MULTIPLICATIVE n-TH ROOT FUNCTIONS OVER FINITE SEMIGROUPS, GROUPS, FIELDS AND COMMUTATIVE RINGS

BOAZ COHEN

Communicated by Alexandru Zaharescu

In this paper, we study the existence and uniqueness of multiplicative n-th root functions $\sqrt[n]{\ }$ over *finite* semigroups, in order to implement these ideas on finite groups, fields and commutative rings. A set of sufficient and necessary conditions are presented for existence of multiplicative n-th root functions over different algebraic structures. It is also shown that once the existence is established, the uniqueness is guaranteed. In addition, we describe the construction procedure of such a function.

AMS 2020 Subject Classification: 18B40, 20M15, 20D99, 11T99.

Key words: finite semigroups, finite groups, finite fields, finite commutative rings, n-th roots.

1. INTRODUCTION

Given a real number $a \in \mathbb{R}$, a *square-root* of a is any $b \in \mathbb{R}$ for which $b^2 = a$. It is well known that any positive real number has two square roots, one positive and one negative. That fact, along with the observation that the square-root of 0 is 0, allow us to define the *principal* square root of a, which is denoted by $\sqrt{a}$, to be its non-negative square-root. One of the most familiar properties of the principal square-root function is its *multiplicativity property* which states that $\sqrt{ab} = \sqrt{a}\sqrt{b}$ for every two non-negative real numbers a and b.

The concept of square-root functions can be carried on into a wider medium: by a *square-root function* over a field $\mathbb{F}$ we mean a function $r : \mathbb{F}^{(2)} \to \mathbb{F}$, where $\mathbb{F}^{(2)} := \{a^2 : a \in \mathbb{F}\}$, such that $r(x)^2 = x$ for every $x \in \mathbb{F}^{(2)}$. For example, if $\mathbb{F} = \mathbb{R}$, then $\mathbb{R}^{(2)} = [0, \infty)$. In this case, both functions $r_1(x) = \sqrt{x}$ and $r_2(x) = -\sqrt{x}$ are examples of square-root functions over $\mathbb{R}$. It turns out that among all square-root functions over $\mathbb{R}$, the function r_1 above is the only square-root function which satisfies the multiplicity property. Generally, the existence of a multiplicative square-root function is not guaranteed over every field. For example, over the field of complex numbers $\mathbb{C}$ such a multiplicative

MATH. REPORTS **26(76)** (2024), *3-4*, 219–250
doi: 10.59277/mrar.2024.26.76.3.4.219

square-root function does not exist. Indeed, as one can verify, in this case $\mathbb{C}^{(2)} = \mathbb{C}$ and if we had a multiplicative square-root function $r : \mathbb{C} \to \mathbb{C}$, then on the one hand $r(1) = r((-1)^2) = r(-1)^2 = -1$, but on the other hand $r(1) = r(1^2) = r(1)^2 = 1$, a contradiction. In view of this, it is natural to ask, in which fields can a multiplicative square-root function be defined, and in these cases, is this function unique? This problem in general was treated by Waterhouse in [12] and by Gładki in [3] and [4], in which an extensive treatment of this problem was given for both finite and infinite fields. The goal of this paper is to study the existence and uniqueness of multiplicative n-th root functions over several *finite* algebraic structures. To do so, we first discuss this issue from a more general point of view, by solving the problem for finite semigroups. We then apply the results to finite groups, commutative rings and fields.

Let S be a semigroup, written multiplicatively, and let $n \geqslant 2$ be an integer. For any $a \in S$, we define the *n-th power* of a to be a^n. The *set* of n-th powers of the elements of S is denoted by $S^{(n)}$, that is $S^{(n)} := \{a^n : a \in S\}$. Given an element $a \in S$, any solution $x \in S$ of the equation

$$x^n = a$$

is called an *n-th root of a*. In general, a may not have an n-th root. On the other hand, it may have more than one. The *set* of the n-th roots of a is denoted by $a^{\frac{1}{n}}$, that is $a^{\frac{1}{n}} := \{b \in S : b^n = a\}$. Note that a has an n-th root if and only if $a \in S^{(n)}$. Therefore, $S^{(n)}$ can also be referred as the set of elements of S which have an n-th root. An *n-th root function (abbreviated as RF) over S* is a function $r : S^{(n)} \to S$ that maps every element of $S^{(n)}$ to one of its n-th roots. In other words, r is an n-th RF if $r(x) \in x^{\frac{1}{n}}$, or equivalently, if $r(x)^n = x$ for every $x \in S^{(n)}$. An n-th RF r over S such that $r(x) = x$ for every $x \in S^{(n)}$, is referred to as *trivial.* It should be noted that in general, a trivial n-th RF may not exists over S. A 2-nd RF and a 3-rd RF are also called a *square-RF* and a *cube-RF*, respectively. We say that an n-th RF r over S is *multiplicative* if $S^{(n)}$ is a subsemigroup of S and r is a semigroup homomorphism from $S^{(n)}$ into S, that is, if $r(xy) = r(x)r(y)$ for every $x, y \in S^{(n)}$. The term "multiplicative n-th root function" is abbreviated as *n-th MRF.* It should be emphasized that $S^{(n)}$ may not be a subsemigroup of S and in these cases an n-th MRF does not exist over S. Furthermore, if $S^{(n)}$ is a subsemigroup of S, then the existence of an n-th MRF over S is not guaranteed. We note that if S is commutative, then $S^{(n)}$ is subsemigroup of S for every n.

We also need the notion of n-commutativity. Let n be a positive integer. Then a semigroup S is *n-commutative* if $(ab)^n = a^n b^n$ for each $a, b \in S$. If R

is a subset of a semigroup S, then R is *n-commutative* if R is a subsemigroup of S and $(ab)^n = a^n b^n$ for each $a, b \in R$.

As an illustrative example, consider the set of residues modulo 18, namely the set $\mathbb{Z}_{18} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{17}\}$ with respect to modular multiplication. In this case

$$\mathbb{Z}_{18}^{(2)} = \{\overline{0}^2, \overline{1}^2, \overline{2}^2, \ldots, \overline{17}^2\} = \{\overline{0}, \overline{1}, \overline{4}, \overline{7}, \overline{9}, \overline{10}, \overline{13}, \overline{16}\}.$$

Since

$$\begin{array}{ll} \overline{0}^{\frac{1}{2}} = \{\overline{0}, \overline{6}, \overline{12}\} & \overline{9}^{\frac{1}{2}} = \{\overline{3}, \overline{9}, \overline{15}\} \\ \overline{1}^{\frac{1}{2}} = \{\overline{1}, \overline{17}\} & \overline{10}^{\frac{1}{2}} = \{\overline{8}, \overline{10}\} \\ \overline{4}^{\frac{1}{2}} = \{\overline{2}, \overline{16}\} & \overline{13}^{\frac{1}{2}} = \{\overline{7}, \overline{11}\} \\ \overline{7}^{\frac{1}{2}} = \{\overline{5}, \overline{13}\} & \overline{16}^{\frac{1}{2}} = \{\overline{4}, \overline{14}\} \end{array}$$

there are $3^2 \cdot 2^6 = 576$ different square-RF's over $\mathbb{Z}_{18}$. It turns out that among them, only the following function is multiplicative

$$\begin{array}{ll} r(\overline{0}) = \overline{0} & r(\overline{9}) = \overline{9} \\ r(\overline{1}) = \overline{1} & r(\overline{10}) = \overline{10} \\ r(\overline{4}) = \overline{16} & r(\overline{13}) = \overline{7} \\ r(\overline{7}) = \overline{13} & r(\overline{16}) = \overline{4}. \end{array}$$

Our goal in this paper is to study the existence and uniqueness of n-th MRF's over *finite* semigroups, in order to implement these ideas on finite groups, fields and commutative rings.

We begin our study in Section 2, in which a brief overview of some special concepts in semigroups theory is given. In Section 3, we discuss n-th MRF's over finite semigroups. One of our main results in Section 3 is Theorem 3.6:

THEOREM 3.6. *Suppose that S is a finite semigroup and $n \geqslant 2$ is an integer. Then there exists an n-th MRF r over S iff $S^{(n)}$ is an n-commutative subsemigroup of S,* $\operatorname{ind}(S) \leqslant n$ *and* $\gcd(n, \operatorname{per}(S)) = \gcd(n^2, \operatorname{per}(S))$. *Furthermore, if such a function exists, then it is unique and it is given by*

$$r(x) = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{\operatorname{per}(S^{(n)})}$.

Recall that $S^{(n)}$ is n-commutative if and only if $S^{(n)}$ is a subsemigroup of S and $(ab)^n = a^n b^n$ for every $a, b \in S^{(n)}$. In addition, $\operatorname{per}(S)$ is the least common multiple of the periods of all the elements in S and $\operatorname{ind}(S)$ is the maximal index among the indices of the elements of S. The notions of period and index are defined in Section 2.

The n-th MRF, in case of existence, is denoted by our more familiar surd notation $\sqrt[n]{\ }$. We remark that due to uniqueness, there is no ambiguity in using this notation.

Section 4 focuses on n-th MRF's over finite groups. When referring to groups, n-commutativity is called being *n-abelian*. In the following theorem, we gather the main results on the n-th MRF's over finite groups, which can be obtained by the application of the results for semigroups:

THEOREM 4.2. *Suppose that G is a finite group and $n \geqslant 2$ is an integer. Then there exists a n-th MRF r over G if and only if $G^{(n)}$ is an n-abelian subgroup of G and $\gcd(n, \exp(G)) = \gcd(n^2, \exp(G))$. Furthermore, if r exists, then the following assertions hold:*

(a) *r is the unique n-th MRF over G and is given by $r(x) = x^e$, where e is the least positive integer such that $ne \equiv 1 \pmod{|G^{(n)}|}$. Furthermore, r is non-trivial if and only if $e > 1$.*

(b) *$G^{(n)} \trianglelefteq G$ and consequently $r(x^g) = r(x)^g$ for every $x \in G^{(n)}$ and $g \in G$.*

(c) *$\exp(G/G^{(n)}) \mid n$.*

As an application of Theorem 4.2, we analyze the problem of existence of non-trivial n-th MRF's over certain families of groups:

THEOREM 4.6. *There exist no non-trivial n-th MRF's over finite non-abelian simple groups for every integer $n \geqslant 2$.*

THEOREM 4.8. *Let p be an odd prime number and let $n \geqslant 2$ be an integer. In addition, suppose that m, k are positive integer such that $m \geqslant 2k$ and consider the following p-group*

$$C_{p^m} \rtimes C_{p^k} = \langle a, b \mid a^{p^m} = 1, b^{p^k} = 1, bab^{-1} = a^{p^{m-k}+1} \rangle.$$

Then there exists a non-trivial n-th MRF over $C_{p^m} \rtimes C_{p^k}$ if and only if $n \equiv 1 \pmod{p^k}$ and $n \not\equiv 1 \pmod{p^m}$.

In Section 5, we consider n-th MRF's over finite commutative rings (with identity). One of our main results is Theorem 5.3:

THEOREM 5.3. *Suppose that R is a finite commutative ring and $n \geqslant 2$ is an integer. Then there exists an n-th MRF over R iff $\gcd(n, \exp(R^*)) = \gcd(n^2, \exp(R^*))$ and $R^{(n)} \setminus \{0\}$ has no nilpotent elements. Furthermore, in this case, the n-th root function is given by*

$$\sqrt[n]{x} = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{|R^*|/u}$ and u is the number of n-th roots of unity in R.

As an application of Theorem 5.3, we obtained a criterion for the existence of an n-th MRF's over finite fields and over the ring $\mathbb{Z}_m$ of residues modulo m.

COROLLARY 5.4. *Suppose that $\mathbb{F}$ is a finite field and $n \geqslant 2$ is an integer. Then there exists an n-th MRF over $\mathbb{F}$ if and only if* $\gcd(n, |\mathbb{F}|-1) = \gcd(n^2, |\mathbb{F}|-1)$. *Furthermore, in this case, the n-th root function is given by*

$$\sqrt[n]{x} = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{\frac{|\mathbb{F}|-1}{u}}$ and $u =$ $\gcd(n, |\mathbb{F}|-1)$.

