Funktionen auf endlichen Gruppen

Von HANS LAUSCH (Clayton) und WILFRIED NÖBAUER (Wien)

Dem Andenken an Andor Kertész gewidmet

1. Die Menge aller Funktionen auf einer universalen Algebra A mit Werten in A, versehen mit den durch punktweise Ausführung der Operationen von A definierten Operationen, bildet selbst wieder eine Algebra, zu deren Operationen noch die Komposition von Funktionen dazugenommen wird. Die so erhaltene Algebra $F(A)$ und gewisse ihrer Unteralgebren sind in den letzten Jahren von verschiedenen Autoren unter verschiedenen Gesichtspunkten studiert worden, sowohl vom Standpunkt der universalen Algebra aus, als auch für „in der Natur auftretende" Algebren A, wie etwa Gruppen, Ringe oder Verbände (ein Teil der ausgedehnten Literatur über dieses Gebiet ist in [2] zusammengestellt). In dieser Arbeit setzen wir A stets als endliche Gruppe G voraus, wir bemerken aber, daß die Definitionen zum Großteil auch für beliebige universale Algebren A sinnvoll bleiben und sich wohl auch einige der Ergebnisse auf andere Klassen von Algebren übertragen lassen.

2. Sei also $G=\langle G; +, -, 0\rangle$ eine — additiv geschriebene — endliche Gruppe und $\langle F(G); +, -, 0, o\rangle$ die von allen Funktionen auf G mit Werten in G gebildete Algebra, versehen mit den durch punktweise Ausführung der Operationen von G erklärten Operationen $+$, $-$, 0 und der Funktionenkomposition o. Es ist wohlbekannt, daß $F(G)$ mit diesen Operationen einen Fastring mit Einselement 1 der Ordnung $|G|^{|G|}$ bildet (wie üblich bezeichnen wir die Kardinalzahl einer Menge M mit $|M|$). Die Einheitengruppe von $F(G)$ — d. h. die von den bezüglich o invertierbaren Elementen von G gebildete Gruppe — bezeichnen wir mit $\mathfrak{E}(F(G))$, und ganz allgemein bezeichnen wir die Einheitengruppe einer Halbgruppe oder eines Fastringes S mit Einselement stets mit $\mathfrak{E}(S)$. Es besteht $\mathfrak{E}(F(G))$ aus allen Permutationen von G und hat daher die Ordnung $|G|!$ Übrigens ist bekannt (siehe [1], [3]), daß der Fastring $F(G)$ stets einfach ist, ausgenommen den Fall $|G|=2$.

3. Es gibt nun im wesentlichen zwei Möglichkeiten, Unterfastringe von $\langle F(G); +, -, 0, o\rangle$ bzw. Unterhalbgruppen von $\langle F(G); o, 1\rangle$ zu definieren, nämlich entweder durch Invarianzeigenschaften oder durch ein Bildungsgesetz für die Elemente des Unterfastringes oder der Unterhalbgruppe.

Im ersten Fall ist gegeben eine Menge von Relationen $R_i(a_1, a_2, \ldots, a_{n_i})$ auf G. Dann bildet die Menge aller $\varphi\in F(G)$ mit

$$R_i(a_1, a_2, \ldots, a_{n_i}) \Rightarrow R_i(\varphi a_1, \varphi a_2, \ldots, \varphi a_{n_i})$$

jedenfalls eine Unterhalbgruppe $\mathscr{H}(R_i)$ von $\langle F(G); o, 1\rangle$, die Einheitengruppe $\mathscr{E}(\mathscr{H}(R_i))$ dieser Unterhalbgruppe bildet daher eine Untergruppe von $\mathscr{E}(F(G))$. Dieses $\mathscr{H}(R_i)$ kann — muß aber nicht — sogar ein Unterfastring von $F(G)$ sein.

Im zweiten Fall ist gegeben eine Menge W von Elementen von $F(G)$, und man betrachtet die durch W erzeugte Unterhalbgruppe von $\langle F(G); o, 1\rangle$ bzw. den durch W erzeugten Unterfastring von $F(G)$.

Wir geben zunächst drei Beispiele für auf die erste Art konstruierte Unteralgebren von $F(G)$:

a) $R(a, b, c)$ gelte genau dann, wenn $a+b=c$. In diesem Fall ist $\mathscr{H}(R)$ die *Endomorphismenhalbgruppe* $E(G)$ und daher $\mathscr{E}(\mathscr{H}(R))$ die Automorphismengruppe $A(G)$ von G. Es ist aber $\mathscr{H}(R)$ nur dann ein Unterfastring von $F(G)$, wenn G abelsch ist — denn nur in diesem Fall ist $1+1\in\mathscr{H}(R)$.

b) Es durchlaufe N die Menge $\mathfrak{N}$ der Normalteiler von G. Es gelte $R_N(a, b)$ genau dann, wenn $a\equiv b \bmod N$. In diesem Fall ist $\mathscr{H}(R_N|N\in\mathfrak{N})$ die Menge jener Funktionen von $F(R)$, die mit allen Kongruenzen von G „verträglich" sind. Wir nennen diese Funktionen die „*kompatiblen*" Funktionen und bezeichnen ihre Menge mit $C(G)$. Man erkennt sogleich, daß $C(G)$ ein Unterfastring von $F(G)$ ist.

c) Es durchlaufe U die Menge $\mathfrak{U}$ der Untergruppen von G. Es gelte $R_U(a)$ genau dann, wenn $a\in U$. In diesem Fall ist $\mathscr{H}(R_U|U\in\mathfrak{U})$ die Menge aller jener Funktionen von $F(R)$, die alle Untergruppen von G „erhalten". Wir nennen diese Funktionen die „*konservativen*" Funktionen und bezeichnen ihre Menge mit $K(G)$. Auch $K(G)$ ist ein Unterfastring von $F(G)$.

