak{A}_\mathfrak{p} = 1$ nach (3. 5) $A_\mathfrak{p} \sim (\alpha, Z^\mathfrak{p}, S_\mathfrak{p}) \sim 1$, also nach (2. 2), daß α Norm aus $Z^\mathfrak{p}$ ist. Da dies für alle $\mathfrak{p}$ gilt, ist dann nach dem Normensatz (0. 2) α Norm aus Z. Das bedeutet, wieder nach (2. 2), $A \sim 1$, also $\mathfrak{A} = 1$. —

Mittels (6. 11) kann in Umkehrung zu (3. 11) bewiesen werden:

(6. 12) *Zerfällt $\mathfrak{A}$ überall, so zerfällt $\mathfrak{A}$ schlechthin*:

Aus $\mathfrak{A}_\mathfrak{p} = 1$ für alle $\mathfrak{p}$ folgt $\mathfrak{A} = 1$.

Beweis. Es ist zu zeigen, daß der Index m von $\mathfrak{A}$ gleich 1 ist.

Angenommen, es sei $m \neq 1$, und es sei p ein Primteiler von m. Dann sei K ein galoisscher Zerfällungskörper von $\mathfrak{A}$ endlichen Grades über k, und

$$k \leqq K_0 < K_1 < \ldots < K_s = K$$

eine Körperkette mit den Eigenschaften:

K_0 ist über k von zu p primem Grad h,

K_i ist über K_{i-1} zyklisch.

Die Existenz einer solchen Kette ergibt sich unmittelbar aus dem bekannten Sylowschen Gruppensatz und der Auflösbarkeit der p-Gruppen (sogar mit K_i über K_{i-1} durchweg vom Grade p). Aus dem überall Zerfallen von $\mathfrak{A}$ folgt nach (3. 4), daß auch alle Erweiterungen $\mathfrak{A}_{K_i}$ überall zerfallen. Unter Anwendung von (6. 11) folgt jetzt aus dem schlechthin Zerfallen von $\mathfrak{A}_{K_s}$ sukzessive, daß $\mathfrak{A}_{K_{s-1}}, \ldots, \mathfrak{A}_{K_0}$ schlechthin zerfallen. Hiernach wäre der Körper K_0 vom zu p primen Grade h ein Zerfällungskörper für $\mathfrak{A}$. Das ist ein Widerspruch, weil h dann nach (1. 4) durch den Index m, also durch p teilbar sein müßte.

(6. 2) Kriterium für Zerfällungskörper von $\mathfrak{A}$. In Umkehrung zu (3. 41) ergibt sich jetzt weiter:

(6. 21) *Ist K Zerfällungskörper von $\mathfrak{A}$ für alle Primstellen $\mathfrak{P}$ von K, so ist K Zerfällungskörper schlechthin von $\mathfrak{A}$:*

Aus $(\mathfrak{A}_\mathfrak{p})_{K_\mathfrak{P}} = 1$ für alle $\mathfrak{P}$ folgt $\mathfrak{A}_K = 1$.

Beweis. Nach (3. 4) zerfällt $\mathfrak{A}_K$ dann überall, nach (6. 12) also schlechthin.

Aus den beiden komplementären Tatsachen (3. 41) und (6. 21) ergibt sich durch Zusammenfassen der notwendigen und hinreichenden Kriterien (5. 2) für Zerfällungskörper im Kleinen für die einzelnen $\mathfrak{P}$ das notwendige und hinreichende Kriterium für Zerfällungskörper im Großen:

(6. 22) *Damit ein algebraischer Erweiterungskörper K endlichen Grades über k Zerfällungskörper für die Algebrenklasse $\mathfrak{A}$ ist, ist notwendig und hinreichend, daß für jede Primstelle $\mathfrak{p}$ und k und sämtliche ihr zugeordneten Primstellen $\mathfrak{P}$ von K jeweils der $\mathfrak{p}$-Index $m_\mathfrak{p}$ von $\mathfrak{A}$ ein Teiler der $\mathfrak{P}$-Grade $n_\mathfrak{P}$ von K ist: $m_\mathfrak{p} \mid n_\mathfrak{P}$.*

(6. 3) Die Differente von $\mathfrak{A}$. Aus (3. 2) und (4. 3) ergibt sich:

Die Differente ∂ von $\mathfrak{A}$ ist als Produkt ihrer sämtlichen $\mathfrak{p}$-Beiträge $\partial_\mathfrak{p}$ gegeben durch:

$$\partial = \prod_\mathfrak{p} \wp^{m_\mathfrak{p} - 1},$$

wo $\wp$ jeweils das zu der (endlichen) Primstelle $\mathfrak{p}$ von k gehörige zweiseitige Primideal von $\mathfrak{A}$ bezeichnet.

Hieraus ergibt sich insbesondere, daß der p-Index $m_\mathfrak{p}$ nur für endlich viele Primstellen p von 1 verschieden ist.

(6. 4) Zyklische Darstellung von $\mathfrak{A}$. Ich beweise jetzt die für die weiteren Zwecke ausreichende Teilaussage des Hauptsatzes:

(6. 41) *Jede Algebrenklasse $\mathfrak{A}$ ist zyklisch darstellbar, d. h. besitzt zyklische Zerfällungskörper Z.*

Beweis. Nach (6. 22) und (6. 3) genügt es, einen zyklischen Körper Z über k so zu konstruieren, daß für die endlich vielen p, für die $\mathfrak{A}$ einen p-Index $m_\mathfrak{p} \neq 1$ hat, jeweils der p-Grad $n_\mathfrak{p}$ von Z ein Multiplum von $m_\mathfrak{p}$ wird. Dies kann nun stets sogar durch einen Kreiskörper $Z = W$ über k erreicht werden.