It should be noted that the first part of this result can be also obtained as a consequence of Corollary 2.8 in [4]. We mention the following special case of Corollary 5.4, when $\mathbb{F} = \mathbb{Z}_p$ is the field of residues modulo a prime p. In this case, it can be shown that there exists a multiplicative square-RF over $\mathbb{Z}_p$ if and only if $p \equiv 3 \pmod 4$. Furthermore, this square-RF is given by

$$\sqrt{x} = x^{\frac{p+1}{4}}.$$

See Example 5.5 for more details.

COROLLARY 5.6. *Suppose that $m > 1$ and $n \geqslant 2$ are integers and let $m = p_1^{a_1} \cdots p_s^{a_s}$ be the decomposition of m into distinct prime factors. Then there exists an n-th MRF over $\mathbb{Z}_m$ if and only if*

$$\max\{a_1, \ldots, a_s\} \leqslant n \quad \textit{and} \quad \gcd\big(n, \lambda(m)\big) = \gcd\big(n^2, \lambda(m)\big),$$

where λ is the universal exponent of m. Furthermore, in this case, the n-th root function is given by

$$\sqrt[n]{x} = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{\frac{\varphi(m)}{u_n(m)}}$ and $u_n(m)$ is the number of n-th roots of unity in $\mathbb{Z}_m$.

We recall that $\varphi(m) := |\mathbb{Z}_m^*|$ and that the universal exponent of m is defined by $\lambda(m) := \exp(\mathbb{Z}_m^*)$. As an example, let us consider the ring $\mathbb{Z}_{54}$. In this case, $m = 54 = 2^1 \cdot 3^3$ and it can be shown that $\lambda(54) = 18$. Therefore, by Corollary 5.6 there exists an n-th MRF over $\mathbb{Z}_{54}$ if and only if $\max\{1, 3\} \leqslant n$ and $\gcd(n, \lambda(54)) = \gcd(n^2, \lambda(54))$, that is, if and only if $3 \leqslant n$ and $\gcd(n, 18) = \gcd(n^2, 18)$. In particular, it follows that a multiplicative square-RF and cube-RF do not exist over $\mathbb{Z}_{54}$, while a multiplicative forth-RF does exist. In order to find an explicit formula for this forth-RF, first note that

$$\mathbb{Z}_{54}^{(4)} = \{\overline{0}, \overline{1}, \overline{4}, \overline{7}, \overline{10}, \overline{13}, \overline{16}, \overline{19}, \overline{22}, \overline{25}, \overline{27}, \overline{28}, \overline{31}, \overline{34}, \overline{37}, \overline{40}, \overline{43}, \overline{46}, \overline{49}, \overline{52}\}.$$

Now, by Corollary 5.6, we have that $\sqrt[4]{x} = x^e$, where e is the least positive integer such that $4e \equiv 1 \pmod{\varphi(54)/u_4(54)}$. In this case, $\varphi(54) = 18$ and it can be shown that $\overline{-1}, \overline{1}$ are the only forth-root of unity in $\mathbb{Z}_{54}$. Hence,

$u_4(54) = 2$, so $4e \equiv 1 \pmod 9$ and its least solution is $e = 7$. Therefore, the multiplicative forth-root function over $\mathbb{Z}_{54}$ is given by

$$\sqrt[4]{x} = x^7$$

for every $x \in \mathbb{Z}_{54}^{(4)}$. As an illustrative example, note that on the one hand we get that

$$\sqrt[4]{\overline{13} \cdot \overline{4}} = \sqrt[4]{\overline{52}} = \overline{52}^7 = \overline{34},$$

and on the other hand

$$\sqrt[4]{\overline{13}}\,\sqrt[4]{\overline{4}} = \overline{13}^7 \cdot \overline{4}^7 = \overline{31} \cdot \overline{22} = \overline{34}$$

so $\sqrt[4]{\overline{13} \cdot \overline{4}} = \sqrt[4]{\overline{13}}\,\sqrt[4]{\overline{4}}$, as expected.

2. PRELIMINARIES: MONOGENIC SEMIGROUPS

Let S be a semigroup. Given an element $a \in S$, we define $\langle a \rangle := \{a, a^2, a^3, \dots\}$. Clearly, $\langle a \rangle$ it is a subsemigroup of S and is referred to as the *monogenic subsemigroup* of S generated by a. If S is a semigroup in which there exists an element a such that $S = \langle a \rangle$, then S is said to be a *monogenic semigroup.*

If S is a finite semigroup, then there are repetitions among the powers of a, so there exist positive integers $1 \leqslant \alpha < \beta$ such that

$$a^\alpha = a^\beta.$$

If β is the least exponent satisfying such an equality, then all elements in the sequence $\{a, a^2, \dots, a^{\beta-1}\}$ are distinct, and therefore, the exponent α is uniquely determined by β. Thus

$$\langle a \rangle = \{a, a^2, a^3, \dots, a^\alpha, \dots, a^{\beta-1}\}$$

and α is the least exponent such that there exists $\gamma > \alpha$ with $a^\alpha = a^\gamma$. Under these settings, we define the *order* of a as $\operatorname{ord}(a) := \beta - 1$, the *index* of a as $\operatorname{ind}(a) := \alpha$ and the *period* of a as $\operatorname{per}(a) := \beta - \alpha$. The following scheme summarizes these definitions:

$$\overbrace{a, a^2, a^3, \dots, \overbrace{a^\alpha, a^{\alpha+1}, a^{\alpha+2}, \dots, a^{\beta-1}}^{\substack{\text{the size of that list}\\ \text{is the period of } a}}}^{\substack{\text{the size of that list}\\ \text{is the order of } a}}$$

$$\underbrace{a, a^2, a^3, \dots, a^\alpha}_{\substack{\text{the size of that list}\\ \text{is the index of } a}}$$

Note that as $a^\alpha = a^\beta$, under these definitions,

$$a^{\operatorname{ind}(a)} = a^{\operatorname{ind}(a)+\operatorname{per}(a)} = a^{\operatorname{ord}(a)+1}$$

and $a^x = a^y$ if and only if either $x = y$ or

$$x \equiv y \pmod{\operatorname{per}(a)} \quad \text{and} \quad \operatorname{ind}(a) \leqslant \min\{x, y\}.$$

As an illustrative example, let us consider the monogenic subsemigroup $\langle \overline{10} \rangle$ of $S = \mathbb{Z}_{112}$ with respect to modular multiplication. In this case, we get that

$$\begin{aligned}\langle \overline{10} \rangle &= \{\overline{10}, \overline{10}^2, \overline{10}^3, \overline{10}^4, \ldots\} \\ &= \{\overline{10}, \overline{100}, \overline{104}, \overline{\mathbf{32}}, \overline{96}, \overline{64}, \overline{80}, \overline{16}, \overline{48}, \overline{\mathbf{32}}, \overline{96}, \overline{64}, \ldots\}.\end{aligned}$$

Thus, $\operatorname{ind}(\overline{10}) = 4$, $\operatorname{per}(\overline{10}) = 6$ and $\operatorname{ord}(\overline{10}) = 9$. As another example, consider the monogenic subsemigroup $\langle \overline{3} \rangle$ of $S = \mathbb{Z}_6$ with respect to modular multiplication. In this case, we get that $\langle \overline{3} \rangle = \{\overline{3}, \overline{3}^2, \overline{3}^3, \ldots\} = \{\overline{3}, \overline{3}, \overline{3}, \ldots\}$, so in this case, $\operatorname{ind}(\overline{3}) = 1$, $\operatorname{per}(\overline{3}) = 1$ and $\operatorname{ord}(\overline{3}) = 1$.

Given an element a of a finite semigroup S, the monogenic subsemigroup $\langle a \rangle$ is determined, up to isomorphism, by the index and the period of a. In other words, for every $a, b \in S$, $\langle a \rangle \cong \langle b \rangle$ if and only if a and b have the same index and period (see [7, p. 12]). Furthermore, it can be shown that the generator a of the finite monogenic subsemigroup $\langle a \rangle$ is uniquely determined by $\langle a \rangle$, unless $\langle a \rangle$ is a group (see [7, p. 40]).

An important subset of $\langle a \rangle$ is the *kernel* of $\langle a \rangle$, which is defined by

$$K_a \coloneqq \{a^\alpha, a^{\alpha+1}, \ldots, a^{\beta-1}\}.$$

By [7, pp. 11–12] the subset K_a forms a cyclic group of order $\operatorname{per}(a)$. For example, the kernel of the monogenic subsemigroup $\langle \overline{10} \rangle$ of $S = \mathbb{Z}_{112}$ is

$$K_{\overline{10}} = \{\overline{10}^4, \overline{10}^5, \ldots, \overline{10}^9\} = \{\overline{32}, \overline{96}, \overline{64}, \overline{80}, \overline{16}, \overline{48}\}.$$

This set forms a cyclic group of order 6 generated by $\overline{10}^7 = \overline{80}$ with $\overline{10}^6 = \overline{64}$ as an identity element. Note that by the definition of the kernel, it follows that $\langle a \rangle$ is a group if and only if $\operatorname{ind}(a) = 1$. In addition, it is worth noting that if e is the identity element of K_a, then $K_a = \{e, ea, ea^2, \ldots, ea^{\rho-1}\}$, where $\rho = \operatorname{per}(a)$. Since e is an idempotent, it follows that $(ea)^k = ea^k$ for every $k \geqslant 1$. Thus $K_a = \langle ea \rangle$. Furthermore, if $o(x)$ denotes the order of x as an element of the group K_a, then $o((ea)^n) = o(ea)/\gcd(n, o(ea))$ for every positive integer n. But $o(x) = \operatorname{per}(x)$ for every $x \in K_a$ and since $\operatorname{per}(ea^n) = \operatorname{per}(a^n)$, it follows that

$$\operatorname{per}(a^n) = \frac{\operatorname{per}(a)}{\gcd(n, \operatorname{per}(a))}$$

for every positive integer n.

Given a finite subset $A = \{a_1, \ldots, a_n\}$ of a finite semigroup S, we further define

$$\begin{aligned}\operatorname{per}(A) &\coloneqq \operatorname{lcm}(\operatorname{per}(a_1), \ldots, \operatorname{per}(a_n)) \\ \operatorname{ind}(A) &\coloneqq \max\{\operatorname{ind}(a_1), \ldots, \operatorname{ind}(a_n)\}.\end{aligned}$$

Note that, in particular, for $A = S$ we get that $a^{\mathrm{ind}(S)} = a^{\mathrm{ind}(S)+\mathrm{per}(S)}$ for all $a \in S$.

Another important concept is the *exponent* of S, denoted by $\exp(S)$, which is defined to be the smallest positive integer ω such that all the elements of $S^{(\omega)}$ are idempotents. Recall that an element e of a semigroup S is *idempotent* if $e^2 = e$. We remark that $\exp(S)$ is well defined since by [7, p. 12], for every $a \in S$, there exists a positive integer k such that a^k is idempotent. Note that by the definition of the exponent $a^{\exp(S)} = a^{2\exp(S)}$ for every $a \in S$, so $\mathrm{ind}(a) \leqslant \exp(S)$ and $\mathrm{per}(a) \mid \exp(S)$ for every $a \in S$. Therefore, $\mathrm{ind}(S) \leqslant \exp(S)$ and $\mathrm{per}(S) \mid \exp(S)$. In general, it may happen that $\mathrm{per}(S) \neq \exp(S)$. For example, let

$$S = \Bigg\{ \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{a}, \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{b}, \underbrace{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}}_{c}, \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{d}, \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}}_{e} \Bigg\}.$$

Under usual multiplication of matrices, we get the following multiplication table

	a	b	c	d	e
a	a	b	e	e	e
b	e	e	a	b	e
c	c	d	e	e	e
d	e	e	c	d	e
e	e	e	e	e	e

As one can see, S is a non-commutative finite semigroup. Note that $a = a^2$, $b^2 = b^3$, $c^2 = c^3$, $d = d^2$ and $e = e^2$, so every element has period 1. Thus, $\mathrm{per}(S) = 1$ and $\mathrm{ind}(S) = 2$. Furthermore, $\exp(S) = 2$ since a, d, e are the idempotent elements of S and $S^{(2)} = \{a, d, e\}$.

