RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

WILLIBALD DÖRFLER

Halbgruppen und Automaten

Rendiconti del Seminario Matematico della Università di Padova, tome 50 (1973), p. 1-18

<http://www.numdam.org/item?id=RSMUP_1973__50__1_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 50 (1973)

Halbgruppen und Automaten.

WILLIBALD DÖRFLER (*)

In einer Reihe von Arbeiten wurden Automorphismengruppen von Automaten untersucht. Siehe dazu das Literaturverzeichnis, insbesondere das Buch von F. Gécseg und I. Peák [5], in dem ein Großteil der bisher gewonnenen Ergebnisse enthalten ist. Das Ziel der vorliegenden Arbeit ist es, die enge Beziehung zwischen Halbgruppen von Abbildungen einer Menge S und Automaten mit der Zustandsmenge S zum Beweis verschiedener Sätze über solche Halbgruppen bzw. über Automaten zu verwenden. Dabei werden hauptsächlich unendliche Automaten betrachtet. Es ergeben sich unter anderem Verallgemeinerungen von bisher nur für endliche Automaten bewiesenen Sätzen. Auch Sätze über endliche Permutationsgruppen werden für unendliche Mengen bewiesen. Wir bemerken noch, daß in der Arbeit implizit das Auswahlaxiom verwendet wird, ohne daß darauf ausdrücklich verwiesen wird.

DEFINITION. *Ein Automat A ist ein Tripel (S, I, M), wo S eine Menge, I eine Halbgruppe und $M\colon S\times I\to S$ eine Abbildung ist mit*

$$M(s, xy) = M\big(M(s, x), y\big)$$

für alle $s\in S$ und $x, y\in I$. M heißt die Überführungsfunktion, die Elemente von S sind die Zustände von A. Man nennt I die Eingabehalbgruppe von A.

Jedem Zustand $s\in S$ entspricht eine *Äquivalenzrelation* R_s auf der

---

(*) Indirizzo dell'A.: 3. Institut für Mathematik-Technische Hochschule - Karlsplatz 13 - A-1040 Wien, Austria.

Halbgruppe I durch die Definition

$$xR_sy \quad \text{genau dann, wenn} \quad M(s, x) = M(s, y) \text{ ist}.$$

Im allgemeinen ist R_s keine Kongruenz auf I. Eine Kongruenzrelation R auf I erhält man durch die folgende Definition.

DEFINITION. *Zwei Elemente $x, y \in I$ stehen in der Relation R, wenn xR_sy gilt für alle s.*

Somit ist xRy genau dann, wenn für alle $s \in S$ $M(s, x) = M(s, y)$. Man sieht sofort [4], daß R eine Kongruenzrelation auf I bildet. Die Klassen $[x]$ von I nach R bilden somit eine Halbgruppe I/R unter der Verknüpfung $[x][y] := [xy]$. Man nennt I/R die *charakteristische Halbgruppe* von A [5]. Jedem Element $[x] \in I/R$ entspricht eine Abbildung f von S in sich durch

$$f(s) := M(s, x) \quad \text{für } x \in [x]$$

Entsprechen den Klassen $[x]$ bzw. $[y]$ die Abbildungen f bzw. g, so entspricht der Klasse $[x][y]$ die Abbildung $g \circ f$. Denn es gilt

$$(g \circ f)(s) = g(f(s)) = g(M(s, x)) = M(M(s, x), y) = M(s, xy)$$

Da verschiedenen Klassen aus I/R verschiedene Abbildungen entsprechen, bilden die so erhaltenen Abbildungen eine Halbgruppe $F = F(A)$, die antiisomorph zu I/R ist.

DEFINITION [7]. *Der Automat A heißt stark zusammenhängend (st. zush.), wenn es zu allen s, $t \in S$ ein $x \in I$ gibt mit $M(s, x) = t$.*

DEFINITION. *Eine Halbgruppe F von Abbildungen auf der Menge S heißt transitiv, wenn es zu allen s, $t \in S$ ein $f \in F$ gibt mit $f(s) = t$. F heißt semiregulär, wenn aus $f(s_0) = s_0$ für ein $s_0 \in S$ folgt $f(s) = s$ für alle $s \in S$, also $f = \mathrm{id}$. Ferner heißt F regulär, wenn F transitiv und semiregulär ist.*

Aus diesen Definitionen ist ersichtlich, daß der Automat A genau dann st. zush. ist, wenn $F(A)$ transitiv ist.

Ist auf S eine Abbildungshalbgruppe F gegeben, so erhält man einen Automaten A mit $F(A) = F$ auf folgende Weise. Es sei F' die

Halbgruppe mit den Elementen aus F und der Verknüpfung $f \square g := g \circ f$, *wo* $\circ$ die Verknüpfung in F ist. Es sei $A = (S, F', M)$ mit $M(s, f) := f(s)$. Dann ist

$$M(s, f \square g) = (f \square g)(s) = (g \circ f)(s) = gM(s, f) = M\big(M(s, f), g\big) .$$

Also ist A ein Automat und klarerweise gilt $F(A) = F$. Wir bezeichnen den so konstruierten Automaten A mit $A(F)$. Es ist somit $F\big(A(F)\big) = F$.

DEFINITION *Sind* $A = (S, I, M)$ *und* $B = (T, I, N)$ *zwei Automaten, so heißt eine Abbildung* $\varphi\colon S \to T$ *ein Homomorphismus, wenn für alle* $s \in S$ *und* $x \in I$ *gilt*

$$\varphi M(s, x) = N\big(\varphi(s), x\big) .$$

Ist φ bijektiv, so ist φ ein *Isomorphismus* und A und B heißen dann isomorph. Es ist klar, was man unter einem *Endomorphismus* bzw. *Automorphismus* von A zu verstehen hat. Mit $E(A)$ bezeichnen wir die *Endomorphismenhalbgruppe* und mit $G(A)$ die *Automorphismengruppe* von A.

Die Automaten A und $A\big(F(A)\big)$ haben dieselbe Automorphismengruppe und dieselbe Endomorphismenhalbgruppe.

Eine wichtige Eigenschaft stark zusammenhängender Automaten A ist, daß $G(A)$ eine semireguläre Permutationsgruppe ist [10].

Diese Begriffe kann man im Zusammenhang mit $F(A)$ einführen, man vergleiche [1].

