On graph of a group mapping and its centralizers

Yuwen Cheng, Feng-Kuo Huang*
Department of Mathematics, National Taitung University
Taitung 95002, TAIWAN
e-mail: yucheng@nttu.edu.tw; fkhuang@nttu.edu.tw

Chiou-Shing Wang
Department of Business Administration, Kao Yuan University
Lujhu 821, TAIWAN
e-mail: abwang@cc.kyu.edu.tw

Abstract

The aim of this paper is to use the graphical properties of a group mapping to study the algebraic properties of its centralizers. Equivalent conditions for the simplicity of the centralizer nearring of a given group mapping is given. Examples are provided to demonstrate and delimit our results.

2000 Mathematics Subject Classification: Primary 16Y30; Secondary 20M20, 05C90.
Key words and phrases: digraph, centralizer, nearring, semigroup

1 Introduction

The purpose of this paper is to study the interplay between the graphical properties of a function on a group G and the algebraic properties of its

*Corresponding author.

centralizers. Let G be a group and $\alpha\colon G \to G$ a function (homomorphism). The set $M_\alpha(G) = \{f \in M(G) \mid f \circ \alpha = \alpha \circ f\}$ is a semigroup with respect to composition of functions if α was a function, and is a nearring with respect to pointwise addition and composition of functions if α was a homomorphism. The simplest nearring (in some sense) of this type is $M_k(\mathbb{Z}_n)$ where k, a nonnegative integer, is considered as an endomorphism of the cyclic group $(\mathbb{Z}_n, +)$ via $k(z) = kz \in \mathbb{Z}_n$. Be aware that the abelian nearring $M_k(\mathbb{Z}_n)$ need not to be zero-symmetric.

In Section Two, the graph of a given function $\alpha\colon G \to G$ is defined and a binary relation is associated to this graph. Using this relation, a characterization for centralizers of function α is given in Theorem 2.2. It is also shown that $M_\alpha(G)$ acts transitively on G if and only if the circular length of elements in the orbit space $\mathcal{O}^*_\alpha(G)$ are equal in Corollary 2.7. Conditions guarantee the existence of idempotents are given in Lemma 2.8. In Section Three, the function α is assumed to be a homomorphism of a group G and thus the centralizer $M_\alpha(G)$ is a nearring. Theorem 3.2 shows that $M_\alpha(G)$ is 2-primitive if and only if all the orbits in $\mathcal{O}^*_\alpha(G)$ have the same length. Conditions characterize when $M_\alpha(G)$ is a field is given in Corollary 3.6. It is shown that if $M_\alpha(G)$ is a finite field, then G is an elementary abelian group in Corollary 3.7.

Examples are provided to demonstrate or delimit our results of investigations. For terminologies not defined in details in this paper, please refer [5, 6] and [1, 7], but note that we are using left nearrings instead of right nearrings as in [6].

2 Graph of a function and its orbit

The first two results in this section is highly motivated by [3]. However, finiteness condition is not assumed for G in general. Let G be a group and α a function from G to G. Let $\mathcal{G}_\alpha(G) := (V_\alpha(G), E_\alpha(G))$ be the digraph with vertex set $V_\alpha(G) = G$ and direct edge set $E_\alpha(G) = \{(x, x\alpha) \mid x \in G\}$. This $\mathcal{G}_\alpha(G)$ is the graphical representation for the function α. Observe that $\mathcal{G}_\alpha(G)$ is a *functional* graph in the sense that the outdegree of each vertex in this graph is equal to one.

A vertex x in the graph $\mathcal{G}_\alpha(G)$ is called *initial* if its indegree is zero (or equivalently, it has no preimages). It is called *circular* if there exists a positive integer t such that $x\alpha^t = x$. The smallest positive integer t such that $x\alpha^t = x$ is called the *length of circularity* (or *circular length*) of x and will be denoted by $c_\alpha(x)$. Let $\mathcal{O}_\alpha(x) = \{x\alpha^t \mid t \in \mathbb{N} \cup \{0\}\}$ be the orbit of x acted by function α. Define a function on the group G as $p_\alpha\colon G \to \mathbb{Z} \cup \{\infty\}$. If the orbit $\mathcal{O}_\alpha(x)$ is finite and x is circular, let $p_\alpha(x) = 0$. If the orbit $\mathcal{O}_\alpha(x)$ is finite and x is not circular, let $p_\alpha(x)$ be the smallest positive integer such that $x\alpha^{p_\alpha(x)}$ is a circular element and define $c_\alpha(x) = c_\alpha(x\alpha^{p_\alpha(x)})$. This definition is well defined. When $\mathcal{O}_\alpha(x)$ is finite, there must exist $s, t \in \mathbb{N} \cup \{0\}$ such that $x\alpha^s = x\alpha^{s+t} = (x\alpha^s)\alpha^t$ and thus $x\alpha^s$ is circular. Furthermore, since $\mathcal{G}_\alpha(G)$ is functional, a connected component of $\mathcal{G}_\alpha(G)$ contains at most one cycle and $c_\alpha(x)$ is the length of this cycle. If the orbit $\mathcal{O}_\alpha(x)$ is infinite, then define $c_\alpha(x) = 0$ and $p_\alpha(x) = \infty$. The number $p_\alpha(x)$ is called the *length of path* (or *path length*) of x. When no confusion will arise, $c(x)$ and $p(x)$ will be used for $c_\alpha(x)$ and $p_\alpha(x)$ respectively.