Nun geben wir drei Beispiele für auf die zweite Art konstruierte Teilalgebren von $F(G)$:

d) $W=\{-a+1+a|a\in G\}$. Es ist wohlbekannt, daß W eine Unterhalbgruppe von $F(G)$ — ja sogar eine Untergruppe von $A(G)$ — bildet, nämlich die Gruppe $I(G)$ der *inneren Automorphismen* von G.

e) $W=\{1\}$. Wie man sofort erkennt, besteht die von W erzeugte Untergruppe von $\langle F(G); +, -, 0\rangle$ aus allen Funktionen der Gestalt $n1$ mit $n\in\mathbf{N}$ (natürliche Zahlen) und bildet somit einen Unterfastring von $F(G)$, nämlich den Fastring der „*Grätzerschen Polynomfunktionen*". Wie ebenfalls fast unmittelbar zu sehen, ist dieser Fastring isomorph zum Restklassenring des Ringes der ganzen Zahlen nach dem Exponenten von G, ist daher (zumindest im Fall einer endlichen Gruppe G) nicht weiter interessant.

f) $W=\{G, 1\}$, wo G die Menge der konstanten Funktionen von $F(G)$ bezeichnet. Wie ebenfalls leicht zu sehen, besteht die von W erzeugte Untergruppe von $\langle F(G); +, -, 0\rangle$ aus allen Funktionen der Gestalt $a_1+1+a_2+1+\ldots+a_r+1+a_{r+1}$ mit $r\geqq 0$, $a_i\in G$ und bildet somit einen Unterfastring $P(G)$ von $F(G)$, nämlich den Fastring der „*Polynomfunktionen*".

4. Im Zusammenhang mit diesen Unterhalbgruppen bzw. Unterfastringen $U(G)$ von $F(G)$ oder allgemeiner $U(A)$ von $F(A)$ mit beliebiger Algebra A (wo etwa $U=E, C, K, P$ ist) wurden bisher vor allem drei Arten von Problemen untersucht, nämlich erstens Fragen über die Struktur von $U(G)$ bzw. $\mathscr{E}(U(G))$ bei gegebenem U und G, zweitens das Problem, alle G zu charakterisieren, für welche $U(G)$ oder insbesondere $\mathscr{E}(U(G))$ gegebene Eigenschaften hat (z. B. für welche G das $\mathscr{E}(P(G))$ abelsch, nilpotent, überauflösbar oder auflösbar ist), und schließlich drittens Fragen über den Zusammenhang zwischen den verschiedenen $U(G)$ eines gegebenen G. So ist etwa bekannt, daß $P(G)=F(G)$ genau für die nichtabelschen endlichen ein-

fachen Gruppen und für die Gruppe der Ordnung 2 gilt. (Die Gruppen mit $P(G)=F(G)$ heißen *polynomvollständig*). In diesem Falle ist bei gegebenem U also jedenfalls $U(G)$ in $P(G)$ enthalten, und man kann nun die Frage erheben nach sämtlichen Gruppen G, für die dies der Fall ist (diese Gruppen wollen wir als *U-polynomvollständig* bezeichnen). Ebenso kann man nach jenen Gruppen fragen, für welche $\mathfrak{E}(U(G))$ in $\mathfrak{E}(P(G))$ enthalten ist. Diese Gruppen nennen wir *U-permutationspolynomvollständig*. Klarerweise ist jede U-polynomvollständige Gruppe auch U-permutationspolynomvollständig. Daß die Umkehrung im allgemeinen nicht gilt, werden wir etwas später sehen.

Wir wollen im folgenden einige Ergebnisse zu diesen drei Problemkreisen herleiten. Dazu bemerken wir zunächst, daß stets $P(G)\subseteqq C(G)$. Setzen wir

$$P_0(G) = \{\varphi|\varphi\in P(G), \varphi(0) = 0\}$$

dann ist $P_0(G)$ der von $I(G)$ erzeugte Unterfastring von $\langle F(G); +, -, 0, o\rangle$, und es sind $P(G)\cap E(G)$ und $P(G)\cap K(G)$ in $P_0(G)$ enthalten. Setzen wir $L(G)=\{a+1|a\in G\}$ — klarerweise ist $L(G)$ Unterhalbgruppe von $P(G)$ — dann gilt $P(G)=L(G)\circ P_0(G)$.

5. Nun wollen wir $K(G)$ etwas näher untersuchen. Es sei $\mathfrak{Z}$ die Menge aller zyklischen Untergruppen von G. Bezeichnen wir für $Z\in\mathfrak{Z}$ mit $e(Z)$ die Menge der erzeugenden Elemente von Z, so ist $\{e(Z)|Z\in\mathfrak{Z}\}$ eine Klasseneinteilung von G. Wie sofort zu sehen, gilt $\varrho\in K(G)$ dann und nur dann, wenn $\varrho e(Z)\subseteqq Z$ für alle $Z\in\mathfrak{Z}$. Überdies gilt $\varrho\in\mathfrak{E}(K(G))$ genau dann, wenn $\varrho e(Z)=e(Z)$ für alle $Z\in\mathfrak{Z}$, denn ist dies erfüllt, dann ist ϱ in $K(G)$ enthalten und eine Permutation; treffen umgekehrt diese beiden Aussagen zu, dann ist ϱ auch auf jedem Z eine Permutation, muß daher jedes Element von $e(Z)$ wieder auf ein Element von $e(Z)$ abbilden. Daraus ergibt sich folgender

Satz. *Ist $\mathfrak{Z}$ die Menge aller zyklischen Untergruppen von G und bezeichnet φ die Eulersche Funktion, dann gilt*

$$|K(G)| = \prod(|Z|^{\varphi(|Z|)}|Z\in\mathfrak{Z})$$

$$|\mathfrak{E}(K(G))| = \prod(\varphi(|Z|)!\,|Z\in\mathfrak{Z})$$

und es ist $\mathfrak{E}(K(G))$ isomorph zum direkten Produkt $\prod(\mathrm{Sym}\,\varphi(|z|)|z\in\mathfrak{Z})$.