It is worth mentioning that if $\mathrm{ind}(a) \leqslant \mathrm{per}(a)$ for all $a \in$ S, then $\mathrm{per}(S) = \exp(S)$. Indeed, in this case, $a^{\mathrm{per}(a)}$ is the identity element of K_a, so $a^{\mathrm{per}(S)}$ is idempotent for all $a \in$ S. Hence, $\exp(S) \leqslant \mathrm{per}(S)$ and since $\mathrm{per}(S) \mid \exp(S)$, we deduce that $\mathrm{per}(S) = \exp(S)$, as claimed.

In the case $S = G$ is a finite group, we get that $\mathrm{ind}(a) = 1$ and $\mathrm{per}(a) = \mathrm{ord}(a)$ for every $a \in G$, so $\mathrm{ind}(G) = 1$ and $\mathrm{per}(G) = \exp(G)$. Here, $\exp(G)$ denotes, as usual, the least positive integer k such that $a^k = 1_G$ for all $a \in G$.

3. THE n-TH MRF'S OVER FINITE SEMIGROUPS

In this section, we establish the main properties of the n-th MRF's over finite semigroups. We begin with the following two important theorems, which plays a key role in our analysis.

THEOREM 3.1. *Suppose that S is a finite semigroup, $n \geqslant 2$ is an integer and $a \in S^{(n)}$. If r is an n-th MRF over S, then*

(a) $\langle a\rangle = \langle r(a)\rangle$ *and consequently* $r(a) \in S^{(n)}$.

(b) $\langle a\rangle$ *forms a group and its order satisfies* $\gcd(n, \operatorname{ord}(a)) = 1$.

(c) r *is an automorphism of* $S^{(n)}$.

(d) $r(a)$ *is the unique n-th root of a in* $S^{(n)}$.

Proof. (a) Suppose that $a \in S^{(n)}$ and set $r(a) = b$. Then $b \in S$ and $a = b^n$. Note that since $a = b^n$, it follows that $a \in \langle b\rangle$, so $\langle a\rangle \subseteq \langle b\rangle$. Therefore, in order to prove our assertion, it suffices to prove that $\operatorname{ord}(a) = \operatorname{ord}(b)$.

Let α, β be the index and the period of a, respectively, and let γ, δ be the index and the period of b, respectively. So $a^\alpha = a^{\alpha+\beta}$ and $b^\gamma = b^{\gamma+\delta}$. First, we prove that $\alpha = \gamma$ and $\beta = \delta$. Indeed, note that

$$b^\alpha = r(a)^\alpha = r(a^\alpha) = r(a^{\alpha+\beta}) = r(a)^{\alpha+\beta} = b^{\alpha+\beta}.$$

Thus $b^\alpha = b^{\alpha+\beta}$, so $\gamma \leqslant \alpha$ and $\alpha \equiv \alpha + \beta \pmod{\delta}$, that is, $\gamma \leqslant \alpha$ and $\delta \mid \beta$. Similarly

$$a^\gamma = (b^n)^\gamma = (b^\gamma)^n = (b^{\gamma+\delta})^n = (b^n)^{\gamma+\delta} = a^{\gamma+\delta}.$$

Thus $a^\gamma = a^{\gamma+\delta}$, so $\alpha \leqslant \gamma$ and $\gamma \equiv \gamma + \delta \pmod{\beta}$, that is, $\alpha \leqslant \gamma$ and $\beta \mid \delta$. Therefore $\alpha = \gamma$ and $\beta = \delta$, as claimed. It follows that $\langle a\rangle \cong \langle b\rangle$, so $\operatorname{ord}(a) = \operatorname{ord}(b)$, as required.

(b) In order to prove that $\langle a\rangle$ is a group, it suffices to prove that the index α of a is 1. Indeed, $\langle a\rangle = \langle b\rangle$ by Part (a), so in particular $b \in \langle a\rangle$. Hence, there exists a positive integer k such that $b = a^k$. Since $a = b^n$, it follows that $a = a^{kn}$. But $1 < kn$ since $n \geqslant 2$, so we deduce that $\alpha = 1$, as claimed.

Next, we prove that $\gcd(n, \operatorname{ord}(a)) = 1$. Note that by the first part of this proof, it follows that $1 \equiv kn \pmod{\beta}$, so $\gcd(n, \beta) = 1$. Since $\langle a\rangle$ is a group, it follows that $\operatorname{ord}(a) = \beta$, so $\gcd(n, \operatorname{ord}(a)) = 1$, as claimed.

(c) By definition, r is a homomorphism from $S^{(n)}$ into S. In addition, r is injective. Indeed, if $a, b \in S^{(n)}$ and $r(a) = r(b)$, then $r(a)^n = r(b)^n$, so $a = b$, as required. Finally, we verify that $\operatorname{im}(r) = S^{(n)}$. Since r is injective, it suffices to verify that $\operatorname{im}(r) \subseteq S^{(n)}$. But this follows immediately form Part (a) since $r(a) \in S^{(n)}$ for every $a \in S^{(n)}$.

(d) Set $r(a) = b$. By definition, b is an n-th root of a and by Part (a) we know that $b \in S^{(n)}$. We prove that if $a = c^n$ for some $c \in S^{(n)}$, then $b = c$. Indeed, since r is multiplicative, it follows that $b = r(a) = r(c^n) = r(c)^n = c$, as required. $\square$

Theorem 3.2. *Suppose that S is a finite semigroup and $n \geqslant 2$ is an integer. Then $S^{(n)} = S$ if and only if* $\operatorname{ind}(S) = 1$ *and* $\gcd(n, \exp(S)) = 1$. *Consequently, if* $\operatorname{ind}(S) = 1$ *and* $\gcd(n, \exp(S)) = 1$, *then every $a \in S$ has a unique n-th root in S.*

Proof. Set $\omega = \exp(S)$ and suppose that $\operatorname{ind}(S) = 1$ and $\gcd(n, \omega) = 1$. Consider the function $f : S \to S^{(n)}$ defined by $f(x) = x^n$. Observe that f is onto. Thus, in order to prove that $S^{(n)} = S$, it suffices to prove that f is also one-to-one. So suppose that $f(a) = f(b)$ for some $a, b \in S$. Set $\alpha = \operatorname{per}(a)$ and $\beta = \operatorname{per}(b)$. Since $\operatorname{ind}(S) = 1$, it follows that $\operatorname{ind}(a) = 1$ and $\operatorname{ind}(b) = 1$. Thus $a = a^{1+\alpha}$ and $b = b^{1+\beta}$. First, note that by induction, we obtain that $a = a^{1+k\alpha}$ and $b = b^{1+k\alpha}$ for every non-negative integer k. Recall that $\operatorname{per}(S) \mid \omega$ and since $\gcd(n, \omega) = 1$, it follows that $\gcd(n, \operatorname{lcm}(\alpha, \beta)) = 1$. Therefore, there exists a positive integer t such that $nt \equiv 1 \pmod{\operatorname{lcm}(\alpha, \beta)}$. In addition, since $\alpha \mid \operatorname{lcm}(\alpha, \beta)$ and $\beta \mid \operatorname{lcm}(\alpha, \beta)$, there exist positive integers k, m such that $nt = 1 + k\alpha$ and $nt = 1 + m\beta$. Now, using our assumption that $a^n = b^n$, we get that

$$a = a^{1+k\alpha} = a^{nt} = (a^n)^t = (b^n)^t = b^{nt} = b^{1+m\beta} = b,$$

as required.

Conversely, suppose that $S^{(n)} = S$ and consider again the function $f : S \to S^{(n)}$ defined by $f(x) = x^n$. Clearly, f is onto and since $|S^{(n)}| = |S|$, we conclude that f is one-to-one. In other words, for every $x, y \in S$, the assumption $x^n = y^n$ implies that $x = y$.

First, we prove that $\operatorname{ind}(S) = 1$. Suppose by the way of contradiction that $\operatorname{ind}(S) > 1$. Therefore, there exists $a \in S$ such that $\operatorname{ind}(a) > 1$. Set $\alpha = \operatorname{ind}(a)$ and $\beta = \operatorname{per}(a)$. Note that since $\alpha > 1$ and $n \geqslant 2$, it follows that $\alpha \leqslant 2(\alpha - 1) \leqslant n(\alpha - 1)$. In addition, since $n(\alpha - 1) \equiv n(\alpha - 1 + \beta) \pmod{\beta}$, we deduce that $a^{n(\alpha-1)} = a^{n(\alpha-1+\beta)}$, that is

$$(a^{\alpha-1})^n = (a^{\alpha-1+\beta})^n.$$

But f is one-to-one, so $a^{\alpha-1} = a^{\alpha-1+\beta}$, which contradicts the minimality of α.

Next, we prove that $\gcd(n, \omega) = 1$. Suppose by the way of contradiction that $\gcd(n, \omega) \neq 1$ and let p be a prime number such that $p \mid \omega$ and $p \mid n$. We begin by proving that there exists $a \in S$ such that $a^\omega \neq a^{\omega/p}$. Suppose otherwise that $a^\omega = a^{\omega/p}$ for every $a \in S$. Since a^ω is idempotent, we deduce that $a^{\omega/p}$ is idempotent for every $a \in S$, which implies by the minimality of the exponent, that $\omega \leqslant \omega/p$, a contradiction. Thus, there exists $a \in S$ such that $a^\omega \neq a^{\omega/p}$, as claimed. Now, note that since a^ω is idempotent, it follows that $(a^\omega)^{n/p} = a^\omega$ and $(a^\omega)^n = a^\omega$. Hence

$$(a^{\omega/p})^n = (a^\omega)^{n/p} = a^\omega = (a^\omega)^n,$$

which contradicts the fact that f is one-to-one. $\square$

In order to prove our main result, we need first the following three propositions.

PROPOSITION 3.3. *Let a, b, n be positive integers. Then*

(a) $\gcd(n, a) = \gcd(n^2, a)$ *and* $\gcd(n, b) = \gcd(n^2, b)$ *if and only if we have that* $\gcd(n, \operatorname{lcm}(a, b)) = \gcd(n^2, \operatorname{lcm}(a, b))$.

(b) $\gcd(n, \operatorname{lcm}(a, b)) = 1$ *if and only if* $\gcd(n, a) = 1$ *and* $\gcd(n, b) = 1$.

Proof. (a) For convenience, we denote $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ by (a, b) and $[a, b]$, respectively. Suppose that $(n, a) = (n^2, a)$ and $(n, b) = (n^2, b)$. Using the identity $(a, [b, c]) = [(a, b), (a, c)]$ from [9, p. 23], we obtain that

$$(n, [a, b]) = [(n, a), (n, b)] = [(n^2, a), (n^2, b)] = (n^2, [a, b]),$$

as required. Conversely, suppose that $(n, [a, b]) = (n^2, [a, b])$. Clearly, $(n, a) \mid n^2$ and $(n, a) \mid a$, so $(n, a) \mid (n^2, a)$. In addition, $(n^2, a) \mid a$ and $a \mid [a, b]$, so $(n^2, a) \mid [a, b]$. Since $(n^2, a) \mid n^2$, it follows that $(n^2, a) \mid (n^2, [a, b])$. By our assumption, $(n, [a, b]) = (n^2, [a, b])$, so $(n^2, a) \mid (n, [a, b])$ and hence $(n^2, a) \mid n$. Since $(n^2, a) \mid a$, we deduce that $(n^2, a) \mid (n, a)$. Thus $(n^2, a) = (n, a)$ and similarly $(n^2, b) = (n, b)$.

(b) The assertion follows by the identity $(n, [a, b]) = [(n, a), (n, b)]$ and by noting that $[x, y] = 1$ if and only if $x = 1$ and $y = 1$ for every two positive integers x, y. $\square$

PROPOSITION 3.4. *Suppose that S is a finite semigroup and $n \geqslant 2$ is an integer. Then*

(a) *If $a \in S^{(n)}$, then $\langle a \rangle \subseteq S^{(n)}$.*

(b) *If S is n-commutative, then $S^{(n)}$ is a subsemigroup of S.*

Proof. Part (a) is trivial. For Part (b), let $a, b \in S^{(n)}$. Then there exist $x, y \in S$ such that $a = x^n$ and $b = y^n$. Since S is n-commutative, it follows that $ab = x^n y^n = (xy)^n$. But $xy \in S$ since S is a semigroup, so $ab \in S^{(n)}$, as required. $\square$

We remark that the converse of Proposition 3.4(b) does not hold. As a counterexample, take S to be the quaternion group $\mathrm{Q}_8 = \{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$. As one can verify, in this case, $\mathrm{Q}_8^{(3)} = \mathrm{Q}_8$, so $\mathrm{Q}_8^{(3)}$ is indeed a subgroup. But Q_8 is not 3-abelian since $(\mathrm{ij})^3 = \mathrm{k}^3 = -\mathrm{k}$, while $\mathrm{i}^3\mathrm{j}^3 = (-\mathrm{i})(-\mathrm{j}) = \mathrm{ij} = \mathrm{k}$.

