Thai Journal of Mathematics
Special Issue (Annual Meeting in Mathematics, 2006) : 25–30

Regularity of Semigroups of Multihomomorphisms of $(\mathbb{Z}_n, +)$

W. Teparos and Y. Kemprasit

Abstract : An element a of a semigroup S is called *regular* if $a = aba$ for some $b \in S$, and S is called a *regular semigroup* if every element of S is regular. For a group G, denote by $\mathrm{MHom}(G)$ the semigroup, under composition, of all multihomomorphisms of G into itself. It is known that the elements of $\mathrm{MHom}(\mathbb{Z}_n, +)$ are precisely $I_{k,a}$ where $k, a \in \mathbb{Z}$ and $I_{k,a}(\overline{x}) = \overline{ax} + k\mathbb{Z}_n$ for all $x \in \mathbb{Z}$, and $|\mathrm{MHom}(\mathbb{Z}_n, +)| = \sum_{k|n} k$. Our purpose is to show that for $k, a \in \mathbb{Z}$, $I_{k,a}$ is a regular element of the semigroup $\mathrm{MHom}(\mathbb{Z}_n, +)$ if and only if a and $\dfrac{(n,k)}{(n,k,a)}$ are relatively prime, and $\mathrm{MHom}(\mathbb{Z}_n, +)$ is a regular semigroup if and only if n is square-free.

Keywords : Multihomomorphism, regular semigroup
2000 Mathematics Subject Classification : 32A12, 20M17

1 Introduction

The cardinality of a set X is denoted by $|X|$.

By a *multifunction* from a nonempty set X into a nonempty set Y, we mean a function $f : X \to P^*(Y)$ where $P(Y)$ is the power set of Y and $P^*(Y) = P(Y) \setminus \{\emptyset\}$. For $A \subseteq X$, let $f(A) = \bigcup_{a \in A} f(a)$.

Continuity of multifunctions between two topological spaces were studied by Whyburn [6], Smithson [4] and Feichtinger [2]. Multihomomorphisms between groups were defined naturally in [5] as follows: A multifunction f from a group G into a group G' is called a *multihomomorphism* if $f(xy) = f(x)f(y) (= \{ st \mid s \in f(x) \text{ and } t \in f(y) \})$ for all $x, y \in G$. Denote by $\mathrm{MHom}(G, G')$ the set of all multihomomorphisms from G into G', and write $\mathrm{MHom}(G)$ for $\mathrm{MHom}(G, G)$. Clearly, $\mathrm{MHom}(G)$ is a semigroup under composition.

For cyclic groups G and G', the elements of $\mathrm{MHom}(G, G')$ were characterized and $|\mathrm{MHom}(G, G')|$ was determined in [5] and moreover, necessary and sufficient conditions for $f \in \mathrm{MHom}(G, G')$ to be surjective, that is, $\bigcup_{x \in G} f(x) = G'$, were given in [3]. In [1], the authers provided remarkable necessary conditions for f

belonging to MHom(G, G') when G' is a subgroup of the additive group $(\mathbb{R}, +)$ and a subgroup of the multiplicative group $(\mathbb{R}^*, \cdot)$ where $\mathbb{R}$ is the set of real numbers and $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$.

Let $\mathbb{Z}$ be the set of integers, $\mathbb{Z}^+ = \{x \in \mathbb{Z} | x > 0\}$ and for $n \in \mathbb{Z}^+$, let $(\mathbb{Z}_n, +)$ be the additive group of integers modulo n. The congruence class modulo n of x will be denoted by $\overline{x}$. Then $\mathbb{Z}_n = \{ \overline{x} \mid x \in \mathbb{Z} \} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ and $|\mathbb{Z}_n| = n$. For $a_1, a_2, \ldots, a_m \in \mathbb{Z}$, not all 0, the g.c.d. of $a_1, a_2, \ldots, a_m$ is denoted by $(a_1, a_2, \ldots, a_m)$. It is clearly seen that $k\mathbb{Z}_n = (k, n)\mathbb{Z}_n$ for all $k \in \mathbb{Z}$ and $k\mathbb{Z}_n + l\mathbb{Z}_n = (k, l)\mathbb{Z}_n$ for all $k, l \in \mathbb{Z}$, not both 0. If $k, a \in \mathbb{Z}$, define the multifunction $I_{k,a}$ from $\mathbb{Z}_n$ into itself by

$$I_{k,a}(\overline{x}) = \overline{ax} + k\mathbb{Z}_n \quad \text{for all } x \in \mathbb{Z}.$$

The following results are known.