DEFINITION. *Es sei* F *eine Abbildungshalbgruppe auf* S. *Dann ist* F^+ *die Menge aller Abbildungen* $g\colon S \to S$ *mit* $f \circ g = g \circ f$ *für alle* $f \in F$ *und* F^* *die Menge der Permutationen in* F^+.

In der Theorie der Permutationsgruppen heißt F^* der *Zentralisator* von F, s. [12].

Es ist F^+ ein Monoid mit der Identität als neutralem Element und F^* ist eine Permutationsgruppe.

Mit unseren Bezeichnungen ist dann für den Automaten A $E(A) = F(A)^+$ und $G(A) = F(A)^*$. Ferner kann man formulieren: ist F auf S transitiv, so ist F^* eine semireguläre Permutationsgruppe.

Zunächst führen wir einige einfache Sätze über Gruppen und Halbgruppen von Abbildungen an, wobei die Verknüpfung stets das Nacheinanderausführen der Abbildungen ist.

SATZ 1. *Eine Gruppe G von Abbildungen von S ist genau dann eine Permutationsgruppe auf S, wenn zu jedem $s \in S$ ein $t \in S$ und ein $g \in G$ existieren mit $g(t) = s$.*

BEWEIS. Die Voraussetzungen seien erfüllt und e sei das neutrale Element von G. Es seien $s, t \in S$ und $g \in G$ wie im Satz angegeben. Wegen $e \circ g = g$ ist $e(s) = e(g(t)) = g(t) = s$. Daher ist $e = \mathrm{id}$ auf S. Sind f und f' in G zueinander invers, so ist $f \circ f' = f' \circ f = e = \mathrm{id}$. Somit sind f und f' bijektiv, also Permutationen von S.

FOLGERUNG 1. *Jede transitive Abbildungsgruppe ist eine Permutationsgruppe.*

FOLGERUNG 2. – *Ist ein $f \in G$ bijektiv, so ist G Permutationsgruppe.*

Daß aber keineswegs alle Abbildungsgruppen Permutationsgruppen sind, zeigt schon das folgende einfache Beispiel.

BEISPIEL. – $S = \{1, 2, 3\}$, $G = \{e, f\}$.

	1	2	3
e	3	2	3
f	2	3	2

	e	f
e	e	f
f	f	e

Im Gegensatz zu transitiven Gruppen kann man über transitive Halbgruppen keine ähnliche Aussage machen. Es gibt transitive Halbgruppen, die keine Gruppen sind.

BEISPIEL. $S = \{1, 2\}$, $F = \{f, g\}$.

	1	2
f	2	2
g	1	1

	f	g
f	f	g
g	f	g

Bekanntlich [1] gilt: Ist $|S| < \infty$ und ist F eine semireguläre Halbgruppe von Abbildungen der Menge S, so ist F eine semireguläre Permutationsgruppe. Der Satz ist für unendliche Mengen S falsch, wie einfache Beispiele zeigen. Jedoch gilt:

SATZ 2. *Eine reguläre Halbgruppe F von Abbildungen ist eine reguläre Permutationsgruppe.*

BEWEIS. Es sei $f \in F$ beliebig und $f(s) = t$ für ein $s \in S$. Dann gibt es ein $g \in F$ mit $g(t) = s$; also ist $(g \circ f)(s) = s$ und daher $g \circ f = \mathrm{id}$. Analog erhält man $f \circ g = \mathrm{id}$. Somit gibt es in F ein neutrales Element $e = \mathrm{id}$ und zu jedem $f \in F$ ein inverses Element g mit $f \circ g = g \circ f = e$. Also ist F eine Gruppe und wegen Satz 1 eine Permutationsgruppe.

LEMMA 1. *Ist die Halbgruppe F von Abbildungen transitiv, so ist F^+ ein semireguläres Monoid surjektiver Abbildungen.*

BEWEIS. In F^+ liegt auf jeden Fall die Identität id von S, die daher in F^+ das neutrale Element ist. Es sei $f \in F^+$ beliebig und $f(s) = s$ für ein $s \in S$. Wähle $t \in S$ beliebig und ein $g \in F$ mit $g(s) = t$. Dann ist

$$f(t) = (f \circ g)(s) = (g \circ f)(s) = g(s) = t\,.$$

Somit ist $f = \mathrm{id}$ und F^+ semiregulär. Sei wieder $f \in F^+$ beliebig und $s \in S$. Man wähle ein $t_1 \in S$ und zu $t = f(t_1)$ ein $g \in F$ mit $g(t) = s$. Dann ist $s = g(t) = (g \circ f)(t_1) = f\big(g(t_1)\big)$ und f ist surjektiv.

BEMERKUNG. Man kann Beispiele konstruieren, wo $F^+ \neq F^*$ ist unter den Voraussetzungen von Lemma 1, das heißt, wo nicht alle Abbildungen aus F^+ injektiv sind. Man vergleiche dazu die Sätze 3 bis 7, sowie Satz 13, Folgerung 3.

SATZ 3. *Ist G eine primitive Permutationsgruppe auf S, so ist $G^+ = G^*$.*

BEWEIS. Nach Lemma 1 ist jedes f aus G^+ surjektiv, weil G transitiv ist. Sei $f \in G^+$ fest gewählt. Mit $U(s)$ bezeichnen wir $f^{-1}(s)$ für $s \in S$. Für jedes $g \in G$ folgt dann aus $gU(s) \cap U(r) \neq \emptyset$, daß $gU(s) = U(r)$ ist. Man kann ein $t \in U(s)$ so wählen, daß $g(t) \in U(r)$ ist. Es gilt: $g(s) = g\big(f(t)\big) = f\big(g(t)\big) = r$. Daher ist für alle $q \in U(s)$

$$f\big(g(q)\big) = g\big(f(q)\big) = g(s) = r\,,$$

was gleichbedeutend mit $g(q) \in U(r)$ ist. Es folgt $gU(s) \subset U(r)$. Ist für ein $v \in U(s_1)$, $s_1 \neq s$, das Bild $g(v) \in U(r)$, so gilt $g(s_1) = g\big(f(v)\big) = f\big(g(v)\big) = r$, was $g(s) = r$ widerspricht. Da g bijektiv ist, erhält man daraus, daß $gU(s) = U(r)$ ist. Daher bilden die Mengen $U(s)$, $s \in S$, ein Imprimitivitätssystem von G. Aus der Primitivität von G erhält man $|U(s)| = 1$ für alle s und somit ist f injektiv.