Als nächstes wollen wir alle K-polynomvollständigen endlichen Gruppen bestimmen. Angenommen, es ist G eine solche, dann gilt $K(G)\subseteqq P_0(G)\subseteqq C(G)$, d. h. es ist jede konservative Funktion auf G auch kompatibel. Angenommen, es sei G nicht einfach und es sei N ein nichttrivialer Normalteiler von G. Die Gesamtheit aller $\psi\in K(G)$ ist nach dem vorhergehenden Satz gegeben durch die ψ mit

$$\psi a = n(a)a \quad \text{mit willkürlichem} \quad n: G\to\mathbf{N}$$

Sind nun $a, b\notin N$ voneinander verschieden und ist $b\equiv a \bmod N$, dann gilt $n(b)b\equiv n(a)a\equiv n(a)b \bmod N$, daher $(n(b)-n(a))b\equiv 0 \bmod N$, also $n(b)\equiv n(a) \bmod \mathbf{o}$, wenn $\mathbf{o}\neq 1$ die Ordnung von b modulo N bezeichnet. Andererseits kann man aber n willkürlich wählen, also auch so, daß diese Bedingung nicht erfüllt ist. Daher ist G jedenfalls einfach. Ist G zyklisch von der Ordnung p, dann gilt $|P_0(G)|=p$ und $K(G)=p^{p-1}$, daher ist G in diesem Fall K-polynomvollständig nur für $p=2$. Somit gilt folgender

Satz. *Eine endliche Gruppe ist dann und nur dann K-polynomvollständig, wenn sie polynomvollständig ist.*

Etwas schwieriger zu beantworten scheint die Frage nach allen K-permutationspolynomvollständigen Gruppen zu sein. In dieser Hinsicht gilt jedenfals:

Ist G eine C-permutationspolynomvollständige Gruppe, die höchstens nichttriviale Normalteiler vom Index 2 besitzt, dann ist G auch K-permutationspolynomvollständig.

BEWEIS. Sei $\varphi\in\mathscr{E}(K(G))$ und N ein beliebiger Normalteiler von G. Dann impliziert $a\in N$, daß auch $\varphi a\in N$. Ist aber $a\notin N$ dann gilt auch $\varphi a\notin N$, denn andernfalls wäre φa kein erzeugendes Element der durch a erzeugten zyklischen Gruppe. Also gilt $\mathscr{E}(K(G))\subseteq\mathscr{E}(C(G))$ und unsere Behauptung ist bewiesen.

Da wir später die Existenz von nicht polynomvollständigen, aber C-polynomvollständigen Gruppen beweisen werden, welche nur nichttriviale Normalteiler vom Index 2 besitzen, ist damit auch die Existenz von nicht polynomvollständigen, aber K-permutationspolynomvollständigen Gruppen bewiesen.

6. Wir beschäftigen uns nun mit den kompatiblen Abbildungen auf Gruppen. Dabei erweist es sich zunächst als zweckmäßig, die Gruppenoperation multiplikativ und x statt 1 zu schreiben. Eine vollständige Beschreibung der kompatiblen Abbildungen ist uns nur für wenige Gruppenklassen gelungen, für welche folgender Satz wesentlich ist:

Satz. *Sei G eine endliche Gruppe mit nur einem minimalen Normalteiler N und $\varphi\in C(G)$, weiters $\{g_1, \ldots, g_r\}$ ein volles Vertretersystem für die Nebenklassen von G nach N, dessen Vertreter für die Nebenklasse uN mit $\overline{uN}$ bezeichnet sei. Dann ist*

$$\varphi(g_i n) = \overline{\psi(g_i N)}\,\pi_i(n) \quad i = 1, 2, \ldots, r,\ n\in N, \quad wo \quad \psi\in C(G/N) \quad und \quad \pi_i\in F(N).$$

Umgekehrt ist jede solche Abbildung eine kompatible Abbildung auf G.

BEWEIS. Sei $\varphi\in C(G)$. Dann gibt es $\psi\in C(G/N)$ mit $\varphi(g_i)=\overline{\psi(g_i N)}\,n_i$ mit $n_i\in N$. Weiters ist $\varphi(g_i n)=\varphi(g_i)\varrho_i(n)$, $n\in N$, mit $\varrho_i\in F(N)$, und damit $\varphi(g_i n)=\overline{\psi(g_i N)}\,n_i\varrho_i(n)$. Aber $\pi_i: n\to n_i\varrho_i(n)$ gehört ebenfalls zu $F(N)$. Sei umgekehrt $\varphi\in F(G)$ mit $\varphi(g_i n)=\overline{\psi(g_i N)}\,\pi_i(n)$ und $1\neq M\lhd G$. Da N der einzige minimale Normalteiler von G ist, gilt $N\subseteq M$. Wenn $g\equiv h \bmod M$ gilt und $g=g_{i_1}n_1$, $h=g_{i_2}n_2$, $n_1, n_2\in N$ ist, dann gilt

$$\varphi(g) \equiv \overline{\psi(gN)}\,\pi_{i_1}(n_1) \equiv \overline{\psi(gN)} \equiv \overline{\psi(RN)} \equiv \overline{\psi(RN)}\,\pi_{i_2}(n_2) \equiv \varphi(h) \bmod M,$$

da $\psi\in C(G/N)$ und $M/N\lhd G/N$ ist. Also ist $\varphi\in C(G)$.