Theorem 1.1. ([5]) *$MHom(\mathbb{Z}_n, +) = \{I_{k,a} | k, a \in \mathbb{Z}\}$.*

Theorem 1.2. ([5]) *The following statements hold.*

(i) *If $k, l \in \mathbb{Z}^+$, $k|n$, $l|n$, $a \in \{0, 1, \ldots, k-1\}$, $b \in \{0, 1, \ldots, l-1\}$ and $I_{k,a} = I_{l,b}$, then $k = l$ and $a = b$.*

(ii) *$MHom(\mathbb{Z}_n, +) = \{ I_{k,a} \mid k \in \mathbb{Z}^+, k|n \text{ and } a \in \{0, 1, \ldots, k-1\}\}$.*

(iii) *$|MHom(\mathbb{Z}_n, +)| = \displaystyle\sum_{\substack{k\in\mathbb{Z}^+ \\ k|n}} k$.*

Note that in Theorem 1.2, (iii) is directly obtained from (i) and (ii).

An element a of a semigroup S is called *regular* if $a = aba$ for some $b \in S$. Denote by Reg(S) the set of all regular elements of S. If every element of S is regular, that is , Reg$(S) = S$, S is called a *regular semigroup*. Our purpose is to show that for $k, a \in \mathbb{Z}$, $I_{k,a}$ is a regular element of MHom$(\mathbb{Z}_n, +)$ if and only if a and $\dfrac{(n, k)}{(n, k, a)}$ are relatively prime, and MHom$(\mathbb{Z}_n, +)$ is a regular semigroup if and only if n is square-free. Recall that n is called *square-free* if for every $a \in \mathbb{Z}$ with $a > 1$, $a^2 \nmid n$. Hence n is square-free if and only if either $n = 1$ or n is a product of distinct primes.

2 The Regularity of MHom$(\mathbb{Z}_n, +)$

Throughout this section, let n be a positive integer. The following three lemmas are needed.

Lemma 2.1. *If $r, s, t \in \mathbb{Z}$, $r \neq 0$ and $t \neq 0$ are such that $r \mid (s, \dfrac{t}{(s, t)})$, then $r^2 \mid t$.*

Proof. From the asumption, $r \mid s$ and $r|\dfrac{t}{(s, t)}$. Then $r(s, t)|t$. Hence $r|s$ and $r|t$ which implies that $r|(s, t)$, and thus $r^2|r(s, t)$. But $r(s, t)|t$, so $r^2|t$. □

Lemma 2.2. *For* $k, l, a, b \in \mathbb{Z}$,

$$I_{k,a}I_{l,b} = \begin{cases} I_{(k,al),ab} & \text{if } k \neq 0, \\ I_{al,ab} & \text{if } k = 0. \end{cases}$$

Proof. For $x \in \mathbb{Z}$,

$$\begin{aligned} I_{k,a}I_{l,b}(\overline{x}) &= I_{k,a}(\overline{bx} + l\mathbb{Z}_n) \\ &= \overline{a}(\overline{bx} + l\mathbb{Z}_n) + k\mathbb{Z}_n \\ &= \overline{abx} + al\mathbb{Z}_n + k\mathbb{Z}_n \\ &= \begin{cases} \overline{abx} + (k, al)\mathbb{Z}_n = I_{(k,al),ab}(\overline{x}) & \text{if } k \neq 0, \\ \overline{abx} + al\mathbb{Z}_n = I_{al,ab}(\overline{x}) & \text{if } k = 0, \end{cases} \end{aligned}$$

so the lemma is proved. □

Lemma 2.3. *If* $k, l, a, b \in \mathbb{Z}$ *are such that* $I_{k,a} = I_{l,b}$*, then* $k\mathbb{Z}_n = l\mathbb{Z}_n$ *and* $(n, k)|(a - b)$.

Proof. We have that $k\mathbb{Z}_n = I_{k,a}(\overline{0}) = I_{l,b}(\overline{0}) = l\mathbb{Z}_n$. Then $I_{k,a} = I_{k,b}$, so $\overline{a} + k\mathbb{Z}_n = I_{k,a}(\overline{1}) = I_{k,b}(\overline{1}) = \overline{b} + k\mathbb{Z}_n$. Hence $\overline{a - b} = \overline{kt}$ for some $t \in \mathbb{Z}$, thus $n|(a - b - kt)$. Since $(n, k)|n$ and $(n, k)|kt$, it follows that $(n, k)|(a - b)$. □

