Commentationes Mathematicae Universitatis Carolinae

Jan Kastl

Die K-abgeschlossenen Teilmengen der Halbgruppen

Commentationes Mathematicae Universitatis Carolinae, Vol. 17 (1976), No. 1, 135--146

Persistent URL: http://dml.cz/dmlcz/105681

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

17,1 (1976)

DIE K-ABGESCHLOSSENEN TEILMENGEN DER HALBGRUPPEN

Jan KASTL, Praha

Inhalt: Man untersucht den Zusammenhang der k-stelligen assoziativen Operationen mit den zweistelligen assoziativen Operationen. Es ist bewiesen, dass jede k-stellige assoziative Operation auf der Menge X aus einer zweistelligen assoziativen Operation γ auf Y, $Y \supseteq X$ zu bekommen ist. Anderseits untersucht man auch, "wieviel-stellige" Operationen jede zweistellige assoziative Operation γ auf den Teilmengen $Z \subseteq Y$ bilden kann.

Schlüsselwörter: k-stellige assoziative Operation, additive Unteharlbgruppe der natürlichen Zahlen,

AMS: 20M20 Ref. Ž.: 2.721.4

Im ersten Teil der Arbeit wird ein nicht langer Beweis der Tatsache angeführt, dass es für jede auf der Menge X operierende k-stellige assoziative Operation λ eine Menge Y, $Y \supseteq X$, und auf Y operierende zweistellige assoziative Operation γ gibt, die die Operation λ durch die ersichtliche Vorschrift $\lambda(x_1,\ldots,x_k) = \gamma(x_1,\ldots,\gamma(x_{k-1},x_k)..)$ bildet. Im Grund dieses Beweises liegt ein Verfahren der Konkretisierung von Operation λ mit Hilfe der Abbildungskomposition.

Im zweiten Teil wird es untersucht, "wieviel-stellige" Operationen eine Halbgruppe auf ihren Teilmengen bilden kann.

Wie V. Koubek bemerkt hat, bilden alle solchen Zahlen für gegebene Teilmenge eine Unterhalbgruppe der additiven Halbgruppe natürlicher Zahlen. Es wird gezeigt, dass anderseits ein System von Abbildungen einer endlichen Menge in sich selbst (bzw. ein System von endlichen Quadratmatrizen) zur gegebenen Unterhalbgruppe N_1 der natürlichen Zahlen konstruiert werden kann, für das Folgendes gilt: Dieses System ist auf die Komposition von $k + 1$ Abbildungen (bzw. auf das Produkt von $k + 1$ Matrizen) genau dann abgeschlossen, wenn $k \in N_1$ gilt.

Grundbegriffe: Mengen werden mit grossen Buchstaben wie X, X, ... bezeichnet, die Menge der natürlichen Zahlen bezeichnen wir mit N, dabei nehmen wir an, dass $0 \notin N$. Im üblichen Sinne verwenden wir zur Beschreibung von Mengen die Klammern $\{ \dots \}$. X^k $(k \in N)$ heisst die k-te kartesische Potenz der Menge X. Der Pfeil $f: X \longrightarrow Y$ stellt eine Abbildung der Menge X in die Menge Y dar, ihre Komposition mit der Abbildung $g: Y \longrightarrow Z$ beschreiben wir $g \circ f: X \longrightarrow Z$.

Bemerken wir noch, dass wir jenen Teil der indizierten Menge für leer halten, der mit natürlichen Zahlen von m bis $m - 1$ indiziert wird -- z.B. für $k = 1$ ist

$$\{ x_1, \dots, x_{k-1}, y_k, \dots, y_{k+r} \} = \{ y_1, \dots, y_{r+1} \} .$$

Definition: Unter einer k-stelligen Operation λ auf der Menge X (k ist eine natürliche Zahl) verstehen wir beliebige Abbildung $\lambda: X^k \longrightarrow X$.

