Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

fortgeführt von

C. W. Borchardt, K. Weierstrass, L. Kronecker,
L. Fuchs, K. Hensel, L. Schlesinger

gegenwärtig herausgegeben von

Helmut Hasse

unter Mitwirkung von

W. Brödel, M. Deuring, O. Haupt,
G. Köthe, H. Rohrbach, W. Schmeidler

Band 189

In 4 Heften

Walter de Gruyter & Co.
vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlagsbuchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.
Berlin 1952

Inhaltsverzeichnis des Bandes 189

Seite

Armsen, Paul, Verallgemeinerungen von Sequenzen in Permutationen 77

Hornich, Hans, Zur Lösbarkeit von gewissen elliptischen Differentialgleichungen 204

Jaeckel, K., Über die Eigenlösungen gewisser Integralgleichungen der Potentialtheorie 141

Jonas, Hans, Die allgemeinen äquidistanten Transformationen der von Bianchi entdeckten isometrischen Paare Tschebyschefscher Netze 207

Kanold, Hans-Joachim, Über ein spezielles System von zwei diophantischen Gleichungen 243

Kasch, Friedrich, Über den Satz vom primitiven Element bei Schiefkörpern . . 150

Kropp, Gerhard, Lalouvères Quadratura circuli 1

Krull, Wolfgang, Zur Arithmetik der endlichen diskreten Hauptordnungen . . . 118

Lyra, Gerhard, Über eine Konvergenzfrage bei der Auflösung linearer Differentialgleichungen in der Umgebung einer Stelle der Bestimmtheit 238

Mohr, Ernst, Die Konstruktion der Greenschen Funktion im erweiterten Sinne . 129

— —, Nachtrag zu meiner Arbeit: Beweis des sogenannten Fundamentalsatzes der Algebra im reellen Gebiete 250

Nakayama, Tadasi, On construction and characterization of Galois algebras with given Galois groups 100

Reeb, G., Sur les éléments de contact linéaires du second ordre attachés à un système différentiel 186

Sade, Albert, Omission dans les listes de Norton pour les carrés $7 \cdot 7$ 190

Schmidt, Adam, Lineare partielle Differentialgleichungen mit konstanten Koeffizienten 160

Schöneborn, Heinz, Über Linearformenmoduln unendlichen Ranges. I 168

— —, Über Linearformenmoduln unendlichen Ranges. II 193

Tietz, Horst, Eine Rekursionsformel der Faberschen Polynome 192

— —, Beweis der Konvergenz eines Verfahrens von W. Bartky zur Berechnung von bestimmten Integralen 246

Über den Satz vom primitiven Element bei Schiefkörpern.

Von *Friedrich Kasch* in Münster[1]).

I. Problemstellung und Ergebnisse.

Der Satz vom primitiven Element lautet für kommutative Körper bekanntlich folgendermaßen:

Eine endliche, separable Erweiterung eines kommutativen Körpers kann stets durch Adjunktion eines geeigneten Elementes erzeugt werden.

Diesen Satz hat man in der historischen Entwicklung der Galoisschen Theorie zunächst als wesentliches Beweismittel herangezogen, dann aber schrittweise festgestellt, daß man ihn bei ihrem Aufbau vermeiden kann. Gerade diese Entwicklung hat es zu einem wesentlichen Teil erst ermöglicht, die Galoissche Theorie auf Schiefkörper zu übertragen, wie dies in jüngster Zeit von Jacobson[2]) und Cartan[3]) durchgeführt worden ist. Man kann sich nun nachträglich fragen, was sich aus der nichtkommutativen Galoisschen Theorie für den Satz vom primitiven Element folgern läßt. Von diesem Standpunkt aus wird man sich bei der Beantwortung der aufgeworfenen Frage auf galoissche Erweiterungen beschränken, die im kommutativen Fall separabel sind. Man bezeichnet bekanntlich einen Schiefkörper L als eine *galoissche Erweiterung* des Grundschiefkörpers H, wenn der Schiefkörper, der aus allen den Elementen aus L besteht, die bei den Automorphismen von L über H einzeln fest bleiben, mit H übereinstimmt.

Zunächst ist klar, daß man den Satz vom primitiven Element nicht wörtlich auf das Nichtkommutative übertragen kann. Betrachtet man zum Beispiel einen Schiefkörper L endlichen Ranges über seinem Zentrum Z, der bekanntlich galoissch über Z ist, so erhält man durch Adjunktion eines beliebigen Elementes aus L zu Z nur jeweils einen kommutativen Oberkörper von Z, also keinesfalls L.

Der neue Satz, der im kommutativen Spezialfall mit dem bekannten Satz vom primitiven Element übereinstimmt, lautet folgendermaßen:

Ist L galoissche Erweiterung endlichen Ranges des Grundschiefkörpers H und ist das Zentrum des Transformatorenkörpers von L über H separabel über dem Zentrum von L,

[1]) Diese Arbeit in stilistisch anderer Fassung wurde von der Mathematisch-Naturwissenschaftlichen Fakultät der Universität zu Münster/Westf. als Dissertation angenommen.

[2]) *N. Jacobson*, A note on division rings, Amer. Journal of Math. **69** (1947), 27—36.

[3]) *H. Cartan*, Théorie de Galois pour les corps non commutatifs, Ann. Éc. Norm. (3) **64** (1947), 59—77.

so besitzt L zwei erzeugende Elemente über H:

$$L = H(a, a'),$$

die bezüglich eines inneren Automorphismus konjugiert sind[3a]).

