ARCHIVES OF MATHEMATICS
ARCHIV DER MATHEMATIK
ARCHIVES MATHÉMATIQUES

Herausgegeben in Verbindung
mit dem Mathematischen Forschungsinstitut in Oberwolfach
von H. Kneser und W. Süss

VOL. 4 · 1953

VERLAG BIRKHÄUSER
BASEL · STUTTGART

Inhalt — Contents — Sommaire

Halblineare Abbildungen und die Rangrelation bei GALOISschen Erweiterungen

Von FRIEDRICH KASCH in Göttingen

Fragestellung

Die Ausdehnung der GALOISschen Theorie auf beliebige galoissche Schiefkörpererweiterungen durch N. JACOBSON [3] und H. CARTAN [1] stützt sich auf gewisse Ergebnisse über halblineare Abbildungen. Bei der Verallgemeinerung dieser Theorie auf einfache Ringe (im Sinne einer Automorphismentheorie), wie sie kürzlich T. NAKAYAMA angegeben hat [5], werden entsprechende Ergebnisse über halblineare Abbildungen aufgestellt, doch auf anderem Wege bewiesen. Hier soll gezeigt werden, daß man bereits mit dem ursprünglichen Ansatz zum Ziel kommt. Dies ist nicht nur methodisch von Interesse, sondern vor allem deshalb, weil sich dabei eine Verallgemeinerung eines der wesentlichen Ergebnisse der GALOISschen Theorie, nämlich der Rangrelation ergibt. Wie aus einer Bemerkung von T. NAKAYAMA hervorgeht [1]), konnte diese Verallgemeinerung auf dem von ihm eingeschlagenen Weg bisher nicht bewiesen werden.

Die Verallgemeinerung der Rangrelation folgt fast unmittelbar aus einem Ergebnis, das ich kürzlich mitgeteilt habe ([4], Hilfssatz 1), und das hier unter etwas allgemeineren Voraussetzungen noch einmal hergeleitet werden soll, da die dabei benutzte Schlußweise auch bei einer weiteren Überlegung verwendet wird.

Halblineare Abbildungen

Von den im folgenden als *einfach* oder *halbeinfach* bezeichneten Ringen setzen wir voraus, daß sie ein Einselement besitzen und der Minimalbedingung genügen. Sei nun A ein einfacher Ring, so betrachten wir A zunächst als Modul ohne Operatorenbereich und bezeichnen mit $\mathfrak{E}$ den Ring aller Endomorphismen von A. Die Endomorphismen denken wir uns durch Multiplikation von rechts auf die Elemente von A ausgeübt: es sei also $a\mathfrak{e}$ das Bild von $a \in A$ bei dem Endomorphismus $\mathfrak{e} \in \mathfrak{E}$. Statt $a\mathfrak{e}$ schreiben wir auch $(a\mathfrak{e})$.

Jedes Element $a \in A$ erzeugt sowohl als Rechts- als auch als Linksmultiplikator von A einen Endomorphismus von A, den wir mit a^r bzw. a^l bezeichnen wollen. Dann gilt also mit beliebigem $x \in A$:

$$x a^r = x a\,, \qquad x a^l = a x\,.$$

[1]) Vgl. Fußnote 3

Da A ein Einselement besitzt, sind A und der Ring der Rechtsmultiplikatoren A^r (ring-)isomorph und A und A^l inversisomorph.

Wir haben hier A^r-halblineare Abbildungen zu untersuchen, d. h. Abbildungen $\mathfrak{v} \in \mathfrak{E}$, die der *Vertauschungsregel*

(1) $$a^r \mathfrak{v} = \mathfrak{v}(a\,\mathfrak{g})^r\,, \qquad a^r \in A^r$$

mit einem festen, zu $\mathfrak{v}$ gehörenden Ringautomorphismus $\mathfrak{g}$ von A^r (und damit auch von A) genügen. Ist a ein beliebiges Element aus A, so gilt auf Grund von (1):

$$a\,\mathfrak{v} = 1 \cdot a^r\,\mathfrak{v} = (1\,\mathfrak{v})\,(a\mathfrak{g})^r = a \cdot \mathfrak{g}(1\,\mathfrak{v})^l\,.$$

Setzt man noch $1\,\mathfrak{v} = t$, so ist also

$$\mathfrak{v} = \mathfrak{g}\,t^l\,.$$

Umgekehrt stellt auch jeder solche Ausdruck eine A^r-halblineare Abbildung von A dar, insbesondere sind also die Automorphismen von A A^r-halblineare Abbildungen.