Die k-stellige Operation λ auf der Menge X halten wir für assoziativ, sofern für jedes Paar $1 \leq i,j \leq k$ und für beliebige $x_1,..,x_{2k-1} \in X$ folgende Gleichung gilt:

$$\lambda(\underbrace{x_1,..,x_{i-1}}_{i-1},\ \lambda(x_i,..,x_{k+i-1}),\ \underbrace{x_{k+i},..,x_{2k-1}}_{k-i}) =$$

$$= \lambda(\underbrace{x_1,..,x_{j-1}}_{j-1},\ \lambda(x_j,..,x_{k+j-1}),\ \underbrace{x_{k+j},..,x_{2k-1}}_{k-j}) .$$

Definition: Sei γ eine zweistellige assoziative Operation auf der Menge X . Die Teilmenge $Y \subseteq X$ heisst k-abgeschlossene Teilmenge der Halbgruppe (X,γ) ($2 \leq k \in N$) , wenn für jedes k-Tupel $(x_1,..,x_k) \in Y^k$ gilt:

$$\gamma(x_1,\ \gamma(x_2,..,\ \gamma(x_{k-1},x_k)\ ..\ )) \in Y .$$

Das Zeichen N(Y) bezeichnet die Menge aller solchen natürlichen Zahlen r , für die Y (r + 1)-abgeschlossene Teilmenge der Halbgruppe (X,γ) ist.

Y ist eine k-abgeschlossene Teilmenge der (X,γ) genau dann, wenn γ im natürlichen Sinne eine k-stellige Operation auf Y bildet — d.h., wenn die k-stellige (selbstverständlich assoziative) Operation λ , die durch die klare Vorschrift $\lambda(x_1,..,x_k) = \gamma(x_1,..,\ \gamma(x_{k-1},x_k)\ ..\ )$ $(x_1,..,x_k \in X)$ auf der Menge X definiert ist, bei der Begrenzung auf die Menge Y^k eine k-stellige Operation auf der Menge Y bildet.

Behauptung 1: Sei λ eine k-stellige assoziative Operation auf der Menge X ($k \geq 2$). Es besteht ein System F von den Abbildungen gewisser Menge Z in sich selbst und eine injektive Abbildung $\varphi : X \longrightarrow F$ derart, dass für jede $x_1,..,x_k \in X$ $\varphi(\lambda(x_1,..,x_k)) = \varphi(x_1) \circ .. \circ \varphi(x_k)$ gilt.

Das System F ist dabei auf die Abbildungskomposition abgeschlossen und hat gleichwertige Mächtigkeit wie die Menge Z.

Beweis: Man nehme ein festes Element ι derart, dass $\iota \notin X$. Wir definieren die Menge Z'' als System aller formalen Ausdrücke $Z'' = \{\lambda(\underbrace{\iota,..,\iota}_{i},x_1,..,x_{k-i}) ; x_1,...,x_{k-1} \in X , 1 \leq i \leq k\}$. Dabei nehmen wir an, dass $X \cap Z'' = \emptyset$ gilt.

Man bezeichne $Z' = X \cup Z''$. Auf der Menge Z' definieren wir folgenderweise die Relation φ :

1) für jedes $1 \leq i \leq k-2$ und für jede $1 \leq m , n \leq k-i$, $x_1...,x_{2k-i-1} \in X$ befinden sich in der Relation φ diese Elemente:

$\lambda(\underbrace{\iota,...,\iota}_{i},x_1,...,x_{k-i-m}, \lambda(x_{k-i-m+1},...,x_{2k-i-m}) ,$

$x_{2k-i-m+1},..,x_{2k-i-1})$,

$\lambda(\underbrace{\iota,..,\iota}_{i},x_1,..,x_{k-i-n}, \lambda(x_{k-i-n+1},..,x_{2k-i-n}) ,$