PROPOSITION 3.5. *Suppose that S is a finite semigroup and $n \geqslant 2$ is an integer. Then*

(a) $\gcd(n, \operatorname{per}(S^{(n)})) = 1$ *if and only if* $\gcd(n, \operatorname{per}(S)) = \gcd(n^2, \operatorname{per}(S))$.

(b) $\operatorname{ind}(S^{(n)}) = 1$ *if and only if* $\operatorname{ind}(S) \leqslant n$.

Proof. (a) Suppose that $S = \{a_1, \dots, a_k\}$ and for each $1 \leqslant i \leqslant k$ set $d_i = \operatorname{per}(a_i)$. Recall that $\operatorname{per}(a_i^n) = d_i / \gcd(n, d_i)$ for each $1 \leqslant i \leqslant k$. Hence

$$\begin{aligned}\gcd(n, \operatorname{per}(S^{(n)})) &= \gcd\big(n, \operatorname{lcm}\big(\operatorname{per}(a_1^n), \dots, \operatorname{per}(a_k^n)\big)\big)\\ &= \gcd\Big(n, \operatorname{lcm}\Big(\frac{d_1}{\gcd(n, d_1)}, \dots, \frac{d_k}{\gcd(n, d_k)}\Big)\Big).\end{aligned}$$

Using Proposition 3.3(b), we deduce that $\gcd(n, \operatorname{per}(S^{(n)})) = 1$ if and only if

$$\gcd\Big(n, \frac{d_i}{\gcd(n, d_i)}\Big) = 1$$

for each $1 \leqslant i \leqslant k$. Since

$$\gcd\Big(n, \frac{d_i}{\gcd(n, d_i)}\Big) = \frac{\gcd(n \gcd(n, d_i), d_i)}{\gcd(n, d_i)} = \frac{\gcd(n^2, nd_i, d_i)}{\gcd(n, d_i)} = \frac{\gcd(n^2, d_i)}{\gcd(n, d_i)},$$

it follows that $\gcd\big(n, \frac{d_i}{\gcd(n,d_i)}\big) = 1$ if and only if $\gcd(n^2, d_i) = \gcd(n, d_i)$. By Proposition 3.3(a), we deduce that $\gcd(n^2, d_i) = \gcd(n, d_i)$ for every $1 \leqslant i \leqslant k$ if and only if

$$\gcd\big(n, \operatorname{lcm}(d_1, \dots, d_k)\big) = \gcd\big(n^2, \operatorname{lcm}(d_1, \dots, d_k)\big),$$

that is, if and only if $\gcd(n, \operatorname{per}(S)) = \gcd(n^2, \operatorname{per}(S))$, as required.

(b) Note that it suffices to prove that $\operatorname{ind}(a^n) = 1$ if and only if $\operatorname{ind}(a) \leqslant n$ for every $a \in S$. Set $\beta = \operatorname{per}(a)$ and $\delta = \operatorname{per}(a^n)$. Now

$$\begin{aligned}\operatorname{ind}(a^n) = 1 &\Leftrightarrow a^n = (a^n)^{1+\delta}\\ &\Leftrightarrow a^n = a^{n+n\delta}\\ &\Leftrightarrow \operatorname{ind}(a) \leqslant n \text{ and } n \equiv n + n\delta \pmod{\beta}\\ &\Leftrightarrow \operatorname{ind}(a) \leqslant n \text{ and } \beta \mid n\delta.\end{aligned}$$

But $\delta = \beta / \gcd(n, \beta)$ and $\gcd(n, \beta) \mid n$, so $\beta \mid n\delta$. Therefore, $\operatorname{ind}(a^n) = 1$ if and only if $\operatorname{ind}(a) \leqslant n$, as claimed. □

We are ready now to prove our main theorem.

THEOREM 3.6. *Suppose that S is a finite semigroup and $n \geqslant 2$ is an integer. Then there exists an n-th MRF r over S iff $S^{(n)}$ is n-commutative subsemigroup of S,* $\operatorname{ind}(S) \leqslant n$ *and* $\gcd(n, \operatorname{per}(S)) = \gcd(n^2, \operatorname{per}(S))$. *Furthermore, if such a function exists, then it is unique and it is given by*

$$r(x) = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{\operatorname{per}(S^{(n)})}$.

Proof. Suppose that there exists an n-th MRF r over S. We begin by proving that $(S^{(n)})^{(n)} = S^{(n)}$. First of all, since $S^{(n)} \subseteq S$, it follows that $(S^{(n)})^{(n)} \subseteq S^{(n)}$. Additionally, if $x \in S^{(n)}$, then $r(x) \in S^{(n)}$ by Theorem 3.1(a), so $x = r(x)^n \in (S^{(n)})^{(n)}$. Hence, $(S^{(n)})^{(n)} \supseteq S^{(n)}$ and therefore $(S^{(n)})^{(n)} = S^{(n)}$, as claimed. Since $S^{(n)}$ is a semigroup, it follows by Theorem 3.2 that $\mathrm{ind}(S^{(n)}) = 1$ and $\gcd(n, \exp(S^{(n)})) = 1$. Recall that since $\mathrm{ind}(S^{(n)}) = 1$, we deduce that $\exp(S^{(n)}) = \mathrm{per}(S^{(n)})$. Hence, $\mathrm{ind}(S^{(n)}) = 1$ and $\gcd(n, \mathrm{per}(S^{(n)})) = 1$, and by Proposition 3.5, it follows that $\mathrm{ind}(S) \leqslant n$ and $\gcd(n, \mathrm{per}(S)) = \gcd(n^2, \mathrm{per}(S))$, as required. We are left to prove that $S^{(n)}$ is n-commutative. So, suppose that $x, y \in S^{(n)}$. By Theorem 3.1(c), r is an automorphism of $S^{(n)}$, so there exist $a, b \in S^{(n)}$ such that $r(a) = x$ and $r(b) = y$. Since r is multiplicative, it follows that $xy = r(a)r(b) = r(ab)$. Hence $(xy)^n = ab = x^n y^n$, as required.

Conversely, suppose that $\mathrm{ind}(S) \leqslant n$ and $\gcd(n, \mathrm{per}(S)) = \gcd(n^2, \mathrm{per}(S))$ and that $S^{(n)}$ is n-commutative subsemigroup of S. First, by Proposition 3.5, we deduce that $\gcd(n, \mathrm{per}(S^{(n)})) = 1$ and $\mathrm{ind}(S^{(n)}) = 1$. Hence, by Theorem 3.2, every $a \in S^{(n)}$ has a unique n-th root $\widehat{a}$ in $S^{(n)}$. Now, consider the function $r : S^{(n)} \to S^{(n)}$ defined by $r(x) = \widehat{x}$. Note that r is an n-th RF over S, so it suffices to prove that r is multiplicative. Let $x, y \in S^{(n)}$. On the one hand, since $S^{(n)}$ is a semigroup, it follows that $xy \in S^{(n)}$. Thus, $\widehat{xy}$ is the unique n-th root of xy in $S^{(n)}$. On the other hand, $\widehat{x}, \widehat{y} \in S^{(n)}$ and since $S^{(n)}$ is n-commutative semigroup, it follows that $\widehat{x}\widehat{y} \in S^{(n)}$ and $(\widehat{x}\widehat{y})^n = (\widehat{x})^n (\widehat{y})^n = xy$. Thus, $\widehat{x}\widehat{y}$ is an n-th root of xy in $S^{(n)}$ and by uniqueness $\widehat{xy} = \widehat{x}\widehat{y}$, that is, $r(xy) = r(x)r(y)$, as required.

Next, we turn to prove that there exists at most one n-th MRF over S. Suppose that r and $\widetilde{r}$ are two n-th MRF's over S. By Theorem 3.1(d), any $x \in S^{(n)}$ has a unique n-th root in $S^{(n)}$. In addition, since by Theorem 3.1(a) both $r(x)$ and $\widetilde{r}(x)$ are n-th roots in $S^{(n)}$, we deduce that $r(x) = \widetilde{r}(x)$, as required.

Finally, we prove that in case of existence, any n-th MRF r is of the form $r(x) = x^e$, where e is a positive integer such that $ne \equiv 1 \pmod{\mathrm{per}(S^{(n)})}$. Before we begin, note that since $\gcd(n, \mathrm{per}(S)) = \gcd(n^2, \mathrm{per}(S))$, it follows by Proposition 3.5(a) that $\gcd(n, \mathrm{per}(S^{(n)})) = 1$, so a positive number e such that $ne \equiv 1 \pmod{\mathrm{per}(S^{(n)})}$ indeed exists. Now, given $x \in S^{(n)}$, note that $x^e \in S^{(n)}$ by Proposition 3.4(a). Furthermore, since $\mathrm{ind}(S) \leqslant n$, it follows by Proposition 3.5(b) that $\mathrm{ind}(S^{(n)}) = 1$, so $\mathrm{ind}(x) = 1$. In addition, since $\mathrm{per}(x) \mid \mathrm{per}(S^{(n)})$ and since $ne \equiv 1 \pmod{\mathrm{per}(S^{(n)})}$, it follows that $ne \equiv 1 \pmod{\mathrm{per}(x)}$. By noting that $1 = \mathrm{ind}(x) < ne$, we deduce that $(x^e)^n = x^{ne} = x$, so x^e is an n-th root of x in $S^{(n)}$. Since by Theorem 3.1(d) every element of $S^{(n)}$ has a unique n-th root in $S^{(n)}$, it follows that $r(x) = x^e$, as required. $\square$

Remark 1. The necessary and sufficient conditions for existence of n-th MRF's, given in Theorem 3.6, can be replaced with the aid of Proposition 3.5 as follows: there exists an n-th MRF over S if and only if $S^{(n)}$ is n-commutative, $\operatorname{ind}(S^{(n)}) = 1$ and $\gcd(n, \operatorname{per}(S^{(n)})) = 1$. These equivalent conditions are sometimes more usable then those stated in Theorem 3.6.

Remark 2. The least positive integer e in Theorem 3.6, for which the set $r(x) = x^e$ can be replaced by another least positive integer e' satisfying $ne' \equiv 1 \pmod{m}$, where m is any positive integer such that $\gcd(n, m) = 1$ and $\operatorname{per}(S^{(n)}) \mid m$. In order to establish that claim, it suffices to prove that $e \equiv e'$ $(\operatorname{mod} \operatorname{per}(S^{(n)}))$. First, note that since $\gcd(n, m) = 1$, the congruence $ne' \equiv 1$ $\pmod{m}$ is indeed solvable. Now, since $\operatorname{per}(S^{(n)}) \mid m$, it follows that $ne' \equiv 1$ $(\operatorname{mod} \operatorname{per}(S^{(n)}))$. Hence $ne \equiv ne'$ $(\operatorname{mod} \operatorname{per}(S^{(n)}))$, so $e \equiv e'$ $(\operatorname{mod} \operatorname{per}(S^{(n)}))$ since $\gcd(n, m) = 1$, as required. As we see, expressing r in term of e' rather than e, can be more convenient in some cases.

By Theorem 3.6, if an n-th MRF over S exists, it is unique. This unique function is denoted by the familiar surd notation $\sqrt[n]{\ }$. Thus, by definition, the function $x \mapsto \sqrt[n]{x}$ (in case it exists) satisfies $\sqrt[n]{x}^{\,n} = x$ and $\sqrt[n]{xy} = \sqrt[n]{x}\sqrt[n]{y}$ for every $x, y \in S^{(n)}$. As we have shown, likewise the familiar real n-th roots functions, this function can be written also in exponential notation.