Dabei versteht man unter dem *Transformatorenkörper* von L über H die Gesamtheit der Elemente aus L, die innere Automorphismen von L über H erzeugen, zuzüglich des Elementes Null von L, also der Elemente aus L, die mit allen Elementen aus H einzeln vertauschbar sind.

Daraus folgt, daß bei jedem kommutativen Körper L die angegebene Separabilitätsvoraussetzung erfüllt ist. Diese stellt also nicht eine Verallgemeinerung der Separabilitätsvoraussetzung dar, die im Kommutativen für die Existenz eines primitiven Elementes notwendig ist. Die Voraussetzung, daß L über H galoissch ist, schließt vielmehr definitionsgemäß im kommutativen Fall die Separabilität von L über H ein.

Da bei einem kommutativen Körper L jeder innere Automorphismus mit dem identischen übereinstimmt, ist dann $a = a'$ und man erhält den bekannten Satz vom primitiven Element zurück.

Die Voraussetzungen des Satzes sind z. B. erfüllt, wenn L Schiefkörper endlichen Ranges über seinem Zentrum Z ist. Der Transformatorenkörper von L über Z ist in diesem Falle L selbst.

Der Beweis für den angegebenen Satz zerfällt in zwei Teile. Im ersten Teil wird ein geeigneter Zwischenkörper M zwischen H und L herausgegriffen, der über H ein erzeugendes Element besitzt, $M = H(a)$. Als geeignet erweist sich ein maximaler Zwischenkörper M ohne innere Automorphismen über H.

Der Nachweis eines solchen Zwischenkörpers M fällt im Spezialfall einer Erweiterung L endlichen Ranges über ihrem Zentrum Z mit der bekannten Tatsache zusammen, daß man aus L einen maximalen kommutativen Unterkörper herausgreifen kann, der über Z separabel ist und folglich ein erzeugendes Element über Z besitzt.

Die Automorphismengruppe von L über einem maximalen Zwischenkörper ohne innere Automorphismen über H hat eine besonders einfache Struktur: Sie enthält nur innere Automorphismen mit kommutativem Transformatorenkörper.

Diese Tatsache ermöglicht im zweiten Teil des Beweises den Nachweis eines zu a bezüglich eines inneren Automorphismus konjugierten, erzeugenden Elementes a' von L über M. Dabei wird die angegebene Separabilitätsvoraussetzung benutzt.

II. Vorbereitungen.

1. Halbkommutative Polynomringe. Unter einem *halbkommutativen Polynomring* $L[x]$ verstehen wir einen Polynomring mit Koeffizienten aus einem nicht notwendig kommutativen Körper L[4]) in der Unbestimmten x, die mit den Elementen aus L kommutativ verbunden ist.

Bei den weiteren Überlegungen werden halbkommutative Polynomringe herangezogen. Wir stellen daher vorweg die folgenden einfachen Tatsachen zusammen, deren Beweis ebenso wie im kommutativen Fall erfolgt:

1. In $L[x]$ können der rechts- und linksseitige Euklidische Algorithmus durchgeführt werden. Folglich ist $L[x]$ Hauptidealring und es existiert der Quotientenkörper $L(x)$.

[3a]) Anmerkung bei der Korrektur. Es wurde mir eine Arbeit von *A. A. Albert* bekannt [Two element generation of a separable algebra, Bull. Amer. Math. Soc. **50** (1944), 786—788], in der gezeigt wird, daß jede separable Algebra zwei erzeugende Elemente besitzt, jedoch nicht, daß es zwei *konjugierte* erzeugende Elemente gibt. Durch eine Kombination der Überlegung von *A. A. Albert* und des obigen Satzes kann gezeigt werden, daß jede separable Algebra ebenfalls zwei konjugierte erzeugende Elemente enthält.

[4]) Im folgenden wollen wir stets unter der Bezeichnung *Körper* sowohl kommutative als auch Schiefkörper verstehen.

2. Eine Identität zwischen Polynomen aus $L[x]$ geht bei Einsetzung eines Elementes aus dem Zentrum Z von L für x in eine Gleichung zwischen den durch diese Einsetzung entstehenden Elemente über.

3. Aus 1. und 2. folgt, daß ein Polynom aus $L[x]$ nur endlich viele Nullstellen in Z besitzt.

4. Betrachtet man Z als Argumente- und L als Wertebereich, so kann man in $L[x]$ die Lagrangesche Interpolationsformel einführen: Zu n verschiedenen Elementen $z_1, z_2, \ldots, z_n$ aus Z und n beliebigen Elementen $t_1, t_2, \ldots, t_n$ aus L gibt es ein Polynom höchstens $(n-1)$-ten Grades $T(x)$ in $L[x]$, welches an den Stellen z_i die Werte t_i besitzt. $T(x)$ ist gegeben durch

$$T(x) = P(x) \sum_{i=1}^{n} \frac{t_i}{(x-z_i)P'(z_i)}$$

mit

$$P(x) = (x-z_1)(x-z_2)\cdots(x-z_n), \quad P'(z_i) = (z_i-z_1)\cdots(z_i-z_{i-1})(z_i-z_{i+1})\cdots(z_i-z_n).$$

2. Hilfsmittel aus der Galoisschen Theorie. Es sollen hier diejenigen Ergebnisse aus der Galoisschen Theorie zusammengestellt werden, die wir bei den weiteren Überlegungen benutzen. Dabei setzen wir das allgemeine Schema der Galoisschen Theorie als bekannt voraus.

a) Zunächst führen wir einige Bezeichnungen ein. Gegeben sei ein beliebiger Körper L und eine Automorphismengruppe $\mathfrak{H}$ von L. Die Elemente aus L, die bei allen Automorphismen aus $\mathfrak{H}$ fest bleiben, bilden einen Unterkörper von L, den wir den zu $\mathfrak{H}$ gehörigen *Fixkörper* nennen.