$x_{2k-i-n+1},..,x_{2k-i-1})$

2) für $i = k-1$ und jedes $x \in X$ $\lambda(\iota,..,\iota,x) \varphi x$. Bezeichnen wir mit R die durch φ gebildete Äquivalenzrelation auf der Menge Z'. Es ist zu sehen, dass die Beziehung $\lambda(\underbrace{\iota,..,\iota}_{i},x_1,..,x_{k-i}) R \lambda(\underbrace{\iota,..,\iota}_{j},y_1,..,y_{k-j})$ für zwei Elemente aus Z'' nur dann gelten kann, wenn $i = j$ ist. Für beliebiges $x \in X$ bildet die Menge $\{x, \lambda(\iota,..,\iota,x)\}$ eine ganze Äquivalenzklasse der Relation R ; $\{\lambda(\iota,..,\iota)\} = \tau$ ist auch eine Äquivalenzklasse.

Man bezeichne die Menge aller Äquivalenzklassen der Relation R mit $Z = Z'/R$ und mit $[z']$ die Äquivalenzklasse, die das Element $z' \in Z'$ enthält. Für jedes $a \in X$ können wir jetzt zwei Abbildungen $l_a, p_a: Z \to Z$ durch folgende Vorschriften definieren:

$$l_a\,[\lambda(\underset{--i---}{\iota,..,\iota}, \underset{---k-i--}{x_1,..,x_{k-i}})] = [\lambda(\underset{-i-1--}{\iota,..,\iota}, a, \underset{---k-i--}{x_1,..,x_{k-i}})]$$

$$p_a\,[\lambda(\underset{--i---}{\iota,..,\iota}, \underset{---k-i--}{x_1,..,x_{k-i}})] = [\lambda(\underset{-i-1--}{\iota,..,\iota}, \underset{---k-i--}{x_1,..,x_{k-i}}, a)]$$

$(1 \leq i \leq k,\ x_1,..,x_{k-i} \in X)$.

Die Abbildungen sind korrekt definiert. Man bemerke dazu, dass erstens $[\lambda(\iota,..,\iota,x)] = [x]$ und zweitens

$$\lambda(\underset{--i---}{\iota,..,\iota}, \underset{---k-i--}{x_1,..,x_{k-i}}) \wp \lambda(\underset{--i---}{\iota,..,\iota}, \underset{---k-i--}{y_1,..,y_{k-i}}) \Longrightarrow$$

$$\Longrightarrow \lambda(\underset{-i-1--}{\iota,..,\iota}, a, \underset{---k-i--}{x_1,..,x_{k-i}}) \wp \lambda(\underset{-i-1--}{\iota,..,\iota}, a, \underset{---k-i--}{y_1,..,y_{k-i}}),$$

$$\lambda(\underset{-i-1--}{\iota,..,\iota}, \underset{---k-i--}{x_1,..,x_{k-i}}, a) \wp \lambda(\underset{-i-1--}{\iota,..,\iota}, \underset{---k-i--}{y_1,..,y_{k-i}}, a)$$

(für $2 \leq i \leq k$ und $i = 1$).

Für beliebige $a, b \in X$ gilt jetzt: $l_a \circ p_b = p_b \circ l_a$. Sei nämlich $[\lambda(\underset{--i---}{\iota,..,\iota}, \underset{---k-i--}{x_1,..,x_{k-i}})]$ ein beliebiges Element der Menge Z, dann können wir schreiben:

$$(l_a \circ p_b)\,[\lambda(\underset{--i---}{\iota,..,\iota}, x_1,..,x_{k-i})] =$$

$$= l_a\,[\lambda(\underset{-i-1--}{\iota,..,\iota}, x_1,..,x_{k-i}, b)] =$$

wenn $i \geq 2$

$$= [\lambda(\underset{-i-2--}{\iota,..,\iota}, a, x_1,\ldots,x_{k-i}, b)] =$$

wenn $i = 1$

$$= [\lambda(\underset{-k-2--}{\iota,..,\iota}, a, \lambda(x_1,..,x_{k-1}, b))] =$$

$= [\lambda(\underbrace{\upsilon,..,\upsilon}_{k-2}, \lambda(a,x_1,..,x_{k-1}),b)] =$

$= (p_b \circ l_a)\ [\lambda(\underbrace{\upsilon,..,\upsilon}_{i},x_1,..,x_{k-i})]$.