Folgerung 1: *Sei $G=Z_{p^\alpha}$ die zyklische Gruppe der Ordnung p^α, wo p eine Primzahl und $\alpha>0$, ganz, ist. Wenn wir die Gruppe additiv schreiben, also als die additive Gruppe der ganzen Zahlen mod p^α auffassen, können wir jedes Element von Z_{p^α} eindeutig darstellen als $\sum_{i=0}^{\alpha-1} p^i r_i \bmod p^\alpha$, $0\leqq r_i<p$. Dann sind alle $\varphi\in C(G)$ eindeutig gegeben durch die Abbildungen*

$$\varphi: \sum_{i=0}^{\alpha-1} p^i r_i \to \sum_{i=0}^{\alpha-1} p^i \pi_i(r_0, \ldots, r_i) \bmod p^\alpha$$

wo π_i eine beliebige Abbildung von $\{0, \ldots, p-1\}^{i+1}$ in $\{0, \ldots, p-1\}$ ist. Insbesondere ist $|C(G)|=p^{p\frac{p^{\alpha}-1}{p-1}}$, daher ist G genau dann C-polynomvollständig, wenn $p=2$ und $\alpha=1$.

BEWEIS. Daß jede kompatible Abbildung diese Gestalt hat und diese Abbildungen alle kompatibel sind, folgt aus dem Satz mittels Induktion nach α, da Z_{p^α} nur einen minimalen Normalteiler Z_p hat. Daß jedes $\varphi \in C(G)$ das geordnete α-tupel $(\pi_0, \ldots, \pi_{\alpha-1})$ eindeutig bestimmt, folgt aus der Eindeutigkeit der Darstellung der Elemente von Z_{p^α}. Hieraus ergibt sich auch die Aussage über die Ordnung von $C(G)$.

Folgerung 2: *Sei G eine endliche Gruppe, deren einziger nichttrivialer Normalteiler N Index 2 hat, wobei N eine nichtabelsche einfache Gruppe ist. Dann gilt $C(G)=P(G)$.*

BEWEIS. Sei $\varphi \in C(G)$ und $G=N \cup gN$ die Nebenklassenzerlegung von G nach N. Dann gilt $\varphi(g^\alpha n)=g^{\lambda(\alpha)}\pi_\alpha(n)$ für $n \in N$, $\alpha=0, 1$, wobei $\lambda: \{0,1\} \to \{0,1\}$ eine Abbildung ist. Umgekehrt ist jede solche Abbildung kompatibel, da N der einzige minimale Normalteiler von G ist. Also gilt $|C(G)|=4|F(N)|^2$. Wegen [2], ch. 1, Prop. 12.5. ist aber jede Abbildung von G nach N eine Polynomabbildung. Denn für $u \neq v$ gilt, da G kein Zentrum hat, $(cu)^2 \neq (cv)^2$ für mindestens ein $c \in G$, also gibt es eine Polynomabbildung ϱ von G nach N mit $\varrho u \neq \varrho v$. Die Abbildungen $x \to g^\alpha x^\beta \psi(x)$, wo $\alpha, \beta=0, 1$ und ψ die Abbildungen von G nach N durchläuft, sind aber paarweise verschiedene Polynomabbildungen von G in sich, daher gilt

$$4|F(N)|^2 = |C(G)| \geqq |P(G)| \geqq 4|F(N)|^2$$

woraus sich die Behauptung ergibt.

Folgerung 3: *Sym n ist C-polynomvollständig genau dann, wenn $n \neq 3, 4$ ist.*

BEWEIS. Für $n=1, 2$ ist die Behauptung trivial, für $n \geqq 5$ ergibt sie sich aus der letzten Folgerung. Da *Sym* 3 ein homomorphes Bild von *Sym* 4 ist, genügt es, die Behauptung für $n=3$ zu beweisen. Die alternierende Gruppe *Alt* 3 liefert zwei Nebenklassen, *Alt* 3 und g *Alt* 3, $g \in$ *Sym* $3 \setminus$ *Alt* 3. Sei $\varphi \in C(G)$ gegeben durch $\varphi(g\ Alt\ 3)=1$, $\varphi(1)=1$, $\varphi(x)=x$, $\varphi(x^2)=1$, wo *Alt* $3=[x]$, die von x erzeugte Untergruppe von *Sym* 3 ist. Wäre $\varphi \in P(G)$, so wäre φ, wegen $\varphi(1)=1$, von der Form $\varphi(y)=g_1^{-1}yg_1 \ldots g_r^{-1}yg_r$ mit $y, g_i \in G$. Insbesondere wäre $x=\varphi(x)=g_1^{-1}xg_1 \ldots g_r^{-1}xg_r$, daher

$$\varphi(x^2) = g_1^{-1}x^2g_1 \ldots g_r^{-1}x^2g_r = (g_1^{-1}xg_1 \ldots g_r^{-1}xg_r)^2 = \varphi(x)^2 = x^2,$$

da *Alt* 3 abelsch ist. Aber $x^2 \neq 1$, Widerspruch. Daher ist $\varphi \notin P(G)$ und *Sym* 3 nicht C-polynomvollständig.

Bemerkung: [2], ch. 5, Remark 5.32 zeigt, daß *Sym* 3 jedoch C permutationspolynomvollständig ist.