BEMERKUNG. Ist jedoch G imprimitiv, so ist im allgemeinen $G^+ \neq G^*$ wie man an Beispielen sehen kann.

DEFINITION. *Ist F eine Abbildungshalbgruppe auf S, so heißt eine Partition π von S zulässig, wenn für jedes B aus S/π und jedes $f \in F$ ein $B' \in S/\pi$ existiert mit $fB \subset B'$. Die Menge S und die Partition, deren Klassen die Elemente von S sind, sind trivialerweise zulässig. Eine transitive Halbgruppe F heißt primitiv, wenn es zu F nur diese trivialen zulässigen Partitionen gibt.*

DEFINITION. *Ist F eine Abbildungshalbgruppe auf S, so stehen zwei Elemente s, $t \in S$ in der Relation P, wenn $s = t$ ist, oder wenn es f, $g \in F$ gibt mit $f(s) = t$ und $g(t) = s$. Es ist P eine Äquivalenzrelation auf S, und wir nennen die Klassen nach P die Transitivitätsgebiete von F in S.*

Im folgenden beweisen wir drei Lemmata, die auch für sich von Interesse sind.

LEMMA 2. *Ist F eine transitive Abbildungshalbgruppe auf S und H eine Unterhalbgruppe von F^+, so bilden die Transitivitätsgebiete von H eine zulässige Partition von S zu F.*

BEWEIS. Es seien B_α, $\alpha \in J$, die Transitivitätsgebiete von $H \subset F^+$. Gibt es zu s, $t \in S$ ein $g \in H$ mit $g(s) = t$, so ist $g\big(f(s)\big) = f\big(g(s)\big) = f(t)$ für alle $f \in F$. Daraus ist ersichtlich, daß aus sPt bezüglich H folgt, daß $f(s)Pf(t)$ gilt, woraus sich die Behauptung ergibt.

LEMMA 3. *Unter den Voraussetzungen von Lemma 2 gibt es zu jedem Transitivitätsgebiet B von H und jedem $f \in F$ ein Transitivitätsgebiet B' von H mit $fB = B'$.*

BEWEIS. Nach Lemma 2 gibt es zu B und $f \in F$ ein B' mit $fB \subset B'$. Ist $s \in B' - fB \neq \emptyset$, so gilt für jedes $t \in fB$ bezüglich H die Relation sPt. Wir wählen zu einem $t \in fB$ ein $g \in F$ mit $g(t) \in B \cap f^{-1}(t)$. Dann gilt $g(s)Pg(t)$, also $g(s) \in B$. Ist andererseits $h \in H$ mit $h(t) = s$, so kann für kein $u \in B \cap f^{-1}(t)$ gelten $h(u) \in B$, weil aus $f\big(h(u)\big) = h\big(f(u)\big) = h(t) = s$ der Widerspruch $s \in fB$ folgen würde. Ist daher h so gewählt, daß $h(t) = s$ ist, so ist $h\big(g(t)\big) = g\big(h(t)\big) = g(s)$ nicht in B. Dieser Widerspruch beweist das Lemma.

LEMMA 4. *Unter den Voraussetzungen von Lemma 2 gilt: sind $s \neq t$ aus einem Transitivitätsgebiet von H und ist $f \in F$, so ist $f(s) \neq f(t)$.*

BEWEIS. Es seien $s \neq t$ und f wie angegeben. Es gibt ein $h \in H$ mit $h(s) = t$. Ist $f(s) = f(t)$, so erhält man $h(f(s)) = f(s)$. Wir wählen ein $g \in F$ mit $g(f(s)) = s$. Dann erhält man den Widerspruch, daß $h(s) = s$ ist.

SATZ 4. *Ist F eine primitive Abbildungshalbgruppe auf S, so können nur folgende zwei Fälle auftreten:*

(I) *Es ist $F^+ = F^*$ und F und F^* sind reguläre Permutationsgruppen.*

(II) *$F^+ = F^*$ und beide bestehen nur aus der identischen Abbildung.*

BEWEIS. Da F primitiv ist, kann F nur die trivialen zulässigen Partitionen besitzen. Ist S das einzige Transitivitätsgebiet von F^+, so sind F und F^+ transitiv und man kann Satz 6 (sh. unten) anwenden, der die Aussage von (*I*) liefert. Mit einem Beweis, der völlig analog zum ersten Teil des Beweises von Satz 3 verläuft, zeigt man, daß für jedes $f \in F^+$ die Mengen $f^{-1}(s)$, $s \in S$, eine zulässige Partition zu F bilden. Daher müssen alle $f \in F^+$ injektiv und damit wegen Lemma 1 Permutationen sein. Das liefert im zweiten möglichen Fall, daß alle Transitivitätsgebiete von F^+ nur aus einem Element bestehen, die Behauptung in (II).

Aus Satz 4 kann man eine entsprechende Aussage über primitive Permutationsgruppen gewinnen, die das Resultat von Satz 3 verschärft. Man vergleiche dazu [1], wo ähnliche Ergebnisse für $|S| < \infty$ gewonnen wurden.

Aus Lemma 3 und 4 kann man noch schließen, daß alle Transitivitätsgebiete von $H \subset F^+$ dieselbe Kardinalzahl haben, wenn F transitiv ist.

DEFINITION [4]. *Ein Automat $A = (S, I, M)$ heißt abelsch, wenn für alle $s \in S$ und $x, y \in I$ gilt*

$$M(s, xy) = M(s, yx) .$$

Ist A st. zush. und abelsch, so heißt A perfekt.

Perfekte Automaten wurden von Fleck in [3] untersucht. Die dort enthaltenen Resultate gelten auch für unendliche Automaten. Insbesondere ist für jeden perfekten Automaten A die Gruppe $G(A)$ regulär. Offensichtlich ist A abelsch genau dann, wenn $F(A)$ abelsch ist.