Wir bezeichnen die identische Abbildung der Menge Z mit $l_\upsilon : Z \longrightarrow Z$. Man nehme folgendes System F der Abbildungen:

$$F = \{\underbrace{l_\upsilon \circ .. \circ l_\upsilon}_{i} \circ \underbrace{l_{a_1} \circ .. \circ l_{a_{k-i}}}_{k-i} ;\ 1 \leq i \leq k ,\ a_1,..,a_{k-i} \in X\}.$$

Jetzt können wir behaupten: Für jedes $z \in Z$ existiert genau ein $f \in F$ derart, dass $f(\tau) = z$ gilt.

Sei z ein beliebiges Element der Menge Z , $z =$

$= [\lambda(\underbrace{\upsilon,..,\upsilon}_{i},\underbrace{x_1,..,x_{k-i}}_{k-i})] =$

$= (\underbrace{l_\upsilon \circ .. \circ l_\upsilon}_{i} \circ \underbrace{l_{x_1} \circ .. \circ l_{x_{k-i}}}_{k-i})\ [(\upsilon,..,\upsilon)]$.

Man verwende weiter folgende Implikation: $f_1, f_2, g \in F$, $(f_1 \circ f_2)(\tau) = g(\tau) \Longrightarrow f_1 \circ f_2 = g$. Für z gilt jedoch:

$(f_1 \circ f_2)(z) = (f_1 \circ f_2 \circ p_{x_{k-i}} \circ .. \circ p_{x_1})\ [\lambda(\upsilon,..,\upsilon)] =$

$= (p_{x_{k-i}} \circ .. \circ p_{x_1} \circ f_1 \circ f_2)(\tau) = (p_{x_{k-i}} \circ .. \circ p_{x_1} \circ g)(\tau) =$

$= g(z)$.

Für $f_1 = l_\upsilon$ also $f(\tau) = g(\tau) \Longrightarrow l_\upsilon \circ f = f = g$. Danach sind das System F und die Menge Z gleichmächtig.

Für $f_1, f_2 \in F$ muss auch ein $h \in F$ derart existieren, dass $h(\tau) = (f_1 \circ f_2)(\tau)$ ist, d.h. $f_1 \circ f_2 = h \in F$. Das System F wird also auf die Abbildungskomposition abgeschlossen.

Definieren wir die Abbildung $\varphi : X \longrightarrow F$ wie $\varphi(x) =$ $= l_x$. Da $l_x(\tau) = \{x, \lambda(\upsilon,..,\upsilon,x)\}$ gilt, ist φ sicher eine injektive Abbildung. Dabei sehen wir:

$(\varphi(x_1) \circ \ldots \circ \varphi(x_k))(\tau) = [\lambda(x_1,..,x_k)] =$
$= \varphi(\lambda(x_1,..,x_k))(\tau)$ (für beliebiege $x_1,..,x_k \in X$). Es muss also gelten: $\varphi(x_1) \circ .. \circ \varphi(x_k) = \varphi(\lambda(x_1,..,x_k))$. Der Beweis ist dadurch vollendet.

Die Halbgruppe $(F, \circ)$ bildet also auf der k-abgeschlossenen Teilmenge $\varphi(X)$ eine k-stellige Operation, die in der bekannten Bedeutung mit der auf der Menge X operierenden Operation λ isomorph ist.

Man beachte noch, dass die Menge Z für den Fall der endlichen Menge X auch endlich ist.

Bemerkung 1: Die Bildung der k-stelligen assoziativen Operation λ aus der zweistelligen assoziativen Operation γ ist in der Tat ein treuer Funktor $\mathcal{G}$ aus der Varietät aller Halbgruppen in die Varietät der k-stelligen assoziativen Operationen. Wie es aus der Theorie der universellen Algebren folgt (siehe z.B. den Grund des Beweises aus [1] - III. 4.2), gibt es zu diesem Funktor $\mathcal{G}$ einen Linksadjungierten $\mathcal{F}$.