Satz. *Sei $G=G_1 \times G_2$ ein direktes Produkt von Untergruppen G_1, G_2 und $\varphi \in C(G)$. Dann gibt es $\varphi_i \in C(G_i)$, $i=1, 2$, derart, daß*

$$\varphi(g_1g_2) = \varphi_1(g_1)\varphi_2(g_2), \quad g_i \in G_i, \quad i = 1, 2.$$

BEWEIS. Es existieren Abbildungen $\varphi_i: G \to G_i$, $i=1, 2$, sodaß

$$\varphi(g_1 g_2) = \varphi_1(g_1 g_2)\varphi_2(g_1 g_2).$$

Da $G_2 \lhd G$, gilt

$$\varphi_1(g_1 g_2) \equiv \varphi(g_1 g_2) \equiv \varphi(g_1) \equiv \varphi_1(g_1) \mod G_2$$

und damit $\varphi_1(g_1 g_2)\varphi_1(g_1)^{-1} \in G_1 \cap G_2 = 1$. Es folgt $\varphi_1(g_1 g_2) = \varphi_1(g_1)$, ebenso $\varphi_2(g_1 g_2) = \varphi_2(g_2)$, insgesamt also $\varphi(g_1 g_2) = \varphi_1(g_1)\varphi_2(g_2)$. Da jeder Normalteiler von G_i auch Normalteiler von G ist, folgt, daß die Einschränkungen von φ_i auf G_i kompatibel sind. Hieraus ergibt sich die Behauptung.

Folgerung: *Sei $G = G_1 \times G_2$ endlich und $(|G_1|, |G_2|) = 1$. Wenn dann φ_i ganz $C(G_i)$ durchläuft, $i=1, 2$, so durchläuft*

$$\varphi: g_1 g_2 \to \varphi_1(g_1)\varphi_2(g_2)$$

ganz $C(G)$ und $(\varphi_1, \varphi_2) \to \varphi$ ist ein Fastringisomorphismus von $C(G_1) \times C(G_2)$ auf $C(G)$.

BEWEIS. Sei $\varphi_i \in C(G_i)$ und $\varphi(g_1 g_2) = \varphi_1(g_1)\varphi_2(g_2)$. Wenn $N \lhd G$, so ist $N = (G_1 \cap N)(G_2 \cap N)$ wegen $(|G_1|, |G_2|) = 1$. Wenn $g_i \in G_i$, $n \in N$, so ist $g_1 g_2 n = g_1 n_1 g_2 n_2$, $n_i \in G_i \cap N$. Daher ist

$$\varphi(g_1 g_2 n) \equiv \varphi_1(g_1 n_1)\varphi_2(g_2 n_2) \equiv \varphi_1(g_1)\varphi_2(g_2) \equiv \varphi(g_1 g_2) \mod N,$$

da $\varphi_i \in C(G_i)$. Also gilt $\varphi \in C(G)$.

Wegen des Satzes ist jedes $\varphi \in C(G)$ von der angegebenen Form. Falls für φ_i, $\psi_i \in C(G_i)$ gilt

$$\varphi_1(g_1)\varphi_2(g_2) = \psi_1(g_1)\psi_2(g_2), \quad \text{für alle} \quad g_i \in G_i, \quad i = 1, 2$$

so ist $\varphi_1(g_1) \equiv \psi_1(g_1) \mod G_2$ und wegen $G_1 \cap G_2 = 1$ ist $\varphi_1 = \psi_1$, ebenso $\varphi_2 = \psi_2$. Daß $(\varphi_1, \varphi_2) \to \varphi$ ein Homomorphismus bezüglich Funktionenmultiplikation und Funktionenkomposition ist, rechnet man leicht nach.

7. Der letzte Satz ermöglicht es uns insbesondere, das Studium von $C(G)$ für endliche nilpotente Gruppen G auf das für p-Gruppen zurückzuführen. Für den Fall, daß G eine endliche abelsche p-Gruppe ist, werden wir eine vollständige Beschreibung von $C(G)$ erhalten. Wir gehen dabei schrittweise in Lemmas vor und benützen wieder durchwegs additive Schreibweise für die Gruppenoperation.

Lemma. *Sei $G = Z_p \oplus Z_p$ die elementar-abelsche Gruppe der Ordnung p^2. Dann gilt $C(G) = P(G)$.*

BEWEIS. Sei $\varphi \in C(G)$ und $\varphi(0) = 0$. Wenn $x \in G$ ist, so gilt dann $\varphi(x) = k(x)x$ für eine ganze Zahl $k(x)$. Wenn $x, y \in G$, so ist $y \equiv x \mod [y-x]$, daher $\varphi(y) - \varphi(x) \in [y-x]$, also $k(y)y - k(x)x \in [y-x]$. Trivialerweise gilt $k(y)y - k(y)x \in [y-x]$, daher $(k(y)-k(x))x \in [y-x] \cap [x]$. Für $y \notin [x]$ und $x \neq 0$ gilt aber $[y-x] \cap [x] = 0$, daher $p \mid (k(y)-k(x))$, und da G nichtzyklisch ist, gibt es stets solche y. Falls aber $y \notin [x]$, so auch $y \notin [rx]$, für jede ganze Zahl r. Daher gilt auch $p \mid (k(y)-k(rx))$, falls $p \nmid r$. Insgesamt haben wir daher $k(y) \equiv k(x) \mod p$ für alle y, $x \in G \setminus \{0\}$. Da wir für $k(0)$ jede ganze Zahl nehmen können und da $\exp G = p$, läßt sich φ schreiben als $\varphi(x) = kx$, für ein ganzes k. Ist nun φ beliebig, so erfüllt $\psi: x \to (\varphi(x) - \varphi(0))$ die Bedingung $\psi(0) = 0$, also gilt $\varphi(x) = \varphi(0) + kx$, für ein ganzes k. Daher ist $\varphi \in P(G)$.