In der Tat: Um die angegebene Bedingung $m_\mathfrak{p} \mid n_\mathfrak{p}$ zunächst für die endlichen Primstellen p zu erfüllen, wähle man W als Klassenkörper über k zu einer derartigen zyklischen Kongruenzklasseneinteilung der absoluten Normen, daß die betreffenden $\mathfrak{N}(\mathfrak{p}) = p^{f_\mathfrak{p}^\circ}$ jeweils in Klassen von durch $m_\mathfrak{p}$ teilbarem Exponenten fallen. Das wird erreicht, wenn in der zugrunde liegenden Kongruenzklasseneinteilung der rationalen Zahlen die betreffenden Primzahlen p jeweils in Klassen fallen, deren Exponenten k_p durch das kleinste Multiplum aller zu p gehörigen $m_\mathfrak{p} f_\mathfrak{p}^\circ$ teilbar sind. Um $m_\mathfrak{p} \mid n_\mathfrak{p}$ auch für die unendlichen p zu erfüllen, genügt es, die Einteilung noch so zu wählen, daß -1 in der Klasse vom Exponenten 2 liegt. Damit ist die Existenz eines Körpers W mit den erforderlichen Eigenschaften auf das Existenztheorem (0. 3) und die Existenzaussage in (0. 4) zurückgeführt. —

Die volle Aussage des Hauptsatzes lautet:

(6. 42) *Jedes Element A aus $\mathfrak{A}$, also jede einfache normale Algebra, ist zyklisch.*

Oder auch: $\mathfrak{A}$ *besitzt zyklische Zerfällungskörper Z für jedes Multiplum $n = mr$ des Index m als Grad.*

Um diese Tatsache zu beweisen, kommt man nicht mehr mit Kreiskörpern aus, braucht vielmehr ein schärferes Existenztheorem. Ein solches hinreichend scharfes Existenztheorem hat inzwischen Engström [1] bewiesen. Auch ergibt sich ein solches, wohl in größtmöglicher Allgemeinheit, aus der kürzlich erschienenen Dissertation von Grunwald [1]; siehe Grunwald [2].

Dieses schärfere Existenztheorem gibt dann in ähnlicher Weise, als Folge aus der in (4. 4) festgestellten Gleichheit von p-Exponent $l_\mathfrak{p}$ und p-Index $m_\mathfrak{p}$, noch die Tatsache:

(6. 43) *Der Exponent l jeder Klasse $\mathfrak{A}$ ist gleich ihrem Index m.*

Der gemeinsame Wert ist das kleinste gemeinsame Multiplum aller p-*Indizes $m_\mathfrak{p}$.*

Siehe dazu im einzelnen Hasse [8].

Im folgenden wird von den auf den schärferen Existenzsatz gegründeten Aussagen (6. 42) und (6. 43) kein Gebrauch gemacht werden.

(6. 5) Struktur der Gesamtgruppe $\mathfrak{G}$. In Umkehrung zu (3. 12) hat man nach (6. 12) wegen der Gruppeneigenschaft unmittelbar:

(6. 51) *Aus* $\mathfrak{A}_\mathfrak{p} = \overline{\mathfrak{A}}_\mathfrak{p}$ *für alle* $\mathfrak{p}$ *folgt* $\mathfrak{A} = \overline{\mathfrak{A}}$.

Nimmt man die beiden komplementären Tatsachen (3. 12) und (6. 51) zusammen, so ergibt sich durch Zusammenfassen der in (5. 1) für die einzelnen $\mathfrak{A}_\mathfrak{p}$ als charakteristisch erkannten Invarianten $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$, daß das System aller $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$ ein volles Invariantensystem für die Klasse $\mathfrak{A}$ ist:

(6. 52) *Es ist* $\mathfrak{A} = \overline{\mathfrak{A}}$ *dann und nur dann, wenn* $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \left(\frac{\overline{\mathfrak{A}}}{\mathfrak{p}}\right) \bmod 1$ *für alle* $\mathfrak{p}$ *ist.*

Ferner gilt gemäß (5. 11):

(6. 53) *Es ist*

$$\left(\frac{\mathfrak{A}\mathfrak{B}}{\mathfrak{p}}\right) \equiv \left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) + \left(\frac{\mathfrak{B}}{\mathfrak{p}}\right) \bmod 1.$$

Nach (6. 52), (6. 53) wird die Gesamtgruppe $\mathfrak{G}$ durch das System der $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$ isomorph auf eine gewisse Untergruppe der direkten Summe aller den einzelnen $\mathfrak{p}$ gemäß (5. 12) entsprechenden additiven Gruppen mod 1 abgebildet. Diese Untergruppe ist aber nicht die volle direkte Summe. Denn es gilt die fundamentale Tatsache:

(6. 54) *Zwischen den* $\mathfrak{p}$*-Invarianten einer Klasse* $\mathfrak{A}$ *besteht stets die Summenrelation*

$$\sum_\mathfrak{p} \left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv 0 \bmod 1.$$

Beweis. Es sei W ein gemäß dem Beweis von (6. 41) konstruierter zyklischer Kreiskörper über k, der $\mathfrak{A}$ zerfällt. W habe den Grad n und die $\mathfrak{p}$-Grade $n_\mathfrak{p}$.