Using the idea developed in [3], a binary relation $\preccurlyeq$ can be introduced on G as following. Given $x, y \in G$, we say

$$x \preccurlyeq y \quad \text{if and only if} \quad c(x) \mid c(y) \text{ and } p(x) \leq p(y),$$

where $c(x) \mid c(y)$ means $c(x)$ is a factor of $c(y)$. This relation is reflexive, transtive but not necessarily antisymmetric. In $M_2(\mathbb{Z}_5)$, the length of path of each elements is 0 and the length of circularity are $c(0) = 1$, $c(1) = c(2) = c(3) = c(4) = 4$. Thus $2 \preccurlyeq 3$ and $3 \preccurlyeq 2$ but $2 \neq 3$. It can immediately be seen that $x \preccurlyeq y$ if and only if $x\alpha \preccurlyeq y\alpha$. Even though the relation $\preccurlyeq$ is not a partial order, it can be used to study the centralizers of the function α. The following result had been shown for finite graph [3], we reestablish them using different approach in a more general setting.

Lemma 2.1. *Let $f\colon G \to G$. If $f \in M_\alpha(G)$ then $xf \preccurlyeq x$ for all $x \in G$.*

Proof. Let $x \in G$. The orbit $\mathcal{O}_\alpha(x)$ is either finite or infinite. If $\mathcal{O}_\alpha(x)$ is infinite, then it is clear that $xf \preccurlyeq x$ by definition. If $\mathcal{O}_\alpha(x)$ is finite, then $x\alpha^{p(x)}$ is circular, and thus $(x\alpha^{p(x)})\alpha^{c(x)} = x\alpha^{p(x)}$. Observe that

$$(xf)\alpha^{p(x)} = (x\alpha^{p(x)})f = ((x\alpha^{p(x)})\alpha^{c(x)})f = ((xf)\alpha^{p(x)})\alpha^{c(x)}.$$

Which shows that $(xf)\alpha^{p(x)}$ is circular with $c(xf) \mid c(x)$ and $p(xf) \leq p(x)$. Therefore $xf \preccurlyeq x$. □

To determine those mappings $f\colon G \to G$ which commute with α, the idea of a minimal generating set of the graph $\mathcal{G}_\alpha(G)$ had been introduced in [3]. A subset $M \subseteq G$ is a *generating set* of the graph $\mathcal{G}_\alpha(G)$ if every element of G is of the form $x\alpha^t$ for some $t \in \mathbb{N} \cup \{0\}$ and some $x \in M$ where α^0 stands for the identity mapping of G. A generating set is *minimal* if no proper subset can be a generating set.

For any $z \in G$ and M a generating set for $\mathcal{G}_\alpha(G)$, observe that $z = x\alpha^k$ for some $x \in M$ and $k \in \mathbb{N} \cup \{0\}$. Therefore $zf = (x\alpha^k)f = (xf)\alpha^k$ if

$f \in M_\alpha(G)$. Thus the function $f \in M_\alpha(G)$ is determined by xf for all $x \in M$. Moreover, if $xf = xg$ and $g \in M_\alpha(G)$, then $g = f$. Hence f is uniquely determined by xf for all $x \in M$. Explicitly, the following result, a modification from [3, Theorem 2.3], addresses these observations. Be aware that no finiteness condition is imposed on G instead of a finite minimal generating set for the digraph $\mathcal{G}_\alpha(G)$.

Theorem 2.2. *Let $\mathcal{G}_\alpha(G)$ be the digraph of a group mapping $\alpha\colon G \to G$ with a finite minimal generating set M and $f\colon G \to G$ a mapping. Then $f \in M_\alpha(G)$ if and only if there exist a map $f'\colon M \to G$ such that $xf = xf'$ for all $x \in M$ and if $x, y \in M$ such that $x\alpha^s = y\alpha^t$ for some $s, t \in \mathbb{N} \cup \{0\}$, then $xf'\alpha^s = yf'\alpha^t$. Moreover, this function f is a unique extension of the map f' and it is given by $x\alpha^s f = xf'\alpha^s$ for all $s \in \mathbb{N} \cup \{0\}$ and $x \in M$.*

Proof. If $f \in M_\alpha(G)$, then define $f' = f|_M\colon M \to G$ be the restriction map of f on M. Conversely, assume a mapping $f'\colon M \to G$ satisfying the hypothesis and define $f\colon G \to G$ via $x\alpha^s f = xf'\alpha^s$ for $s \in \mathbb{N} \cup \{0\}$ and $x \in M$. The uniqueness of f is clear from the definition. It remains to show that f is a well defined function in $M_\alpha(G)$. Since M is a minimal generating set for $\mathcal{G}_\alpha(G)$, each element $a \in G$ is equal to $x\alpha^s$ for some $s \in \mathbb{N} \cup \{0\}$ and $x \in M$. Thus $\mathrm{dom} f = G$. Moreover, if $a = x\alpha^s = y\alpha^t$ for some $s, t \in \mathbb{N} \cup \{0\}$ and $x, y \in M$, that is when the representation of element $a \in G$ by elements in M is not unique, then $x\alpha^s f = xf'\alpha^s = yf'\alpha^t = y\alpha^t f$ and thus f is a well-defined function on G. Furthermore, let $a \in G$ and $a = x\alpha^t$ for some $x \in M$, $t \in \mathbb{N} \cup \{0\}$. Then $a\alpha f = x\alpha^{t+1} f = xf'\alpha^{t+1} = (xf'\alpha^t)\alpha = (x\alpha^t f)\alpha = af\alpha$. Thus $f \in M_\alpha(G)$. □