Über halblineare Abbildungen beweisen wir nun den folgenden

Satz: [2]) 1. *Die A^r-halblinearen Abbildungen $\mathfrak{v}_i = \mathfrak{g}_i\,t_i^l$, $i = 1, \ldots, n$ sind dann und nur dann linear abhängig über A^r, wenn es darunter Abbildungen $\mathfrak{v}_1, \ldots, \mathfrak{v}_m$ gibt (bei geeigneter Numerierung), so daß für die zugehörigen Automorphismen*

$$\mathfrak{g}_j = \mathfrak{g}_1\,a_j^l(a_j^{-1})^r\,, \quad a_j \in A\,, \quad j = 1, \ldots, m$$

gilt und die Elemente $t_1 a_1, \ldots, t_m a_m$ linear abhängig über dem Zentrum Z von A sind.

2. *Ist $\mathfrak{N}$ ein zweiseitiger A^r-Modul, der über A^r durch endlich viele A^r-halblineare Abbildungen erzeugt wird, dann besitzt jeder zweiseitige A^r-Untermodul $\mathfrak{U}$ von $\mathfrak{N}$ ebenfalls diese Eigenschaft.*

Bevor wir den Beweis führen, wollen wir die erste Behauptung noch etwas anders formulieren. Sie besagt, daß A^r-halblineare Abbildungen, deren zugehörige Automorphismen in verschiedenen Klassen nach der Gruppe aller inneren Automorphismen von A liegen, über A^r linear unabhängig sind und daß A^r-halblineare Abbildungen $\mathfrak{v}_1, \ldots, \mathfrak{v}_m$, deren zugehörige Automorphismen innere sind, für die also

$$\mathfrak{g}_j = a_j^l(a_j^{-1})^r\,, \qquad j = 1, \ldots, m$$

gilt, dann und nur dann linear abhängig über A^r sind, wenn die Elemente $t_1 a_1, \ldots, t_m a_m$ linear abhängig über Z sind.

Zum Beweis der ersten Behauptung des Satzes nehmen wir an, daß $\mathfrak{v}_1, \ldots, \mathfrak{v}_n$ linear unabhängig über A^r seien und es sei (bei geeigneter Numerierung)

(2) $$\mathfrak{v}_1\,a_1^r + \cdots + \mathfrak{v}_m\,a_m^r = 0\,, \qquad a_j \neq 0 \quad (j = 1, \ldots, m)$$

eine kürzeste Darstellung der Null mit Hilfe dieser Abbildungen, d. h. es gebe keine solche Darstellung mit weniger von Null verschiedenen Koeffizienten. Zur Abkür-

[2]) Vgl. [1], lemme 1, lemme 2; [3], lemma 1, lemma 2; [2], lemme 2; [4], Hilfssatz 1.

zung bezeichnen wir den Ausdruck auf der linken Seite von (2) mit $\mathfrak{u}$. Da A^r einfach ist, gibt es endlich viele Elemente $b_i^r, c_i^r \in A^r$, so daß $\sum_i b_i^r a_1^r c_i^r = 1 \quad (1^r = 1)$ gilt. Auf Grund der Vertauschungsregel ist auch $\sum_i (b_i \mathfrak{g}_1^{-1})^r \mathfrak{u}\, c_i^r$ eine Darstellung der Null mit Hilfe von $\mathfrak{v}_1, \ldots, \mathfrak{v}_m$, bei der außerdem der Koeffizient von $\mathfrak{v}_1$ gleich 1 ist. Wir können daher annehmen, daß dies bereits für $\mathfrak{u}$ zutrifft, d. h. daß $a_1^r = 1$ gilt. Dann kann keiner der Koeffizienten von $\mathfrak{u}$ Nullteiler sein, denn dann wäre $\mathfrak{u}$ keine kürzeste Darstellung der Null. Wegen $a_1^r = 1$ und der Vertauschungsregel besteht für beliebiges $a^r \in A^r$ die folgende Gleichung:

$$a^r \mathfrak{u} - \mathfrak{u}(a\mathfrak{g}_1)^r = \mathfrak{v}_2 \left[(a\mathfrak{g}_2)^r a_2^r - a_2^r (a\mathfrak{g}_1)^r\right] + \cdots + \mathfrak{v}_m \left[(a\mathfrak{g}_m)^r a_m^r - a_m^r (a\mathfrak{g}_1)^r\right].$$