Die in $\mathfrak{H}$ enthaltenen inneren Automorphismen bilden einen Normalteiler von $\mathfrak{H}$. Ein Element aus L, welches einen in $\mathfrak{H}$ enthaltenen inneren Automorphismus erzeugt, heißt ein zu $\mathfrak{H}$ gehöriger *Transformator*.

Besteht die Menge der zu $\mathfrak{H}$ gehörigen Transformatoren aus den von Null verschiedenen Elementen eines Unterkörpers von L, so heißt $\mathfrak{H}$ eine *ausgezeichnete Automorphismengruppe*.

Geht man von einem beliebigen Unterkörper H von L aus, so ist die Gruppe $\mathfrak{G}_H^L$ aller Automorphismen von L über H, selbstverständlich ausgezeichnet, denn die mit den Elementen aus H einzeln vertauschbaren Elemente aus L bilden einen Unterkörper von L. Die in $\mathfrak{G}_H^L$ enthaltene Untergruppe der inneren Automorphismen bezeichnen wir mit $\mathfrak{T}_H^L$ und den zugehörigen Transformatorenkörper mit T_H^L.

Unter Z_L verstehen wir das Zentrum des Körpers L.

Es sei jetzt L galoissche Erweiterung endlichen Ranges von H und K ein Zwischenkörper zwischen H und L. Dann gilt[5]):

(1) Die Galoisgruppe $\mathfrak{G}_H^L$ von L über H ist ausgezeichnet.

(2) Zwischen dem Rang r von L über H, dem Index d von $\mathfrak{T}_H^L$ in $\mathfrak{G}_H^L$ und dem Rang n von T_H^L über Z_L besteht die Beziehung

$$r = d \cdot n.$$

(3) Jeder Zwischenkörper K ist galoisscher Unterkörper von L, und die Galoisgruppe von L über K ist ausgezeichnete Untergruppe von $\mathfrak{G}_H^L$. Umgekehrt ist jede ausgezeichnete Untergruppe von $\mathfrak{G}_H^L$ Galoisgruppe von L über einem Zwischenkörper zwischen H und L. Die Beziehung zwischen den ausgezeichneten Untergruppen und den Zwischenkörpern ist also eineindeutig.

---

[5]) Diese Ergebnisse sind der unter [2]) zitierten Arbeit von *Cartan* entnommen. Wir zitieren sie im folgenden mit $G(1)$ bis $G(5)$.

(4) Wenn ein Isomorphismus eines Zwischenkörpers K innerhalb L die Elemente von H einzeln fest läßt, so kann er zu einem Automorphismus von L über H fortgesetzt werden.

(5) Ist K invariant bei allen Automorphismen aus $\mathfrak{G}_H^L$, d. h. geht K bei allen Automorphismen aus $\mathfrak{G}_H^L$ als Ganzes (nicht notwendig elementweise) in sich über, so ist K galoissche Erweiterung von H. Notwendig und hinreichend für die Invarianz von K ist die Bedingung, daß $\mathfrak{G}_K^L$ Normalteiler von $\mathfrak{G}_H^L$ ist. $\mathfrak{G}_H^K$ ist dann isomorph zur Faktorgruppe $\mathfrak{G}_H^L/\mathfrak{G}_K^L$.

b) Aus diesen Ergebnissen der Galoisschen Theorie leiten wir eine Folgerung her.

Satz 1. *L sei galoissche Erweiterung endlichen Ranges von H und besitze nur innere Automorphismen über H. Ein Zwischenkörper M zwischen H und L ist dann und nur dann maximaler Zwischenkörper ohne innere Automorphismen über H*[6]*, wenn der Transformatorenkörper T_M^L von L über M maximaler kommutativer Unterkörper des Transformatorenkörpers T_H^L von L über H ist.*

Beweis. 1. T_M^L sei maximaler kommutativer Unterkörper von T_H^L. Das Element t erzeuge einen inneren Automorphismus von M über H. Es liegt dann sowohl in M als auch in T_H^L. Da es in M enthalten ist, muß es mit allen Elementen aus T_M^L vertauschbar sein. Daraus folgt, da T_M^L maximaler kommutativer Unterkörper von T_H^L ist und $t \in T_H^L$, daß t bereits in T_M^L liegt. Dann erzeugt es aber nur den identischen inneren Automorphismus von M.

Betrachten wir jetzt ein Element $a \in L$, welches nicht in M liegt. Da L galoissch über M ist, kann a nicht bei allen Automorphismen von L über M fest bleiben, und da die Automorphismen von L über M innere Automorphismen sind, die durch die von Null verschiedenen Elemente aus T_M^L erzeugt werden, gibt es in T_M^L ein Element b, welches mit a nicht vertauschbar ist. Da $\mathfrak{T}_M^L$ Galoisgruppe von L über M und T_M^L kommutativ ist, muß T_M^L in M enthalten sein. Folglich besitzt $M(a)$ den durch b erzeugten, vom identischen verschiedenen inneren Automorphismus. Damit ist M als maximaler Zwischenkörper ohne innere Automorphismen über H erkannt.