$$A = (\alpha, W, S)$$

sei die zu W gehörige zyklische Darstellung von $\mathfrak{A}$. Nach (3. 5) ist dann

$$A_\mathfrak{p} \sim (\alpha, W^\mathfrak{p}, S_\mathfrak{p}), \quad \text{wo} \quad S_\mathfrak{p} = S^{\frac{n}{n_\mathfrak{p}}}.$$

Ich betrachte zunächst die (endlich vielen) endlichen $\mathfrak{p}$ mit $m_\mathfrak{p} \neq 1$. Für diese ist $W^\mathfrak{p}$ nach Konstruktion von W der unverzweigte Körper vom Grade $n_\mathfrak{p}$ über $k_\mathfrak{p}$. Demgemäß lassen sich die Invarianten $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$ gemäß (5. 1) ausdrücken. Dazu hat man nur statt der Erzeugenden $S_\mathfrak{p}$ die Frobenius-Artin-Automorphismen $F_\mathfrak{p} = \left(\frac{W}{\mathfrak{p}}\right)$ einzuführen. Sei also

$$F_\mathfrak{p} = S_\mathfrak{p}^{\lambda_\mathfrak{p}} = S^{n\frac{\lambda_\mathfrak{p}}{n_\mathfrak{p}}} \qquad [\text{mit } (\lambda_\mathfrak{p}, n_\mathfrak{p}) = 1].$$

Dann ist nach (2. 3)

$$A_\mathfrak{p} \sim (\alpha^{\lambda_\mathfrak{p}}, W^\mathfrak{p}, F_\mathfrak{p}),$$

und somit nach (5. 1)

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \frac{\lambda_\mathfrak{p}\, \bar{\nu}_\mathfrak{p}}{n_\mathfrak{p}} \bmod 1,$$

wenn α genau durch $\mathfrak{p}^{\bar{\nu}_\mathfrak{p}}$ teilbar ist.

Ich betrachte ferner die (unendlich vielen) endlichen $\mathfrak{p}$ mit $m_\mathfrak{p} = 1$. Für sie ist $\mathfrak{A} = 1$, also einerseits

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv 0 \bmod 1,$$

andererseits nach (2. 2)

α Norm einer Zahl aus $W^\mathfrak{p}$.

Da zu den jetzt betrachteten $\mathfrak{p}$ insbesondere die Primteiler des Moduls M der W entsprechenden Kongruenzklasseneinteilung gehören, so ist also jedenfalls α Normenrest mod M. Da α nach (2. 2) nur bis auf eine beliebige Zahlnorm aus W als Faktor bestimmt ist, darf daher insbesondere α prim zu M angenommen werden. Ferner sind daher die Beiträge der jetzt betrachteten $\mathfrak{p}$ zu α Idealnormen aus W.

Zusammengenommen hat dann also α eine Idealzerlegung:

$$\alpha = \prod_{\substack{m_\mathfrak{p} \neq 1 \\ \mathfrak{p}\ \text{endl.}}} \mathfrak{p}^{\bar{\nu}_\mathfrak{p}} \cdot N(\mathfrak{c}),$$

wo $\mathfrak{c}$ ein zu M primes Ideal aus W ist.

Ich betrachte weiter die unendlichen $\mathfrak{p}$ mit $m_\mathfrak{p} \neq 1$ (also $\mathfrak{p}$ reell, $m_\mathfrak{p} = 2$). Für sie ist einerseits nach dem bei (5. 12) Bemerkten

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \frac{1}{2} \bmod 1,$$

andererseits nach (2. 2) α keine Norm aus dem (komplexen) Körper $W^\mathfrak{p}$, also negativ.

Ich betrachte schließlich die unendlichen (reellen) $\mathfrak{p}$ mit $m_\mathfrak{p} = 1$. Für sie ist wieder $\mathfrak{A} = 1$, also einerseits

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv 0 \bmod 1,$$

andererseits α Norm aus dem (komplexen) Körper $W^\mathfrak{p}$, also positiv.

Hiernach ist $\operatorname{sgn} \mathfrak{N}(\alpha) = (-1)^a$, wo a die Anzahl der unendlichen $\mathfrak{p}$ mit $m_\mathfrak{p} \neq 1$ bezeichnet.

Zusammengenommen gehört somit α zur Hauptklasse der W entsprechenden Klasseneinteilung oder zu der Klasse der Ordnung 2, je nachdem a gerade oder ungerade ist. Genau dasselbe gilt dann für das Produkt $\prod_{\substack{m_\mathfrak{p} \neq 1 \\ \mathfrak{p}\ \text{endl.}}} \mathfrak{p}^{\bar{\nu}_\mathfrak{p}}$. Nach dem in (0. 4) vorangestellten Artinschen Reziprozitätsgesetz für W ist dementsprechend

$$\prod_{\substack{m_\mathfrak{p} \neq 1 \\ \mathfrak{p}\ \text{endl.}}} F_\mathfrak{p}^{\bar{\nu}_\mathfrak{p}} = S^{\frac{n}{2}a},$$

denn $S^{n/2}$ ist (falls überhaupt $a \neq 0$ und somit n gerade ist) das Element der Ordnung 2 in der galoisschen Gruppe von W. Stellt man auch die linke Seite in dieser Relation mit Hilfe der zuvor eingeführten Bezeichnungen als Potenz von S dar, so ergibt sich:

$$\sum_{\substack{m_\mathfrak{p} \neq 1 \\ \mathfrak{p} \text{ endl.}}} \frac{\lambda_\mathfrak{p} \bar{\nu}_\mathfrak{p}}{n_\mathfrak{p}} + \frac{a}{2} \equiv 0 \bmod 1.$$