Theorem 2.4. *For* $k, a \in \mathbb{Z}$, $I_{k,a}$ *is a regular element of the semigroup MHom*$(\mathbb{Z}_n, +)$ *if and only if* a *and* $\dfrac{(n, k)}{(n, k, a)}$ *are relatively prime.*

Proof. First, assume that $I_{k,a}$ is a regular element of $\mathrm{MHom}(\mathbb{Z}_n, +)$. Then there are $l, b \in \mathbb{Z}$ such that $I_{k,a} = I_{k,a}I_{l,b}I_{k,a}$. By Lemma 2.2, $I_{k,a}I_{l,b}I_{k,a} = I_{s,a^2b}$ for some $s \in \mathbb{Z}$, and so by Lemma 2.3, $(n, k)|(a^2b - a)$. This implies that $\dfrac{(n, k)}{(n, k, a)}|\dfrac{a}{(n, k, a)}(ab - 1)$. But $\dfrac{(n, k)}{(n, k, a)}$ and $\dfrac{a}{(n, k, a)}$ are relatively prime, thus $\dfrac{(n, k)}{(n, k, a)}|(ab - 1)$. Therefore $ab + \dfrac{(n, k)}{(n, k, a)}t = 1$ for some $t \in \mathbb{Z}$. Consequently, a and $\dfrac{(nk)}{(n, k, a)}$ are relatively prime.

Conversely, assume that a and $\dfrac{(n, k)}{(n, k, a)}$ are relatively prime. Then there are $b, c \in \mathbb{Z}$ such that $ab + \dfrac{(n, k)}{(n, k, a)}c = 1$. It follows that $\overline{(a^2b - a)x} = \overline{(ab - 1)ax} = \overline{\left(\dfrac{(n, k)}{(n, k, a)}cax\right)} = (n, k)\overline{\left(\dfrac{a}{(n, k, a)}cx\right)} \in (n, k)\mathbb{Z}_n = k\mathbb{Z}_n$ for every $x \in \mathbb{Z}$. Consequently, $\overline{a^2bx} + k\mathbb{Z}_n = \overline{ax} + k\mathbb{Z}_n$ for every $x \in \mathbb{Z}$. By Lemma 2.2,

$$I_{k,a}I_{k,b}I_{k,a} = \begin{cases} I_{(k,a(k,bk)),a^2b} = I_{k,a^2b} & \text{if } k \neq 0, \\ I_{0,a^2b} = I_{k,a^2b} & \text{if } k = 0. \end{cases}$$

Thus for every $x \in \mathbb{Z}$, $I_{k,a}I_{k,b}I_{k,a}(\overline{x}) = \overline{a^2bx} + k\mathbb{Z}_n = \overline{ax} + k\mathbb{Z}_n = I_{k,a}(\overline{x})$, so $I_{k,a}I_{k,b}I_{k,a} = I_{k,a}$. Hence $I_{k,a}$ is a regular element of $\mathrm{MHom}(\mathbb{Z}_n,+)$, as desired. □

Corollary 2.5. *Let QF be the set of all square-free positive integers. Then the following statements hold.*

(i) $Reg(MHom(\mathbb{Z}_n,+))$

$$= \{\ I_{k,a}\ |\ k \in \mathbb{Z}^+, k|n, a \in \{0,1,\ldots,k-1\}\ \textit{and}\ (a, \frac{k}{(k,a)}) = 1\}$$
$$= \{\ I_{k,a}\ |\ k \in QF, k|n\ \textit{and}\ a \in \{0,1,\ldots,k-1\}\}$$
$$\cup \{\ I_{k,a}\ |\ k \in \mathbb{Z}^+ \backslash QF, k|n, a \in \{0,1,\ldots,k-1\}\ \textit{and}\ (a, \frac{k}{(k,a)}) = 1\}$$

(ii) $|Reg(MHom(\mathbb{Z}_n,+))|$

$$= \sum_{\substack{k \in QF \\ k|n}} k + \sum_{\substack{k \in \mathbb{Z}^+ \backslash QF \\ k|n}} |\{a \in \{0,1,\ldots,k-1\}\ |\ (a, \frac{k}{(k,a)}) = 1\}|$$

Proof. (i) The first equality follows from Theorem 1.2(ii) and Theorem 2.4 and the second equality is obtained from Lemma 2.1.

