# Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und Zahlentheorie

Von Emmy Noether, Göttingen

1. Die Theorie der hyperkomplexen Systeme, der Algebren, hat in den letzten Jahren einen starken Aufschwung genommen; aber erst in allerneuester Zeit ist die Bedeutung dieser Theorie für kommutative Fragestellungen klar geworden. Über diese Bedeutung des Nichtkommutativen für das Kommutative möchte ich heute berichten: und zwar will ich das im einzelnen verfolgen an zwei klassischen, auf Gauss zurückgehenden Fragestellungen, dem Hauptgeschlechtssatz und dem eng damit verbundenen Normensatz. Diese Fragestellungen haben sich im Laufe der Zeit in ihrer Formulierung immer wieder gewandelt: bei Gauss treten sie auf als Abschluss seiner Theorie der quadratischen Formen; dann spielen sie eine wesentliche Rolle in der Charakterisierung der relativ zyklischen und abelschen Zahlkörper durch die Klassenkörpertheorie, und schliesslich lassen sie sich aussprechen als Sätze über Automorphismen und über das Zerfallen von Algebren, und diese letztere Formulierung gibt dann zugleich eine Übertragung der Sätze auf beliebige relativ galoissche Zahlkörper.

Mit dieser Skizze, die ich später ausführen werde, möchte ich zugleich das *Prinzip* der Anwendung des Nichtkommutativen auf das Kommutative erläutern: *Man sucht vermöge der Theorie der Algebren invariante und einfache Formulierungen für bekannte Tatsachen über quadratische Formen oder zyklische Körper zu gewinnen, d. h. solche Formulierungen, die nur von Struktureigenschaften der Algebren abhängen. Hat man einmal diese invarianten Formulierungen bewiesen* – und das ist in den oben angegebenen Beispielen der Fall – *so ist damit von selbst eine Übertragung dieser Tatsachen auf beliebige galoissche Körper gewonnen.*

2. Vor einer Einzelausführung möchte ich noch einen allgemeinen Überblick über die verschiedenen Methoden und die weiteren Resultate geben. Vorerst ist zu bemerken, dass die Hauptschwierigkeit in der Gewinnung der Formulierung für allgemeine galoissche Körper liegt, wozu ohne die hyperkomplexe Methode gar kein Ansatzpunkt vorhanden war; in den angeführten Beispielen ist der zugrunde liegende Übergang zum Nichtkommutativen gewonnen durch die *gleichzeitige Betrachtung von Körper und Gruppe* vermöge des „verschränkten Produkts" und seiner Multiplikationskonstanten, der „Faktorensysteme" (vgl. 3). Man erhält so eine einfache normale Algebra über dem Grundkörper und jede solche Algebra ist im wesentlichen so erzeugbar. Solche verschränkte Produkte sind zuerst von Dickson

betrachtet worden[1]), während sich die Theorie der Faktorensysteme durch Speiser, Schur, R. Brauer[2]) von ganz anderem Ausgangspunkt her entwickelt hatte, von der Frage der absolut irreduziblen Darstellungen. Erst durch die Verschmelzung beider Theorien liess sich ein genügend einfacher und weitreichender Aufbau erzielen, um kommutative Fragen damit angreifen zu können[3]).

Dabei ergeben sich zugleich auch für bekannte Tatsachen neue und durchsichtige Beweise: ich möchte hier auf einen bald in den Math. Ann. erscheinenden hyperkomplexen Beweis des Reziprozitätsgesetzes für zyklische Körper hinweisen, den H. Hasse gegeben hat[4]), vermöge einer invarianten Formulierung seines Normenrestsymbols, auf der Theorie des verschränkten Produkts beruhend. Und weiter auf eine hyperkomplexe Begründung der Klassenkörpertheorie im Kleinen, auf derselben Grundlage beruhend, die neuerdings C. Chevalley gegeben hat, wobei aber noch neue algebraische Sätze über Faktorensysteme zu entwickeln waren[5]). Zugleich muss ich aber doch einschränkend bemerken, dass die Methode der verschränkten Produkte allein allem Anschein nach *nicht* die volle Theorie der galoisschen Zahlkörper ergibt. Das folgt aus neuen noch unpublizierten Resultaten von Artin, die an den obigen Beweis von Hasse im Sinn des angegebenen Prinzips anschliessen, aber nur Anzahlgleichheiten an Stelle von vollen Isomorphiesätzen ergeben.