Diese Relation besagt aber nach den obigen Ausführungen über die Werte der Invarianten $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$ gerade die Behauptung. —

Unter Anwendung des allgemeinen Satzes von der arithmetischen Progression in k kann man schließlich zeigen, daß die in (6. 54) festgestellte Relation die einzige allgemeine Relation zwischen den Invarianten $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$ einer Klasse $\mathfrak{A}$ ist, indem man nämlich beweist:

(6. 55) *Zu jedem den Primstellen* $\mathfrak{p}$ *von* k *zugeordneten System rationaler Zahlen* $\varrho_\mathfrak{p}$ *mit den Eigenschaften*:

(i) *nur endlich viele* $\varrho_\mathfrak{p}$ *sind gebrochen*,

(ii) *für die unendlichen (reellen)* $\mathfrak{p}$ *ist* $\varrho_\mathfrak{p} \equiv 0$ *oder* $\frac{1}{2} \bmod 1$,

(iii) *es ist* $\sum_\mathfrak{p} \varrho_\mathfrak{p} \equiv 0 \bmod 1$

existiert eine Algebrenklasse $\mathfrak{A}$ *über* k *mit*

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \varrho_\mathfrak{p} \bmod 1$$

für alle $\mathfrak{p}$.

Beweis. Sei in reduzierter Darstellung

$$\varrho_\mathfrak{p} \equiv \frac{\mu_\mathfrak{p}}{m_\mathfrak{p}} \bmod 1.$$

Dann sei W ein zyklischer Kreiskörper über k, dessen $\mathfrak{p}$-Grade $n_\mathfrak{p}$ jeweils durch die reduzierten Nenner $m_\mathfrak{p}$ teilbar sind, so daß also die $\varrho_\mathfrak{p}$ auch auf die Nenner $n_\mathfrak{p}$ erweitert werden können:

$$\varrho_\mathfrak{p} \equiv \frac{\nu_\mathfrak{p}}{n_\mathfrak{p}} \bmod 1.$$

Ein solcher Körper W existiert nach (0. 3), (0. 4), weil nach (i) nur endlich viele $m_\mathfrak{p} \neq 1$ sind, und weil insbesondere nach (ii) die gestellte Bedingung für die unendlichen $\mathfrak{p}$ erfüllt werden kann.

Es sei nun S ein erzeugender Automorphismus von W. Ich konstruiere dann eine zyklische Algebra

$$A = (\alpha, W, S)$$

zu W als Zerfällungskörper derart, daß ihre Klasse $\mathfrak{A}$ die Invarianten $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \varrho_\mathfrak{p} \bmod 1$ hat. Um das zu erreichen, unterwerfe ich die Zahl α aus k geeigneten Bedingungen:

Für die endlichen $\mathfrak{p}$ mit $m_\mathfrak{p} \neq 1$ sei α genau durch $\mathfrak{p}^{\bar{\nu}_\mathfrak{p}}$ teilbar, wenn wie im Beweis von (6. 54)

$$\left(\frac{W}{\mathfrak{p}}\right) = F_\mathfrak{p} = S_\mathfrak{p}^{\lambda_\mathfrak{p}}$$

ist und $\bar{\nu}_\mathfrak{p}$ gemäß

$$\nu_\mathfrak{p} \equiv \lambda_\mathfrak{p}\, \bar{\nu}_\mathfrak{p} \mod n_\mathfrak{p}$$

bestimmt ist. Dann wird, wie dort, in der Tat

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \frac{\lambda_\mathfrak{p}\, \bar{\nu}_\mathfrak{p}}{n_\mathfrak{p}} \equiv \frac{\nu_\mathfrak{p}}{n_\mathfrak{p}} \equiv \varrho_\mathfrak{p} \mod 1.$$

Für die endlichen $\mathfrak{p}$, die im Modul der W entsprechenden Kongruenzklasseneinteilung aufgehen (nach Konstruktion von W ist für diese $\mathfrak{p}$ sicher $m_\mathfrak{p} = 1$), sei α prim zu $\mathfrak{p}$ und Norm einer Zahl aus $W^\mathfrak{p}$; hierzu genügt es, daß α jeweils primer Normenrest von $W^\mathfrak{p}$ nach dem $\mathfrak{p}$-Führer $\mathfrak{f}_\mathfrak{p}$ von W ist. Dann ist wieder, wie im Beweis von (6. 54),

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \varrho_\mathfrak{p} \equiv 0 \mod 1.$$

Für die unendlichen (reellen) $\mathfrak{p}$ habe α das Vorzeichen $(-1)^{\bar{\nu}_\mathfrak{p}}$. Dann ist auch für diese $\mathfrak{p}$

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \varrho_\mathfrak{p} \mod 1.$$

Den bisherigen Bedingungen für α kann nach dem allgemeinen Satz von der arithmetischen Progression durch eine Zahl der Form

$$\alpha = \prod_{\substack{m_\mathfrak{p} \neq 1 \\ \mathfrak{p}\ \text{endl.}}} \mathfrak{p}^{\bar{\nu}_\mathfrak{p}} \cdot \mathfrak{q}$$

entsprochen werden, wo $\mathfrak{q}$ ein von allen bisher genannten $\mathfrak{p}$ verschiedenes Primideal aus k ist. Es ist dann auch für die bisher nicht genannten $\mathfrak{p}$, von $\mathfrak{q}$ zunächst abgesehen,

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv 0 \equiv \varrho_\mathfrak{p} \mod 1.$$

Mittels (6. 54) und der vorausgesetzten Relation (iii) ergibt sich jetzt, daß schließlich auch

$$\left(\frac{\mathfrak{A}}{\mathfrak{q}}\right) \equiv -\sum_{\mathfrak{p} \neq \mathfrak{q}} \left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv -\sum_{\mathfrak{p} \neq \mathfrak{q}} \varrho_\mathfrak{p} \equiv \varrho_\mathfrak{q} \mod 1$$

ist. Das vollendet den Beweis.