Example 3.7. Consider the set of residues $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{7}\}$ with respect to modular multiplication. Note that, in this case

$$\langle \overline{2} \rangle = \{\overline{2}, \overline{4}, \overline{0}, \overline{0}, \overline{0}, \ldots\}.$$

Thus, $\operatorname{ind}(\overline{2}) = 3$, so $\operatorname{ind}(\mathbb{Z}_8) \geqslant 3$. It follows by Theorem 3.6 that a multiplicative square-RF does not exist over $\mathbb{Z}_8$.

Example 3.8. Consider the semigroup S consisting of the $m \times m$ zero matrix O and all the $m \times m$ matrices E_{ij} with 1 on the ij entry and 0 elsewhere. As one can verify, S forms a finite semigroup of order $m^2 + 1$ under matrix multiplication. Note that for every $i, j \in \{1, 2, \ldots, m\}$

$$E_{ij}^2 = \begin{cases} O & \text{if } i \neq j \\ E_{ii} & \text{if } i = j. \end{cases}$$

Hence, $\operatorname{ind}(S) = 2$ and $\operatorname{per}(S) = 1$. Therefore, $S^{(n)} = S^{(2)} = \{O, E_{11}, \ldots, E_{mm}\}$ for every integer $n \geqslant 2$. In addition, note that $S^{(n)}$ is commutative, which implies that $S^{(n)}$ is n-commutative. Therefore, by Theorem 3.6, we deduce that there exists an n-th MRF $x \mapsto \sqrt[n]{x}$ over S. Furthermore, since $e = 1$ trivially satisfies the congruence $ne \equiv 1$ $(\operatorname{mod} \operatorname{per}(S^{(n)}))$, it follows that $\sqrt[n]{x} = x$ for every $x \in S^{(n)}$, so there is no non-trivial n-th MRF over S.

Example 3.9. Consider the set of residues $\mathbb{Z}_{26} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{25}\}$ with respect to modular multiplication. In this case

$$\mathbb{Z}_{26}^{(3)} = \{\overline{0}, \overline{1}, \overline{5}, \overline{8}, \overline{12}, \overline{13}, \overline{14}, \overline{18}, \overline{21}, \overline{25}\}$$

and

$$\begin{aligned}
\langle\overline{0}\rangle &= \{\overline{0}, \overline{0}, \overline{0}, \ldots\} & \langle\overline{13}\rangle &= \{\overline{13}, \overline{13}, \overline{13}, \ldots\}\\
\langle\overline{1}\rangle &= \{\overline{1}, \overline{1}, \overline{1}, \ldots\} & \langle\overline{14}\rangle &= \{\overline{14}, \overline{14}, \overline{14}, \ldots\}\\
\langle\overline{5}\rangle &= \{\overline{5}, \overline{25}, \overline{21}, \overline{1}, \overline{5}, \overline{25}, \ldots\} & \langle\overline{18}\rangle &= \{\overline{18}, \overline{12}, \overline{8}, \overline{14}, \overline{18}, \overline{12}, \ldots\}\\
\langle\overline{8}\rangle &= \{\overline{8}, \overline{12}, \overline{18}, \overline{14}, \overline{8}, \overline{12}, \ldots\} & \langle\overline{21}\rangle &= \{\overline{21}, \overline{25}, \overline{5}, \overline{1}, \overline{21}, \overline{25}, \ldots\}\\
\langle\overline{12}\rangle &= \{\overline{12}, \overline{14}, \overline{12}, \overline{14}, \ldots\} & \langle\overline{25}\rangle &= \{\overline{25}, \overline{1}, \overline{25}, \overline{1}, \ldots\}.
\end{aligned}$$

Observe that $\operatorname{ind}(x) = 1$ and $\operatorname{per}(x) \in \{1, 2, 4\}$ for every $x \in \mathbb{Z}_{26}^{(3)}$. Thus $\operatorname{ind}(\mathbb{Z}_{26}^{(3)}) = 1$ and $\operatorname{per}(\mathbb{Z}_{26}^{(3)}) = 4$. Additionally, since $\mathbb{Z}_{26}$ is commutative, it follows by Theorem 3.6 that there exists a (unique) multiplicative cube-RF over $\mathbb{Z}_{26}$. By noticing that $e = 3$ satisfies the congruence $3e \equiv 1 \pmod 4$, we obtain that this cube-RF is

$$\sqrt[3]{x} = x^3,$$

where $x \in \mathbb{Z}_{26}^{(3)}$. Hence,

$$\sqrt[3]{\overline{0}} = \overline{0} \qquad \sqrt[3]{\overline{1}} = \overline{1} \qquad \sqrt[3]{\overline{5}} = \overline{21} \qquad \sqrt[3]{\overline{8}} = \overline{18} \qquad \sqrt[3]{\overline{12}} = \overline{12}$$

$$\sqrt[3]{\overline{13}} = \overline{13} \qquad \sqrt[3]{\overline{14}} = \overline{14} \qquad \sqrt[3]{\overline{18}} = \overline{8} \qquad \sqrt[3]{\overline{21}} = \overline{5} \qquad \sqrt[3]{\overline{25}} = \overline{25}.$$

COROLLARY 3.10. *Suppose that S is a finite commutative semigroup and $m, n \geqslant 2$ are integers. In addition, suppose that there exists an n-th MRF over S. If $n \mid m$ and if m has exactly the same prime divisors as n, then there exists an m-th MRF over S. In particular, there exists an n^k-th MRF over S for every positive integer k.*

Proof. By Theorem 3.6, the existence of an n-th MRF over S implies that $\operatorname{ind}(S) \leqslant n$ and $\gcd(n, \operatorname{per}(S)) = \gcd(n^2, \operatorname{per}(S))$. Note that since S is commutative, it suffices to prove that

$$\operatorname{ind}(S) \leqslant m \quad \text{and} \quad \gcd(m, \operatorname{per}(S)) = \gcd(m^2, \operatorname{per}(S)).$$

First, since $\operatorname{ind}(S) \leqslant n$ and $n \mid m$, it follows that $\operatorname{ind}(S) \leqslant m$. Next, suppose that $p^a \| n$, where p is a prime and $a \geqslant 1$, and let $b \geqslant 0$ such that $p^b \| \gcd(n, \operatorname{per}(S))$. Then $b \leqslant a$. We claim that $p^b \| \operatorname{per}(S)$. Indeed, suppose otherwise that $p^{b+1} \mid \operatorname{per}(S)$. Since $p^{2a} \| n^2$ and $b + 1 \leqslant a + 1 \leqslant 2a$, it follows that $p^{b+1} \mid n^2$, so $p^{b+1} \mid \gcd(n^2, \operatorname{per}(S))$, which contradicts the fact that $\gcd(n, \operatorname{per}(S)) = \gcd(n^2, \operatorname{per}(S))$. So $p^b \| \operatorname{per}(S)$ and since $n \mid m$, we deduce that $p^b \| \gcd(m, \operatorname{per}(S))$ and $p^b \| \gcd(m^2, \operatorname{per}(S))$. Now, n and m have the same prime divisors, so $\gcd(n, \operatorname{per}(S)) = \gcd(m, \operatorname{per}(S))$ and $\gcd(n^2, \operatorname{per}(S)) = \gcd(m^2, \operatorname{per}(S))$. Therefore, $\gcd(m, \operatorname{per}(S)) = \gcd(m^2, \operatorname{per}(S))$, as required. $\square$

Recall that given two finite semigroups $(S, \cdot)$ and $(T, \bullet)$, then $S \times T$ with the binary operation $*$ defined by $(x_1, y_1) * (x_2, y_2) = (x_1 \cdot x_2, y_1 \bullet y_2)$ is a semigroup. Note also that since $\mathrm{per}((x, y)) = \mathrm{lcm}(\mathrm{per}(x), \mathrm{per}(y))$ and $\mathrm{ind}((x, y)) = \max\{\mathrm{ind}(x), \mathrm{ind}(y)\}$ for every $(x, y) \in S \times T$, it follows that $\mathrm{ind}(S \times T) = \max\{\mathrm{ind}(S), \mathrm{ind}(T)\}$ and $\mathrm{per}(S \times T) = \mathrm{lcm}(\mathrm{per}(S), \mathrm{per}(T))$.

The next result, which is useful in the sequel, follows straightforwardly from the definition of $S \times T$.

Proposition 3.11. *Suppose that S and T are finite semigroups and $n \geqslant 2$ is an integer. Then there exist n-th MRF's over S and over T if and only if there exists an n-th MRF over $S \times T$.*

4. THE n-TH MRF OVER FINITE GROUPS

In this section, we implement the previous results assuming that $S = G$ is a finite group with identity element $1 = 1_G$. Recall that in the case of a finite group G, $\mathrm{ind}(G) = 1$, so $\mathrm{per}(G) = \exp(G)$, where here $\exp(G)$ denotes, as usual, the least positive integer k such that $x^k = 1$ for all $x \in G$. As a matter of terminology, in the framework of groups, the concept of n-commutative group is referred as n-abelian group. Thus, the group G is *n-abelian* if and only if $(ab)^n = a^n b^n$ for every $a, b \in G$. Notice that 2-abelian and 3-abelian groups are abelian (see [6, pp. 35, 48]). Recall also that an n-th MRF r over G is *trivial* if and only if $r(x) = x$ for all $x \in G^{(n)}$.

In the following proposition, we summarize some basic results that is used in the rest of this section.

Proposition 4.1. *Suppose that G is a finite group and $n \geqslant 2$ is an integer. Then*

(a) $G^{(n)} = G$ *if and only if* $\gcd(n, |G|) = 1$. *Consequently, if* $\gcd(n, |G|) = 1$, *then every $a \in G$ has a unique n-th root.*

(b) *If r is an n-th MRF over G, then r is trivial if and only if* $\exp(G^{(n)}) \mid n - 1$. *Consequently, if either* $\exp(G) \mid n$ *or* $\exp(G) \mid n - 1$, *then r is trivial.*

(c) *If $G^{(n)}$ is a subgroup of G, then* $\gcd(n, \exp(G)) = \gcd(n^2, \exp(G))$ *if and only if* $\gcd(n, |G^{(n)}|) = 1$.

Proof. (a) is well known. To prove (b), note that since in the framework of groups $r(x) = x$ if and only if $x^{n-1} = 1$ for every $x \in G^{(n)}$, it follows that r is trivial if and only if $\exp(G^{(n)}) \mid n - 1$, as required. Furthermore, if $\exp(G) \mid n$, then $G^{(n)} = \{1\}$ and $\exp(G^{(n)}) \mid n-1$, so r is trivial by the first part of the proof. If $\exp(G) \mid n-1$, then $\exp(G^{(n)}) \mid n-1$ since $G^{(n)} \leqslant G$. Thus, by the first part of the proof r is trivial, as required.

Now, we turn to proving (c). Since $\gcd(n, \exp(G)) = \gcd(n^2, \exp(G))$ if and only if $\gcd(n, \exp(G^{(n)})) = 1$ by Proposition 3.5(a), it suffices to prove that $\gcd(n, |G^{(n)}|) = 1$ if and only if $\gcd(n, \exp(G^{(n)})) = 1$. Indeed, we notice that if $\gcd(n, |G^{(n)}|) = 1$, then $\gcd(n, \exp(G^{(n)})) = 1$ since $\exp(G^{(n)}) \mid |G^{(n)}|$. Conversely, suppose otherwise that $\gcd(n, |G^{(n)}|) \neq 1$ and let p be a prime number such that $p \mid n$ and $p \mid |G^{(n)}|$. Then, $G^{(n)}$ has an element of order p, so $p \mid \exp(G^{(n)})$. Hence $\gcd(n, \exp(G^{(n)})) \neq 1$, a contradiction. □

We note that over any finite group G, we can construct a trivial n-th MRF over G for *some* integer $n \geqslant 2$. For example, if $n \geqslant 2$ is an integer such that $\exp(G) \mid n$, then $G^{(n)} = \{1\}$, so the function r defined by $r(1) = 1$, is a trivial MRF over G. Naturally, we are interested in non-trivial n-th MRF's.