Methoden, die eine volle Isomorphie – allerdings Operatorisomorphie – ergeben, hat man nun schon im Algebraischen. Es handelt sich um die Fortführung von Ansätzen von A. Speiser[6]) und zwar um die Auffassung des galoischen Körpers als „Galoismodul", d. h. als eines Moduls nach dem Grundkörper, der die Substitutionen der galoisschen Gruppe als Operatoren gestattet. Und es besteht Operatorisomorphie zwischen Körper und Gruppenring (Gruppenalgebra) in dem Sinn, dass eindeutiges Entsprechen zwischen den Elementen statthat derart, dass Linearformen nach dem Grundkörper sich entsprechen, und dass den Substitutionen der galoisschen Gruppe im Körper die Multiplikation im Gruppenring zugeordnet ist. Diesen von mir aufge-

[1]) Vgl. sein Buch „Algebren und ihre Zahlentheorie", Zürich 1927, § 34.

[2]) Vgl. etwa *R. Brauer* „Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen", und die dort Anm. 2 angegebene Literatur, Math. Ztschr. 28 (1928).

[3]) Diesen Aufbau habe ich zuerst in einer Vorlesung Winter 1929/30 entwickelt, wiedergegeben in Kap. 2 von *H. Hasse* Theory of cyclic algebras, Transac, 134 (1932). Über das ganze in dem Vortrag behandelte Gebiet orientiert ein Bericht von *M. Deuring* über hyperkomplexe Zahlen und zahlentheoretische Anwendungen, der in der Sammlung „Ergebnisse der Mathematik" erscheinen soll.

[4]) *H. Hasse,* Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper (insbesondere Normenrestsymbol und Reziprozitätsgesetz). Math. Ann. 107 (1932/33).

[5]) *C. Chevalley,* Sur la théorie du symbole de restes normiques; wird im J. f. Math. 169 erscheinen.

[6]) *A. Speiser,* Gruppendeterminante und Körperdiskriminante. Math. Ann. 77 (1916).

stellten Satz[7]) hat M. Deuring bewiesen[8]), der darauf einen Beweis der galoisschen Theorie gegründet hat, wobei die Operatorisomorphie die Zuordnung von Gruppe und Körper realisiert. Weitergehende Struktursätze – ebenfalls von Deuring – laufen formalen Tatsachen der Artinschen L-Reihen parallel und ergeben einen strukturmässigen Zugang zu den Artinschen Führern. Diese Artinschen L-Reihen und Führer[9]), die mit allgemeinen Gruppencharakteren gebildet sind, stellen neben Speiser[6]) die erste Verbindung von Zahlentheorie und Darstellungstheorie dar, einen ersten Vorstoss über die abelschen Körper hinaus. Sie haben der ganzen Entwicklung einen starken Impuls gegeben, insbesondere hat sich die Theorie der Galoismoduln daran orientiert.

3. Ich möchte jetzt die an die Spitze gestellten Probleme, Normensatz und Hauptgeschlechtsatz im einzelnen verfolgen. Zuerst die *Definition des verschränkten Produkts:* Es sei $K/k$ ein galoisscher Körper $n$-ten Grads, $\mathfrak{G}$ seine Gruppe. Das verschränkte Produkt bedeutet eine gleichzeitige Einbettung von $K$ und $\mathfrak{G}$ in eine Algebra $A$ derart, dass die Automorphismen von $K$ innere werden. Es mögen $u_{S_1}, \ldots, u_{S_n}$ Symbole bedeuten, die den $n$ Gruppenelementen entsprechen; dann setzt man $A$ zuerst als Linearformenmodul vom Rang $n$ nach $K$ an:

(1) $A = u_{S_1}K + \ldots + u_{S_n}K$ (d. h. $A$ besteht aus allen Linearformen $u_{S_1}a_1 + \ldots + u_{S_n}a_n$ mit $a_i$ beliebig in $K$).

Vermöge der Forderung des inneren Automorphismus – erzeugt durch die $u_S$, allgemeiner $u_S K^*$[10]) – wird $A$ zu einem Ring, also zu einer Algebra vom Rang $n^2$ über $k$. Die Forderung drückt sich nämlich aus durch

(2) $u_S^{-1} z u_S = z^S$[11]) oder $z u_S = u_S z^S$ für jedes $z$ aus $K$.