Zusammengenommen hat sich das folgende Resultat über die Struktur der R. Brauerschen Algebrenklassengruppe $\mathfrak{G}$ über k ergeben:

(6. 56) *Die Gruppe $\mathfrak{G}$ wird durch die Invarianten $\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right)$ isomorph abgebildet auf diejenige Untergruppe der direkten Summe der den einzelnen Primstellen $\mathfrak{p}$ von k gemäß* (5. 12) *entsprechenden additiven Gruppen* mod 1, *die durch die Relation* (iii) *in* (6. 55) *gekennzeichnet ist.*

Für die anschließend entwickelte Theorie des Normenrestsymbols und insbesondere den Beweis des Reziprozitätsgesetzes wird von den Tatsachen (6. 55), (6. 56), die sich auf den allgemeinen Satz von der arithmetischen Progression stützen, kein Gebrauch gemacht werden.

(6. 6) Theorie des Normenrestsymbols (Beweis des Reziprozitätsgesetzes in der Produktform). Sei ein zyklischer Körper Z vom Grade n über k gegeben, und sei S ein erzeugender Automorphismus von Z.

Zunächst sollen die in (5. 3) gegebene Definition des Normenrestsymbols und die dort anschließend darüber bewiesenen Tatsachen unter dem Gesichtspunkt der Entstehung des dortigen Körpers $Z^{\mathfrak{p}}$ durch $\mathfrak{p}$-adische Erweiterung von Z ausgesprochen werden.

Die Definition des Symbols $\left(\frac{\alpha, Z}{\mathfrak{p}}\right)$ kann in die folgende Form gesetzt werden: Sei $\mathfrak{A}$ die Klasse der zyklischen Algebra

$$A = (\alpha, Z, S)$$

und sei

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \frac{\bar{\nu}_{\mathfrak{p}}}{n} \bmod 1$$

die Darstellung ihrer $\mathfrak{p}$-Invariante als Bruch vom Nenner n. Dann ist

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = S^{-\bar{\nu}_{\mathfrak{p}}}.$$

Die Tatsachen (5. 31) und (5. 32) liefern im Hinblick auf das in (3. 3) und nach (5. 32) Bemerkte:

(6. 61) *Das Symbol* $\left(\frac{\alpha, Z}{\mathfrak{p}}\right)$ *vermittelt eine isomorphe Abbildung der Normenrestklassengruppe nach dem* $\mathfrak{p}$*-Führer* $\mathfrak{f}_{\mathfrak{p}}$ *von* Z *auf die Zerlegungsgruppe von* Z *für* $\mathfrak{p}$.

Im einzelnen:

(6. 611) *Es ist* $\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = 1$ *dann und nur dann, wenn* α *Normenrest* mod $\mathfrak{f}_{\mathfrak{p}}$ *von* Z *ist.*

(6. 612) *Es ist* $\left(\frac{\alpha\beta, Z}{\mathfrak{p}}\right) = \left(\frac{\alpha, Z}{\mathfrak{p}}\right)\left(\frac{\beta, Z}{\mathfrak{p}}\right)$.

(6. 62) *Ist (ein endliches)* $\mathfrak{p}$ *unverzweigt in* Z*, so drückt sich das Normenrestsymbol durch den Frobenius-Artin-Automorphismus so aus:*

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = \left(\frac{Z}{\mathfrak{p}}\right)^{-\nu_{\mathfrak{p}}};$$

dabei bezeichnet $\nu_{\mathfrak{p}}$ *die Ordnungszahl von* α *in* $\mathfrak{p}$.

Die Tatsache (5. 33) liefert:

(6. 63) *Ist* Z_0 *Teilkörper von* Z*, so ist* $\left(\frac{\alpha, Z_0}{\mathfrak{p}}\right)$ *derjenige Automorphismus von* Z_0*, der durch den Automorphismus* $\left(\frac{\alpha, Z}{\mathfrak{p}}\right)$ *von* Z *geliefert wird.*

Nimmt man zu der Definition in der jetzt gegebenen Form die fundamentale Summenrelation (6. 54) hinzu, so folgt:

(6. 64) (*Produktform des Reziprozitätsgesetzes*). *Es ist*

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, Z}{\mathfrak{p}}\right) = 1.$$

Zusammen mit (6. 61) und (6. 612) ergibt (6. 64) insbesondere leicht die Identität der hier gegebenen Definition des Normenrestsymbols mit der Definition in meiner früheren Arbeit [3].

(6. 7) Übergang zum Artinschen Reziprozitätsgesetz (Isomorphiesatz der Klassenkörpertheorie im Großen). Es hat keine Schwierigkeit, von den vorstehend erhaltenen Tatsachen, insbesondere der Produktformel (6. 64) ausgehend die Gültigkeit der folgenden *Kernaussage des Artinschen Reziprozitätsgesetzes* zu erschließen:

(6. 71) *Das Artin-Symbol* $\left(\frac{Z}{\mathfrak{a}}\right)$ *für zum Führer* $\mathfrak{f}$ *von* Z *prime Ideale* $\mathfrak{a}$ *aus* k *vermittelt eine homomorphe Abbildung der* $Z \bmod \mathfrak{f}$ *zugeordneten Idealklassengruppe in* k *in die galoissche Gruppe von* Z.