Proposition 4.1(a) implies that if $\gcd(n, |G|) = 1$, then there exists a unique n-th RF over G. It should be stressed that this function does not have to be multiplicative. To illustrate this, consider the symmetric group of three elements $\mathrm{S}_3 = \{(), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$. Note that in this case

$$\begin{array}{lll} ()^{\frac{1}{5}} = \{()\} & (1\,3)^{\frac{1}{5}} = \{(1\,3)\} & (1\,2\,3)^{\frac{1}{5}} = \{(1\,3\,2)\} \\ (1\,2)^{\frac{1}{5}} = \{(1\,2)\} & (2\,3)^{\frac{1}{5}} = \{(2\,3)\} & (1\,3\,2)^{\frac{1}{5}} = \{(1\,2\,3)\} \end{array}$$

so there exists a (non-trivial) unique 5-th RF over S_3 defined by

$$\begin{array}{lll} \sqrt[5]{()} = () & \sqrt[5]{(1\,3)} = (1\,3) & \sqrt[5]{(1\,2\,3)} = (1\,3\,2) \\ \sqrt[5]{(1\,2)} = (1\,2) & \sqrt[5]{(2\,3)} = (2\,3) & \sqrt[5]{(1\,3\,2)} = (1\,2\,3). \end{array}$$

However, this function is not multiplicative since $\sqrt[5]{(1\,2)}\sqrt[5]{(1\,3)} \neq \sqrt[5]{(1\,2)(1\,3)}$.

In the following theorem, we gather the main results on n-th MRF's over finite groups.

THEOREM 4.2. *Suppose that G is a finite group and $n \geqslant 2$ is an integer. Then there exists a n-th MRF r over G if and only if $G^{(n)}$ is an n-abelian subgroup of G and $\gcd(n, \exp(G)) = \gcd(n^2, \exp(G))$. Furthermore, if r exists, then the following assertions hold:*

(a) *r is the unique n-th MRF over G and it is given by $r(x) = x^e$, where e is the least positive integer such that $ne \equiv 1 \pmod{|G^{(n)}|}$. Furthermore, r is non-trivial if and only if $e > 1$.*

(b) *$G^{(n)} \trianglelefteq G$ and consequently $r(x^g) = r(x)^g$ for every $x \in G^{(n)}$ and $g \in G$.*

(c) $\exp(G/G^{(n)}) \mid n$.

Proof. The first statement of the theorem follows by applying Theorem 3.6 to finite groups.

(a) By Theorem 3.6, r is unique and is given by $r(x) = x^e$, where e is the least positive integer satisfying $ne \equiv 1 \pmod{\exp(G^{(n)})}$. Note that by Proposition 4.1(b), r is trivial if and only if $n \equiv 1 \pmod{\exp(G^{(n)})}$. Hence, r is non-trivial if and only if $e > 1$, as claimed. Furthermore, since $\gcd(n, \exp(G)) = \gcd(n^2, \exp(G))$, we deduce by Proposition 4.1(c) that $\gcd(n, |G^{(n)}|) = 1$. Now, by noticing that $\exp(G^{(n)}) \mid |G^{(n)}|$, it follows by Remark 2 that we may choose e to be the least positive integer such that $ne \equiv 1 \pmod{|G^{(n)}|}$, as required.

(b) Since there exists an n-th MRF over G, it follows that $G^{(n)}$ is a subgroup of G. If $a \in G^{(n)}$, then $a = b^n$ for some $b \in G$ and if $g \in G$, then

$$a^g = g^{-1}ag = g^{-1}b^n g = (g^{-1}bg)^n = (b^g)^n \in G^{(n)}.$$

Hence $G^{(n)} \trianglelefteq G$. In addition, if $b = r(a)$, then $b \in G^{(n)}$ by Theorem 3.1(a) and hence $b^g \in G^{(n)}$. Since b^g is an n-th root of a^g, it follows by Theorem 3.1(d) that $r(a^g) = b^g = r(a)^g$, as claimed.

(c) By Part (b) the quotient $G/G^{(n)}$ is well defined. Since $g^n \in G^{(n)}$ for every $g \in G$, it follows that the order of every element of $G/G^{(n)}$ divides n. Hence $\exp(G/G^{(n)}) \mid n$, as required. $\square$

Remark 3. The necessary and sufficient conditions for existence of n-th MRF's, given in Theorem 4.2, can be replaced with the aid of Proposition 4.1(c) as follows: There exists an n-th MRF r over G if and only if $G^{(n)}$ is an n-abelian subgroup of G and $\gcd(n, |G^{(n)}|) = 1$.

If G is a finite abelian group, then $G^{(n)}$ is n-abelian and we get the following result.

Corollary 4.3. *Suppose that G is a finite abelian group and $n \geqslant 2$ is an integer. Then there exists an n-th MRF over G if and only if* $\gcd(n, \exp(G)) = \gcd(n^2, \exp(G))$. *In particular, an n-th MRF exists if* $\gcd(n, \exp(G)) = 1$.

If G is non-abelian, then the existence of an n-th MRF over G requires $G^{(n)}$ to be n-abelian. The following result of Alperin [1] gives a criterion for a finite group to be n-abelian. Even though, it is quite difficult to pin down the structure of n-abelian groups from such a description.

Theorem (Alperin). *A finite group is n-abelian if and only if it is a homomorphic image of a subgroup of the direct product of a finite abelian group, a finite group of exponent dividing n and a finite group of exponent dividing $n - 1$.*

In the case of the multiplicative square-root and third-root functions, Theorem 4.2 and Remark 3 imply the following result.

Corollary 4.4. *Suppose that G is a finite group and let $n \in \{2,3\}$. Then there exists an n-th MRF over G if and only if $G^{(n)}$ is an abelian subgroup of G and $n \nmid |G^{(n)}|$. Consequently, either $G = G^{(n)}$ or* $\exp(G/G^{(n)}) = n$.

Proof. Let $n \in \{2,3\}$. By Theorem 4.2 and Remark 3, there exists an n-th MRF over G if and only if $G^{(n)}$ is n-abelian subgroup of G and $\gcd(n, |G^{(n)}|) = 1$. If $G^{(n)}$ is an abelian subgroup of G and $n \nmid |G^{(n)}|$, then $G^{(n)}$ is n-abelian and $\gcd(n, |G^{(n)}|) = 1$ since n is a prime, so an n-th MRF over G exists. Conversely, suppose that $G^{(n)}$ is n-abelian subgroup of G and $\gcd(n, |G^{(n)}|) = 1$. Then $n \nmid |G^{(n)}|$ and $(ab)^n = a^n b^n$ for every $a, b \in G^{(n)}$. Since $n \in \{2,3\}$, $G^{(n)}$ is an abelian subgroup of G. Therefore, there exists an n-th MRF over G if and only if $G^{(n)}$ is an abelian subgroup of G and $n \nmid |G^{(n)}|$, as required.

For the second part of the corollary, since $\exp(G/G^{(n)}) \mid n$ by Theorem 4.2(c), it follows that either $G = G^{(n)}$ or $\exp(G/G^{(n)}) = n$, as required. □

Example 4.5. For an integer $m \geqslant 2$, let us consider the Dihedral group

$$D_{2m} = \langle a, b \mid a^m = b^2 = 1, bab^{-1} = a^{-1} \rangle.$$

Since $(a^\alpha b)^2 = 1$ for every integer α, it follows that $D_{2m}^{(2)} = \langle a^2 \rangle$ which is cyclic of order $\frac{m}{\gcd(m,2)}$. Since $\frac{m}{\gcd(m,2)}$ is odd if and only if $4 \nmid m$, it follows by Corollary 4.4 that there exists a multiplicative square-root function over D_{2m} if and only if $4 \nmid m$. Notice that this function is non-trivial if and only if $m > 2$. In particular, there exists a non-trivial multiplicative square-root function over $D_6 \cong S_3$, but not over D_8.

In the following theorems, we investigate the existence of a non-trivial n-th MRF's over certain families of groups.

Theorem 4.6. *There exist no non-trivial n-th MRF's over finite non-abelian simple groups for every integer $n \geqslant 2$.*

Proof. Suppose that r is an n-th MRF over a simple group G. By Theorem 4.2(b), $G^{(n)}$ is a normal subgroup of G and since G is simple, it follows that either $G^{(n)} = \{1\}$ or $G^{(n)} = G$.

If $G^{(n)} = \{1\}$, then $\exp(G^{(n)}) \mid n-1$, so r is trivial by Proposition 4.1(b). If, on the other hand, $G^{(n)} = G$, then $\gcd(n, |G|) = 1$ by Proposition 4.1(a). Since G is a non-abelian simple group, it follows by Feit–Thompson theorem, that G is of even order and hence, n is an odd integer. Moreover, the set $H = \langle x \in G \mid x^2 = 1 \rangle$ is a non-trivial normal subgroup of G. Hence $H = G$ and if $g \in G$, then $g = a_1 a_2 \cdots a_k$, where the a_i's are involutions. Since G is n-abelian and n is an odd integer, it follows that

$$g^n = (a_1 a_2 \ldots a_k)^n = a_1^n a_2^n \ldots a_k^n = a_1 a_2 \ldots a_k = g.$$

Therefore $g^{n-1} = 1$ for each $g \in G$, which implies that $\exp(G) \mid n-1$. Thus, r is trivial by Proposition 4.1(b). $\square$

Theorem 4.7. *Let G be a p-group for some prime p and let $n \geqslant 2$ be an integer. Then there exists a non-trivial n-th MRF over G if and only if $p \nmid n$, G is n-abelian and* $\exp(G) \nmid n-1$*.*

Proof. Suppose that $p \nmid n$, G is n-abelian group and $\exp(G) \nmid n-1$. Since $p \nmid n$ and G is a p-group, it follows by Proposition 4.1(a) that $G^{(n)} = G$. Hence, $G^{(n)}$ is an n-abelian subgroup of G, $\gcd(n, |G^{(n)}|) = 1$ and $\exp(G^{(n)}) \nmid n-1$. Thus, by Theorem 4.2, Remark 3 and Proposition 4.1(b) there exists a non-trivial n-th MRF over G.

Conversely, suppose that r is a non-trivial n-th MRF over G. Then $G^{(n)}$ is a normal subgroup of G by Theorem 4.2(b). Suppose by contradiction that $G^{(n)} \neq G$. Since r is non-trivial, it follows that $G^{(n)} \neq \{1\}$, so $p \mid |G^{(n)}|$. In addition, $p \mid \exp(G/G^{(n)})$ since $G^{(n)} \neq G$. But by Theorem 4.2(c) $\exp(G/G^{(n)}) \mid n$, so $p \mid \gcd(n, |G^{(n)}|)$ in contradiction to $\gcd(n, |G^{(n)}|) = 1$, which is required by Remark 3. Therefore $G^{(n)} = G$. Since r is non-trivial, we deduce that $\exp(G) \nmid n-1$. In addition, $\gcd(n, |G|) = 1$ by Proposition 4.1(a), so $p \nmid n$, as required. $\square$

In the following theorem, we discuss the existence of an n-th MRF over certain non-abelian p-groups.

Theorem 4.8. *Let p be an odd prime number and let $n \geqslant 2$ be an integer. In addition, suppose that m, k are positive integers such that $m \geqslant 2k$ and consider the following p-group*

$$C_{p^m} \rtimes C_{p^k} = \langle a, b \mid a^{p^m} = 1, b^{p^k} = 1, bab^{-1} = a^{p^{m-k}+1} \rangle.$$

Then there exists a non-trivial n-th MRF over $C_{p^m} \rtimes C_{p^k}$ if and only if $n \equiv 1 \pmod{p^k}$ and $n \not\equiv 1 \pmod{p^m}$.

Proof. We begin by noting that by [10, pp. 414–415] the presentation above indeed defines a group. Moreover, every element in G is of the form $a^\alpha b^\beta$, where $\alpha \in \{0, 1, \ldots, p^m - 1\}$, $\beta \in \{0, 1, \ldots, p^k - 1\}$ and the product rule is

$$(a^\alpha b^\beta)(a^\gamma b^\delta) = a^{\alpha + \gamma (p^{m-k}+1)^\beta} b^{\beta + \delta}.$$

Note that since $m \geqslant 2k$, it follows that $j(m-k) \geqslant 2(m-k) \geqslant m$ for every $2 \leqslant j \leqslant \beta$. Hence

$$(1 + p^{m-k})^\beta = \sum_{j=0}^{\beta} \binom{\beta}{j} p^{j(m-k)} \equiv 1 + \beta p^{m-k} \pmod{p^m},$$

so the product rule can be simplified as follows

$$(a^\alpha b^\beta)(a^\gamma b^\delta) = a^{\alpha+\gamma+\beta\gamma p^{m-k}} b^{\beta+\delta}.$$

Using induction, we get that

$$(a^\alpha b^\beta)^n = a^{n\alpha+\frac{n(n-1)}{2}\alpha\beta p^{m-k}} b^{n\beta}$$

for every n. Notice that $\frac{p^m-1}{2}$ is an integer, so $(a^\alpha b^\beta)^{p^m} = 1$. Hence, we have $\exp(G) = p^m$.