The condition $xf'\alpha^s = yf'\alpha^t$ imposed on function $f'\colon M \to G$ in Theorem 2.2 seems quite technical. However it is necessary for the extension function f to be well-defined. For instance, Let $A = \{a, b, c, d, e, f\}$ and $\alpha\colon A \to A$ is defined as $\alpha = \{(a, b), (b, a), (c, d), (d, e), (e, f), (f, c)\}$ where the ordered pair (x, y) means $x\alpha = y$. It is not difficult to see that the set $M = \{b, c\}$ is a minimal generating set for the graph $\mathcal{G}_\alpha(A)$. Define a function $f'\colon M \to A$ as $f' = \{(b, d), (c, a)\}$. Consider the extension $f\colon A \to A$ of f' using the relation $(x\alpha^s)f = (xf')\alpha^s$, this f is not well-defined. Observe that $a = b\alpha = b\alpha^3$. On the one hand, $af = (b\alpha)f = (bf')\alpha = d\alpha = e$ and, on the other hand, $af = (b\alpha^3)f = (bf')\alpha^3 = d\alpha^3 = c$. Thus the extension f of f' is not well-defined.

In the above theorem, a finite minimal generating set M is used to characterize elements of $M_\alpha(G)$. If we choose a representative from each connected component θ_x containg vertex x, is it possible to use these representatives of connected components to characterize $M_\alpha(G)$? The following discussion give partial answers to this question. In Theorem 2.2, a technical condition is imposed on the function $f'\colon M \to G$, that is, when $x\alpha^s = y\alpha^t$ then $xf'\alpha^s = yf'\alpha^t$. In the remain of this section, this condition will be investigated further.

Let the orbit space of G acting by α, denoted $\mathcal{O}_\alpha(G)$, be the set of all connected components of the graph $\mathcal{G}_\alpha(G)$, and θ_x a connected component in $\mathcal{O}_\alpha(G)$ containing x. Hereafter, θ_x is also used to denote the vertex set $V(\theta_x)$ of the digraph θ_x when no confusion will arise. It can easily be seen that θ_x contains all the preimages $z\alpha^{-1}$ for all $z \in \theta_x$. Denote $|\theta_x|$ the cardinality of all the vertices in the subgraph θ_x. Define $c(\theta_x)$, $p(\theta_x) \in \mathbb{Z} \cup \{\infty\}$ as $c(\theta_x) := \sup\{c(z) \mid \text{ for all } z \in \theta_x\}$ and $p(\theta_x) := \sup\{p(z) \mid \text{ for all } z \in \theta_x\}$. Here $c(\theta_x)$ and $p(\theta_x)$ are called the *circular length* and *path length* of the connected component θ_x respectively. Some binary relations can be defined on $\mathcal{O}_\alpha(G)$. Define

$$\theta_x \prec_c \theta_y \quad \text{if and only if} \quad c(\theta_x) \mid c(\theta_y);$$

$$\theta_x \prec_p \theta_y \quad \text{if and only if} \quad p(\theta_x) \le p(\theta_y);$$

$$\theta_x \prec \theta_y \quad \text{if and only if} \quad c(\theta_x) \mid c(\theta_y) \ \text{ and } \ p(\theta_x) \le p(\theta_y).$$

Similar to the relation $\preccurlyeq$ defined on elements of G, these relations on $\mathcal{O}_\alpha(G)$ are reflexive and transitive but not necessarily antisymmetric.

Lemma 2.3. *Let $\theta_x \in \mathcal{O}_\alpha(G)$. Then $y \in \theta_x$ if and only if there exist $s, t \in \mathbb{N} \cup \{0\}$ such that $y\alpha^s = x\alpha^t$.*

Proof. Consider the two orbits $\mathcal{O}_\alpha(x) = \{x, x\alpha, x\alpha^2, \cdots\}$ and $\mathcal{O}_\alpha(y) = \{y, y\alpha, y\alpha^2, \cdots\}$. Recall that $\mathcal{G}_\alpha(G)$ is a functional graph and so is the subgraph θ_x. Since θ_x is connected, $\mathcal{O}_\alpha(x) \cap \mathcal{O}_\alpha(y) \neq \emptyset$. Therefore there exist $s, t \in \mathbb{N} \cup \{0\}$ such that $y\alpha^s = x\alpha^t$. On the other hand, observe that $y \in x\alpha^t\alpha^{-s}$, thus $y \in \theta_x$ by definition. □

Proposition 2.4. *Let $f \in M_\alpha(G)$. If $y \in \theta_x$ for some $x \in G$, then $yf \in \theta_{xf}$.*

Proof. Let $f \in M_\alpha(G)$ and $y \in \theta_x$ for some $x \in G$. By Lemma 2.3, we have $x\alpha^s = y\alpha^t$ for some $s, t \in \mathbb{N} \cup \{0\}$. Then

$$(yf)\alpha^t = (y\alpha^t)f = (x\alpha^s)f = (xf)\alpha^s.$$

Thus $yf \in \theta_{xf}$ by Lemma 2.3. □

Note that if x, y are generating elements of $\mathcal{G}_\alpha(G)$, and x, y are connected (i.e., in the same connected component), then xf' and yf' shall be in the same connected component by Theorem 2.2 and Proposition 2.4.