2. M sei maximaler Zwischenkörper ohne innere Automorphismen über H. Wir überlegen zunächst, daß T_M^L kommutativ ist. Angenommen, T_M^L wäre nicht kommutativ und u eines seiner Elemente, das nicht in seinem Zentrum liegt. u ist dann nicht in M enthalten, da die Elemente aus M mit allen Elementen aus T_M^L einzeln vertauschbar sind. $M(u)$ ist also ein echter Oberkörper von M innerhalb L. Auf Grund der zu Anfang erwähnten Eigenschaften des halbkommutativen Polynomrings $M[x]$ folgt hier ebenso wie bei einem kommutativen Körper, daß $M(u)$ über M eine Basis aus Potenzen von u besitzt. Dabei ist zu berücksichtigen, daß man u, da es als Element aus T_M^L mit allen Elementen aus M vertauschbar ist, in Polynome aus $M[x]$ einsetzen darf.

Das Element $t \in M(u)$ erzeuge einen inneren Automorphismus von $M(u)$ über H und besitze die Basisdarstellung

$$t = \sum_{i=1}^{n} a_i u^i, \quad a_i \in M.$$

Da t und u mit allen Elementen $h \in H$ vertauschbar sind, besteht die Beziehung

$$\sum_{i=1}^{n} h a_i u^i = \sum_{i=1}^{n} a_i h u^i, \quad h \in H.$$

Wegen der Eindeutigkeit der Basisdarstellung ist dabei

$$h a_i = a_i h,$$

[6]) Der identische innere Automorphismus ist selbstverständlich hier wie auch im folgenden stets zugelassen.

das heißt aber, daß die Elemente a_i im Transformatorenkörper von M über H liegen. Da M nach Voraussetzung keine inneren Automorphismen über H besitzt, sind die Elemente a_i mit allen Elementen aus M vertauschbar. Da auch u mit allen Elementen aus M kommutativ verbunden ist, erzeugt t nur den identischen inneren Automorphismus von $M(u)$. Also ist $M(u)$ ein echter Oberkörper von M ohne innere Automorphismen über H. Damit haben wir einen Widerspruch zur Voraussetzung über M. Folglich muß T_M^L kommutativ sein.

Ist T_N^L ein T_M^L umfassender, maximaler kommutativer Unterkörper von T_H^L und ist N der Fixkörper von $\mathfrak{T}_N^L$, so ist auf Grund der Galoisschen Theorie $N \subseteq M$ und auf Grund des ersten Teils des Beweises N ein maximaler Zwischenkörper ohne innere Automorphismen über H. Da dies für M vorausgesetzt wird, ist $N=M$ und folglich T_M^L ein maximaler kommutativer Unterkörper von T_H^L.

III. Einfache Erweiterungen.

Zur Behandlung der einfachen Erweiterungen ziehen wir einen Hilfssatz heran, der vom Kommutativen her bekannt ist.

Hilfssatz 1. *Gegeben sei ein beliebiger Körper L und ein Unterkörper H von L mit unendlich vielen Elementen. $G_1, G_2, \ldots, G_m$ seien vom identischen verschiedene Isomorphismen von L über H in einen L enthaltenden Oberkörper von H. Dann gibt es ein Element $b \in L$, welches bei keinem der gegebenen Isomorphismen in sich übergeführt wird:*

$$bG_j - b \neq 0 \qquad \text{für } j=1,\ldots,m.$$

Beweis. Der Beweis läßt sich vom Kommutativen unmittelbar übertragen. Der Vollständigkeit halber sei er kurz angegeben.

Da die gegebenen Isomorphismen vom identischen verschieden sind, gibt es zu jedem G_j ein Element $b_j \in L$ mit der Eigenschaft $b_j G_j - b_j \neq 0$. Das gesuchte Element hat dann die Gestalt

$$b = \sum_{i=1}^{m} h_i b_i,$$

wobei die h_i geeignete Elemente aus H sind. Die Forderung, daß b bei den gegebenen Isomorphismen von seinen Konjugierten verschieden sein soll, führt zu den Ungleichungen

$$bG_j - b = \sum_{i=1}^{m} h_i (b_i G_j - b_i) \neq 0 \qquad \text{für } j=1,\ldots,m.$$

Durch Induktion zeigt man nun leicht, daß diese Ungleichungen tatsächlich mit Elementen h_i aus H befriedigt werden können, wobei man einerseits die Voraussetzung benutzt, daß H unendlich viele Elemente enthält, und andererseits die Tatsache, daß in jeder Ungleichung ein von Null verschiedener Koeffizient, $b_j G_j - b_j$, vorkommt.

Diesen Hilfssatz benutzen wir, um eine hinreichende Bedingung für die Existenz eines erzeugenden Elementes aufzustellen.