First, we prove that G is n-abelian if and only if $n^2 \equiv n \pmod{p^k}$. On the one hand, since $2(m-k) \geqslant m$, we obtain that $a^{p^{2(m-k)}} = 1$, so by the product rule

$$\begin{aligned}(a^\alpha b^\beta)^n (a^\gamma b^\delta)^n &= \left(a^{n\alpha+\frac{n(n-1)}{2}\alpha\beta p^{m-k}} b^{n\beta}\right)\left(a^{n\gamma+\frac{n(n-1)}{2}\gamma\delta p^{m-k}} b^{n\delta}\right)\\ &= a^{n(\alpha+\gamma)+\frac{n(n-1)}{2}p^{m-k}(\alpha\beta+\gamma\delta)+n\beta(n\gamma+\frac{n(n-1)}{2}\gamma\delta p^{m-k})p^{m-k}} b^{n(\beta+\delta)}\\ &= a^{n(\alpha+\gamma)+\frac{n(n-1)}{2}p^{m-k}(\alpha\beta+\gamma\delta)+n^2\beta\gamma p^{m-k}} b^{n(\beta+\delta)}.\end{aligned}$$

On the other hand,

$$\begin{aligned}\left((a^\alpha b^\beta)(a^\gamma b^\delta)\right)^n &= \left(a^{\alpha+\gamma+\beta\gamma p^{m-k}} b^{\beta+\delta}\right)^n\\ &= a^{n(\alpha+\gamma+\beta\gamma p^{m-k})+\frac{n(n-1)}{2}(\alpha+\gamma+\beta\gamma p^{m-k})(\beta+\delta)p^{m-k}} b^{n(\beta+\delta)}\\ &= a^{n(\alpha+\gamma+\beta\gamma p^{m-k})+\frac{n(n-1)}{2}(\alpha+\gamma)(\beta+\delta)p^{m-k}} b^{n(\beta+\delta)}.\end{aligned}$$

Therefore, G is n-abelian if and only if

$$\begin{aligned}n(\alpha+\gamma)+&\frac{n(n-1)}{2}p^{m-k}(\alpha\beta+\gamma\delta)+n^2\beta\gamma p^{m-k}\\ &\equiv n(\alpha+\gamma+\beta\gamma p^{m-k})+\frac{n(n-1)}{2}(\alpha+\gamma)(\beta+\delta)p^{m-k} \pmod{p^m},\end{aligned}$$

that is, if and only if

$$n^2\beta\gamma p^{m-k} \equiv n\beta\gamma p^{m-k} + \frac{n(n-1)}{2}(\alpha\delta+\gamma\beta)p^{m-k} \pmod{p^m}$$

for every integers $\alpha, \beta, \gamma, \delta$. Since p is odd, the above congruence is equivalent to

$$2n^2\beta\gamma \equiv 2n\beta\gamma + n(n-1)(\alpha\delta+\gamma\beta) \pmod{p^k},$$

that is, to

$$n(n-1)(\beta\gamma-\alpha\delta) \equiv 0 \pmod{p^k} \qquad (*).$$

Clearly, $(*)$ is true for every $\alpha, \beta, \gamma, \delta$ if and only if $n(n-1) \equiv 0 \pmod{p^k}$, as claimed.

Now, we turn to proving our main assertion. If $n \equiv 1 \pmod{p^k}$ and $n \not\equiv 1 \pmod{p^m}$, then $p \nmid n$ and $\exp(G) \nmid n-1$, since $\exp(G) = p^m$. In addition, $n^2 \equiv n \pmod{p^k}$, so by the first part of the proof G is n-abelian. Therefore, by Theorem 4.7, there exists a non-trivial n-th MRF over G.

Conversely, suppose that there exists a non-trivial n-th MRF over G. Then $p \nmid n$, G is an n-abelian and $\exp(G) \nmid n-1$ by Theorem 4.7. Hence $n \not\equiv 1 \pmod{p^m}$ and $n^2 \equiv n \pmod{p^k}$ by the first part of the proof. But $p \nmid n$, so $n \equiv 1 \pmod{p^k}$, as required. □

Example 4.9. Given an odd prime p, let us consider the set

$$G = \left\{ \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix} : \overline{a}, \overline{b} \in \mathbb{Z}_{p^2} \text{ and } a \equiv 1 \pmod{p} \right\}.$$

Note that

$$\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{c} & \overline{d} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{ac} & \overline{ad+b} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

In addition, since $ac \equiv 1 \pmod{p}$ whenever $a \equiv 1 \pmod{p}$ and $c \equiv 1 \pmod{p}$, it can be easily verified that G is a non-abelian group of order p^3. By [5, p. 50] there exist, up to isomorphism, only two non-abelian group of order p^3, namely $C_{p^2} \rtimes C_p = \langle a, b \mid a^{p^2} = 1, b^p = 1, bab^{-1} = a^{p+1} \rangle$ and $(C_p \times C_p) \rtimes C_p = \langle a, b, c \mid a^p = 1, b^p = 1, c^p = 1, ab = bac, ca = ac, cb = bc \rangle$. Now, if m is any positive integer, then it can be shown using induction that

$$(*) \qquad \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix}^m = \begin{pmatrix} \overline{a}^m & \overline{b}(\overline{1} + \overline{a} + \overline{a}^2 + \cdots + \overline{a}^{m-1}) \\ \overline{0} & \overline{1} \end{pmatrix},$$

so, in particular

$$\begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}^p = \begin{pmatrix} \overline{1} & \overline{p} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

Therefore $\exp(G) \neq p$, so $G \cong C_{p^2} \rtimes C_p$.

By Theorem 4.8, there exists a non-trivial n-th MRF over G if and only if $n \equiv 1 \pmod{p}$ and $n \not\equiv 1 \pmod{p^2}$, that is, if and only if $p \| n-1$. Let us describe the corresponding $(p+1)$-th root function. In this case, since $\gcd(p+1, |G|) = 1$, it follows that $G^{(p+1)} = G$. By Theorem 4.2, this function is of the form $r(x) = x^e$, where e is the least positive integer such that $(p+1)e \equiv 1 \pmod{p^3}$. Note that $p^3 + 1 = (p+1)(p^2 - p + 1)$, so $e = p^2 - p + 1$. Thus

$$\sqrt[p+1]{\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix}} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix}^{p^2-p+1}$$

This expression can be simplified as follows: Note that by [9, p. 42], $a^{\varphi(p^2)} \equiv 1 \pmod{p^2}$, where φ denotes the Euler totient function. Hence $a^{p^2-p+1} \equiv a$

(mod p^2). In addition, recall that $a \equiv 1 \pmod p$, so let k be the integer such that $a = 1 + pk$. Then

$$a^m = (1+pk)^m = 1 + \binom{m}{1} pk + \sum_{j=2}^{m} \binom{m}{j} p^j k^j \equiv 1 + mpk \pmod{p^2}$$

for every non-negative integer m. Hence

$$\begin{aligned} 1 + a + a^2 + \cdots + a^{p^2-p} &\equiv \sum_{m=0}^{p^2-p} (1+mpk) \\ &= (1+p^2-p)\left(1 + \frac{p-1}{2} p^2 k\right) \equiv 1 - p \pmod{p^2} \end{aligned}$$

and by $(*)$ we deduce that

$$\sqrt[p+1]{\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix}} = \begin{pmatrix} \overline{a} & (\overline{1} - \overline{p})\overline{b} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

As an illustrative example, if $p = 3$, then there exists a multiplicative forth-root function over G and this function is given by

$$\sqrt[4]{\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix}} = \begin{pmatrix} \overline{a} & \overline{7b} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

Note that on the one hand,

$$\sqrt[4]{\begin{pmatrix} \overline{2} & \overline{4} \\ \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{3} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}} = \sqrt[4]{\begin{pmatrix} \overline{6} & \overline{8} \\ \overline{0} & \overline{1} \end{pmatrix}} = \begin{pmatrix} \overline{6} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}$$

and on the other hand

$$\sqrt[4]{\begin{pmatrix} \overline{2} & \overline{4} \\ \overline{0} & \overline{1} \end{pmatrix}} \sqrt[4]{\begin{pmatrix} \overline{3} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}} = \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{3} & \overline{5} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{6} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix},$$

so

$$\sqrt[4]{\begin{pmatrix} \overline{2} & \overline{4} \\ \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{3} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}} = \sqrt[4]{\begin{pmatrix} \overline{2} & \overline{4} \\ \overline{0} & \overline{1} \end{pmatrix}} \sqrt[4]{\begin{pmatrix} \overline{3} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}},$$

as expected.

The MRF's discussed in Theorem 4.8 and in Example 4.9 were over non-abelian p-groups with exponent at least p^2. In the next theorem, we wish to discuss the existence of MRF over non-abelian finite group with exponent p. In order to do so, we need a new notation: given a finite group G and an integer n, let $f_n : G \to G$ be the function defined by $f_n(x) = x^n$. Note that G is n-abelian if and only if f_n is a homomorphism of G into G. The following result is useful.

Theorem (Trotter [11]). *Suppose that G is a finite group and $n \geqslant 2$ is an integer. If f_n is an automorphism of G, then f_{n-1} is a homomorphism of G into G.*

In addition, we say that a finite group G is *trivially n-abelian* if either $x^n = 1$ for each $x \in G$ or $x^n = x$ for each $x \in G$, that is, if either $\exp(G) \mid n$ or $\exp(G) \mid n-1$. Now, we are ready to prove.

Theorem 4.10. *Let G be a non-abelian finite group of prime exponent p and let $n \geqslant 2$ be an integer. Then G is n-abelian if and only if it is trivially n-abelian. Consequently, there exist no non-trivial n-th MRF's over G.*

Proof. Clearly, if G is trivially n-abelian, then it is n-abelian. Conversely, suppose that G is n-abelian. Note that in order to prove our assertion, it suffices to prove that either $p \mid n$ or $p \mid n-1$. Suppose by way of contradiction that $p \nmid n$ and $p \nmid n-1$. Since $\exp(G) = p$, it follows that G is a p-group. Thus $\gcd(n, |G|) = 1$, so $G^{(n)} = G$ by Proposition 4.1(a). Let $m \geqslant 0$ and $0 \leqslant d < p$ be integers such that $n = mp + d$. Since $p \nmid n$ and $p \nmid n-1$, it follows that $d \geqslant 2$. In view of the fact that $\exp(G) = p$ and $n = mp + d$, we deduce that $g^n = g^d$ for every $g \in G$, and since G is n-abelian, it follows that G is also d-abelian. Let k be the smallest integer in $\{2, 3, \ldots, d\}$ such that G is k-abelian. If $k = 2$, then G is abelian, which contradicts our assumption. If $2 < k \leqslant d$, then $p \nmid k$, since $d < p$. Hence $G^{(k)} = G$ by Proposition 4.1(a) and we deduce that $f_k(x) = x^k$ is an automorphism of G. By Trotter's result it follows that $f_{k-1}(x) = x^{k-1}$ is a homomorphism of G into G, so G is $(k-1)$-abelian, which contradicts the minimality of k.