SATZE 5. *Eine abelsche transitive Halbgruppe F von Abbildungen ist eine reguläre Permutationsgruppe und es ist $F^+ = F^*$.*

BEWEIS. Wir bilden zu F den Automaten $A(F)$. Da mit F auch F' (sh. oben) abelsch ist, folgt aus den Voraussetzungen, daß $A(F)$ perfekt ist und somit ist $G(A) = F^*$ transitiv. Mit Lemma 1 folgt wegen $F \subset G(A)^+$, daß F semiregular, also regulär ist. Aus Satz 2 folgt die Behauptung. Die Gleichung $F^+ = F^*$ ergibt sich aus der später bewiesenen Folgerung 3 zu Satz 13.

SATZ 6. *Ist F eine transitive Abbildungshalbgruppe und ist F^+ transitiv, so ist F eine reguläre Permutationsgruppe und $F^+ = F^*$.*

BEWEIS. Es gilt $F \subset (F^+)^+$. Aus Lemma 1 erhalten wir, daß F semiregulär und somit regulär ist. Die Behauptung folgt aus Satz 2. $F^+ = F^*$ folgt wieder aus Satz 13, Folgerung 3, zu deren Beweis ja nur der erste Teil der Behauptung von Satz 6 verwendet wird.

SATZ 7. *Ist $|S| < \infty$ und F eine transitive Halbgruppe von Abbildungen von S, so ist $F^+ = F^*$.*

BEWEIS. F^+ ist eine semireguläre Halbgruppe. Da $|S| < \infty$ ist, ist F^+ Permutationsgruppe und daher $F^+ = F^*$. Man kann auch direkt mit Lemma 1 schließen.

FOLGERUNG. *Für einen endlichen stark zusammenhängenden Automaten ist jeder Endomorphismus ein Automorphismus.*

Ist $|S| = \infty$, so ist Satz 7 nicht mehr richtig. Man erhält aus Lemma 1 jedoch den ersten Teil des folgenden Satzes.

SATZ 8. *Jeder Endomorphismus eines stark zusammenhängenden Automaten A ist surjektiv. Ist A st. zush. und die Endomorphismenhalbgruppe $E(A)$ transitiv, dann ist $E(A) = G(A)$.*

BEWEIS. Da A st. zush. ist, ist $F(A)$ transitiv. Nach Voraussetzung ist auch $E(A) = F(A)^+$ transitiv. Da auch $E(A)^+ \supset F(A)$ transitiv ist, folgt $E(A) = G(A)$ aus Satz 6.

DEFINITION. *Auf der Zustandsmenge S des Automaten $A = (S, I, M)$ ist die Relation SZ erklärt durch:*

$$sSZt \quad \textit{wenn } s = t \textit{ ist, oder wenn } \text{es } x, y \in I$$
$$\textit{gibt mit} \quad M(s, x) = t \quad \textit{und} \quad M(t, y) = s\,.$$

Man sieht sofort, daß SZ eine Äquivalenzrelation ist, und daß die Klassen K nach SZ mit $|K| > 1$ maximale st. zush. Teilmengen von

S sind, wobei eine Teilmenge von S stark zusammenhängend heißen soll, wenn je zwei ihrer Elemente in der Relation SZ stehen. Wir nennen die Klassen nach SZ die *starken Komponenten* von A. Es ist klar, daß die starken Komponenten von A die Transitivitätsgebiete von $F(A)$ sind. Es ist A st. zush. genau dann, wenn A nur aus einer starken Komponente besteht.

Man kann die Zustandsmenge S von A noch gröber einteilen, indem man folgende Relation Z auf S erklärt:

sZt wenn $s = t$ ist, oder wenn es eine endliche Folge $s = s_0, s_1, \ldots, s_n = t$ von Zuständen und Elemente $x_i \in S$, $i = 0, 1, \ldots, n-1$, gibt, sodaß für alle $i = 0, 1, \ldots, n-1$ entweder $M(s_i, x_i) = s_{i+1}$ oder $M(s_{i+1}, x_i) = s_i$ gilt.

Z ist ebenfalls eine Äquivalenzrelation, und die Klassen nach Z nennen wir die *Komponenten* von Z. Besteht A nur aus einer Komponente, so soll A *zusammenhängend* heißen. Es ist klar, daß jede starke Komponente in einer Komponente enthalten ist. Ferner ist jede Komponente L von A bezüglich M abgeschlossen, dh. aus $s \in L$, $x \in L$ folgt $M(s, x) \in L$.

Sind K_1 und K_2 zwei starke Komponenten von A und gibt es $s \in K_1$, $t \in K_2$ und $x \in I$ mit $M(s, x) = t$, so kann kein Element aus I einen Zustand aus K_2 in einen Zustand aus K_1 überführen. Wir definieren daher $K_1 \leqslant K_2$, wenn es s, t und x wie oben gibt. Dann ist $\leqslant$ eine Ordnung auf der Menge der starken Komponenten.

Aus Lemma 2 bis 4 erhalten wir leicht folgendes Resultat.

SATZ 9. *Ist die Endomorphismenhalbgruppe $E(A)$ des Automaten $A = (S, I, M)$ transitiv, so bildet jedes $f \in E(A)$ jede starke Komponente von A auf eine starke Komponente ab. Ferner können nur die folgenden zwei Fälle auftreten:*

(I) *Alle starken Komponenten sind einpunktig und zu keinem $s \in S$ gibt es ein $x \in I$ mit $M(s, x) = s$.*

(II) *Auf den starken Komponenten K von A werden paarweise isomorphe Automaten $\bar{K} = (K, \bar{I}, M|K \times \bar{I})$ induziert, wobei $\bar{I}$ die Halbgruppe aller Elemente von I ist, die K in sich überführen.*

BEWEIS. Es muß noch gezeigt werden, daß $\bar{I}$ unabhängig von der jeweiligen starken Komponente ist. Gilt $M(s, x) = t$ und ist $f \in E(A)$, so ist $M(f(s), x) = f(t)$. Sind s und t in einer starken Komponente von A, so auch $f(s)$ und $f(t)$. Aus beiden Tatsachen folgt die Behauptung.

BEMERKUNG. Ist A nicht st. zush., so kann aus der Transitivität von $E(A)$ nicht auf die Transitivität von $G(A)$ geschlossen werden. Siehe aber Satz 11.