Dabei ist das *Artin-Symbol* erklärt durch:

$$\left(\frac{Z}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}} \left(\frac{Z}{\mathfrak{p}}\right)^{\nu_{\mathfrak{p}}}, \text{ wenn } \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}};$$

der *Führer* von Z ist als das Produkt $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{f}_{\mathfrak{p}}$ der $\mathfrak{p}$-Führer von Z zu verstehen; und die $Z \bmod \mathfrak{f}$ zugeordnete Idealklassengruppe in k wird durch die Strahlklassen $\bmod \mathfrak{f}$ der Normen zu $\mathfrak{f}$ primer Ideale aus Z als Hauptklasse geliefert. Die Behauptung drückt sich also folgendermaßen aus:

$\left(\frac{Z}{\mathfrak{a}}\right) = 1$, wenn $\mathfrak{a}$ in der Hauptklasse liegt, d. h. wenn ein zu $\mathfrak{f}$ primes Ideal $\mathfrak{c}$ in Z existiert, derart, daß

$$\mathfrak{a}\, N(\mathfrak{c}) = \alpha \equiv 1 \bmod \mathfrak{f}$$

ist.

Beweis. Unter den genannten Voraussetzungen ist α Normenrest $\bmod \mathfrak{f}_{\mathfrak{p}}$ von Z für jedes nicht in $\mathfrak{a}$ aufgehende $\mathfrak{p}$; daher ist nach (6. 611)

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = 1$$

für alle diese $\mathfrak{p}$. Für die in $\mathfrak{a}$ aufgehenden $\mathfrak{p}$ dagegen ist nach (6. 62)

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = \left(\frac{Z}{\mathfrak{p}}\right)^{-\nu_{\mathfrak{p}}}.$$

Die Anwendung der Produktformel (6. 54) liefert jetzt ohne weiteres die Behauptung $\left(\frac{Z}{\mathfrak{a}}\right) = 1$. —

Will man das *volle Artinsche Reziprozitätsgesetz* und damit den *Isomorphiesatz der Klassenkörpertheorie im Großen* haben, so muß man wieder weitergehende Tatsachen aus der Klassenkörpertheorie heranziehen.

Daß einerseits die in (6. 71) genannte Abbildung auf die ganze galoissche Gruppe von Z erfolgt, ergibt sich ohne weiteres aus dem Frobeniusschen Dichtigkeitssatz (oder auch nur Existenzsatz), nach dem es zu dem erzeugenden Automorphismus S von Z Primideale $\mathfrak{p}$ mit $\left(\frac{Z}{\mathfrak{p}}\right) = S$ (d. h. also in Z unzerlegt bleibende Primideale $\mathfrak{p}$) gibt *).

Daß andererseits die in (6. 71) genannte Abbildung isomorph ist, ergibt sich ohne weiteres aus der analytischen Grundlage der Klassenkörpertheorie, daß nämlich die Klassenanzahl der $Z \bmod \mathfrak{f}$ zugeordneten Idealklasseneinteilung in k nicht größer sein kann als der Grad n von Z.

Unter Anwendung dieser analytischen Hilfsmittel erhält man dann also aus (6. 71):

(6. 72) *Das Artin-Symbol* $\left(\frac{Z}{\mathfrak{a}}\right)$ *für zum Führer* $\mathfrak{f}$ *von* Z *prime Ideale* $\mathfrak{a}$ *aus* k *vermittelt eine isomorphe Abbildung der* $Z \bmod \mathfrak{f}$ *zugeordneten Idealklassengruppe in* k *auf die galoissche Gruppe von* Z.

Die in geläufiger Weise zu vollziehende Verallgemeinerung der hier nur für zyklische Körper Z über k entwickelten Theorie des Normenrestsymbols und Reziprozitätsgesetzes auf beliebige abelsche Körper über k bietet keinerlei Schwierigkeiten, so daß ich hier darauf nicht besonders einzugehen brauche.

7. Anhang.

Von den in der Einleitung zusammengestellten Tatsachen (0. 1) bis (0. 4) aus der Klassenkörpertheorie, die für die vorstehend entwickelte Theorie wesentlich gebraucht wurden, ist allein der Normensatz (0. 2) ein wirklich tiefliegender allgemeiner Satz, während die übrigen Tatsachen (0. 1), (0. 3), (0. 4) nur ganz einfache, leicht unabhängig beweisbare Spezialfälle der allgemeinen Klassenkörpersätze sind.

Für eine Begründung der ganzen Klassenkörpertheorie mit nichtkommutativen Hilfsmitteln wäre es natürlich erwünscht, auch einen unabhängigen Beweis des Normensatzes zu besitzen. In dieser Hinsicht ist es interessant, daß der Normensatz, oder vielmehr der mit seiner Hilfe erschlossene und ihn als Spezialfall enthaltende allgemeine Satz (6. 12):

Zerfällt A überall, so zerfällt A auch schlechthin

sich als ein Theorem über quadratische diophantische Gleichungen formulieren läßt.