(3) $u_S u_T = u_{ST}\, a_{S,T}$ mit $a_{S,T}$ in $K^*$

(4) $a_{ST,R}\, a_{S,T}^R = a_{S,TR}\, a_{T,R}$ (Assoziativgesetz aus $[u_S u_T]\, u_R = u_S\, [u_T u_R]$)

$A$ heisst das verschränkte Produkt von $K$ mit $\mathfrak{G}$ bei Faktorensystem $a_{S,\,T}$; man beweist, dass $A$ eine einfache normale Algebra über $k$ wird, also ein Matrizenring $r$-ten Grads $D_r$ über der zugeordneten Divisionsalgebra $D$, und dass $K$ maximaler kommutativer Unterkörper, also Zerfällungskörper wird (d. h. die Erweiterung des Koeffizientenbereichs $k$ mit einem zu $K$ isomorphen Körper ergibt eine *zerfallende* Algebra, einen vollen Matrizenring über dem Zentrum). Umgekehrt gibt es zu vor-

[7]) *E. Noether*, Normalbasis bei Körpern ohne höhere Verzweigung, Satz 3, J. f. Math. 167 (1932) (der Beweis enthält eine Lücke).

[8]) *M. Deuring*, Galoissche Theorie und Darstellungstheorie. Math. Ann. 107 (1932).

[9]) *E. Artin*, Über eine neue Art von L-Reihen, Math. Sem. Hamburg 3 (1924). Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren, ebenda, 8 (1931). Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, J. f. M. 164 (1931).

[10]) $K^*$ entsteht aus $K$ durch Weglassung der Null; diese Bezeichnung wird allgemein benutzt.

[11]) $z^S$ bedeutet wie üblich das durch die Substitution $S$ aus $z$ entstehende Element.

gegebener Divisionsalgebra $D$ immer Matrizenringe $D_r$, die auf die angegebene Art als verschränktes Produkt erzeugbar sind.

Geht man von $u_S$ zu $v_S = u_S c_S$ mit $c_S$ in $K^*$ über, was denselben Automorphismus erzeugt, so entstehen ,,assoziierte" Faktorensysteme.

(5) $\bar{a}_{S,T} = a_{S,T} c_S^T c_T / c_{ST}$.

Assoziierte Faktorensysteme werden in eine Klasse $(a)$ zusammengefasst, ebenso fasst man alle zu $A$ ähnlichen Algebren, d.h. alle $D_r$ mit $r = 1, 2, \ldots$ in eine Klasse $\mathfrak{A}$ zusammen. *Die Klassen* $\mathfrak{A}$ *und* $(a)$ *entsprechen sich ein-eindeutig: die Klassen mit festem Zerfällungskörper K bilden gegenüber direkter Produktbildung eine abelsche Gruppe, die isomorph ist dem gliedweisen Produkt der Klassen von Faktorensystemen. Einselement ist die zerfallende Algebrenklasse bezw. das System aller Transformationsgrössen* $c_S^T c_T / c_{ST}$. Es handelt sich um die von R. Brauer bemerkte Gruppe der Algebrenklassen.

4. Ich will jetzt durch *Spezialisierung* auf *zyklische Zerfällungskörper* auf den Zusammenhang mit dem *Normbegriff* kommen, und damit auf die Formulierung des verallgemeinerten *Normensatzes* nach dem zu Anfang auseinandergesetzten Prinzip. Ist $Z$ zyklisch, $S$ eine erzeugende Substitution seiner Gruppe – die zugehörige Algebra wird dann als zyklisch bezeichnet – so kann man den Potenzen von $S$ die Potenzen von $u$ entsprechen lassen, also

(1') $A = Z + uZ + \ldots + u^{n-1}Z$
(2') $zu = uz^S$
(3') $u^n = a$
(4') $a$ liegt im Grundkörper $k^*$
(5') $\bar{a} = a . N(c)$, wenn $v = uc$ gesetzt.