Dies ist wieder eine Darstellung der Null. Da sie weniger von Null verschiedene Koeffizienten als $\mathfrak{u}$ aufweist, müssen darin alle Koeffizienten verschwinden:

$$(3) \qquad (a\mathfrak{g}_j)\, a_j = a_j (a\mathfrak{g}_1), \qquad j = 1, \ldots, m.$$

Da, wie zuvor festgestellt, alle a_j regulär sind, folgt

$$(4) \qquad \mathfrak{g}_j = \mathfrak{g}_1\, a_j^l (a_j^{-1})^r, \qquad j = 1, \ldots, m.$$

Setzt man diese Gleichungen in (2) ein, so erhält man

$$\mathfrak{g}_1 (a_1^l t_1^l + \cdots + a_m^l t_m^l) = 0,$$

also

$$t_1 a_1 + \cdots + t_m a_m = 0.$$

Damit ist gezeigt, daß die Bedingung notwendig ist. Um festzustellen, daß sie hinreichend ist, durchlaufe man den Schluß in umgekehrter Richtung, wobei zu berücksichtigen ist, daß Elemente, die innere Automorphismen erzeugen, nur bis auf Faktoren aus Z bestimmt sind und daß man ohne Einschränkung $a_1 = 1$ annehmen kann.

Zum Beweis der zweiten Behauptung sei $\mathfrak{v}$ eine beliebige A^r-halblineare Abbildung aus $\mathfrak{R}$. Ist $\mathfrak{v} a^r$ $(a^r \neq 0)$ von den halblinearen Abbildungen $\mathfrak{v}_1, \ldots, \mathfrak{v}_n$ linear abhängig, so folgt auf Grund der angegebenen Schlußweise, daß bereits $\mathfrak{v}$ von $\mathfrak{v}_1, \ldots, \mathfrak{v}_n$ linear abhängig ist. Folglich bildet ein maximales System linear unabhängiger halblinearer Abbildungen aus dem endlichen Erzeugendensystem von $\mathfrak{R}$ eine Basis von $\mathfrak{R}/A^r$.

Sei nun $\mathfrak{v}_1, \ldots, \mathfrak{v}_n$ eine feste Basis aus A^r-halblinearen Abbildungen von $\mathfrak{R}/A^r$. Den Beweis führen wir durch Induktion nach der Anzahl der von Null verschiedenen Koeffizienten der Elemente aus $\mathfrak{U}$ in der Darstellung durch diese Basis. Der Induktionsbeginn ist klar und die Behauptung sei richtig für alle Elemente aus $\mathfrak{U}$ mit weniger als m von Null verschiedenen Koeffizienten. Das Element $\mathfrak{u} \in \mathfrak{U}$ besitze (bei geeigneter Numerierung der Basiselemente) die Darstellung

$$\mathfrak{u} = \mathfrak{v}_1 a_1^r + \cdots + \mathfrak{v}_m a_m^r, \qquad a_j \neq 0, \qquad j = 1, \ldots, m.$$