SATZ 10. *Es sei A ein Automat mit endlich vielen starken Komponenten und transitiver Endomorphismenhalbgruppe $E(A)$. Dann ist jede Komponente von A stark zusammenhängend.*

BEWEIS. Es sei L eine Komponente von A und $K_1, \ldots, K_n$ die starken Komponenten von L. Ist $n = 1$, so ist nichst zu zeigen. Also sei $n \geqslant 2$. Bezüglich der Ordnung $\leqslant$ gibt es ein minimales Element unter den K_i, etwa K_1, und ein maximales Element, etwa K_n. Aus der Transitivität von $E(A)$ folgt mit Lemma 2, daß es ein $f \in E(A)$ gibt mit $fK_n = K_1$. Für alle $x \in I$ und $s \in K_n$ ist $M(s, x) \in K_n$, symbolisch $K_n I \subset K_n$, und aus dem starken Zusammenhang von K_n folgt $K_n I = K_n$. Daher gilt $K_1 I = (fK_n)I = f(K_n I) = fK_n = K_1$. Die Beziehung $K_1 I = K_1$ ergibt zusammen mit der Voraussetzung, daß L eine Komponente ist, einen Widerspruch dazu, daß K_1 minimales Element bezüglich der Ordnung $\leqslant$ der starken Komponenten ist.

BEMERKUNG. Für unendlich viele starke Komponenten gilt Satz 10 nicht. Es ist klar, wie der analoge Satz für Halbgruppen und Transitivitätsgebiete zu formulieren ist. Diese Bemerkung gilt auch für den folgenden Satz.

SATZ 11. *Ist jede Komponente von A stark zusammenhängend und ist $E(A)$ transitiv, so ist auch $G(A)$ transitiv.*

BEWEIS. Nach Satz 8 besitzt jeder der Automaten, die auf den (starken) Komponenten K von A induziert werden, eine transitive Automorphismengruppe. Dabei ist der auf K induzierte Automat $\bar{K}$ gegeben als $\bar{K} = (K, I, M|K \times I)$. Da nach Satz 9 alle Komponenten isomorphe Automaten bestimmen, folgt die Behauptung.

SATZ 12. *Eine semireguläre Gruppe G von Abbildungen ist eine Permutationsgruppe auf S.*

BEWEIS. Es sei e das neutrale Element von G und $f \in G$ beliebig. Für $s \in S$ ist dann $e(f(s)) = f(s)$, und daher muß e die Identität auf S sein. Mit Satz 1 folgt die Behauptung.

DEFINITION. *Ein Automat $A = (S, I, M)$ heißt zustandsunabhängig, wenn für alle $x, y \in I$ aus $xR_s y$ für ein $s \in S$ folgt, daß xRy gilt. Das*

heißt, aus $M(s, x) = M(s, y)$ *für ein* $s \in S$ *folgt* $M(t, x) = M(t, y)$ *für alle* $t \in S$.

Das folgende Lemma 5 dient zum Beweis von Satz 13. Wenn man umgekehrt den Satz 13 auf einem anderen Wege beweist, so erhält man aus diesem Satz unmittelbar die Aussage des Lemmas mit Hilfe eines Resultates von Trauth (vgl. dazu [5] statement 5.6.1).

LEMMA 5. *Ist für den Automaten* $A = (S, I, M)$ *die Halbgruppe* $F(A)$ *eine semireguläre Permutationsgruppe, so ist der Automat* A *zustandsunabhängig.*

BEMERKUNG. Die Umkehrung zu Lemma 5 gilt nicht. Es gibt endliche zustandsunabhängige und st. zush. Automaten, für die $F(A)$ keine Gruppe bildet (siehe [5] Seite 264).

BEWEIS. Wir zeigen zunächst, daß eine Permutationsgruppe G auf S genau dann semiregulär ist, wenn aus $\varphi(s) = \psi(s)$ für $\varphi, \psi \in G$ und ein $s \in S$ folgt, daß $\varphi = \psi$ ist. Da G eine Gruppe ist, erhält man aus $\varphi(s) = \psi(s)$ die Beziehung $\psi^{-1}\varphi(s) = s$. Ist G semiregulär, ist daher $\psi^{-1}\varphi = \mathrm{id}$ und $\varphi = \psi$. Umgekehrt folgt aus $\varphi(s) = s = \mathrm{id}(s)$ und unserer Voraussetzung $\varphi = \mathrm{id}$. Es sei $s \in S$ und $[x]_s$ eine Klasse von I nach R_s. $[x]_s$ ist die Vereinigung gewisser Klassen $[x_\alpha]$, $\alpha \in J$, nach der Relation R. Jeder Klasse $[x_\alpha]$ entspricht genau ein Element $f_\alpha \in F(A)$ und es ist $f_\alpha(s) = f_\beta(s)$ für alle $\alpha, \beta \in J$. Da $F(A)$ semiregulär ist, erhält man $f_\alpha = f_\beta$ für alle $\alpha, \beta \in J$, das heißt $f_\alpha(t) = f_\beta(t)$ für alle $t \in S$. Daraus ist ersichtlich, daß zwei Elemente $x, y \in I$, die in der Relation R_s stehen, für alle $t \in S$ in der Relation R_t stehen, also gilt xRy. Es war $s \in S$ beliebig, und somit ist A zustandsunabhängig.

DEFINITION. *Es sei* $A = (S, I, M)$ *ein Automat. Mit* $T(s)$, *für* $s \in S$, *bezeichnen wir die Menge* $\{x | x \in I$ und $M(s, x) = s\}$.

LEMMA 6. *Ist für den Automaten* A *die Halbgruppe* $F(A)$ *eine semireguläre Permutationsgruppe, so ist für alle* $s, t \in S$ $T(s) = T(t)$.

BEWEIS. Es sei $[x] \in I/R$. Nach Voraussetzung ist I/R eine Gruppe Gruppe und $[y]$ sei das inverse Element zu $[x]$ in I/R. Ferner sei $[x_0]$ das neutrale Element in R/I. Es sei für $s \in S$ $M(s, x) = t$ und $M(t, y) = s_1$. Wir nehmen an, daß s und t in derselben starken Komponente von A liegen, sodaß es ein $z \in I$ gibt mit $M(t, z) = s$. Aus $M(s, xy) = s_1$ folgt wegen $[x][y] = [x_0]$, daß $M\ (s, x_0) = s_1$ ist. Weiters

ist $s = M(t, z) = M(t, zx_0) = s_1$, sodaß wir $M(s, x_0) = s$ erhalten. Daher gilt für alle $v \in [x_0]$ und alle $s \in S$ die Beziehung $M(s, v) = s$ und kein Element einer anderen Klasse als $[x_0]$ aus I/R kann irgendeinen Zustand von S in sich überführen, weil $F(A)$ und damit I/R semiregulär ist.