Lemma 2.5. *Let $f \in M_\alpha(G)$. Then $\theta_{xf} \prec_c \theta_x$ for all $x \in G$.*

Proof. By definition, $c(\theta_x)$ is the supreum of all the number $c(z)$ for all $z \in \theta_x$. Since $\mathcal{G}_\alpha(G)$ is functional, there is at most one cycle in θ_x. Therefore $c(\theta_x) = c(z)$ for all $z \in \theta_x$. In particular, $c(\theta_x) = c(x)$. Hence $c(\theta_{xf}) = c(xf)$ is a factor of $c(x) = c(\theta_x)$ by Lemma 2.1. Thus $\theta_{xf} \prec_c \theta_x$. $\square$

When α is a bijection, then each vertex $a \in \mathcal{G}_\alpha(G)$ has both indegree and outdegree equal to 1, $\text{indeg}(a) = \text{outdeg}(a) = 1$. Consequently, no vertex in $\mathcal{G}_\alpha(G)$ is a leaf or each vertex is circular. Thus the orbit space $\mathcal{O}_\alpha(G)$ contains a (connected) cycle or is a union of cycles. For the remaining in this section, we consider $\mathcal{O}_\alpha(G)$ equipped with the binary relation $\prec_c$. By a minimal element θ_x in $(\mathcal{O}_\alpha(G), \prec_c)$, we mean if there exists $\theta_y \prec_c \theta_x$ then $c(\theta_y) = c(\theta_x)$. Using these notions and terminologies, Lemma 2.1 can be improved as following.

Theorem 2.6. *Let α be a bijection of a finite group G such that $0\alpha = 0$, and $x, y \in G \setminus \{0\}$. Then there exists $f \in M_\alpha(G)$ such that $xf = y$ if and only if $\theta_y \prec_c \theta_x$.*

Proof. Let $f \in M_\alpha(G)$ such that $xf = y$. Therefore $\theta_y \prec_c \theta_x$ by Lemma 2.5. Conversely, assume $\theta_y \prec_c \theta_x$. Since α is a bijection, the orbit space $\mathcal{O}_\alpha(G)$ is a union of cycles. Choose x as the generating element for the cycle θ_x. Let M be a minimal generating set of $\mathcal{G}_\alpha(G)$ containing x. Define a map $f' \colon M \to G$ such that $xf' = y$ and $af' = 0$ for all $a \in M \setminus \{x\}$. If $y \in \theta_x$, then $y \notin M$ since M is a minimal generating set of $\mathcal{G}_\alpha(G)$ and x is the generating element for θ_x. If $y \notin \theta_x$ and $y \in M$, then there exist no $s, t \in \mathbb{N} \cup \{0\}$ such that $x\alpha^s = y\alpha^t$ by Lemma 2.3. Thus the hypothesis in Theorem 2.2 is fulfilled, and the proof is completed by extending the function f' to $f \in M_\alpha(G)$. $\square$

While working on group mappings, it is natural to require additional property that $0\alpha = 0$. In fact, this is a consequence when α is a homomorphism. A special case when $\{0\}$ is an isolated vertex, we will consider the orbit space without $\{0\}$. The collection of the remaining connected components is denoted $\mathcal{O}^*_\alpha(G)$. Explicitely, $\mathcal{O}^*_\alpha(G) = \mathcal{O}_\alpha(G) \setminus \{\theta_0\}$.

Let G be a group and $(M(G), \circ)$ the semigroup of all mappings on G. A subsemigroup S of $M(G)$ is said to act *transitively* on G if for all nonzero $x, y \in G$, there exists an $f \in S$ such that $xf = y$.

Corollary 2.7. *Let α be a bijection of a finite group G with $0\alpha = 0$. Then $M_\alpha(G)$ acts transitively on G if and only if the circular length of elements in $\mathcal{O}^*_\alpha(G)$ are equal.*

Proof. Let $x, y \in G \setminus \{0\}$. Then there exists $f, g \in M_\alpha(G)$ such that $xf = y$ and $yg = x$ if and only if $c(\theta_y) \mid c(\theta_x)$ and $c(\theta_x) \mid c(\theta_y)$ by Theorem 2.6, which is equivalent to $c(\theta_x) = c(\theta_y)$. Hence result. □

The following result is crucial for further developments in centralizer nearrings.