(ii) is obtained from (i) and Theorem 1.2(i). □

Theorem 2.6. *The semigroup $MHom(\mathbb{Z}_n,+)$ is regular if and only if n is square-free.*

Proof. From Theorem 1.1 and Theorem 2.4, we have respectively that

$$\mathrm{MHom}(\mathbb{Z}_n,+) = \{\ I_{k,a}\ |\ k,a \in \mathbb{Z}\}$$

and
$$\mathrm{Reg}(\mathrm{MHom}(\mathbb{Z}_n,+)) = \{\ I_{k,a}\ |\ k,a \in \mathbb{Z}\ \text{and}\ (a, \frac{(n,k)}{(n,k,a)}) = 1\}$$

First, assume that n is not square-free. Then there exists an integer $r > 1$ such that $r^2|n$. Then $(r, \frac{(n,n)}{(n,n,r)}) = (r, \frac{n}{r}) = r > 1$ which implies that $I_{n,r} \in \mathrm{MHom}(\mathbb{Z}_n,+) \backslash \mathrm{Reg}(\mathrm{MHom}(\mathbb{Z}_n,+))$. This proves that if $\mathrm{MHom}(\mathbb{Z}_n,+)$ is a regular semigroup, then n is square-free.

For the converse, assume that n is square-free. Then k is square-free for every $k \in \mathbb{Z}^+$ with $k|n$. Therefore we deduce from Corollary 2.5 (i) that

$$\mathrm{Reg}(\mathrm{MHom}(\mathbb{Z}_n,+)) = \{\ I_{k,a}\ |\ k \in \mathbb{Z}^+, k|n\ \text{and}\ a \in \{0,1,\ldots,k-1\}\}.$$

By Theorem 1.2(ii), we have $\mathrm{Reg}(\mathrm{MHom}(\mathbb{Z}_n,+)) = \mathrm{MHom}(\mathbb{Z}_n,+)$. Hence $\mathrm{MHom}(\mathbb{Z}_n,+)$ is a regular semigroup. □

The following corollary is obtained directly from Theorem 1.2(iii) and Theorem 2.6.

Corollary 2.7. *For any prime* p, $MHom(\mathbb{Z}_p, +)$ *is a regular semigroup of order* $1 + p$.

Example 2.8. By Theorem 1.2(iii) and Theorem 2.6, $\mathrm{MHom}(\mathbb{Z}_6, +)$ is a regular semigroup of order $1 + 2 + 3 + 6 = 12$.

By Corollary 2.5(ii),

$$\begin{aligned}|\mathrm{Reg}(\mathrm{MHom}(\mathbb{Z}_{20}, +))| &= (1 + 2 + 5 + 10) + |\{a \in \{0, 1, 2, 3\} \mid (a, \frac{4}{(4, a)}) = 1\}| \\ &\quad + |\{a \in \{0, 1, \ldots, 19\} \mid (a, \frac{20}{(20, a)}) = 1\}| \\ &= 18 + (3 + 15) \\ &= 36\end{aligned}$$

since

for $a \in \{0, 1, 2, 3\}$, $(a, \frac{4}{(4, a)}) = 1 \Leftrightarrow a \in \{0, 1, 3\}$

and

for $a \in \{0, 1, \ldots, 19\}$, $(a, \frac{20}{(20, a)}) = 1 \Leftrightarrow a \in \{0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19\}$.

By Theorem 1.2(iii),

$$\begin{aligned}|\mathrm{MHom}(\mathbb{Z}_{20}, +)\backslash \mathrm{Reg}(\mathrm{MHom}(\mathbb{Z}_{20}, +))| &= (1 + 2 + 4 + 5 + 10 + 20) - 36 \\ &= 42 - 36 = 6.\end{aligned}$$

References

[1] P. Youngkhong and K. Savettaraserance, Multihomomorphisms from groups into groups of real numbers, *Thai J. Math.*, *ICMAA 2006*, submitted.

[2] O. Feichtinger, More on lower semi-continuity, *Amer. Math. Monthly* **83** (1978), 30.

[3] S. Nentheien and P. Lertwichitsilp, Surjective multihomomorphisms between cyclic groups, *Thai J. Math.*, *ICMAA 2006*, submitted.

[4] R. E. Smithson, A characterization of lower semi-continuity, *Amer. Math. Monthly* **75** (1968), 505.

[5] N. Triphop, A. Harnchoowong and Y. Kemprasit, Multihomomorphisms between cyclic groups, *Set-valued Mathematics and Applications*, to appear.

[6] G. T. Whyburn, Continuity of multifunctions, *Proc. Nat. Acad. Sciences*, U.S.A. **54** (1965), 1494-1501.

(Received 25 May 2006)

W. Teparos and Y. Kemprasit
Department of Mathematics
Faculty of Science
Chulalongkorn University
Bangkok 10330, THAILAND.
e-mail: Yupaporn.K@chula.ac.th