Satz 2. *Es sei L galoissche Erweiterung endlichen Ranges über dem Grundkörper H mit unendlich vielen Elementen und K ein Zwischenkörper zwischen H und L. Gibt es zwischen $\mathfrak{G}_K^L$ und $\mathfrak{G}_H^L$ nur endlich viele ausgezeichnete Zwischengruppen, so besitzt K ein erzeugendes Element über H:*

$$K = H(b).$$

Beweis. Aus jeder der endlich vielen Zwischengruppen, ausschließlich $\mathfrak{G}_K^L$, einschließlich $\mathfrak{G}_H^L$, greifen wir je einen Automorphismus heraus, der nicht bereits in $\mathfrak{G}_K^L$ liegt. Diese Automorphismen stellen vom identischen verschiedene Isomorphismen von K über H innerhalb L dar. Auf Grund von Hilfssatz 1 gibt es dann ein Element b

in K, welches bei keinem dieser Automorphismen fest bleibt. Als Element aus K bleibt b bei allen Automorphismen aus $\mathfrak{G}_K^L$, aber nicht bei allen Automorphismen aus jeder $\mathfrak{G}_K^L$ echt umfassenden, ausgezeichneten Untergruppe von $\mathfrak{G}_H^L$ fest. Folglich ist $H(b)$ Fixkörper von $\mathfrak{G}_K^L$ und stimmt daher mit K überein: $K=H(b)$.

Wir benutzen diesen Satz, um gewisse einfache Erweiterungen zu charakterisieren.

Satz 3. *L sei galoissche Erweiterung endlichen Ranges von H. Dann gilt:*

1. *Enthält einer der Körper H oder Z_L nur endlich viele Elemente. so besitzt L ein erzeugendes Element über H.*

2. *Der Fixkörper K der Gruppe $\mathfrak{T}_H^L$, der inneren Automorphismen von L über H, besitzt ein erzeugendes Element über H:*

$$K=H(b).$$

Beweis. a) Hat H nur endlich viele Elemente, so auch L als Erweiterung endlichen Ranges. Ein Körper mit endlich vielen Elementen ist aber bekanntlich kommutativ und besitzt ein erzeugendes Element.

b) Hat Z_L nur endlich viele Elemente, so auch T_H^L wegen $(T_H^L:Z_L)<\infty$ (nach $G(2)$). Da der Index von $\mathfrak{T}_H^L$ in $\mathfrak{G}_H^L$ ebenfalls endlich ist, besitzt jetzt $\mathfrak{G}_H^L$ nur endlich viele Automorphismen. Die Behauptung folgt dann aus dem vorhergehenden Satz für $K=L$.

c) Aus der Endlichkeit von $\mathfrak{G}_H^L/\mathfrak{T}_H^L$ entnimmt man ferner, daß es zwischen $\mathfrak{T}_H^L$ und $\mathfrak{G}_H^L$ nur endlich viele ausgezeichnete Zwischengruppen gibt. Dann folgt die Behauptung, $K=H(b)$, ebenfalls aus dem vorhergehenden Satz.

In diesem Satz ist enthalten, daß eine galoissche Erweiterung endlichen Ranges ohne innere Automorphismen ein erzeugendes Element besitzt, denn dann ist $K=L$.

Wir benutzen den soeben konstruierten Fixkörper K der Gruppe der inneren Automorphismen von L über H, um einen maximalen Zwischenkörper M ohne innere Automorphismen über H zu gewinnen, der über H ein erzeugendes Element besitzt. Dazu greifen wir aus dem Transformatorenkörper T_H^L einen über dem Zentrum von T_H^L separablen, maximalen kommutativen Unterkörper heraus, den wir mit T_M^L bezeichnen. Der Fixkörper M der Gruppe $\mathfrak{T}_M^L$, der, wie aus Satz 1 hervorgeht, ein maximaler Zwischenkörper ohne innere Automorphismen über H ist, stimmt überein mit dem Vereinigungskörper von K und T_M^L. Ein erzeugendes Element a von M über H kann als Linearkombination des erzeugenden Elementes b von K über H und eines erzeugenden Elementes c von T_M^L über $Z_{T_H^L}$ mit Koeffizienten aus H gewonnen werden. Dies soll im folgenden Satz nachgewiesen werden.

Satz 4. *L sei galoissche Erweiterung endlichen Ranges von H. Dann gibt es einen maximalen Zwischenkörper M ohne innere Automorphismen über H, der über H ein erzeugendes Element besitzt:*

$$M=H(a).$$

Beweis. Auf Grund des vorhergehenden Satzes ist die Behauptung erfüllt, falls H nur endlich viele Elemente besitzt. Wir setzen daher jetzt voraus, daß H unendlich viele Elemente enthält. Den Beweis führen wir in mehreren Schritten.

1. *Vorbemerkung.* Zum Transformatorenkörper T_H^L gehören genau die Elemente $t\in L$, die mit allen Elementen aus H einzeln vertauschbar sind, für die also

$$ht=th \text{ für alle } h\in H$$

gilt. Übt man auf diese Gleichung einen Automorphismus $G\in\mathfrak{G}_H^L$ aus, so folgt, da die Elemente aus H dabei fest bleiben:

$$h\cdot tG=tG\cdot h \text{ für alle } h\in H,$$

d. h. das Bildelement von t liegt ebenfalls in T_H^L. T_H^L ist also gegenüber den Automorphismen aus $\mathfrak{G}_H^L$ als Ganzes invariant. Genau so ergibt sich, daß auch das Zentrum $Z_{T_H^L}$ von T_H^L bei diesen Automorphismen invariant ist. Daraus folgt, daß der Rang eines Elementes $c \in T_H^L$ über $Z_{T_H^L}$ gleich dem Rang seiner Bildelemente über $Z_{T_H^L}$ bei den Automorphismen aus $\mathfrak{G}_H^L$ ist.