Lemma 2.8. *Assume $0\alpha = 0$. Let L be a subset of $M_\alpha(G)$ such that $M_\alpha(G)L \subseteq L$. If there exists an $\ell \in L$ with the property that $0\ell = 0$ and $c(\theta\ell) = c(\theta)$ for some cycles θ, $\theta\ell \in \mathcal{O}^*_\alpha(G)$, then L contains an idempotent $e\colon G \to G$ where e is identity on $\theta\ell$ and 0 elsewhere.*

Proof. Let $v \in \theta$ and choose $v\ell$ be a generating element for the cycle $\theta\ell$. Let M be a minimal generating set for $\mathcal{G}_\alpha(G)$ containing vertex $v\ell$. Define a mapping $f'\colon M \to G$ via $v\ell f' = v$ and $xf' = 0$ for all $x \in M \setminus \{v\ell\}$. By Theorem 2.2, there exists $f \in M_\alpha(G)$ such that $xf = xf'$ for all $x \in M$. Explicitely, we have $v\ell f = v$ and $xf = 0$ for all $x \in G \setminus \theta\ell$. Let $z \in \theta\ell$. Then $z = v\ell\alpha^i$ for some $i \in \mathbb{N} \cup \{0\}$ since $v\ell$ is a generating element for the cycle $\theta\ell$. Observe that

$$zf\ell = (v\ell\alpha^i)f\ell = (v\ell f)\alpha^i\ell = v\alpha^i\ell = v\ell\alpha^i = z,$$

and $xf\ell = 0$ for all $x \in G \setminus \theta\ell$. Let $e = f\ell$. Then e is the desired idempotent in L. □

3 Nearrings of centralizers

In this section, the function $\alpha\colon G \to G$ is assumed to be a group homomorphism, and thus $M_\alpha(G)$ is a nearring. The algebraic properties of the nearring of centralizers $M_\alpha(G)$ will be characterized using the graphical properties of the group mapping.

Lemma 3.1. *Let $\alpha\colon G \to G$ be a group endomorphism, and $G(\alpha, \mu, \nu) = \{a \in G \mid p(a) = \mu, c(a) = \nu\}$. Then*

(1) *$G(\alpha, 0, 1)$ is an $M_\alpha(G)$-submodule of G.*

(2) *Suppose $0 \in G$ is the only element with circular length equals to one. Let $m \neq 1$ be a minimal circular length with respect to $\prec_c$. Then $G(\alpha, 0, m) \cup \{0\}$ is an $M_\alpha(G)$-submodule of G.*

Proof. (1) Since α is an endomorphism, $0\alpha = 0$ and thus the circular length $c(0) = 1$ or $0 \in G(\alpha, 0, 1)$. Let $a, b \in G(\alpha, 0, 1)$. Then $(a - b)\alpha = a\alpha - b\alpha = a - b$, and so $c(a - b) = 1$ or $a - b \in G(\alpha, 0, 1)$. Therefore $G(\alpha, 0, 1)$ is a subgroup of G. Furthermore, let $f \in M_\alpha(G)$ and $a \in G(\alpha, 0, 1)$. Then $(af)\alpha = a(f\alpha) = a(\alpha f) = (a\alpha)f = af$. Thus $c(af) = 1$ or $af \in G(\alpha, 0, 1)$.

(2) Observe that if $a, b \in G(\alpha, 0, m)$, then $(a - b)\alpha^m = a - b$. Thus, by minimality of m and Lemma 2.5, $c(a - b) = 1$ or m. If $c(a - b) = 1$, then $a - b = 0$ since 0 is the only element with circular length equals to one. If $c(a - b) = m$, then $a - b \in G(\alpha, 0, m)$. Thus $G(\alpha, 0, m) \cup \{0\}$ is a subgroup of G. A similar argument used in (1) above can show that it is an $M_\alpha(G)$-submodule of G. □

Theorem 3.2. *Let G be a finite group of order at least three and $\alpha\colon G \to G$ a group automorphism. Then the following are equivalent:*

(1) *$M_\alpha(G)$ is a simple nearring.*

(2) *All the orbits in $\mathcal{O}^*_\alpha(G)$ have the same circular length.*

(3) *$M_\alpha(G)$ acts transitively on G.*

(4) *$M_\alpha(G)$ is 1-primitive on G.*

(5) *$M_\alpha(G)$ is 2-primitive on G.*

Proof. To show that (1) implies (2), assume $M_\alpha(G)$ is simple. If the orbits in $\mathcal{O}^*_\alpha(G)$ have different length, then there exists a proper nontrivial $M_\alpha(G)$-submodule H of G by Lemma 3.1. Thus the annihilator Ann$H$ is an ideal of $M_\alpha(G)$ by [6, Corollary 1.43]. This ideal is proper since $M_\alpha(G)$ contains the identity map on G. The mapping $f\colon G \to G$ defined via $af = 0$ for all $a \in H$ and $xf = x$ for all $x \in G \setminus H$ is an element in $M_\alpha(G)$ by Theorem 2.2. Since the function f annihilates H, the ideal Ann$H$ is nontrivial. Thus all the orbits in $\mathcal{O}^*_\alpha(G)$ have the same length.