Gibt es ein Element $\mathfrak{u}' \in \mathfrak{U}$

$$\mathfrak{u}' = \mathfrak{v}_1 b_1^r + \ldots + \mathfrak{v}_m b_m^r \neq 0 ,$$

bei dem nicht alle Koeffizienten von Null verschieden sind, so gibt es nach der angegebenen Schlußweise auch ein solches Element, bei dem ein Koeffizient gleich 1 ist; sei etwa $b_1^r = 1$. Dann sind $\mathfrak{u} - \mathfrak{u}' a_1^r$ und $\mathfrak{u}' a_1^r$ beides Elemente mit weniger als m von Null verschiedenen Koeffizienten, die sich also nach Induktionsannahme linear durch A^r-halblineare Abbildungen aus $\mathfrak{U}$ darstellen lassen. Folglich gilt dies auch für $\mathfrak{u}$ selbst. Gibt es kein Element $\mathfrak{u}'$ mit der angegebenen Eigenschaft, so sei $\mathfrak{u}^*$ ein Element aus dem durch $\mathfrak{u}$ erzeugten zweiseitigen A^r-Modul mit dem ersten Koeffizienten 1:

$$\mathfrak{u}^* = \mathfrak{v}_1 c_1^r + \ldots + \mathfrak{v}_m c_m^r , \qquad c_1^r = 1 .$$

Zunächst gilt $\mathfrak{u} = \mathfrak{u}^* a_1^r$. Zum Beweis bleibt daher nur festzustellen, daß $\mathfrak{u}^*$ bereits eine A^r-halblineare Abbildung ist. Das ergibt sich aber sofort nach der Schlußweise im Beweis der ersten Behauptung. Auch jetzt gilt, daß alle Koeffizienten von $\mathfrak{u}^*$ reguläre Elemente aus A^r sind. Ferner ist $a^r \mathfrak{u}^* - \mathfrak{u}^* (a \mathfrak{g}_1)^r$ ein Element aus $\mathfrak{U}$ mit weniger von Null verschiedenen Koeffizienten als $\mathfrak{u}^*$ und folglich müssen darin alle Koeffizienten verschwinden. Dann gelten die Gleichungen (3) und (4) sinngemäß für $\mathfrak{u}^*$ und man erhält schließlich

$$\mathfrak{u}^* = \mathfrak{g}_1 (c_1^l t_1^l + \ldots + c_m^l t_m^l) .$$

Setzt man noch $t_1 c_1 + \ldots + t_m c_m = t$, so folgt $\mathfrak{u}^* = \mathfrak{g}_1 t^l$ und dies ist eine halblineare Abbildung.

Folgerungen

1. Eine Automorphismengruppe $\mathfrak{G}$ von A heißt (im Sinne von T. Nakayama) *regulär*, wenn sie den folgenden Voraussetzungen genügt: Ist T der durch diejenigen Elemente aus A erzeugte Ring, die in $\mathfrak{G}$ enthaltene innere Automorphismen von A hervorrufen, so sei T einfach und von endlichem Rang über dem Zentrum Z von A; die in $\mathfrak{G}$ enthaltene Gruppe $\mathfrak{G}_0$ von inneren Automorphismen bestehe aus allen inneren Automorphismen, die durch Elemente aus T erzeugt werden und schließlich sei der Index von $\mathfrak{G}_0$ in $\mathfrak{G}$, $(\mathfrak{G} : \mathfrak{G}_0)$, endlich. Bezeichnet C den Fixring von $\mathfrak{G}$, d. h. die Gesamtheit der Elemente aus A, die bei allen Automorphismen aus $\mathfrak{G}$ ungeändert bleiben, so ist mit T auch C einfach und es gilt die Rangrelation

$$(A : C) = (\mathfrak{G} : \mathfrak{G}_0)\,(T : Z) , \tag{5}$$

wobei unter $(A : C)$ sowohl der Links- als auch der Rechtsrang verstanden werden kann, da diese übereinstimmen. Bei nur äußeren Automorphismen, also im Falle $(T : Z) = 1$ ist dies die vom klassischen Fall her bekannte Gleichung zwischen dem Rang einer galoisschen Erweiterung und der Ordnung der Galoisgruppe.

Die Rangrelation (5) soll nun bei sonst gleichen Voraussetzungen für den Fall hergeleitet werden, daß T (und damit auch C) halbeinfach sind. $\mathfrak{G}$ soll dann als *halbregulär* bezeichnet werden [5].