2. Wir betrachten jetzt einen über $Z_{T_H^L}$ separablen, maximalen kommutativen Unterkörper von T_H^L, den wir mit T_M^L bezeichnen. c sei erzeugendes Element von T_M^L über $Z_{T_H^L}$.

Der Fixkörper M von $\mathfrak{T}_M^L$ ist auf Grund von Satz 1 ein maximaler Zwischenkörper ohne innere Automorphismen über K und, da K über H nur äußere Automorphismen besitzt, auch über H.

Wir wollen zeigen, daß das Element c bei den Automorphismen aus $\mathfrak{G}_H^L$ nur endlich viele verschiedene Konjugierte besitzt, die wieder in T_M^L enthalten sind. Auf Grund der Vorbemerkung ist dann klar, daß jedes dieser Konjugierten den Körper T_M^L über $Z_{T_H^L}$ erzeugt. Da $\mathfrak{G}_H^L$ nur endlich viele Klassen nach $\mathfrak{T}_H^L$ besitzt ($G(2)$), genügt es nachzuweisen, daß c bei den Automorphismen aus einer Klasse $G\mathfrak{T}_H^L$ nur endlich viele verschiedene, in T_M^L enthaltene Bildelemente besitzt.

Wir bezeichnen $cG = c'$. Angenommen, es gibt unendlich viele innere Automorphismen $G_i (i = 1,2,\ldots)$, so daß $c'G_i$ verschiedene Elemente aus T_M^L sind. Wir wissen auf Grund der Vorbemerkung:

$$T_M^L = Z_{T_H^L}(c'G_1).$$

Dann erzeugen aber die Automorphismen $G_1^{-1}G_j$ $(j = 2,3,\ldots)$ unendlich viele verschiedene Automorphismen von T_M^L über $Z_{T_H^L}$, denn die Elemente von $Z_{T_H^L}$ bleiben bei diesen inneren Automorphismen selbstverständlich fest. Da T_M^L als kommutative Erweiterung endlichen Ranges von $Z_{T_H^L}$ nur endlich viele verschiedene Automorphismen über $Z_{T_H^L}$ besitzt, haben wir damit einen Widerspruch erhalten. Folglich gibt es bei den Automorphismen aus $\mathfrak{G}_H^L$ nur endlich viele verschiedene Konjugierte von c, die in T_M^L enthalten sind. Diese bezeichnen wir mit

$$c = c_1, \; c_2, \ldots, \; c_r.$$

3. Wir zeigen schließlich:

$$M = H(a) \text{ mit } a = c - hb,$$

wobei b erzeugendes Element von K über H und h ein geeignetes Element aus H ist.

Ist $H = K$, so sei $h = 0$, also $a = c$. Ist $H \subset K$, so wählen wir h folgendermaßen: Sind

$$b, b_1, b_2, \ldots, b_s \; (s \geqq 1),$$

die endlich vielen verschiedenen Konjugierten von b bei den Automorphismen aus $\mathfrak{G}_H^L$ (daß nur endlich viele verschiedene Konjugierte existieren, folgt aus $G(5)$ und $G(2)$, und daß $s \geqq 1$ ist, aus der Voraussetzung $H \subset K$), so sei h ein Element aus H, das von den endlich vielen Lösungen der folgenden Gleichungen verschieden ist:

$$c_i = c + x(b_j - b), \; i = 1,2,\ldots,r; \; j = 1,2,\ldots,s.$$

Da H unendlich viele Elemente enthält, existiert ein solches Element $h \in H$.

Um die Richtigkeit der Gleichung $M = H(a)$ nachzuweisen, haben wir nur zu zeigen, daß die Galoisgruppe von L über $H(a)$ gleich der Galoisgruppe $\mathfrak{T}_M^L$ von L über M ist. Daß die Gruppe der inneren Automorphismen von L über $H(a)$ mit $\mathfrak{T}_M^L$ übereinstimmt, folgt aus der Tatsache, daß die Elemente h und b mit allen Elementen aus T_H^L und c genau mit denen aus T_M^L vertauschbar sind. Für den Fall $H = K$ ist damit der Beweis geführt, da es jetzt keine äußeren Automorphismen gibt.

Angenommen, G ist ein äußerer Automorphismus aus $\mathfrak{G}_H^L$ und $aG=a$, ausführlich

$$cG-h\cdot bG=c-h\cdot b.$$

Da b nur bei den inneren Automorphismen fest bleibt, ist dabei $bG=b_j$. Aus obiger Gleichung folgt dann

$$cG=c+h\cdot(b_j-b).$$

Wegen der Invarianz von T_H^L liegt cG in T_H^L. Auf Grund der rechten Seite der Gleichung ist cG mit allen Elementen aus T_M^L vertauschbar, muß also, da T_M^L maximaler kommutativer Unterkörper von T_H^L ist, in T_M^L liegen; d. h. es ist $cG=c_i$ nach unserer Bezeichnung. Dann besteht die Gleichung

$$c_i=c+h(b_j-b),$$

im Widerspruch zur Wahl von h. Das Element a bleibt also bei keinem äußeren Automorphismus fest. Damit haben wir das gewünschte Ergebnis: Die Automorphismengruppe von L über $H(a)$ ist gleich $\mathfrak{L}_M^L$ und folglich, wie behauptet, $M=H(a)$. Damit ist Satz 4 bewiesen.