To show that (2) implies (1), provided that all the orbits in $\mathcal{O}^*_\alpha(G)$ have the same length m. If $m = 1$, then each element in G is fixed by α and thus α is the identity map. In this case, $M_\alpha(G) = M(G)$, the set of all mappings from G to G, is simple by [5, Theorem 1.43]. If $m \neq 1$, let I be a nontrivial ideal of $M_\alpha(G)$. Then there exists an $f \in I$ such that $\theta_i f = \theta_j$ for some orbits θ_i, $\theta_j \in \mathcal{O}^*_\alpha(G)$ by Proposition 2.4. Since $0 \in G$ is the only element with circular length equals to one, it follows that $0f = 0$ by Lemma 2.1 (and thus $M_\alpha(G)$ is 0-symmetric). Hence I contains an idempotent e_j such that e_j is identity on θ_j and 0 elsewhere by Lemma 2.8. Let $\theta_k \in \mathcal{O}^*_\alpha(G)$ be arbitrary. Consider the map $f_{jk}\colon G \to G$ which maps θ_j to θ_k and 0 elsewhere. Then $f_{jk} \in M_\alpha(G)$ by Theorem 2.6. Since $M_\alpha(G)$ is 0-symmetric and I is an ideal of $M_\alpha(G)$, it follows that $e_j f_{jk} \in I$. Apply Lemma 2.8 again, the idempotent e_k which is identity on θ_k and 0 elsewhere is in I. Now index the orbits in $\mathcal{O}^*_\alpha(G)$ as $\theta_1, \theta_2, \cdots, \theta_n$. Then the identity mapping $1 = e_1 + e_2 + \cdots + e_n \in I$. Hence $I = M_\alpha(G)$, and thus $M_\alpha(G)$ is simple.

The equivalence of (2) and (3) follows from Corollary 2.7.

To show that (3) implies (4), assume that $M_\alpha(G)$ acts transitively on G. Then each nonzero element $a \in G$ is a generator for the $M_\alpha(G)$-module G. If $a = 0$ and the circular length of elements in $\mathcal{O}^*_\alpha(G)$ are greater than one, then $0f = 0$ for all $f \in M_\alpha(G)$ by Lemma 2.5. Moreover, if the circular length of elements in $\mathcal{O}^*_\alpha(G)$ are all equal to one, then $0M_\alpha(G) = G$. Thus G is strongly monogenic. It remains to show that G is a simple $M_\alpha(G)$-module. Recall that a normal subgroup K of G is an $M_\alpha(G)$-ideal of G if $(k + a)f - af \in K$ for all $k \in K$, $a \in G$ and $f \in M_\alpha(G)$. Assume K is a nontrivial $M_\alpha(G)$-ideal of G and pick a nonzero $k \in K$. The hypothesis indicates that all the orbits in $\mathcal{O}^*_\alpha(G)$ have the same length m. Suppose first that $m = 1$. Let a be an arbitrary element in G. The mapping $f \in M(G)$ defined by $kf = a$ and $xf = 0$ for all $x \in G \setminus \{k\}$ is an element in $M_\alpha(G)$ by Theorem 2.2. Consequently, $a = kf - 0f = (k + 0)f - 0f \in K$ or $G \subseteq K$. Furthermore, assume that $m \neq 1$. Then 0 is the unique element with circular length equals to one. Thus $0f = 0$ for all $f \in M_\alpha(G)$ by Lemma 2.5. In particular, $kf = (k + 0)f - 0f \in K$. Since $M_\alpha(G)$ acts transitively on G, $kM_\alpha(G) = G$. Hence $K = G$. Therefore G is a simple and strongly monogenic $M_\alpha(G)$-module and $M_\alpha(G)$ is 1-primitive on G.

To show that (4) implies (3), suppose $M_\alpha(G)$ is 1-primitive on G. Since G is strongly monogenic and $M_\alpha(G)$ contains the identity mapping of G, it follows that $xM_\alpha(G) = G$ for all nonzero $x \in G$. Hence there exists $f \in M_\alpha(G)$ such that $xf = y$ for any nonzero $y \in G$.

The equivalence of (4) and (5) follows from the fact that $M_\alpha(G)$ contains an identity [6, Proposition 3.7]. □

The following example shows that 0-primitivity is not equivalent to the conditions in Theorem 3.2.

Example 3.3. There exists a 0-primitive nearring $M_k(\mathbb{Z}_n)$ which is not simple. Consider the nearring $N = M_5(\mathbb{Z}_8)$. The path length of each elements in $\mathbb{Z}_8$ is 0 and the circular length are $c(1) = c(3) = c(5) = c(7) = 2$, $c(0) = c(2) = c(4) = c(6) = 1$ respectively. Observe that the function $f\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ defined via $0f = 2$ and $xf = 0$ for all $x \in \mathbb{Z}_8 \setminus \{0\}$ is an element in N by Theorem 2.2. Therefore N is not 0-symmetric.