Lemma. *Sei* $G=Z_{p^\alpha}\oplus Z_{p^\alpha}$, $\alpha\geqq 1$. *Dann gilt* $C(G)=P(G)$.

BEWEIS. Mittels Induktion nach α. Für $\alpha=1$ ist die Behauptung gerade die Aussage des vorigen Lemmas. Sei nun $\alpha>1$ und $\{w_1, w_2\}$ ein Erzeugendensystem für G. Dann durchläuft $\bar{z}=r_1w_1+r_2w_2$ ein volles Vertretersystem für $G/p^{\alpha-1}G$ genau einmal, wenn r_i in den Grenzen $0\leqq r_i<p^{\alpha-1}$, $i=1, 2$, läuft. Sei $\varphi\in C(G)$ mit $\varphi(0)=0$, $u\in p^{\alpha-1}G$. Dann gilt $\varphi(\bar{z}+u)=k(\bar{z}+u)+\varrho_{\bar{z}}(u)$, k ganz, $\varrho_{\bar{z}}(u)\in p^{\alpha-1}G$, wegen Induktion. Ist $u'\in p^{\alpha-1}G$, dann gilt

$$\varrho_{\bar{z}}(u)-\varrho_{\bar{z}}(u') = \varphi(\bar{z}+u)-\varphi(\bar{z}+u')-k(u-u')\in[u-u']$$

daher ist $\varrho_{\bar{z}}\in C(p^{\alpha-1}G)$. Wegen Induktion existiert dann $\beta(\bar{z})\in p^{\alpha-1}G$ und eine ganze Zahl $l(\bar{z})$, sodaß $\varrho_{\bar{z}}(u)=\beta(\bar{z})+l(\bar{z})u$. Weiters ist $\bar{z}+u\to\varrho_{\bar{z}}(u)$ kompatibel auf G. Ist nun $\bar{z}'$ ein weiteres Element des Vertretersystems mod $p^{\alpha-1}G$, so gilt

$$\beta(\bar{z})-\beta(\bar{z}')+\big(l(\bar{z})-l(\bar{z}')\big)u = \varrho_{\bar{z}}(u)-\varrho_{\bar{z}'}(u)\in[\bar{z}-\bar{z}']$$

für alle $u\in p^{\alpha-1}G$. Für $u=0$ ergibt sich insbesondere $\beta(\bar{z})-\beta(\bar{z}')\in[\bar{z}-\bar{z}']$, daher auch

$$\big(l(\bar{z})-l(\bar{z}')\big)u\in[\bar{z}-\bar{z}']\cap[u], \quad \text{für alle} \quad u\in p^{\alpha-1}G.$$

Zu $\bar{z}-\bar{z}'$ gibt es $0\neq u_0\in p^{\alpha-1}G$, sodaß $[\bar{z}-\bar{z}']\cap[u_0]=0$, andernfalls wäre $[u]\subseteqq[\bar{z}-\bar{z}']$ für alle $u\in p^{\alpha-1}G$, da $\exp p^{\alpha-1}G=p$, und somit $p^{\alpha-1}G$ zyklisch, Widerspruch. Daher ist $\big(l(\bar{z})-l(\bar{z}')\big)u_0=0$, also $p\big|\big(l(\bar{z})-l(\bar{z}')\big)$. Da $\exp p^{\alpha-1}G=p$, gibt es daher eine ganze Zahl l derart, daß $\varrho_{\bar{z}}(u)=\beta(\bar{z})+lu$. Daher ist

$$-l(\bar{z}-\bar{z}')+\beta(\bar{z})-\beta(\bar{z}') = \varrho_{\bar{z}}(u)-\varrho_{\bar{z}'}(u')-l(\bar{z}-\bar{z}'+u-u')\in[\bar{z}-\bar{z}'+u-u'],$$

für alle $u, u'\in p^{\alpha-1}G$, also

$$-l(\bar{z}-\bar{z}')+\beta(\bar{z})-\beta(\bar{z}')\in\bigcap\big([\bar{z}-\bar{z}'+u]\,|\,u\in p^{\alpha-1}G\big) = [p(\bar{z}-\bar{z}')]\subseteqq pG.$$

Wegen $\alpha>1$ ist $\beta(\bar{z})-\beta(\bar{z}')\in pG$. Daher gilt $l(\bar{z}-\bar{z}')\in pG$. Setzen wir $\bar{z}'=0$, $\bar{z}=w_1$, so ist $lw_1\in pG$, also $p|l$. Wegen $\exp p^{\alpha-1}G=p$ können wir daher $l=0$ nehmen und erhalten $\varrho_{\bar{z}}(u)=\beta(\bar{z})\in p^{\alpha-1}G$. Wegen eines vorhergehenden Satzes läßt sich β schreiben als

$$\beta(\bar{z}) = p^{\alpha-1}\big(\sigma_1(r_1)w_1+\sigma_2(r_2)w_2\big), \quad 0\leqq\sigma_i(r_i)<p$$

und es gilt $\beta(\bar{z})\in[r_1w_1+r_2w_2]$. Also haben wir

$$p^{\alpha-1}\sigma_i(r_i)w_i = \zeta(r_1, r_2)r_iw_i, \quad i=1, 2, \quad \zeta(r_1, r_2) \text{ ganz.}$$

Insbesondere ist $p^{\alpha-1}\sigma_i(r_i)\equiv\zeta(r_1, r_2)r_i \bmod p^\alpha$, somit

$$p^{\alpha-1}\sigma_1(1)\equiv\zeta(1, r_2)\bmod p^\alpha, \quad \text{für} \quad 0\leqq r_2<p^{\alpha-1}.$$