In der Tat, sei e_i eine Basis von A und α_{iji} die zugehörigen Multiplikationskonstanten. Das Zerfallen von A bedeutet dann die Existenz einer Basistransformation

$$\bar{e}_r = \sum_r e_i \xi_{ir}$$

*) Zusatz bei der Korrektur. Wie neuerdings Chevalley [4] gezeigt hat, kann man diesen Nachweis auch rein arithmetisch erbringen.

auf ein vollständiges System von Matrizeneinheiten $\bar{e}_r$, und zwar mit Transformationskoeffizienten ξ_{ir} in k oder in $k_\mathfrak{p}$, je nachdem es sich um das Zerfallen von A schlechthin oder für $\mathfrak{p}$ handelt. Bezeichnet $\bar{\alpha}_{rst}$ das System der Multiplikationskonstanten für die Matrizeneinheiten $\bar{e}_r$ — es besteht nur aus Nullen und Einsen —, so bedeutet jene Transformation das Bestehen eines Systems

$$(Q) \qquad \sum_{i,j} \alpha_{ijl}\, \xi_{ir}\, \xi_{js} = \sum_{t} \bar{\alpha}_{rst}\, \xi_{lt}$$

von inhomogenen quadratischen diophantischen Gleichungen, deren Koeffizienten α_{ijl}, $\bar{\alpha}_{rst}$ zu k gehören, mit Werten der Unbestimmten ξ_{ir} in k bzw. in $k_\mathfrak{p}$, und derart, daß deren Determinante $|\xi_{ir}| \neq 0$ ist.

Der Satz von den überall zerfallenden Algebren läuft dann also auf folgende Tatsache hinaus:

Wenn das Gleichungssystem (Q) *in jedem* $\mathfrak{p}$*-adischen Erweiterungskörper* $k_\mathfrak{p}$ *von* k *eine Lösung mit nicht verschwindender Determinante hat, so hat es auch in* k *selbst eine Lösung mit nicht verschwindender Determinante.*

Das ist eine gewisse Verallgemeinerung des Fundamentalprinzips meiner Arbeiten [1, 2] über quadratische Formen in k. Dort handelt es sich um Systeme homogener quadratischer Gleichungen, wie sie den Darstellbarkeits- und Äquivalenzbeziehungen quadratischer Formen entsprechen.

Es wäre denkbar, daß sich die dortigen Methoden derart ausbauen ließen, daß auch der hier auftretende inhomogene Typus erfaßt wird. Damit wäre dann insbesondere der Normensatz im allgemeinen Falle auf den Normensatz im quadratischen Falle zurückgeführt, der ja für den Beweis des Fundamentalprinzips bei den quadratischen Formen das grundlegende Werkzeug ist.

Übrigens läßt sich auch schon das Resultat meiner Arbeit [2] über die Äquivalenz quadratischer Formen zu einem ersten Schritt in Richtung auf den Beweis des Satzes von den überall zerfallenden Algebren ausnutzen. Mit der Basis e_i von A ist nämlich die quadratische Form

$$F = \sum_{i,j} S(e_i e_j)\, \xi_i\, \xi_j,$$

das ist die Spur des Quadrates des allgemeinen Elementes

$$x = \sum_{i} e_i\, \xi_i$$

von A, kovariant verbunden. Zerfällt nun A überall, so läßt sich diese Form für jedes $\mathfrak{p}$ in $k_\mathfrak{p}$ auf die einem vollständigen System von Matrizeneinheiten $\bar{e}_r$ entsprechende Normalform $\overline{F}$ transformieren. Nach dem angeführten Resultat geht das dann also auch in k selbst.

Damit ist also jedenfalls gezeigt, daß A eine Basis $\bar{e}_r'$ besitzt, für die die Spurenmatrix $S(\bar{e}_r'\, \bar{e}_s')$ dieselbe ist wie bei einem vollständigen Matrizeneinheitensystem $\bar{e}_r$.

Literaturverzeichnis.

A. A. Albert.

[1] On the structure of normal division algebras, Ann. of Math. (2) **30** (1929).

[2] The rank function of any simple algebra, Proc. Nat. Acad. of Sciences **15** (1929).

[3] On the rank equation of any normal division algebra, Bull. Amer. Math. Soc. 1929.

[4] Normal division algebras in $4p^2$ units, p an odd prime, Ann. of Math. (2) **30** (1929).

[5] A note on an important theorem on normal division algebras, Bull. Amer. Math. Soc. 1930.

[6] The structure of pure Riemann matrices with non-commutative multiplication algebras, Rend. del Circ. Mat. di Palermo **55** (1931).

[7] On direct products, cyclic division algebras, and pure Riemann matrices, Trans. Amer. Math. Soc. **33** (1931).

[8] On direct products, Trans. Amer. Math. Soc. **33** (1931).

[9] Division algebras over an algebraic field, Bull. Amer. Math. Soc. 1931.

[10] On the construction of cyclic algebras with a given exponent, Amer. Journ. of Math. **54** (1932).

[11] A determination of all normal division algebras over an algebraic number field (together with Hasse), Trans. Amer. Math. Soc. **34** (1932).

E. Artin.

[1] Zur Arithmetik hyperkomplexer Zahlen, Abhandl. a. d. Math. Sem. Hamburg **5** (1927).

[2] Beweis des allgemeinen Reziprozitätsgesetzes, Abhandl. a. d. Math. Sem. Hamburg **5** (1927).

H. Brandt.

[1] Zur allgemeinen Idealtheorie, Verhandl. d. Schweiz. Naturf. Ges. 1927.

[2] Idealtheorie in Quaternionenalgebren, Math. Annalen **99** (1928).