Jedes Faktorensystem besteht also hier aus einem einzigen im Grundkörper gelegenen Element $a$ – Bezeichnung $A = (a, Z)$ –; die Einsklasse der Faktorensysteme ist durch die *Normen aus* $Z^*$ gegeben, die Gruppe der Algebrenklassen wird isomorph der Faktorgruppe $k^*/N(Z^*)$. Eine zyklische Algebra $(a, Z)$ zerfällt also dann und nur dann, wenn $a$ Norm eines Elements aus $Z$. Dieser Zusammenhang zwischen Norm und Zerfallen gibt die Formulierung des ,,Normensatzes", nämlich den *Satz über die zerfallenden Algebren: Zerfällt eine Algebra an jeder Stelle, so zerfällt sie schlechthin.* Dabei ist die ,,Stelle", wie in der Zahlentheorie üblich, dadurch definiert, dass der Grundkörper $k$ durch seine $\mathfrak{p}$-adische Erweiterung $k_\mathfrak{p}$ ersetzt wird, wo $\mathfrak{p}$ ein Primideal aus $k$ (bezw. den endlichvielen unendlichen Stellen entsprechend, dass $k$ und seine Konjugierten mit dem Körper der reellen Zahlen erweitert werden).

In der Tat ist darin der Normensatz für zyklische Körper enthalten. Denn für zyklische Algebren $(a, Z)$ ist nach dem oben gesagten der Satz gleichbedeutend mit der Aussage: Ist $a$ an jeder (endlichen oder unendlichen) Stelle $\mathfrak{p}$-adische Norm, so ist $a$ Norm einer Zahl aus Z, oder ohne Übergang zum $\mathfrak{p}$-adischen: *Ist $a$ Normenrest nach jedem Primideal $\mathfrak{p}$ aus $k$ (und genügt gewissen Vorzeichenbedingungen), so ist $a$ Norm einer Zahl aus $Z$.* Diese letztere Fassung ist aber der Normensatz, der in der Klassenkörpertheorie bewiesen wird, unter Benutzung der bekannten analytischen Hilfsmittel. Und der Beweis des allgemeinen Satzes über zerfallende Algebren lässt sich aus diesem zyklischen Spezialfall durch rein algebraisch-arithmetische Betrachtungen gewinnen[12]). Eine erste wichtige Folgerung hat Hasse gezogen: *Jede einfache normale Algebra über einem algebraischen Zahlkörper ist zyklisch.* Auf der Suche nach einem Beweis dieser lange vermuteten Tatsache entstand die allgemeine Formulierung.

5. Eine zweite Folgerung aus dem Satz über zerfallende Algebren – wieder mit rein algebraisch-arithmetischen Schlussweisen – ist der an die Spitze gestellte *Hauptgeschlechtssatz*[13]). Seine invariante Formulierung beruht auf der Tatsache, dass die das verschränkte Produkt definierenden Relationen (2) bis (5) rein multiplikativ sind, also sinnvoll bleiben, wenn $K^*$ durch eine abelsche Gruppe $\mathfrak{J}$ ersetzt wird, die nur der Bedingung genügt, dass ihre Automorphismengruppe eine zu $\mathfrak{G}$ isomorphe Untergruppe enthält. An Stelle von (1) tritt dann die „Erweiterung von $\mathfrak{G}$ mit $\mathfrak{J}$" im Sinne der Gruppentheorie. Nimmt man für $\mathfrak{J}$ die Gruppe aller Ideale aus $K$, so werden also die Faktorensysteme Systeme von Idealen; eine Klasseneinteilung in $\mathfrak{J}$ induziert eine Klasseneinteilung für die Faktorensysteme, und zwar wird das im allgemeinen eine feinere Idealklasseneinteilung, als die ursprüngliche. Denn die Forderung, dass die Multiplikation der $u_S$ mit (absoluten) Idealklassen eindeutig ist, sagt nur aus, dass die Transformationsgrössen $c_S^T c_T / c_{ST}$ – die Einsklasse der Elementfaktorensysteme – in der Einsklasse der Idealfaktorensysteme liegen. Tatsächlich genügt aber, wie die Spezialisierung auf die bekannten Fälle zeigt, schon eine etwas weniger feine Einteilung. Ich definiere: *In die Einsklasse der Faktorensysteme werden diejenigen Elemente $a_{S,\,T}$ gerechnet, die an allen (endlichen und unendlichen) Verzweigungsstellen von $K$ zerfallende Algebren erzeugen.* Die so entstehende Erweiterung von $\mathfrak{G}$ werde mit $\mathfrak{G}^*$ bezeichnet; $(\mathfrak{c})$ bedeute die absolute Idealklasse von $\mathfrak{c}$. Dann lautet die