Daher ist

$$p^{\alpha-1}\sigma_2(r_2)\equiv\zeta(1, r_2)r_2\equiv p^{\alpha-1}\sigma_1(1)r_2\bmod p^\alpha$$

also $\sigma_2(r_2)\equiv\sigma_2(1)r_2 \bmod p$ und somit $\sigma_2(1)\equiv\sigma_1(1)\bmod p$. Ebenso erhält man $\sigma_1(r_1)\equiv\sigma_2(1)r_1\equiv\sigma_1(1)r_1 \bmod p$. Also gilt

$$\beta(\bar{z}) = p^{\alpha-1}\sigma_1(1)(r_1w_1+r_2w_2) = p^{\alpha-1}\sigma_1(1)\bar{z} = p^{\alpha-1}\sigma_1(1)(\bar{z}+u),$$

da $\alpha>1$ und $pu=0$. Daher ist $\varphi(z)=\big(k+p^{\alpha-1}\sigma_1(1)\big)z$. Wie im vorigen Lemma folgt $C(G)=P(G)$.

Lemma. *Sei* $G=Z_{p^{\alpha_1}}\oplus Z_{p^{\alpha_2}}$, $\alpha_1\geqq\alpha_2>0$. *Es sei* $Z_{p^{\alpha_1}}=[w_1]$, $Z_{p^{\alpha_2}}=[w_2]$. *Wenn* $z\in G$ *die eindeutige Darstellung*

$$z=(r_1+p^{\alpha_1-\alpha_2}R_1)w_1+r_2w_2,\quad 0\leqq r_1<p^{\alpha_1-\alpha_2},\quad 0\leqq R_1<p^{\alpha_2},\quad 0\leqq r_2<p^{\alpha_2}$$

hat, und wenn $\varphi\in C(G)$, *dann hat* φ *die Form*

$$\varphi(z)=q(z)+p^{\alpha_2}\sigma(r_1)w_1$$

wo

$$\sigma\colon\{0,\ldots,p^{\alpha_1-\alpha_2}-1\}\to\{0,\ldots,p^{\alpha_1-\alpha_2}-1\}$$

eine Vertreterfunktion für ein Element von $C(Z_{p^{\alpha_1-\alpha_2}})$ *und* $q\in P(G)$ *ist. Umgekehrt ist jedes solche* φ *kompatibel.*

Beweis. $\bar z=t_1w_1+r_2w_2$, $0\leqq t_1<p^{\alpha_2}$, $0\leqq r_2<p^{\alpha_2}$, bildet ein volles Vertretersystem für $G/[p^{\alpha}w_1]\cong Z_{p^{\alpha_2}}\oplus Z_{p^{\alpha_2}}$. Sei $\varphi\in C(G)$, $\varphi(0)=0$ und $u\in[p^{\alpha_2}w_1]$, dann gilt wegen des vorhergehenden Lemmas

$$\varphi(\bar z+u)=k(\bar z+u)+\varrho_{\bar z}(u),\ k\text{ ganz},\quad \varrho_{\bar z}(u)\in[p^{\alpha_2}w_1]$$

und $\bar z+u\to\varrho_{\bar z}(u)$ ist kompatibel. Wegen eines früheren Satzes hängt $\varrho_{\bar z}(u)$ nur von r_1 und R_1 ab, also

$$\varrho_{\bar z}(u)=p^{\alpha_2}\sigma(r_1+p^{\alpha_1-\alpha_2}R_1)w_1$$

wo $\sigma(r_1+p^{\alpha_1-\alpha_2}R_1)$ ganz ist. Ist. $\bar z'+u'=(r_1'+p^{\alpha_1-\alpha_2}R_1')w_1+r_2'w_2$ ein weiteres Element von G, geschrieben in der eindeutigen Darstellung von oben, dann gilt

$$p^{\alpha_2}\big(\sigma(r_1+p^{\alpha_1-\alpha_2}R_1)-\sigma(r_1'+p^{\alpha_1-\alpha_2}R_1')\big)w_1=$$

$$=\varrho_{\bar z}(u)-\varrho_{\bar z'}(u')\in\big[(r_1-r_1'+p^{\alpha_1-\alpha_2}(R_1-R_1'))w_1+(r_2-r_2')w_2\big].$$

Da $\varrho_{\bar z}(u)$ nicht von r_2 abhängt, folgt

$$\varrho_{\bar z}(u)-\varrho_{\bar z'}(u)\in\bigcap\big(\big[(r_1-r_1'+p^{\alpha_1-\alpha_2}(R_1-R_1'))w_1+mw_2\big]\,\big|\,0\leqq m<p^{\alpha_2}\big)=$$

$$=[p^{\alpha_2}(r_1-r_1')w_1].$$

Daher hängt σ von R_1 nicht ab und ist kompatibel mod $p^{\alpha_1-\alpha_2}$. Also gilt $\varphi(z)=$ $=kz+p^{\alpha_2}\sigma(r_1)w_1$, und wie vorher folgt allgemein für $\psi\in C(G)$, daß $\psi(z)=$ $=q(z)+p^{\alpha_2}\sigma(r_1)w_1$ mit einer Polynomfunktion q ist.

Sei umgekehrt φ von der angegebenen Gestalt. Zu zeigen ist, daß

$$z\to p^{\alpha_2}\sigma(r_1)w_1$$

kompatibel ist. Sei also

$$z'=r_1'w_1+p^{\alpha_1-\alpha_2}R_1'w_1+r_2'w_2,\quad 0\leqq r_1'<p^{\alpha_1-\alpha_2},\quad 0\leqq R_1'<p^{\alpha_2},\quad 0\leqq r_2<p^{\alpha_2}.$$

Dann gilt

$$p^{\alpha_2}\big(\sigma(r_1)-\sigma(r_1')\big)w_1\in[p^{\alpha_2}(r_1-r_1')w_1]=[p^{\alpha_2}(z-z')]\subseteqq[z-z'],$$

also ist $z\to p^{\alpha_2}\sigma(r_1)w_1$ kompatibel.