LEMMA 7. *Unter den Voraussetzungen von Lemma 6 ist jede Komponente von A stark zusammenhängend und ihre Zustände sind genau die Elemente eines Transitivitätsgebietes von $F(A)$.*

BEWEIS. Es sei wieder $[x_0]$ das neutrale Element von I/R. Ist $M(s, x) = t$, so sei y so gewählt, daß $[x][y] = [x_0]$ ist. Dann haben wir

$$M(t, y) = M(s, xy) = M(s, x_0) = x_0$$

wobei das letzte Gleichheitszeichen aus Lemma 6 folgt. Daraus ergibt ich unmittelbar die Behauptung.

SATZ 13. *Es sei $A = (S, I, M)$ ein Automat, und die Halbgruppe $F(A)$ sei eine semireguläre Permutationsgruppe. Dann ist die Automorphismengruppe $G(A)$ transitiv.*

BEWEIS. Wir betrachten zuerst eine starke Komponente K von A und auf Grund von Lemma 7 den Automaten $B(K) = (K, I, M|K)$, wo $M|K$ die Restriktion von M auf $K \times I$ bedeuten soll. $B = B(K)$ ist st. zush. und wegen Lemma 5 zustandsunabhängig. Für $s, t \in K$ ist $T(s) = T(t)$ nach Lemma 6. Aus den Ergebnissen von [2] oder [8] erhält man, daß die Automorphismengruppe $G(B)$ transitiv ist. Es genügt jetzt zu zeigen, daß je zwei Automaten $B(K)$, $B(K')$ für starke Komponenten K und K' von A isomorph sind. Man wähle $s \in K$ und $s' \in K'$ und definiere $\varphi: K \to K'$ durch

$$\varphi(fs) = f(s') \quad \text{für alle } f \in F(A) .$$

Dann ist φ auf K definiert wegen Lemma 7 und eine bijektive Abbildung auf K'. Nun sei $x \in I$ beliebig, $t \in K$ beliebig.

$$\begin{aligned} \varphi M(t, x) = \varphi M\big(M(s, y), x\big) = \varphi M(s, yx) = \\ = M(s', yx) = M\big(M(s', y), x\big) = M(\varphi t, x) \end{aligned}$$

wobei $y \in I$ so gewählt wird, daß $M(s, y) = t$ ist. Ist f_y die der Klasse

$[y]$ entsprechende Permutation aus $F(A)$, so ist nach Definition von φ

$$\varphi t = \varphi M(s, y) = \varphi(f_y s) = f_y(s') = M(s', y) .$$

Eine analoge Überlegung gilt für yx. Man erhält, daß φ ein Isomorphismus ist und daraus die Behauptung.

FOLGERUNG 1. *Ist F eine semireguläre Gruppe von Abbildungen der Menge S, so ist F^* eine transitive Permutationsgruppe.*

BEMERKUNG. Ist die Permutationsgruppe G auf S semiregulär aber nicht regulär, so ist stets $G^+ \neq G^*$. Dazu seien K_α, $\alpha \in J$, die Transitivitätsgebiete von G und $s_\alpha \in K_\alpha$ fest gewählt. Ferner sei $\beta \in J$. Wir erklären eine Abbildung $f\colon S \to S$ durch

$$f(s_\alpha) := s_\beta \quad \text{für alle } \alpha \in J$$

$$f(g(s_\alpha)) := g(s_\beta) \quad \alpha \in J,\ g \in G .$$

Dann ist $f \in G^+$ und $fS = K_\beta$. Für jedes $f \in G^+$ gilt: sind $s \neq t$ in K_α, so ist $f(s) \neq f(t)$. Denn es gibt ein $g \in G$ mit $g(s) = t$ und wir erhalten

$$f(t) = f(g(s)) = g(f(s)) .$$

Da G semiregulär ist, muß $f(t) \neq f(s)$ sein.

Aus der Vertauschbarkeit von $f \in G^+$ mit allen $g \in G$ erhält man ferner, daß zu jedem $\alpha \in J$ ein $\gamma \in J$ existiert mit $fK_\alpha = K_\gamma$. Das bedeutet, daß die Transitivitätsgebiete von G eine zulässige Partition zu G^+ bilden, was auch aus Lemma 2 folgt. Ferner sieht man mit Lemma 4, daß $f \in G^+$ genau dann in G^* ist, wenn f auf den Transitivitätsgebieten von G eine Permutation induziert.

FOLGERUNG 2. *Ist A ein Automat wie in Satz* 13 *und B der Automat auf einer seiner Komponenten, so ist*

$$G(A) \cong S_k \circ G(B) ,$$

wobei S_k die Gruppe aller Permutationen auf der Menge der starken Komponenten von A und $\circ$ das Kranzprodukt [6] *von Permutationsgruppen bezeichnet.*

FOLGERUNG 3. *Ist G eine reguläre Permutationsgruppe, so ist $G^+ = G^*$ und G^* ist regulär.*

BEWEIS. Nach Satz 13 ist G^* und damit G^+ transitiv. Ferner ist auch $(G^+)^+ \supset G$ transitiv. Anwendung von Satz 6 liefert die Behauptung $G^+ = G^*$. Die Regularität von G^* folgt auch daraus, daß die Automorphismen eines st. zush. Automaten semireguläre Permutationen sind.

Satz 13 gestattet im allgemeinen keine Umkehrung, denn aus der Transitivität von $G(A)$ kann man nur schließen, daß $F(A)$ eine semireguläre Halbgruppe ist. Ist $|S| < \infty$, so folgt, sh. [1] aus der Transitivität von $G(A)$, daß $F(A)$ eine semireguläre Permutationsgruppe ist. Dieses Ergebnis kann man nur unter Einschränkungen auf $|S| = \infty$ verallgemeinern.