First, it will be shown that $\mathbb{Z}_8$ is a type-0 N-module. Note that $\mathbb{Z}_8$ is a faithful monogenic N-module generated by one of the elements $\{1, 3, 5, 7\}$. It remains to show that $\mathbb{Z}_8$ contains no proper nontrivial N-ideals. To assert a normal subgroup H of $\mathbb{Z}_8$ is an N-ideal, the identity $(h + a)f - af \in H$ shall hold for all $h \in H$, $a \in \mathbb{Z}_8$ and $f \in N$. If the subgroup $H_1 = \{0, 4\}$ is an N-ideal, then in particular, $4f - 0f = (4 + 0)f - 0f \in H_1$ for all $f \in N$. Let $g\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ defined by $4g = 6$ and $xg = 0$ for all $x \in \mathbb{Z}_8 \setminus \{4\}$. Then $g \in N$ by Theorem 2.6. But then $4g - 0g = 6 - 0 = 6 \notin H_1$, and thus H_1

is not an N-ideal of $\mathbb{Z}_8$. Next, if $H_2 = \{0, 2, 4, 6\}$ is an N-ideal of $\mathbb{Z}_8$. Then, in particular, $3f - 1f = (2 + 1)f - 1f \in H_2$ for all $f \in N$. Define a map $h\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ via $3h = 6$, $7h = 6$, $1h = 1$, $5h = 5$ and $xh = 0$ for all $x \in H_2$. Then $h \in N$ by Theorem 2.2. But then $3h - 1h = 6 - 1 = 5 \notin H_2$. Thus H_2 is not an N-ideal. It follows that $\mathbb{Z}_8$ is a simple N-module. Consequently, N is 0-primitive.

Now, we will show that N is not simple by finding a nontrivial proper ideal. Recall that $K = \mathbb{Z}_8(5, 0, 1) = \{0, 2, 4, 6\}$ is an N-submodule of $\mathbb{Z}_8$ by Lemma 3.1. Thus the annihilator $\mathrm{Ann}K = \{f \in N \mid af = 0 \text{ for all } a \in K\}$ is an ideal of N by [6, Corollary 1.43]. $\mathrm{Ann}K$ is clearly a nontrivial proper ideal of N for the identity map $\varepsilon \notin \mathrm{Ann}K$ and the function h defined above is in $\mathrm{Ann}K$. Thus N is not simple. It is also worth to mention that $\mathrm{Ann}K$ is a minimal ideal of N with $(\mathrm{Ann}K)^2 \neq 0$.

It is shown in [4, Theorem 1.1] that the 0-symmetric subnearring of $M_\alpha(G)$, where α is an automorphism of a finite group G, is simple if and only if all the orbits in $\mathcal{O}^*_\alpha(G)$ have the same length. Combine this result with Theorem 3.2, we have the following

Corollary 3.4. *Let G be a finite group of order at least three and $\alpha\colon G \to G$ a group automorphism. Then $M_\alpha(G)$ is simple if and only if the 0-symmetric subnearring $M^0_\alpha(G)$ of $M_\alpha(G)$ is simple.*

In the proof of Theorem 3.2, it is found that if 0 is the only element in G with circular length equals to one, then $M_\alpha(G)$ is 0-symmetric. The following result shows that this condition is also necessary.

Proposition 3.5. *Let G be a finite group of order at least three and $\alpha\colon G \to G$ an automorphism. Then $M_\alpha(G)$ is 0-symmetric if and only if the zero element is the unique element in G with circular length equals to one.*

Proof. The "if" part follows from Lemma 2.1. Provided that $M_\alpha(G)$ is 0-symmetric. To the contrary, if there exists a nonzero element $a \in G$ such that $c(a) = 1$. Define a mapping $f\colon G \to G$ via $0f = a$ and 0 elsewhere. A direct verification reveals that $0f\alpha = a\alpha = a = 0\alpha f$ and $xf\alpha = 0\alpha = 0 = x\alpha f$ for $x \in G \setminus \{0\}$. Thus $f \in M_\alpha(G)$ and $M_\alpha(G)$ is not 0-symmetric. This completes the proof. □

A special case in Theorem 3.2 is that there is only one orbit θ in $\mathcal{O}^*_\alpha(G)$. If the circular length $c(\theta) = 1$, then G is a group of order two and the function α is the identity mapping of G. It is shown that $M_1(\mathbb{Z}_2) = M(\mathbb{Z}_2)$ contains a nontrivial proper ideal $M_c(\mathbb{Z}_2)$, the constant subnearring of $M(\mathbb{Z}_2)$ [6, p. 204]. If the circular length $c(\theta) \geq 2$, then G is a group of order at least three.

Thus the unique isolated vertex in G is the zero element. Consequently, $M_\alpha(G)$ is 0-symmetric by Proposition 3.5. Furthermore, observe that $\{0, a\}$ is a minimal generating set for the digraph $\mathcal{G}_\alpha(G)$ whenever a is an arbitrary nonzero element in G. It follows that all the nonzero element in $M_\alpha(G)$ are bijective and thus invertible by Proposition 2.4. Hence $M_\alpha(G)$ is a nearfield. Conversely, if $M_\alpha(G)$ is a nearfield then it is simple and each nonzero element is invertible. Thus the cardinality $|\mathcal{O}^*_\alpha(G)| = 1$ whenever G is a finite group of order at least three and α is a group automorphism by Theorem 3.2 and Lemma 2.8.

Moreover, since addition is commutative in a nearfield [6, Theorem 8.11] and there is only one nonzero generating element for the digraph $\mathcal{G}_\alpha(G)$, pick a nonzero element $a \in G$ as the generating element. Let $f, g \in M_\alpha(G)$. Then $af = a\alpha^i$, $ag = a\alpha^j$ for some $i, j \in \mathbb{N} \cup \{0\}$ by Lemma 2.3. Let $b \in G \setminus \{0\}$. Then $b = a\alpha^k$ for some $k \in \mathbb{N} \cup \{0\}$. Observe that $bfg = (a\alpha^k)fg = a\alpha^{i+j+k} = (a\alpha^k)gf = bgf$. Thus multiplication in $M_\alpha(G)$ is commutative. Consequently, $M_\alpha(G)$ is a field. We have reproved the following result.