[3] Idealtheorie in einer Dedekindschen Algebra, Jahresber. d. Deutschen Math. Ver. **37** (1928), S. *5—7*.

[4] Primidealzerlegung in einer Dedekindschen Algebra, Verhandl. d. Schweiz. Naturf. Ges. 1929.

[5] Zur Idealtheorie Dedekindscher Algebren, Comment. Math. Helvet. **2** (1930).

R. Brauer.

[1] Siehe Noether [1].

[2] Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen, I, Math. Zeitschr. **28** (1928).

[3] Über Systeme hyperkomplexer Größen, Jahresber. d. Deutsch. Math. Ver. **38** (1929), S. *47/48*.

[4] Zur Theorie der hyperkomplexen Zahlen, Math. Zeitschr. **30** (1929).

[5] Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen, II, Math. Zeitschr. **31** (1930).

[6] Siehe Hasse [9].

[7] Über die algebraische Struktur von Schiefkörpern, Journ. f. d. reine u. angew. Math. **166** (1932).

[8] Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind. Journ. f. d. reine u. angew. Math. **168** (1932).

C. Chevalley.

[1] Sur un théorème de M. Hasse, Comptes Rendus de l'Acad. Paris 1930.

[2] Sur la théorie des restes normiques, Comptes Rendus de l'Acad. Paris 1930.

[3] Sur la structure de la théorie du corps de classes, Comptes Rendus de l'Acad. Paris 1932.

[4] Sur la théorie du corps de classes, Thèse de l'Université de Paris 1932, erscheint demnächst an noch nicht feststehender Stelle.

[5] La théorie du symbole de restes normiques, erscheint demnächst im Journ. f. d. reine u. angew. Math.

L. E. Dickson.

[1] Algebras and their arithmetics, Chicago 1923.

[2] New division algebras, Trans. Amer. Math. Soc. **28** (1926).

[3] Algebren und ihre Zahlentheorie (mit letztem Kapitel von Speiser), Zürich 1927.

[4] New division algebras, Bull. Amer. Math. Soc. 1928.

[5] Construction of division algebras, Trans. Amer. Math. Soc. **32** (1930).

M. Deuring.

[1] Zur Theorie der Normen relativzyklischer Körper, Nachr. v. d. Ges. d. Wiss. Göttingen 1931.

H. T. Engström.

[1] Publikation in einer amerikanischen Zeitschrift in Vorbereitung.

W. Grunwald.

[1] Charakterisierung des Normenrestsymbols durch die $\mathfrak{p}$-Stetigkeit, den vorderen Zerlegungssatz und die Produktformel, Math. Annalen **107** (1932).

[2] Ein allgemeines Existenztheorem für algebraische Zahlkörper, erscheint demnächst im Journ. f. d. reine u. angew. Math.

H. Hasse.

[1] Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, Journ. f. d. reine u. angew. Math. **152** (1923).

[2] Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper, Journ. f. d. reine u. angew. Math. **153** (1924).

[3] Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols, Journ. f. d. reine u. angew. Math. **162** (1930).

[4] Die Normenresttheorie relativ-abelscher Zahlkörper als Klassenkörpertheorie im Kleinen, Journ. f. d. reine u. angew. Math. **162** (1930).

[5] Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, Math. Annalen **104** (1931).

[6] Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol, Nachr. v. d. Ges. d. Wiss. Göttingen 1931.

[7] Theorie der zyklischen Algebren über einem algebraischen Zahlkörper, Nachr. v. d. Ges. d. Wiss. Göttingen 1931.

[8] Theory of cyclic algebras over an algebraic number field (Abschnitt I siehe auch schon in Hasse [7]), Trans. Amer. Math. Soc. **34** (1932).

[9] Beweis eines Hauptsatzes in der Theorie der Algebren (gemeinsam mit Brauer und Noether), Journ. f. d. reine u. angew. Math. **167** (1932).

[10] Siehe Albert [11].

K. Hensel.

[1] Eine neue Theorie der algebraischen Zahlen, Math. Zeitschr. 2 (1918).

G. Köthe.

[1] Erweiterung des Zentrums einfacher Algebren, erscheint in den Math. Annalen anschließend an diese Arbeit.

E. Noether.
[1] Über minimale Zerfällungskörper irreduzibler Darstellungen (gemeinsam mit R. Brauer), Sitzungsber. d. Akad. Berlin 1927.
[2] Hyperkomplexe Größen und Darstellungstheorie, Math. Zeitschr. **30** (1931).
[3] Siehe Hasse [9].
[4] Vorlesungen, insbesondere die Vorlesungsausarbeitung vom W. S. 1929/30, Seminare, zahlreiche Unterhaltungen mit ihrem Freundeskreis, insbesondere mit dem Verfasser, sowie Briefe an diesen, 1929—1932.
[5] Nichtkommutative Algebra, erscheint demnächst in der Math. Zeitschr.

F. K. Schmidt.
[1] Zur Klassenkörpertheorie im Kleinen, Journ. f. d. reine u. angew. Math. **162** (1930).

A. Speiser.
[1] Allgemeine Zahlentheorie (siehe auch in Dickson [3]), Vierteljahrsschr. d. Naturf. Ges. Zürich 1926.

B. L. v. d. Waerden.
[1] Moderne Algebra, II, Berlin 1931.

J. H. M. Wedderburn.
[1] On hypercomplex numbers, Proc. of the London Math. Soc. **6** (1909).
[2] On division algebras, Trans. Amer. Math. Soc. **22** (1921).

Marburg, März 1932.

(Eingegangen am 23. 3. 1932.)