Satz 14. *Ist jede Komponente des Automaten A eine starke Komponente und ist $E(A)$ transitiv, so ist $F(A)$ eine semireguläre Permutationsgruppe.*

BEWEIS. Wir verwenden Satz 11. Es ist jede Komponente von A st. zush. und $G(A)$ ist transitiv. Die Automorphismengruppe H einer starken Komponente von A ist eine reguläre Gruppe und nach Folgerung 3 zu Satz 13 ist $H^* = H^+$ eine reguläre Gruppe von Permutationen. Da keine Abbildung aus $F(A)$ ein Element aus einer Komponente K in eine Komponente $K' \neq K$ abbildet, sind alle Abbildungen aus $F(A)$ Permutationen und wegen Lemma 1 ist $F(A) \subset G(A)^+$ semiregulär.

SATZ 15. *Ist G eine reguläre Permutationsgruppe auf S, so ist $G^* \cong G$.*

BEWEIS. Es sei $s \in S$ beliebig gewählt. Wir definieren $\varphi\colon G \to G^*$ durch:

$\varphi(f) := h$ genau dann, wenn $f(s) = h^{-1}(s)$, wobei $f \in G$ und $h \in G^*$ ist. Es ist φ bijektiv, weil G und G^* reguläre Gruppen sind. Es sei $\varphi(f) = h$ und $\varphi(g) = k$. Dann ist:

$$(g \circ f)(s) = g\big(h^{-1}(s)\big) = h^{-1}\big(g(s)\big) = h^{-1}\big(k^{-1}(s)\big) = (k \circ h)^{-1}(s)$$

und man erhält $\varphi(g \circ f) = \varphi(g) \circ \varphi(f)$.

BEMERKUNG. Für $|S| < \infty$ stammt das Ergebnis des Satzes 15 von C. Jordan. Man vergleiche auch [1].

SATZ 16. *Ist G eine semireguläre Permutationsgruppe auf S mit $|S|>2$, so ist $G^{**}=G$.*

BEWEIS. Ist G regulär, so folgt die Behauptung daraus, daß auch G^* und G^{**} reguläre Gruppen sind. Besteht G nur aus der Identität, so ist G^* die vollständige symmetrische Gruppe auf S und G^{**} kann nur aus id_S bestehen. Andernfalls hat G mindestens zwei Transitivitätsgebiete mit mindestens zwei Elementen, und nach Satz 13, Folgerung 2 ist G^* das Kranzprodukt $S \circ H^*$, wo S die symmetrische Gruppe auf der Menge der Transitivitätsgebiete und $H^* = (G|K)^*$ ist, K Transitivitätsgebiet von G. Aus diesen Eigenschaften ist unmittelbar ersichtlich, daß jedes Element f aus G^{**} jedes Transitivitätsgebiet K von G in sich überführt und $f|K \in (G|K)^{**}$ ist. Der Satz folgt aus $(G|K)^{**} = G|K$ und daraus, daß G^* transitiv, also G^{**} semiregulär ist.

Für $|S|<\infty$ hat Brauer [1] den Satz 16 bewiesen. Für $|S|=2$ ist der Satz nicht richtig, weil S_2 abelsch ist.

SATZ 17. *Sind die Voraussetzungen von Satz 16 erfüllt, so gilt $G^{+*}=G^{++}=G$.*

BEWEIS. In jedem Fall ist $G^+ \supseteq G^*$ und daher $(G^+)^* \subseteq G^{**} = G$ wegen Satz 16. Andererseits ist trivialerweise G^{+*} eine Obermenge von G, und wir erhalten $G^{+*}=G$. Es genügt wegen der Transitivität von $G^+ \supset G^*$ (die Inklusion ist echt, wenn G nicht transitiv ist!) zu zeigen, daß alle $f \in G^{++}$ injektiv sind. Denn daraus folgt mit Lemma 1, daß alle Elemente von G^{++} Permutationen und somit in G^{+*} sind. Es seien K_α, $\alpha \in J$, die Transitivitätsgebiete von G und $f \in G^{++}$. Angenommen, es wäre $f(s)=t$ mit $s \in K_\alpha$, $t \in K_\beta$ und $\alpha \neq \beta$. Es gibt ein $h \in G^+$ mit $h(s)=s$ und $h(t) \neq t$, was etwa aus Satz 13, Folgerung 2 folgt. Wir erhalten $t \neq hf(s) = fh(s) = f(s) = t$, Widerspruch! Jedes $f \in G^{++}$ bildet jedes K_α daher in sich ab. Die Restriktion $f|K_\alpha$ ist mit allen Restriktionen $g|K_\alpha$, mit $g \in G^+$ und $g|K_\alpha = K_\alpha$, vertauschbar. $G|K_\alpha$ ist eine reguläre Permutationsgruppe auf K_α. Ist $G^+|K_\alpha = \{g|K_\alpha | g \in G^+, gK_\alpha = K_\alpha\}$, so ist $G^+|K_\alpha = (G|K_\alpha)^+ \cdot (G|K_\alpha)^*$ ist ebenfalls regulär und $(G^+|K_\alpha)^+ = (G|K_\alpha)^{++} = (G|K_\alpha)^{**}$. Die Restriktion $f|K_\alpha$ ist somit bijektiv, womit der Satz bewiesen ist.

Zum Abschluß der Arbeit wird noch eine Anwendung auf das direkte Produkt von Automaten gemacht. Es werden damit Resultate von Pickett [8] auf unendliche Automaten übertragen. Die Beweismethode ist analog zu [8].

DEFINITION [9]. *Es seien* $A = (S, I, M)$ *und* $B = (T, I, N)$ *zwei Automaten mit derselben Halbgruppe* I. *Das direkte Produkt* $A \times B$ *ist der Automat* $(S \times T, I, M \times N)$, *wo* $S \times T$ *das kartesische Produkt von* S *und* T *ist und* $M \times N$ *erklärt ist durch*

$$M \times N\big((s, t), x\big) = \big(M(s, x), N(t, x)\big) .$$

Sind F_1 und F_2 Abbildungshalbgruppen auf den Mengen S und T, so ist die Halbgruppe $F_1 \times F_2$, das *direkte Produkt* von F_1, F_2, erklärt als die Gesamtheit aller Abbildungen $f \times g$ von $S \times T$ mit

$$(f \times g)(s, t) = \big(f(s), g(t)\big)$$

Die Verknüpfung in $S \times T$ ist gegeben durch

$$(f_1 \times g_1) \circ (f_2 \times g_2) = (f_1 \circ f_2) \times (g_1 \circ g_2) .$$

