AUTOMORPHISMS OF FUNCTIONS IN ABELIAN PERMUTATION GROUPS

by STEPHEN D. COHEN and GARY L. MULLEN

(Received 25 November, 1974)

1. Let $\Omega = H_1 \oplus \ldots \oplus H_n$ be an abelian group of permutations of a finite non-empty set S. If H_i is generated by ϕ_i, let $s_{\phi_i}(\alpha)$ denote the length of the cycle of ϕ_i containing α. For any function f on S, let $A(f, \Omega) = \{\phi \in \Omega \,|\, f\phi = f\}$. In Theorem 2 we show that, if for every $i \neq j$ and $\alpha \in S$, $s_{\phi_i}(\alpha)$ and $s_{\phi_j}(\alpha)$ are relatively prime, then $A(f, \Omega) = A(f, H_1) \oplus \ldots \oplus A(f, H_n)$ for all f, while in Theorem 3 we prove the natural converse.

2. Let Ω be a group of permutations of a finite non-empty set S. Let Γ be the set of all functions from S into T where T is a finite set containing at least two elements. If $f, g \in \Gamma$, then f is *equivalent* to g relative to Ω if there exists a $\phi \in \Omega$ such that $f\phi = g$. We say that a permutation $\phi \in \Omega$ is an *automorphism* of a function f relative to Ω if $f\phi = f$. Let $A(f, \Omega)$ denote the group of automorphisms of the function f relative to Ω. For example, if K is the finite field of order q, $S = K^r$ where $r \geqq 1$, $T = K$ and $\Gamma = K[x_1, \ldots, x_r]$, then the above situation reduces to that considered by Carlitz in **[1]**.

If $T = \{\alpha_1, \ldots, \alpha_v\}$ and $f \in \Gamma$, let $S_i = \{\beta \in S \,|\, f(\beta) = \alpha_i\}$. We define π_f, the *partition* of f, to be the collection of non-empty S_i's. If $f, g \in \Gamma$ with $\pi_f = \{S_i\}$ and $\pi_g = \{T_i\}$, then f is equivalent to g relative to Ω if and only if there exists a $\phi \in \Omega$ such that $\phi(S_i) \subseteq T_i$ for $i = 1, \ldots, v$. If we let $g = f$ we may easily prove

LEMMA 1. *If ϕ is a permutation of S, then ϕ is an automorphism of a function f if and only if the cycles of ϕ (regarded as sets) form a refinement of π_f.*

Suppose now that Ω is abelian and that $\Omega = H_1 \oplus \ldots \oplus H_n$ where each H_i is cyclic generated by ϕ_i. If $\phi \in \Omega$ and $\alpha \in S$, let $\sigma_\phi(\alpha)$ denote the cycle of ϕ containing α and $s_\phi(\alpha)$ the length of $\sigma_\phi(\alpha)$.

THEOREM 2. *Let Ω be as above. If for every $i \neq j$ and $\alpha \in S$, $s_{\phi_i}(\alpha)$ and $s_{\phi_j}(\alpha)$ are relatively prime, then*

$$A(f, \Omega) = A(f, H_1) \oplus \ldots \oplus A(f, H_n) \tag{1}$$

for all $f \in \Gamma$.

Proof. Clearly $A(f, H_1) \oplus \ldots \oplus A(f, H_n) \subseteq A(f, \Omega)$ and, if $\psi_i \in H_i$, $\psi_j \in H_j$, then $s_{\psi_i}(\alpha)$ and $s_{\psi_j}(\alpha)$ are relatively prime. Let $\alpha \in S$ and $\psi \in A(f, \Omega)$ so that $f\psi = f\psi_1 \ldots \psi_n = f$ and hence $f(\psi_1^l \ldots \psi_n^l(\alpha)) = f(\alpha)$ for any integer l. By hypothesis and the Chinese Remainder Theorem, we may choose for each i an integer l_i such that $l_i \equiv 1 \pmod{s_{\psi_i}(\alpha)}$ and $l_i \equiv 0 \pmod{s_{\psi_j}(\alpha)}$ for $j \neq i$. Hence $\psi_1^{l_i} \ldots \psi_n^{l_i}(\alpha) = \psi_i(\alpha)$ so that $f(\psi_i(\alpha)) = f(\alpha)$, which implies that $\psi_i \in A(f, H_i)$.

THEOREM 3. *If Ω is as above and* (1) *holds for all $f \in \Gamma$, then for every $i \neq j$ and $\alpha \in S$, $s_{\phi_i}(\alpha)$ and $s_{\phi_j}(\alpha)$ are relatively prime.*

Proof. Suppose that for some $i \neq j$ and some $\alpha \in S$, $(s_{\phi_i}(\alpha), s_{\phi_j}(\alpha)) = s > 1$. Let $\psi_i = \phi_i^{s\phi_i(\alpha)/s}$ and $\psi_j = \phi_j^{s\phi_j(\alpha)/s}$ so that $\psi_i \in H_i$, $\psi_j \in H_j$ and $s_{\psi_i}(\alpha) = s_{\psi_j}(\alpha) = s$.

Case 1. $\sigma_{\psi_i}(\alpha) = \sigma_{\psi_j}(\alpha)$ (as sets). Then there exists an integer k such that $\psi_i \psi_j^{-k}(\alpha) = \alpha$. Let $\psi = \psi_i \psi_j^{-k}$ so that $\sigma_\psi(\alpha) = (\alpha)$. Let $S_1 = \{\alpha\}$, $S_2 = S \backslash S_1$, $\pi = \{S_1, S_2\}$ and f be any function whose partition is π. Then by Lemma 1, $f\psi = f\psi_i\psi_j^{-k} = f$ so that $\psi_i\psi_j^{-k} \in A(f, \Omega)$. Since $\sigma_{\psi_i}(\alpha) \nsubseteq S_1$, then $\psi_i \notin A(f, H_i)$ so that (1) fails to hold.

Case 2. $\sigma_{\psi_i}(\alpha) \neq \sigma_{\psi_j}(\alpha)$. Let $\psi = \psi_i\psi_j$ so that $(\psi_i\psi_j)^s(\alpha) = \alpha$ which implies that $s_\psi(\alpha) \leqq s$. Hence $\sigma_{\psi_i}(\alpha)$ and $\sigma_{\psi_j}(\alpha)$ cannot both be contained in $\sigma_\psi(\alpha)$, so that we may assume that $\sigma_{\psi_i}(\alpha) \nsubseteq \sigma_\psi(\alpha)$. Let $S_1 = \sigma_\psi(\alpha)$, $S_2 = S \backslash S_1$, $\pi = \{S_1, S_2\}$ and f be any function whose partition is π. Then $\psi = \psi_i\psi_j \in A(f, \Omega)$; but $\psi_i \notin A(f, H_i)$, so that again (1) fails to hold.

REFERENCE

1. L. Carlitz, Invariantive theory of equations in a finite field, *Trans. Amer. Math. Soc.* **75** (1953), 405–427.

University of Glasgow
Glasgow G12 8QW

The Pennsylvania State University
Shenango Valley Campus
147 Shenango Avenue
Sharon
Pennsylvania 16146, U.S.A.