Da die Abbildung φ aus der bewiesenen Behauptung injektiv ist, muss die Einheit dieser Adjunktion von Monomorphismen erzeugt werden. Nehmen wir statt der Halbgruppe $(F, \circ)$ und der Abbildung $\varphi : X \to F$ die Unterhalbgruppe ohne identische Abbildung -- $(F', \circ) = (F - \{1_F\}, \circ)$ -- und die gleichermassen definierte Abbildung $\varphi' : X \to F'$, so können wir dann die Adjunktion in der folgenden Form gewinnen:

$$\mathcal{F}(X,\lambda) = (F', \circ), \quad \eta^{(X,\lambda)} : (X,\lambda) \xrightarrow{\varphi'} \mathcal{G}(F', \circ).$$

(Betonen wir noch, dass nämlich folgende Beziehung gilt:

für $a_1,\dots,a_{k-1},b_1,\dots,b_{k-j} \in X$, $1 \leq i,j \leq k-1$

$$l_{a_1} \circ \dots \circ l_{a_{k-i}} = l_{b_1} \circ \dots \circ l_{b_{k-j}} \Longleftrightarrow [\lambda(\underset{\text{---i---}}{\iota,\dots,\iota},a_1,\dots,a_{k-i})] =$$

$$= [\lambda(\underset{\text{---j---}}{\iota,\dots,\iota},b_1,\dots,b_{k-j})] \Longrightarrow i = j \ .\ )$$

Beachten wir jetzt die Formen der Mengen $N(Y)$.

Behauptung 2: Sei (X,γ) eine Halbgruppe und $Y \subseteq X$ ihre Teilmenge. $N(Y)$ ist eine (möglicherweise leere) Unterhalbgruppe der additiven Halbgruppe der natürlichen Zahlen.

Beweis ist trivial.

Behauptung 3: Sei $(N,+)$ die additive Halbgruppe der natürlichen Zahlen. $N_1 \subseteq N$ sei ihre beliebige Unterhalbgruppe. Für die Menge $M = \{r+1 \ ; \ r \in N_1 \cup \{0\}\} \subseteq N$ gilt dann $N(M) = N_1$.

Beweis: Haben wir beliebige $q \in N_1$, $x_1,\dots,x_{q+1} \in M$. Wir können schreiben: $x_1 + \dots + x_q + x_{q+1} = r_1 + \dots + r_q + \dots + r_{q+1} + q + 1$, wo $r_1,\dots,r_{q+1} \in N_1 \cup \{0\}$. Daher $x_1 + \dots + x_{q+1} \in M$. Wir sehen, dass $N_1 \subseteq N(M)$.

Der Fall $q \in N(M) \dot{-} N_1$ führt zum Widerspruch. Für $1 \in M$ müsste nämlich $\underset{\text{---q+1-------}}{1 + \dots + 1 + 1} = q + 1 \in M$ gelten, und wir würden eine ungültige Beziehung $q \in N_1 \cup \{0\}$ bekommen, denn $(N(M) \dot{-} N_1) \cap (N_1 \cup \{0\})$ ist leer. Dadurch haben wir $N_1 = N(M)$ bewiesen.

Möchten wir zu der Unterhalbgruppe $N_1 \subseteq N$ nun solche Halbgruppe (X,γ) finden, die eine Teilmenge Y mit der Eigenschaft $N(Y) = N_1$ enthält, so können wir sogar, wie es folgt, die Endlichkeit der Menge X annehmen.

Lemma 1: Sei (X,γ) eine Halbgruppe und φ ihre Kongruenz. Die Menge der Kongruenzklassen bezeichnen wir mit $X/\varphi = \{[x]\,;\ x\in X\}$. Ist Y $(Y\subseteq X)$ eine k-abgeschlossene Teilmenge von (X,γ), so ist auch $Z = \{[y];\ y\in Y\}$ die k-abgeschlossene Teilmenge der Quotientenhalbgruppe $(X/\varphi\ ,\ \gamma/\varphi)$ $(k\geq 2)$.