Zur Vorbereitung für den nächsten Satz überlegen wir nun noch, daß man a insbesondere so wählen kann, daß es nicht in Z_L liegt, falls nur $Z_L\subset T_H^L$.

Ist $T_M^L\subset T_H^L$, so ist dies stets der Fall, denn dann ist c nicht mit allen Elementen aus T_H^L vertauschbar, die Elemente h und b sind mit diesen vertauschbar und folglich liegt $a=c-hb$ nicht in Z_L.

Setzen wir jetzt $T_M^L=T_H^L$ voraus, so kann das Element c beliebig in T_H^L gewählt werden. Ist $H=K$, so sei $a=c$ und c ein Element aus T_H^L, welches nicht in Z_L liegt. Ein solches Element existiert wegen $Z_L\subset T_H^L$. Ist $H\subset K$, so setzen wir $c=0$. Jetzt kann das Element $h\neq 0$ beliebig in H gewählt werden. Ist b nicht in Z_L enthalten, so sei $a=b$, andernfalls $a=hb$ $(b\neq 0)$, wobei jetzt $h\in H$ nicht in Z_L liegt.

Daß ein solches Element h existiert, folgt daraus, daß bei einer galoisschen Erweiterung mit nur inneren Automorphismen und kommutativem Transformatorenkörper, der Transformatorenkörper im Grundkörper enthalten sein muß. Es ist also $T_H^L\subseteq K$, wobei nach Voraussetzung $Z_L\subset T_H^L$.

Ist $Z_L\subset T_H^L$, so gibt es also stets ein erzeugendes Element a von M über H, welches nicht im Zentrum von L liegt.

IV. Existenz von zwei konjugierten, erzeugenden Elementen.

Alle bisherigen Überlegungen dienten zur Vorbereitung des in der Einleitung angegebenen Satzes, den wir jetzt herleiten wollen.

Satz 5. *Ist L galoissche Erweiterung endlichen Ranges von H und ist das Zentrum des Transformatorenkörpers T_H^L separabel über dem Zentrum von L, so besitzt L über H zwei erzeugende Elemente:*

$$L=H(a,a'),$$

die bezüglich eines inneren Automorphismus von L konjugiert sind[3a]).

Beweis. Aus Satz 3 geht hervor, daß L in folgenden Fällen bereits durch ein Element über H erzeugt wird:

1. Einer der Körper H oder Z_L enthält nur endlich viele Elemente.
2. Es gibt keine inneren Automorphismen von L über H, d. h. $Z_L=T_H^L$.

In diesen Fällen ist der Satz mit $a=a'$ erfüllt.

Auf Grund dieser Feststellung können wir im folgenden voraussetzen, daß H und Z_L unendlich viele Elemente enthalten und $Z_L\subset T_H^L$ ist. Wir betrachten jetzt den im vorher-

gehenden Satz konstruierten Körper M. Über M besitzt L nur innere Automorphismen mit dem kommutativen Transformatorenkörper T_M^L. Da T_M^L über $Z_{T_H^L}$ separabel ist und da außerdem nach Voraussetzung auch $Z_{T_H^L}$ separabel über Z_L ist, stellt insgesamt T_H^L einen separablen kommutativen Körper endlichen Ranges über Z_L dar. Dieser besitzt nur endlich viele Zwischenkörper über Z_L und folglich enthält die Galoisgruppe $\mathfrak{L}_M^L$ von L über M nur endlich viele ausgezeichneten Untergruppen. Aus jeder dieser ausgezeichneten Untergruppen, einschließlich $\mathfrak{L}_M^L$ selbst, greifen wir einen vom identischen verschiedenen Automorphismus heraus:

$$G_1, G_2, \ldots, G_n.$$

Können wir nachweisen, daß es ein zu a bezüglich eines inneren Automorphismus konjugiertes Element a' gibt, welches bei keinem dieser Automorphismen fest bleibt, so besteht die Galoisgruppe von L über $M(a')$ nur aus dem identischen Automorphismus und es ist folglich $L = M(a')$.

Den Nachweis, daß ein solches Element a' existiert, führen wir in drei Hilfssätzen, die auch an sich von Interesse sind. Bevor wir damit beginnen, stellen wir noch einmal die Voraussetzungen zusammen, die wir dabei heranziehen dürfen:

1. Z_L enthält unendlich viele Elemente.

2. $Z_L \subset T_H^L$; im Anschluß an Satz 4 haben wir festgestellt, daß dann das erzeugende Element a von M über H so gewählt werden kann, daß es nicht in Z_L enthalten ist.

3. Da L über M galoissch mit nur inneren Automorphismen ist, gilt $Z_L \subseteq M$. Die vorstehend angegebenen Automorphismen $G_1, G_2, \ldots, G_n$ können daher auch als vom identischen verschiedene Automorphismen von L über Z_L aufgefaßt werden.