SATZ 18. *Es seien* G *und* H *semireguläre Permutationsgruppen auf den Mengen* S *bzw.* T. *Dann gilt*

$$(G^+ \times H^+)^* = G \times H .$$

BEWEIS. Es sei $\varphi \in (G^+ \times H^+)^*$ und (s, t), (s, t') aus $S \times T$. Da H^+ transitiv ist, gibt es $h^+ \in H^+$ mit $h^+(t) = t'$. Es sei $\varphi(s, t) = (q, r)$, $\varphi(s, t') = (m, n)$. Wir erhalten mit id_s = Identität auf S (es ist $\mathrm{id}_s \in G^+$) die Beziehung

$$(m, n) = \varphi(s, t') = \varphi \circ (\mathrm{id}_s \times h^+)(s, t) = (\mathrm{id}_s \times h^+) \circ \varphi(s, t) =$$
$$= (\mathrm{id}_s \times h^+)(q, r) = (q, h^+ r).$$

Daraus folgt $q = m$, dh. $\varphi(s, t)$ und $\varphi(s, t')$ stimmen wieder in der ersten Komponente überein. Ist π_s die Projektion von $S \times T$ auf S so ist

$$\varphi_1 \colon \varphi_1(s) = \pi_s \circ \varphi(s, t) \quad \text{für alle } s \in S$$

eine Abbildung von S in sich. Hat π_T die entsprechende Bedeutung, so ist analog durch

$$\varphi_2 \colon \varphi_2(t) = \pi_T \circ \varphi(s, t) \quad \text{für } t \in T$$

eine Abbildung von T definiert. Da $\varphi(s,t) = (\pi_s\varphi(s,t), \pi_T\varphi(s,t))$ ist, sieht man, daß $\varphi = \varphi_1 \times \varphi_2$ ist. Wir zeigen, daß $\varphi_1 \in (G^+)^+$ und $\varphi_2 \in (H^+)^+$ ist. Dazu seien $g^+ \in G^+$ und $h^+ \in H^+$ beliebig. Dann gilt

$$(g^+\varphi_1(s), h^+\varphi_2(t)) = (g^+ \times h^+) \circ (\varphi_1 \times \varphi_2)(s,t) =$$

$$= (g^+ \times h^+) \circ \varphi(s,t) = \varphi \circ (g^+ \times h^+)(s,t) = (\varphi_1 g^+(s), \varphi_2 h^+(t)),$$

also

$$g^+\varphi_1 = \varphi_1 g^+ \quad \text{und} \quad h^+\varphi_2 = \varphi_2 h^+.$$

Nach Satz 17 ist aber $(G^+)^+ = G$ und $(H^+)^+ = H$ und daher $\varphi \in G \times H$. Daß umgekehrt jedes $\varphi \in G \times H$ in $(G^+ \times H^+)^*$ liegt, ist unmittelbar zu sehen.

Es seien G und H semireguläre Permutationsgruppen auf den Mengen S und T. Wir erklären Automaten $A = (S, G^+ \times H^+, M)$ und $B = (T, G^+ \times H^+, N)$ durch

$$M(s, g^+ \times h^+) = g^+(s), \; N(t, g^+ \times h^+) = h^+(t)$$

für alle $g^+ \in G^+$ und $h^+ \in H^+$. Aus der Transitivität von G^+ bzw H^+ folgt, daß A und B und auch ihr direktes Produkt $A \times B$ st. zush. sind.

SATZ 19. *Es seien G und H semireguläre Permutationsgruppen auf den Mengen S und T. Für die oben definierten Automaten gilt $G(A) = G$, $G(B) = H$ und*

$$G(A \times B) = G \times H.$$

BEWEIS. Aus der Definition von A und B ist ersichtlich, daß $F(A) = G^+$ und $F(B) = H^+$ ist. Daher ist $G(A) = (F(A))^* = (G^+)^* = G$ und analog ist $G(B) = H$. Weiters gilt $F(A \times B) = G^+ \times H^+$ und somit

$$G(A \times B) = (G^+ \times H^+)^* = G \times H$$

nach Satz 18.

Der Satz 19 löst ein von Weeg [11] gestelltes Problem für den Fall unendlicher Automaten.

LITERATUR

[1] W. Brauer, *Gruppentheoretische Untersuchungen bei endlichen Automaten*, ZAMM, **48** (1968), Sonderheft T113-T115.

[2] W. Dörfler, *Zur algebraischen Theorie der Automaten*, EIK **9** (1973), 171-177.

[3] A. C. Fleck, *Isomorphism groups of automata*, J. Assoc. Comp. Machinery, **9** (1962), 469-476.

[4] A. C. Fleck, *On the automorphism group of an automaton*, J. Assoc. Comp. Machinery, **12** (1965), 566-569.

[5] F. Gécseg - I. Peak, *Algebraic theory of automata*, Akadémiai Kiadó, Budapest, 1972.

[6] R. Kochendörffer, *Lehrbuch der Gruppentheorie unter besonderer Berücksichtigung der endlichen Gruppen*, Leipzig, 1966.

[7] E. F. Moore, *Gedanken-experiments on sequential machines*, in « Automata Studies », ed. C. E. Shannon und J. McCarthy, Princeton, 1956.

[8] R. H. Oehmke, *On the structures of an automaton and its input semigroup*, J. Assoc. Comp. Machinery, **10** (1963), 521-525.

[9] H. E. Pickett, *Note concerning the algebraic theory of automata*, J. Assoc. Comp. Machinery, **14** (1967), 282-288.

[10] M. O. Rabin - D. Scott, *Finite automata and their decision problems*, IBM J. Res. Dev., **3** (1959), 114-125.

[11] G. P. Weeg, *The structure of an automaton and its operation preserving group*, J. Assoc. Comp. Machinery, **9** (1962), 345-349.

[12] G. P. Weeg, *The automorphism group of the direct product of strongly related automata*, J. Assoc. Comp. Machinery, **12** (1965), 187-195.

[13] H. Wielandt, *Finite Permutation Groups*, New York, 1964.

Manoscritto pervenuto in Redazione il 17 giugno 1972 e in forma riveduta e corretta il 23 ottobre 1972.