Corollary 3.6. *[4, Corollary 1.3] Let G be a finite group of order at least three and α a group automorphism. Then the following are equivalent.*

(1) *$M_\alpha(G)$ is a field.*
(2) *$M_\alpha(G)$ is a nearfield.*
(3) *The cardinality $|\mathcal{O}^*_\alpha(G)| = 1$.*

In fact, more can be said when $M_\alpha(G)$ is a field. Since $\mathcal{O}^*_\alpha(G)$ contains only one cycle, let $x, y \in G \setminus \{0\}$ and $M = \{0, a\}$ a generating set for $\mathcal{G}_\alpha(G)$. Then $x = a\alpha^i$, $y = a\alpha^j$ for some $i, j \in \mathbb{N} \cup \{0\}$. Define mappings $f', g' \colon M \to G$ via $0f' = 0$, $af' = a\alpha^i$ and $0g' = 0$, $ag' = a\alpha^j$ respectively. Extend these two maps to $f, g \in M_\alpha(G)$. Now observe that $x+y = a\alpha^i + a\alpha^j = af' + ag' = af + ag = a(f+g) = a(g+f) = ag + af = y + x$. Thus G is an abelian group. Furthermore, it is well known that the order of a finite field is equal to p^n for some prime number p and some $n \in \mathbb{N}$. On the other hand, each nonzero element in $M_\alpha(G)$ determines and is uniquely determined (according to the chosen nonzero generating element for $\mathcal{G}_\alpha(G)$) by a nonzero element in G by Corollary 3.6. Thus the cardinality $|M_\alpha(G)| - 1 = |G| - 1$. Consequently, $|G| = |M_\alpha(G)| = p^n$.

If G is not characteristically simple, then it contains a nontrivial proper characteristic subgroup K of G. Since $K\alpha \subseteq K$ for all $\alpha \in \mathrm{Aut}(G)$, it follows that the orbit space $\mathcal{O}^*_\alpha(G)$ contains at least two elements. Thus $M_\alpha(G)$ is not a field by Corollary 3.6. This contradiction implies that G is a finite characteristically simple abelian group with order p^n for some prime number p and some $n \in \mathbb{N}$. In other words, $G \cong \oplus_{i=1}^n \mathbb{Z}_p$.

Corollary 3.7. *Let G be a finite group of order at least three and $\alpha\colon G \to G$ a group automorphism. If $M_\alpha(G)$ is a field then $G \cong \oplus_{i=1}^{n} \mathbb{Z}_p$ for some prime number p and some $n \in \mathbb{N}$.*

Since the additive group $(M_\alpha(G), +)$ is also characteristically simple [6, Theorem 8.11], it follows that $G \cong (M_\alpha(G), +) \cong \oplus_{i=1}^{n} \mathbb{Z}_p$ by Corollary 3.7. We may ask: does the converse of Corollary 3.7 also hold? The following example deny this possibility.

Example 3.8. Let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3 = \{(x, y) \mid 0 \leq x, y \leq 2\}$. It is routine to verify that the following two functions $\alpha, \beta\colon G \to G$ are group automorphisms:

$$(x, y)\alpha = (x + 2y, x + y); \quad (x, y)\beta = (x + 2y, x)$$

for all $(x, y) \in G$. Then $\mathcal{O}_\alpha^*(G) = \{\theta_{(1,0)}\}$ contains only one orbit and thus $M_\alpha(G)$ is a field of order 9. However, $\mathcal{O}_\beta^*(G) = \{\theta_{(1,2)}, \theta_{(1,0)}\}$ with circular length $c(\theta_{(1,2)}) = 2$ and $c(\theta_{(1,0)}) = 6$. So $M_\beta(G)$ is not a field by Corollary 3.6. In fact, it is not even simple by Theorem 3.2.

A quick conclusion from Corollary 3.7 is that when $M_\alpha(\mathbb{Z}_p)$ is a field, then $M_\alpha(\mathbb{Z}_p) \cong \mathbb{Z}_p$ as a field.

References

[1] R. Balakrishnan, K. Ranganathan, *A textbook of graph theory*, Springer, New York, 1999.

[2] P. Birch, A. Oswald, Some comments on near-rings of mappings, *Contrib. General Algebra* **9** (1995) 73–79.

[3] P. Bouchard, Y. Fong, W.-F. Ke, Y.-N. Yeh, Counting f such that $f \circ g = g \circ f$, *Results Math.* **31** (1997) 14–27.

[4] C. J. Maxson, K. C. Smith, The centralizer of a group automorphism, *J. Algebra* **54** (1978) 27–41.

[5] J. D. P. Meldrum, *Near-rings and their links with groups*, Research Notes in Math. **134**, Pitman, London, 1985.

[6] G. Pilz, *Near-rings*, 2nd. revised edition, North-Holland, Amsterdam, 1983.

[7] J. S. Rose, *A course on group theory*, Dover, New York, 1994.