Hilfssatz 2[7]. *Es seien L ein beliebiger Körper und N ein Unterkörper von L, der nicht ganz im Zentrum von L enthalten ist und bei jedem inneren Automorphismus von L als Ganzes invariant bleibt. Dann ist $N = L$.*

Beweis. Es sei a ein Element aus N, welches nicht im Zentrum von L enthalten ist. Ferner sei v ein Element aus L, das mit a vertauschbar und u ein solches, das mit a unvertauschbar ist. Diese Elemente genügen den folgenden Gleichungen:

$$va = av,$$

$$ua = a^* u,$$

$$(u+v)a = a'(u+v),$$

wobei die Konjugierten a^* und a' von a wegen der Invarianz von N ebenfalls in N liegen und $a' - a \neq 0$ ist. Subtrahiert man die letzte Gleichung von der Summe der beiden ersten und faßt entsprechende Glieder zusammen, so erhält man die Beziehung

$$(a^* - a')u = (a' - a)v.$$

Setzt man darin $v = 1$, so folgt, daß jedes mit a unvertauschbare Element u aus L in N enthalten ist. Dann erhält man aus dieser Gleichung aber außerdem, daß auch jedes mit a vertauschbare Element v aus L in N liegt. Das sind aber alle Elemente aus L und es ist folglich wie behauptet $N = L$.

Aus diesem Ergebnis ziehen wir eine Folgerung.

---

[7]) Dieser Hilfssatz stellt eine Verallgemeinerung eines Satzes von *H. Cartan* dar [a. a. O.[2]), Theorem 4], den *H. Cartan* mit Hilfsmitteln aus der Galoisschen Theorie beweist. Nach Beendigung dieser Arbeit wurde mir bekannt, daß diese Verallgemeinerung bereits von *R. Brauer* [On a theorem of H. Cartan, Bull. Amer. Math. Soc. **55** (1949), 619–620] bemerkt worden ist.

Hilfssatz 3. *Ist a ein Element aus einem Körper L, welches nicht in Z_L enthalten ist, und G ein vom identischen verschiedener Automorphismus von L über Z_L, so gibt es ein Element $t \in L$ mit der Eigenschaft*

$$(tat^{-1})G - tat^{-1} \neq 0.$$

Beweis. Da auf Grund des vorhergehenden Hilfssatzes die Konjugierten von a bei inneren Automorphismen von L ein Erzeugendensystem von L über Z_L bilden und G ein vom identischen verschiedener Automorphismus von L ist, muß ein Element t mit der angegebenen Eigenschaft existieren.

Dieses Ergebnis soll nun verallgemeinert werden.

Hilfssatz 4. *L sei ein beliebiger Körper, dessen Zentrum Z_L unendlich viele Elemente enthält und a ein Element aus L, welches nicht in Z_L liegt. Sind $G_1, G_2, \ldots, G_n$ beliebige, aber vom identischen verschiedene Automorphismen von L über Z_L, so gibt es ein zu a bezüglich eines inneren Automorphismus konjugiertes Element $a' = tat^{-1}$ $(t \in L)$, welches bei keinem der gegebenen Automorphismen in sich übergeführt wird:*

$$(tat^{-1})G_i - tat^{-1} \neq 0 \qquad \text{für } i = 1,2,\ldots,n.$$

Beweis. Auf Grund des vorhergehenden Hilfssatzes gibt es zu jedem G_i ein Element $t_i \in L$ mit der Eigenschaft

$$(t_i a t_i^{-1})G_i - t_i a t_i^{-1} \neq 0.$$

Aus den Elementen t_i konstruieren wir das gesuchte Element t mit Hilfe der Lagrangeschen Interpolationsformel.

Dazu benutzen wir den Funktionenkörper $L(x)$, wobei x eine mit allen Elementen von L vertauschbare Unbestimmte ist. Da Z_L unendlich viele Elemente enthält, können wir n verschiedene Elemente aus Z_L vorgeben: $z_1, z_2, \ldots, z_n$. Dann gibt es, wie wir zu Beginn dieser Arbeit festgestellt haben, ein Lagrangesches Interpolationspolynom $T(x)$, welches an den Stellen z_i die Werte t_i annimmt.

Wir betrachten nun die folgenden Ungleichungen:

$$(T(x)aT(x)^{-1})G_i - T(x)aT(x)^{-1} \neq 0 \qquad \text{für } i = 1,2,\ldots,n.$$

Dabei sei $xG_i = x$.

Da für Polynome aus $L(x)$ der Euklidische Algorithmus durchführbar ist, können wir diese Ungleichungen auf die folgende Gestalt bringen:

$$Z_i(x)\frac{1}{N_i(x)} \neq 0,$$

wobei $Z_i(x)$ und $N_i(x)$ Polynome sind. Auf Grund der Voraussetzung über $T(x)$ ist dabei

$$Z_i(z_i)\frac{1}{N_i(z_i)} = (t_i a t_i^{-1})G_i - t_i a t_i^{-1} \neq 0$$

ein Element aus L. Daraus folgt, daß die Polynome $Z_i(x)$ und $N_i(x)$ nicht identisch verschwinden. Dann hat aber das Ungleichungssystem

$$Z_i(x) \neq 0, \; N_i(x) \neq 0 \qquad \text{für } i = 1,2,\ldots,n$$

eine Lösung in Z_L, denn jedes dieser Polynome hat nur endlich viele Nullstellen in Z_L. Da Z_L unendlich viele Elemente enthält, gibt es ein von diesen Nullstellen verschiedenes Element $z \in Z_L$. Dann haben wir offenbar in $T(z) = t$ das gesuchte Element.

Mit dem Beweis dieses Hilfssatzes haben wir auch den Beweis von Satz 5 vollendet.

Eingegangen am 28. April 1950.