*Invariante Formulierung des Hauptgeschlechtssatzes: Entsteht bei der so definierten Klasseneinteilung durch die Substitution $v_S = u_S(\mathfrak{c}_S)$ ein Automorphismus von $\mathfrak{G}^*$ – alle diese $(\mathfrak{c}_S)$ bilden das Hauptgeschlecht –, so ist der Automorphismus ein innerer und wird durch eine Idealklasse $(\mathfrak{b})$ erzeugt.*

Die bekannten Spezialfälle folgen aus einer gleichwertigen, etwas mehr expliziten Formulierung: *Gehören die aus den Idealklassen $(\mathfrak{c}_S)$ gebildeten Transformations-*

[12]) *R. Brauer, H. Hasse, E. Noether,* Beweis eines Hauptsatzes in der Theorie der Algebren. J. f. M. 167 (1932).

[13]) Der Beweis soll in den Math. Ann. erscheinen.

*grössen* $(\mathfrak{c}_S^T)\ (\mathfrak{c}_T)/(\mathfrak{c}_{ST})$ *der Einsidealklasse der Faktorensysteme an, so gibt es eine Idealklasse* $(\mathfrak{b})$, *derart, dass die* $(\mathfrak{c}_S)$ *symbolische* $(1-S)$*te Potenzen werden:* $(\mathfrak{c}_S) = (\mathfrak{b})\ /\ (\mathfrak{b}^S)$ *für alle* $S$ *aus* $\mathfrak{G}$. Denn die Voraussetzung drückt gerade die Automorphismeneigenschaft aus; die Tatsache, dass dieser ein innerer, drückt sich aus durch $v_S = (\mathfrak{b})^{-1}$ $u_S(\mathfrak{b}) = u_S(\mathfrak{b})^{1-S} = u_S(\mathfrak{c}_S)$.

Die Spezialisierung auf den zyklischen Fall ergibt also (unter Beachtung der Normierung): Liegt $N([\mathfrak{c}])$ in der Einsidealklasse der Faktorensysteme, so wird $(\mathfrak{c})$ symbolische $(1-S)$te Potenz: $(\mathfrak{c}) = (\mathfrak{b})^{1-S}$.

6. Um von hier aus auf die bekannte Fassung für zyklische Körper und quadratische Formen zu gelangen, bemerke ich vorerst, dass der Satz für die vollen Idealklassen ausgesprochen ist, sein Inhalt aber derselbe bleibt, wenn man sich wie üblich auf zu den Verzweigungsstellen prime Ideale beschränkt.

Damit geht aber das hier definierte Hauptgeschlecht für quadratische Körper in das Gausssche über; denn den Idealklassen entsprechen die quadratischen Formen, den Normen der Klassen die durch die Formen darstellbaren Zahlen. Dass die Einsklasse die an den Verzweigungsstellen von $K$ zerfallenden Algebren erzeugt, heisst also dass diese darstellbaren Zahlen an den Verzweigungsstellen quadratische Reste werden; die zugehörigen Formen besitzen somit den Totalcharakter der Hauptform, bilden also das Gausssche Hauptgeschlecht. Dass die $(1-S)$te symbolische Potenz in die Duplikation übergeht, ist bekannt.

Für zyklische Körper geht die Fassung in die folgende über: Das Hauptgeschlecht besteht aus allen Idealklassen, deren Normen an den (endlichen und unendlichen) Verzweigungsstellen Normenreste werden. Das ist aber bekanntlich gleichbedeutend mit „Normenrest nach dem Führer", und somit entsteht der übliche Satz als Spezialisierung.

Übrigens kann man auch im allgemeinen Fall beliebiger galoisscher Körper einen nur aus den Verzweigungsstellen zusammengesetzten Führer einführen derart, dass bei Normierung der Faktorensysteme für jede dieser Stellen, der Strahl nur Elemente der Einsklasse enthält.

Hier entsteht die Frage nach dem Zusammenhang mit den im Überblick 2 erwähnten Artinschen Führern, die ja aus denselben Primidealen zusammengesetzt sind; und damit die Frage nach dem Zusammenhang mit der Theorie der Galoismoduln, der zweiten hyperkomplexen Methode. Wie weit diese beiden Methoden reichen werden, muss erst die Zukunft zeigen.