Lemma 2: Für jede additive Unterhalbgruppe $N_1\neq\emptyset$ der Halbgruppe der natürlichen Zahlen gilt $N_1 = \{px\,;\ x\in N_2\}$, wo p eine natürliche Zahl und N_2 eine residuelle Unterhalbgruppe der natürlichen Zahlen ist -- d.h. $\exists\, q\in N$ derart, dass $x\in N$, $x\geq q \Longrightarrow x\in N_2$ gilt.

Beweis: Sei $D = \{d\in N\,;$ für $\forall\, n\in N_1\ \exists\, m\in N$ $dm = n\}$. Es gibt ein maximales Element der Menge D -- $p = \max D$. Nehmen wir $N_2 = \left\{\frac{y}{p}\,;\ y\in N_1\right\}$.

In dieser Unterhalbgruppe $N_2\subseteq N$ muss man schon zwei relative Primzahlen finden. Sei a ein beliebiges Element der Menge N_2, sei $a\neq 1$. Seien $p_1,..,p_k$ $(k\geq 1)$ alle gegenseitig verschiedenen Primzahlen, die a dividieren. Für jedes p_i $(1\leq i\leq k)$ muss ein $x_i\in N_2$ derart existieren, dass p_i x_i nicht dividiert. In N_2 liegt dann Element $b = \sum_{i=1}^{k} p_1..p_{i-1}p_{i+1}..p_k x_i$. Jetzt ist es zu sehen, dass kein p_i das Element b dividiert.

Für diese relative Primzahlen a, b gilt: $x\in N$, $x\geq ab \Longrightarrow x\in N_2$. Sei $x\geq ab$ eine natürliche Zahl. Dann kann man schreiben: $x = c + fb$, wo f und $0\leq c<b$ ganze Zahlen sind. Die Gleichung $a\xi + b\eta = c$ hat für relative Primzahlen a, b solche Lösung, dass ξ_0, η_0 ganze Zahlen

sind, und für ξ_0 noch $0 \leq \xi_0 < b$ gilt. Also $a\xi_0 + b(\eta_0 + f) = x$, $b(\eta_0 + f) = x - a\xi_0 > ab - ab = 0$. $\omega_0 = \eta_0 + f$ ist daher eine natürliche Zahl. Das $x = \underbrace{a + \ldots + a}_{\xi_0} + \underbrace{b + \ldots + b}_{\omega_0}$ muss also ein Element der Halbgruppe N_2 sein.

Behauptung 4: Sei N_1 eine Unterhalbgruppe der natürlichen Zahlen. Dann gibt es eine endliche (sogar kommutative) Halbgruppe (X, γ) und eine Menge $(\emptyset \neq)\ Y \subseteq X$ derart, dass $N(Y) = N_1$ gilt.

Beweis: I. Ist $N_1 = \emptyset$, so nehmen wir die zweielementige Menge $\{a,o\} = X$ mit der Operation γ, die X^2 auf o abbildet. Dann $N(\{a\}) = \emptyset$.

II. Für $N_1 \neq \emptyset$ nehmen wir $N_2 \subseteq N$; $p, q \in N$ nach Lemma 2. Man definiere auf der Menge N die Relation ϱ:

$z_1 \varrho z_2 \Longleftrightarrow$ entweder $z_1 = z_2$

oder $z_1 \geq pq + 1$, $z_2 \geq pq + 1$, $z_1 \equiv z_2 \pmod p$

($\equiv$ ist die bekannte Kongruenz nach den Restklassen).

ϱ ist Kongruen auf der Halbrguppe $(N,+)$ und sie hat nur endliche Anzahl von Äquivalenzklassen.

$(N/\varrho, +/\varrho)$ wird die gesuchte (offensichtlich kommutative) Halbgruppe (X, γ) sein. Wie in der Behauptung 3 nehmen wir die Menge $M = \{r + 1;\ r \in N_1 \cup \{0\}\}$. Wie im Lemma 1 nehmen wir $(\emptyset \neq)\ Y = \{[m]_\varrho;\ m \in M\}$.

