J. Austral. Math. Soc. (Series A) 28 (1979), 214–218

ON SEMIGROUPS AND GROUPS OF LOCAL POLYNOMIAL FUNCTIONS

WILFRIED NÖBAUER

(Received 14 November 1978; revised 8 January 1979)

Communicated by R. Lidl

Abstract

Let Z_n be the factor ring of the integers mod n and t be a positive integer. In this paper some results are given on the structure of the semigroup of all mappings from Z_n into Z_n and on the structure of the group of all permutations on Z_n, which, for any t elements, can be represented by a polynomial function. If $n = ab$ and a, b are relatively prime, then this (semi)group is isomorphic to the direct product of the respective (semi)groups for a and b. Thus it is sufficient to consider only the case where $n = p^e$, p being a prime. In this case it is proved, that the (semi)group is isomorphic to the wreath product of a certain sub(semi)group of the symmetric (semi)group on $Z_{p^{e-1}}$ by the symmetric (semi)group on Z_p. Some remarks on these sub(semi)-groups are given.

Subject classification (*Amer. Math. Soc.* (*MOS*) 1970): 20 B 99, 13 B 25.

Let M be a set, $\operatorname{Sym} M$ the symmetric semigroup on M and $K\operatorname{sym} M$ the symmetric group on M. Let U be a subsemigroup of $\operatorname{Sym} M$. A function $\varphi \in \operatorname{Sym} M$ is called a t-local U-function if for any (not necessarily distinct) elements $a_1, a_2, \ldots, a_t \in M$ there exists a function $f \in U$, such that

$$\varphi(a_i) = f(a_i), \quad i = 1, 2, \ldots, t.$$

Let $L_t(U)$ be the set of all t-local U-functions. As one can see easily, $L_t(U)$ is a subsemigroup of $\operatorname{Sym} M$. Hence the intersection $L(U)$ of all subsemigroups $L_t(U)$ is also a subsemigroup of $\operatorname{Sym} M$, and

$$L_1(U) \supseteq L_2(U) \supseteq \ldots \supseteq L(U) \supseteq U. \tag{1}$$

For any subsemigroup T of $\operatorname{Sym} M$, we denote the intersection of T and $K\operatorname{Sym} M$ by KT and call this subsemigroup of T the invertible kernel of T. Then

$$KL_1(U) \supseteq KL_2(U) \supseteq \ldots \supseteq KL(U) \supseteq KU. \tag{2}$$

If in the chain (1) two members are equal, then clearly the corresponding members in the chain (2) also are equal. If V is a subsemigroup of U, then $L_t(V)$ is a subsemigroup of $L_t(U)$. If M is finite, then $L(U) = U$, $KL(U) = KU$ and all members of the chain (2) are groups.

In this paper we consider the case, where $M = Z/(n) = Z_n$ is a factor ring of the ring Z of the integers and $U = P_1(Z/(n)) = U(n)$ is the set of all polynomial functions on Z_n. Lausch and Nöbauer (1978) have computed the 'length' of the chain of semigroups $L_t(U(n))$; that is, the least t such that $L_t(U(n)) = U(n)$. In this paper some results are given on the structure of the semigroups $L_t(U(n))$ and the groups $KL_t(U(n))$. Since $L_1(U(n)) = \mathrm{Sym}\, Z_n$ and $KL_1(U(n)) = K\,\mathrm{Sym}\, Z_n$, we can assume that $t \geqslant 2$.

THEOREM 1. *If $n = ab$ and a, b are relatively prime, then $L_t(U(n))$ is isomorphic to the direct product $L_t(U(a)) \times L_t(U(b))$, and $KL_t(U(n))$ is isomorphic to the direct product $KL_t(U(a)) \times KL_t(U(b))$.*

PROOF. The first assertion is a special case of Theorem 2 in Dorninger and Nöbauer (1978); but it can also be proved directly as follows:

Let δ be the canonical epimorphism from Z_n to Z_a. We define a function $\varphi_a \in \mathrm{Sym}\, Z_a$ by

$$\varphi_a(\delta u) = \delta\varphi(u)$$

for any $u \in Z_n$, and similarly we define a function $\varphi_b \in \mathrm{Sym}\, Z_b$. A straightforward argument shows, that $(\varphi_a, \varphi_b) \in L_t(U(a)) \times L_t(U(b))$. It is also easy to prove, that

$$\varphi \to (\varphi_a, \varphi_b)$$

defines an isomorphism from $L_t(U(n))$ onto $L_t(U(a)) \times L_t(U(b))$.