Satz. *Sei* $t\geqq 2$ *und* $G=Z_{p^{\alpha_1}}\oplus Z_{p^{\alpha_2}}\oplus\ldots\oplus Z_{p^{\alpha_t}}$, $\alpha_1\geqq\alpha_2\geqq\ldots\geqq\alpha_t$, *und* $Z_{p^{\alpha_1}}=[w_1]$. *Wenn* $z\in G$ *die eindeutige Darstellung*

$$z=(r_1+p^{\alpha_1-\alpha_2}R_1)w_1+y,\quad 0\leqq r_1<p^{\alpha_1-\alpha_2},\quad 0\leqq R_1<p^{\alpha_2},\quad y\in C_{p^{\alpha_2}}\oplus\ldots\oplus C_{p^{\alpha_t}}$$

hat und $\varphi\in C(G)$, *dann läßt sich* φ *schreiben als*

$$\varphi(z)=q(z)+p^{\alpha_2}\sigma(r_1)w_1$$

wo σ *eine kompatible Funktion mod* $p^{\alpha_1-\alpha_2}$ *und* $q\in P(G)$ *ist. Umgekehrt ist jedes solche* φ *kompatibel.*

Beweis. Induktion nach t. Für $t=2$ wurde der Satz im vorigen Lemma bewiesen. Sei nun $t\geqq 3$, $\varphi\in C(G)$, $\varphi(0)=0$. Nach Induktion und einem früheren Satz ist

$$\varphi(z)=kz+p^{\alpha_2}\sigma(r_1)w_1+\tau(r_t)w_t,\ k \text{ ganz, } \sigma \text{ kompatibel mod } p^{\alpha_1-\alpha_2},\ \tau(r_t) \text{ ganz,}$$

wo $z=\bar{z}+r_tw_t$, $\bar{z}\in Z_{p^{\alpha_1}}\oplus\ldots\oplus Z_{p^{\alpha_{t-1}}}$, r_t ganz, $Z_{p^{\alpha_t}}=[w_t]$. Sei in dieser Darstellung $z'=\bar{z}'+r_t'w_t$ ein weiteres Element von $C(G)$. Setzen wir $\varrho(z)=\varphi(z)-kz$, dann ist auch $\varrho(z)$ kompatibel, und es gilt:

$$\big(\tau(r_t)-\tau(r_t')\big)w_t+p^{\alpha_2}\big(\sigma(r_1)-\sigma(r_1')\big)w_1=$$

$$=\varrho(z)-\varrho(z')\in\Big[(r_1-r_1')w_1+\sum_{i=2}^{t}(r_i-r_i')w_i+p^{\alpha_1-\alpha_2}(R_1-R_1')w_1\Big].$$

Da dieses Element unabhängig von $r_2, r_2'\ldots r_{t-1}, r_{t-1}'$ ist, gilt daher

$$\varrho(z)-\varrho(z')\in\bigcap\big([(r_1-r_1')w_1+p^{\alpha_1-\alpha_2}(R_1-R_1')w_1+(r_t-r_t')w_t+u]\big)$$

wo

$$u\in Z_{p^{\alpha_2}}\oplus\ldots\oplus Z_{p^{\alpha_{t-1}}}=[p^{\alpha_2}(r_1-r_1')w_1].$$

Also ist $(\tau(r_t)-\tau(r_t'))w_t=0$, d. h. τ ist eine Konstante und wegen $\varphi(0)=0$ ist $\tau(r_t)=0$ für alle r_t. Daher hat φ die Gestalt des Lemmas. Umgekehrt folgt wie im vorherigen Lemma, daß jedes solche φ kompatibel ist.

Folgerung: *Sei* $G=Z_{p^{\alpha_1}}\oplus\ldots\oplus Z_{p^{\alpha_t}}$, $\alpha_1\geqq\ldots\geqq\alpha_t$, $t\geqq 2$. *Dann durchläuft*

$$\varphi: z\to a+kz+p^{\alpha_2}\sigma(r_1)w_1$$

ganz $C(G)$ *genau einmal, wenn* a *ein volles Vertretersystem mod* p^{α_2} G, k *ein volles Vertretersystem mod* p^{α_2} *und* σ *ein volles Vertretersystem für die kompatiblen Abbildungen mod* $p^{\alpha_1-\alpha_2}$ *durchläuft. Insbesondere gilt:*

$$|C(G)|=|G|p^{2\alpha_2-\alpha_1}|C(Z_{p^{\alpha_1-\alpha_2}})|.$$

Folgerung: *Sei* $G=Z_{p^{\alpha_1}}\oplus\ldots\oplus Z_{p^{\alpha_t}}$, $\alpha_1\geqq\alpha_2\geqq\ldots\geqq\alpha_t$, $t\geqq 2$. *Es ist* G *genau dann C-polynomvollständig, wenn entweder* $\alpha_1=\alpha_2$, *oder* $p=2$ *und* $\alpha_1=\alpha_2+1$.

Beweis. Die Behauptung folgt aus $|P(G)|=|G|p^{\alpha_1}$.

Literatur

1] G. Berman, and R. J. Silverman, Simplicity of Near-rings of Transformations. *Proc. Amer. Math. Soc.* **10** (1959), 456—459.

[2] H. Lausch, and W. Nöbauer, Algebra of Polynomials. *Amsterdam*, 1973.

[3] W. Nöbauer, und W. Philipp, Über die Einfachheit von Funktionenalgebren. *Monatsh. Math.* **66** (1962), 441—452.

(Eingegangen am 20. Januar 1975.)