$N(Y) \supseteq N_1$. Man nehme an, dass es $s \in N(Y)$, $s \notin N_1$ gibt. Dann muss es sein: $\underbrace{[1] + \ldots + [1]}_{s+1} = [s + 1] \in Y$, d.h. es gibt ein $r \in N_1 \cup \{0\}$, $s + 1 \varrho r + 1$. Es zeigt also:

entweder $s + 1 = r + 1 \Longrightarrow s \in N_1 \cup \{0\}$ -- das ist ein Widerspruch,

oder $s + 1 \equiv r + 1 \pmod{p}$, $s + 1 \geq pq + 1$, $r + 1 \geq pq + 1$ -- $s = r + pk$ (k ist eine ganze Zahl), und ebenso kann man schreiben: $r = ph$, $h \geq 0$ ist eine ganze Zahl. Das heisst: $s = p(k + h) \geq pq$, also $k + h \geq q \Longrightarrow k + h \in N_2$. Wir bekommen $s \in N_1$ -- was auch ein Widerspruch ist.

Es gilt wirklich $N(Y) = N_1$.

Korollar 1: Sei N_1 eine Unterhalbgruppe der natürlichen Zahlen. Dann gibt es eine endliche Menge Z und ein System G von Abbildungen aus Z in Z derart, dass $N(G) = N_1$ bezüglich der Abbildungskomposition gilt.

Beweis: Man findet die endliche Halbgruppe (X, γ) und $\emptyset \neq Y \subseteq X$ derart, dass $N(Y) = N_1$ gilt. Diese Halbgruppe werden wir jetzt mit Hilfe der Abbildungen konkretisieren.

Zum Beispiel nach der Behauptung 1 für $k = 2$ ist $\varphi(Y)$ das gesuchte System von Abbildungen.

Korollar 2: Sei N_1 eine Unterhalbgruppe der natürlichen Zahlen. Für den beliebigen Ring R mit der Einheit gibt es dann ein System S endlicher Quadratmatrizen, deren Elemente in R liegen, wobei $N(S) = N_1$ bezüglich des üblichen Matrizenprodukts gilt.

Beweis: Man bezeichne die Quadratmatrix der Ordnung k ($k \in N$) mit $A = (a_{ij})_{\substack{i \in K \\ j \in K}}$, wo K eine Menge der Mächtigkeit k ist. Ein Matrizenprodukt ist dann die Matrix $B.A = (\sum_{j \in K} b_{qj} a_{ji})_{\substack{q \in K \\ i \in K}}$.

Wir nehmen die endliche Menge Z und das System G von Abbildungen aus dem Korollar 1. Zu jeder Abbildung $g: Z \longrightarrow Z$ ordnen wir solche Matrix $A_g = (a_{ij})_{\substack{i\in Z \\ j\in Z}}$ zu:

für jede $x, y \in Z$, $y \neq g(x)$ $a_{y\,x} = 0 \in R$; $a_{g(x)\,x} = 1 \in R$.

Es ist leicht zu sehen, dass das gesuchte System $S = \{A_g ; g \in G\}$ ist.

Bemerkung 2: Zuletzt bemerken wir noch, dass die Systeme G und S aus den Korollarn 1 und 2 bezüglich der entsprechenden Operationen kommutativ sind.

L i t e r a t u r :

[1] COHN P.M.: Universal Algebra, New York, Evanston, and London, Harper-Row, 1965.

[2] MACLANE S.: Categories for the Working Mathematician, Berlin-Heidelberg-New York, Springer, 1972.

[3] TICHÝ T.: Algebraická charakterisace systémů zobrazení (Diplomová práce 1972), unveröffentlicht.

Matematicko-fyzikální fakulta
Universita Karlova
Sokolovská 83, 18600 Praha 8
Československo

(Oblatum 29.9. 1975)