Since, in general, $KL_t(U(m))$ is the set of all those elements of $L_t(U(m))$, which have an inverse element in $L_t(U(m))$, the second assertion also holds.

By Theorem 1, it is sufficient to consider only the case where $n = p^e$, p being a prime and $e > 0$ an integer. First we remark, that $L_1(U(p)) = U(p)$, hence $KL_1(U(p)) = KU(p)$.

Let $W(p^e)$ be the set of all functions of $\mathrm{Sym}\, Z_{p^e}$, which are of the form

$$x \to a_0 + a_1 x + pa_2 x^2 + \ldots + p^{e-1} a_e x^e,$$

where the a_i are given elements of Z_{p^e}. As proved in Lausch and Nöbauer (1973), Lemma 5.9, $W(p^e)$ is a subsemigroup of $U(p^e)$.

THEOREM 2. *If $e \geqslant 2$, then $L_t(U(p^e))$ is isomorphic to the wreath product of $L_t(W(p^{e-1}))$ by $\mathrm{Sym}\, Z_p$, and $KL_t(U(p^e))$ is isomorphic to the wreath product of $KL_t(W(p^{e-1}))$ by $K\,\mathrm{Sym}\, Z_p$.*

PROOF. Assume that $\varphi \in L_t(U(p^e))$ and that $0 \leqslant a < p$, $0 \leqslant x < p^{e-1}$ then

$$\varphi(a+px) = c_a + p\,\psi_a(x),$$

where $0 \leqslant c_a < p$ and $\psi_a \in \operatorname{Sym} Z_{p^{e-1}}$. Given $x_1, x_2, \ldots, x_t$, then there exists $f \in U(p^e)$ such that for all x_i

$$\varphi(a+px_i) = f(a+px_i) = f(a)+f'(a)\,px_i + \tfrac{1}{2}f''(a)\,p^2 x_i^2 + \ldots =$$

$$= f(a) + p(f'(a)\,x_i + p\tfrac{1}{2}f''(a)x_i^2 + \ldots),$$

which shows that $\psi_a \in L_t(W(p^{e-1}))$.

Conversely, given $\varphi \in \operatorname{Sym} Z_{p^e}$ such that

$$\varphi(a+px) = c_a + p\psi_a(x), \quad 0 \leqslant a < p, \quad 0 \leqslant x < p^{e-1}, \quad \psi_a \in L_t(W(p^{e-1}))$$

then, by Lausch and Nöbauer (1973), Proposition 5.61, $\varphi \in L_t(U(p^e))$.

Let $\rho \in \operatorname{Sym} Z_p$ be defined by $\rho a = c_a$, $a = 0, 1, \ldots, p-1$. Then

$$\varphi \to (\rho;\, \psi_0, \psi_1, \ldots, \psi_{p-1})$$

defines a bijection from $L_t(U(p^e))$ onto the set $\operatorname{Sym} Z_p \times L_t(W(p^{e-1}))^p$.

Suppose that under the above bijection the element $\psi \in L_t(U(p^e))$ is mapped onto $(\sigma;\, \chi_0, \chi_1, \ldots, \chi_{p-1})$, then

$$\varphi\psi(a+px) = \varphi(\sigma a + p\chi_a(x)) = \rho\sigma a + p\psi_{\sigma a}\chi_a(x),$$

hence

$$\varphi\psi \to (\rho\sigma;\, \psi_{\sigma 0}\chi_0, \psi_{\sigma 1}\chi_1, \ldots, \psi_{\sigma(p-1)}\chi_{(p-1)}).$$

This proves the first assertion. Since φ is a permutation if and only if ρ and all ψ_i are permutations, the second assertion is also true.

REMARK. It is well known, that $U(p^e)$ is isomorphic to the wreath product of $W(p^{e-1})$ by $\operatorname{Sym} Z_p$ and that $KU(p^e)$ is isomorphic to the wreath product of $KW(p^{e-1})$ by $K\operatorname{Sym} Z_p$.

COROLLARY. *For any* $e \geqslant 1$, $L_t(W(p^e)) = L_{t+1}(W(p^e))$ *if and only if*

$$L_t(U(p^{e+1})) = L_{t+1}(U(p^{e+1})),$$

and $L_t(W(p^e)) = W(p^e)$ *if and only if* $L_t(U(p^{e+1})) = U(p^{e+1})$. *A result of the same kind is true for the invertible kernels of these semigroups.*

From the results of Lausch and Nöbauer (1978) we now easily can obtain the length of the chain of the semigroups $L_t(W(p^e))$, and moreover we can see that there is no equality within this chain.