Sei also $\mathfrak{G}$ halbregulär und $\mathfrak{R}$ bezeichne den durch $\mathfrak{G}$ und A^r erzeugten Endomorphismenring von A. Dieser besitzt auf Grund unseres Satzes den (beidseitigen) Rang $(\mathfrak{G}:\mathfrak{G}_0)\,(T:Z)$ über A^r. Nach J. DIEUDONNÉ ([2], Théorème 2) stimmt dieser Rang mit dem von A/C überein. Wir haben damit

Folgerung 1: *Ist $\mathfrak{G}$ eine halbreguläre Automorphismengruppe des einfachen Ringes A und C der Fixring von $\mathfrak{G}$, so gilt die Rangrelation* (5)[3].

2. Nach T. NAKAYAMA nennt man einen Unterring C von A *schwach normal* unter A, wenn der Zentralisator $\mathfrak{Z}(C^l)$ von C^l in $\mathfrak{E}$ über A^r durch endlich viele A^r-halblineare Abbildungen erzeugt wird. Behält man die Bezeichnung „schwach normal" bei sonst gleichen Voraussetzungen auch für den Fall eines beliebigen, nicht notwendig einfachen Unterringes C von A bei, so gilt

Folgerung 2: *Ist C ein schwach normaler Unterring von A und B ein Ring mit $C \subseteq B \subseteq A$, so ist auch B schwach normal unter A.*

Dies folgt sofort aus der zweiten Behauptung des Satzes, wenn man berücksichtigt, daß $\mathfrak{Z}(B^l) \subseteq \mathfrak{Z}(C^l)$ gilt und $\mathfrak{Z}(B^l)$ zweiseitiger A^r-Modul ist.

Wir haben damit einen neuen Beweis eines Ergebnisses von T. NAKAYAMA erhalten ([5], Lemma 1.5).

Schließlich erwähnen wir noch

Folgerung 3: *Ist C ein schwach normaler Unterring von A und ist B ein Ring mit $C \subseteq B \subseteq A$, über dem A eine Linksbasis besitzt, dann gibt es zu jedem Ringisomorphismus $\mathfrak{q}$ von B in A, bei dem C elementweise fest bleibt, eine A^r-halblineare Abbildung $\mathfrak{v} \in \mathfrak{Z}(C^l)$ mit*

$$b^l\,\mathfrak{v} = \mathfrak{v}(b\,\mathfrak{q})^l \quad \textit{für alle } b \in B\,.$$

Die Voraussetzung, daß A/B eine Linksbasis besitzt, ist z. B. erfüllt, wenn B ein halbeinfacher Ring ist.

Zum Beweis sei $w_1, \ldots, w_n$ eine Linksbasis von A/B. Dann stellt die Zuordnung

$$\sum_{i=1}^{n} b_i w_i \to \sum_{i=1}^{n} (b_i\,\mathfrak{q})\, w_i\,, \qquad (b_i \in B)$$

eine der Bedingung $b^l\,\mathfrak{v} = \mathfrak{v}(b\,\mathfrak{q})^l$ für alle $b \in B$ genügende Abbildung $\mathfrak{v} \in \mathfrak{E}$ dar. Alle Abbildungen aus $\mathfrak{E}$ mit dieser Eigenschaft bilden nun einen zweiseitigen A^r-Untermodul von $\mathfrak{Z}(C^l)$. Da dieser nach unserem Satz durch A^r-halblineare Abbildungen erzeugt wird, gibt es also jedenfalls eine Abbildung der behaupteten Eigenschaft.

[3]) T. NAKAYAMA schreibt in [5], Seite 288 über die Verallgemeinerungsmöglichkeit von (5) auf halbreguläre Automorphismengruppen: "It is also possible to obtain some statements which may be considered as a generalization of our rank relation, but they are rather complicated and clumsy".

Literaturverzeichnis

[1] H. Cartan, Théorie de Galois pour les corps non-commutatifs. Ann. École Norm. **65**, 60—77 (1948).

[2] J. Dieudonné, La théorie de Galois des anneaux simples et semi-simples. Commentarii Math. Helvet., **21**, 154—184 (1948).

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

[4] F. Kasch, Über den Endomorphismenring eines Vektorraums und den Satz von der Normalbasis. Math. Ann. (Im Druck.)

[5] T. Nakayama, Galois theory of simple rings. Trans. Amer. Math. Soc. **73**, 276—292 (1952).

Eingegangen am 16. 6. 1953