REMARK. $L_2(W(p^e)) = L_2(U(p^e))$ and $KL_2(W(p^e)) = KL_2(U(p^e))$.

PROOF. We have only to prove the first statement. Clearly $L_2(W(p^e)) \subseteq L_2(U(p^e))$. Conversely suppose $\varphi \in L_2(U(p^e))$; then φ is a compatible function on Z_{p^e}—that means, for any congruence relation θ on Z_{p^e}, $u \equiv v \bmod \theta$ implies $\varphi(u) \equiv \varphi(v) \bmod \theta$. Taking for θ the congruence relation corresponding to the principal ideal of Z_{p^e}, which is generated by $b-a$, we see that $\varphi(b)-\varphi(a) = r(b-a)$. Thus

$$l(x) = \varphi(a)+r(x-a)$$

is a polynomial, such that $l(a) = \varphi(a)$, $l(b) = \varphi(b)$. Since $l(x) \in W(p^e)$, we now see that $\varphi \in L_2(W(p^e))$, which completes the proof.

Finally, we consider the length of the chain of the invertible kernels of the chain of the semigroups $L_t(U(p^e))$.

LEMMA. *Let $e \geqslant 2$ and $f \neq 2$ be a natural number, such that $L_f(U(p^e)) \supset L_{f+1}(U(p^e))$. Then also $KL_f(U(p^e)) \supset KL_{f+1}(U(p^e))$.*

PROOF. Since there exist permutations of Z_{p^e} which are not compatible, our statement holds for $f = 1$. Suppose that $f > 2$ and $L_f(U(p^e)) \supset L_{f+1}(U(p^e))$. By Lausch and Nöbauer (1978), Theorem 3 and Theorem 4, then $f+\varepsilon(f) \leqslant e$, where $\varepsilon(f)$ is the exponent of the greatest power of p which divides f. Let us consider the function $\pi \in \operatorname{Sym} Z_{p^e}$ defined by

$$\pi(a+px) = (a+px)+p^{f-1}x(x-1)\dots(x-(f-1)),$$

$$a = 0,1,\dots,p-1, \quad x = 0,1,\dots,p^{e-1}.$$

This function is a permutation of Z_{p^e}, since

$$\pi(a+px) = a+p(x+p^{f-2}x(x-1)\dots(x-(f-1))$$

and the function $g \in \operatorname{Sym} Z_{p^{e-1}}$, defined by

$$g(x) = x+p^{f-2}x(x-1)\dots(x-(f-1)),$$

is a permutation of $Z_{p^{e-1}}$, which follows by Lausch and Nöbauer (1973), Proposition 4.31 (since $g'(x) \equiv 1 \bmod p$ for all x). By Lausch and Nöbauer (1978), $\pi \in L_f(U(p^e))$ but $\pi \notin L_{f+1}(U(p^e))$.

THEOREM 3. *The length of the chain of the groups $KL_t(U(p^e))$ equals the length of the chain of the semigroups $L_t(U(p^e))$, unless $p^e = 2^3$ or 3^2, in which cases the length of the first chain is one less than the length of the second chain.*

PROOF. By our lemma, we have only to consider the case, where the length of the second chain equals 3. If, in this case, $KL_2(U(p^e)) = KU(p^e)$, then every compatible permutation is a polynomial function, since, by the proof of the remark, every compatible function on Z_{p^e} is in $L_2(U(p^e))$. But, by our hypothesis on the length of the first chain, not every compatible function is a polynomial function. Thus Z_{p^e} is 1-permutation-hemiprimal, but not 1-hemiprimal in the sense of Nöbauer (1974). In Corollary 6.4 of that paper (by comparing the number of all compatible permutations on Z_{p^e} with the number of all polynomial functions on p^e which are permutations), it has been proved, that Z_{p^e} is 1-permutation hemiprimal, but not 1-hemiprimal, if and only if $p^e = 2^3$ or 3^2.

References

D. Dorninger and W. Nöbauer (1979), "Local polynomial functions on lattices and universal algebras', *Colloq. Math.*, to appear.

H. Lausch and W. Nöbauer (1973), *Algebra of polynomials* (North-Holland, Amsterdam–London).

H. Lausch and W. Nöbauer (1979), 'Local polynomial functions on factor rings of the integers', *J. Austral. Math. Soc.*, to appear.

W. Nöbauer (1974), 'Compatible and conservative functions on residue-class rings of the integers', *Coll. Math. Soc. János Bolyai* **13**, Topics in number theory, 245–257.

Institut für Algebra und
Mathematische Strukturtheorie
Technische Universität
Argentinierstrasse 8
A-1040 Wien
Austria