For the second part of theorem, suppose that r is a non-trivial n-th MRF over G. On the one hand, since r is non-trivial, it follows by Proposition 4.1(b) that $\exp(G) \nmid n$ and $\exp(G) \nmid n-1$. Thus, G is not trivially n-abelian. On the other hand, by Theorem 4.2 it follows that $G^{(n)}$ is n-abelian and since $p \nmid n$, we may deduce that $G^{(n)} = G$, so G is n-abelian. But by the first part of the proof, it follows that G is trivially n-abelian, a contradiction. □

5. *n*-TH MRF OVER FINITE COMMUTATIVE RINGS

If R is a finite ring, then by viewing R as a semigroup with respect to multiplication, Theorem 3.6 provides a necessary and sufficient condition for existence of an n-th MRF over R. Our goal in this section is to provide a simplified criterion for existence of such a function in the special case of finite commutative rings. As an application, we formulate a criterion for the existence of a n-th MRF over finite fields and over the ring $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$ of residues modulo m, for integers $m > 1$.

Throughout this section, we assume that R is a *commutative* ring with an identity element $1 = 1_R$ and a zero element $0 = 0_R$. By a *unit*, k such that $x^k = 0$. The *index of nilpotency* of x is the least positive integer k such that $x^k = 0$. Note that viewing R as a semigroup with respect to multiplication, if $x \in R$ is nilpotent, then $\operatorname{per}(x) = 1$ and $\operatorname{ind}(x)$ is the index of nilpotency of x. If R is a finite commutative ring, then by [2, p. 40] R can be expressed as a direct product of local rings, say

$$R \cong R_1 \times R_2 \times \cdots \times R_s.$$

Moreover, this decomposition is unique up to permutation of the factors. Recall that R is a *local ring* if it has a unique maximal ideal. A basic example of a local ring is the ring $\mathbb{Z}_{p^k}$, where p is a prime number. In this case, the unique maximal ideals is $(\overline{p})$. The ring $\mathbb{Z}_6$, for example, is not local since $(\overline{2})$ and $(\overline{3})$ are both different maximal ideal of $\mathbb{Z}_6$. In the case of $\mathbb{Z}_m$, if $m > 1$ and $m = p_1^{a_1} \cdots p_s^{a_s}$ is its decomposition into distinct prime factors, then the local ring decomposition of $\mathbb{Z}_m$ is

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_s^{a_s}}$$

(see [8, p. 95]).

Proposition 5.1. *Let R be a finite commutative local ring. Then every non-unit element $x \in R$ is nilpotent.*

Proof. Let M be the unique maximal ideal of R. Since R is local, it follows by [8, p. 110] that every element of M is a non-unit, while every element of $R \setminus M$ is a unit. Now, let x be a non-unit element of R and let $\alpha = \operatorname{ind}(x)$, $\beta = \operatorname{ord}(x) + 1$. Then $x^\alpha = x^\beta$ and $\alpha < \beta$, so $x^\alpha(1 - x^{\beta-\alpha}) = 0$. Since x is a non-unit, it follows that $x^{\beta-\alpha} \in M$. If $1 - x^{\beta-\alpha} \in M$, then $1 = x^{\beta-\alpha} + (1 - x^{\beta-\alpha}) \in M$, which is false. Hence $1 - x^{\beta-\alpha}$ is a unit, so $x^\alpha = 0$, as required. □

Proposition 5.2. *Suppose that R is a finite commutative local ring and assume that $n \geqslant 2$ is an integer. Then there exists an n-th MRF over R if and only if* $\gcd(n, \exp(R^*)) = \gcd(n^2, \exp(R^*))$ *and $R^{(n)} \setminus \{0\} \subseteq R^*$.*

Proof. By Theorem 3.6, there exists an n-th MRF over R if and only if $\gcd(n, \operatorname{per}(R)) = \gcd(n^2, \operatorname{per}(R))$ and $\operatorname{ind}(R) \leqslant n$. Hence, it suffices to show that $\operatorname{per}(R) = \exp(R^*)$, and that $\operatorname{ind}(R) \leqslant n$ if and only if $R^{(n)} \setminus \{0\} \subseteq R^*$.

Let $R^* = \{x_1, \ldots, x_k\}$ and $R \setminus R^* = \{x_{k+1}, \ldots, x_n\}$ be the sets of units and non-units in R, respectively. If $x \in R$ is non-unit, then x is nilpotent by Proposition 5.1, so $\operatorname{per}(x) = 1$. Hence

$$\operatorname{per}(R) = \operatorname{lcm}(\operatorname{per}(x_1), \ldots, \operatorname{per}(x_n)) = \operatorname{lcm}(\operatorname{per}(x_1), \ldots, \operatorname{per}(x_k)) = \operatorname{per}(R^*)$$

and since R^* is a finite group, it follows that $\mathrm{per}(R) = \exp(R^*)$, as claimed.

Next, suppose that $\mathrm{ind}(R) \leqslant n$ and let $x \in R^{(n)}$. It suffices to prove that if x is a non-unit, then $x = 0$. Indeed, since x is nilpotent by Proposition 5.1, it follows that $x^k = 0$, where $k = \mathrm{ind}(x)$. By Proposition 3.5(b) $\mathrm{ind}(R^{(n)}) = 1$, so $\mathrm{ind}(x) = 1$ and therefore $x = 0$, as required. Conversely, suppose that $R^{(n)} \setminus \{0\} \subseteq R^*$. It suffices to prove that $\mathrm{ind}(R^{(n)}) = 1$. Indeed, if $x = 0$, then clearly $\mathrm{ind}(x) = 1$. If $x \neq 0$, then by our assumption x is a unit which implies that $\mathrm{ind}(x) = 1$, as required. □

Now, we are ready to prove our main result in this section.

THEOREM 5.3. *Suppose that R is a finite commutative ring and $n \geqslant 2$ is an integer. Then there exists an n-th MRF over R iff* $\gcd(n, \exp(R^*)) = \gcd(n^2, \exp(R^*))$ *and $R^{(n)} \setminus \{0\}$ has no nilpotent elements. Furthermore, in this case, the n-th root function is given by*

$$\sqrt[n]{x} = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{|R^*|/u}$ and u is the number of n-th roots of unity in R.

Proof. Assume that r is an n-th MRF over R. First, we prove that $R^{(n)} \setminus \{0\}$ has no nilpotent elements. Suppose otherwise that $x \in R^{(n)}$ is a non-zero nilpotent element and let k be its index of nilpotency. Set $\alpha = \lceil \frac{k}{n} \rceil$ and $\beta = n\alpha - k$. Note that since $\frac{k}{n} \leqslant \lceil \frac{k}{n} \rceil$, it follows that $\beta \geqslant 0$. In addition, since $x \neq 0$, we deduce that $k \geqslant 2$, so

$$\alpha = \left\lceil \frac{k}{n} \right\rceil < \frac{k}{n} + 1 \leqslant \frac{k}{2} + 1 \leqslant k.$$

Therefore $x^\alpha \neq 0$. Now, $x \in R^{(n)}$, so $x^\alpha \in R^{(n)}$ and since

$$(x^\alpha)^n = x^{k+\beta} = x^k x^\beta = 0$$

we deduce that x^α is an n-th root of 0 in $R^{(n)}$. But clearly $r(0) = 0$, which contradicts the fact that r is injective.

Next, we prove that $\gcd(n, \exp(R^*)) = \gcd(n^2, \exp(R^*))$. Indeed, since R^* is a subsemigroup of R with respect to multiplication and since $r(x) \in \langle x \rangle$ for every $x \in R^*$, it follows that $r(R^*) \subseteq R^*$, which implies that r, restricted to R^*, is an n-th MRF over R^*. In addition, R^* is an abelian group, so by Corollary 4.3, we deduce that $\gcd(n, \exp(R^*)) = \gcd(n^2, \exp(R^*))$, as required.

Conversely, assume that $R^{(n)} \setminus \{0\}$ has no nilpotent elements and that $\gcd(n, \exp(R^*)) = \gcd(n^2, \exp(R^*))$. Let $R_1 \times \cdots \times R_s$ be the local ring decomposition of R. By Proposition 3.11, it suffices to prove that there exist n-th MRF's over R_i for every $1 \leqslant i \leqslant s$. In order to do so, we use Proposition 5.2

and prove that $R_i^{(n)} \setminus \{0\} \subseteq R_i^*$ and that $\gcd(n, \exp(R_i^*)) = \gcd(n^2, \exp(R_i^*))$ for every $1 \leqslant i \leqslant s$. Indeed, note that $R^* \cong R_1^* \times \cdots \times R_s^*$, so $\exp(R^*) = \operatorname{lcm}(\exp(R_1^*), \ldots, \exp(R_s^*))$. Now, since $\gcd(n, \exp(R^*)) = \gcd(n^2, \exp(R^*))$ by our assumption, we deduce that

$$\gcd(n, \operatorname{lcm}(\exp(R_1^*), \ldots, \exp(R_s^*))) = \gcd(n^2, \operatorname{lcm}(\exp(R_1^*), \ldots, \exp(R_s^*))).$$

Hence, by Proposition 3.3(a) it follows that $\gcd(n, \exp(R_i^*)) = \gcd(n^2, \exp(R_i^*))$ for every $1 \leqslant i \leqslant s$, as required.

Next, let $x \in R_i^{(n)} \setminus \{0\}$ and assume that x in a non-unit. By Proposition 5.1 it follows that x is nilpotent. Thus

$$(0, \ldots, x, \ldots, 0) \in R_1^{(n)} \times \cdots \times R_i^{(n)} \times \cdots \times R_s^{(n)}$$

is also a non-zero nilpotent element. Now, since $R \cong R_1 \times \cdots \times R_s$, it follows that $R^{(n)} \cong R_1^{(n)} \times \cdots \times R_s^{(n)}$ (as semigroups under multiplication). Hence, we may deduce that there exists a non-zero nilpotent element of $R^{(n)}$, which contradicts the assumption that $R^{(n)} \setminus \{0\}$ has no nilpotent elements.

Finally, we prove that such an n-th MRF is of the form $\sqrt[n]{x} = x^e$, where e is the least positive integer such that $ne \equiv 1 \pmod{|R^*|/u}$ and u is the number of n-th root of unity in R. By Theorem 3.6 there exists a positive integer e such that $\sqrt[n]{x} = x^e$ for every $x \in R^{(n)}$. By Remark 2, we may choose e to be the least positive integer such that $ne \equiv 1 \pmod{m}$, where m is any positive integer such that $\gcd(n, m) = 1$ and $\operatorname{per}(R^{(n)}) \mid m$. We prove that $m = |(R^*)^{(n)}|$ satisfies these two conditions. Indeed, as mentioned above, r, restricted to R^*, is an n-th MRF over the group R^*. Hence, by Remark 3, it follows that $\gcd(n, |(R^*)^{(n)}|) = 1$, as claimed. We turn to verifying that $\operatorname{per}(R^{(n)}) \mid |(R^*)^{(n)}|$. As we have proved above, there exists an n-th MRF over each ring R_i in the local ring decomposition of R. Hence, by Proposition 5.2, $R_i^{(n)} \setminus \{0\} \subseteq R_i^*$ for each $1 \leqslant i \leqslant s$. Since $(R_i^*)^{(n)} \subseteq R_i^{(n)} \setminus \{0\}$, it follows that $R_i^{(n)} \setminus \{0\} = (R_i^*)^{(n)}$, that is $R_i^{(n)} = \{0\} \cup (R_i^*)^{(n)}$. Using the fact that each R_i^* is an abelian group, we obtain that $\operatorname{per}(R_i^{(n)}) = \operatorname{per}(\{0\} \cup (R_i^*)^{(n)}) = \exp((R_i^*)^{(n)})$, so

$$\begin{aligned}
\operatorname{per}(R^{(n)}) &= \operatorname{per}(R_1^{(n)} \times \cdots \times R_s^{(n)}) = \operatorname{lcm}(\operatorname{per}(R_1^{(n)}), \ldots, \operatorname{per}(R_s^{(n)})) \\
&= \operatorname{lcm}(\exp((R_1^*)^{(n)}), \ldots, \exp((R_s^*)^{(n)})) = \exp((R_1^*)^{(n)} \times \cdots \times (R_s^*)^{(n)}) \\
&= \exp((R_1^* \times \cdots \times R_s^*)^{(n)}) = \exp((R^*)^{(n)}).
\end{aligned}$$

Now, since $\exp((R^*)^{(n)}) \mid |(R^*)^{(n)}|$, we deduce that $\operatorname{per}(R^{(n)}) \mid |(R^*)^{(n)}|$, as claimed.

Now consider the map $f : R^* \to (R^*)^{(n)}$ given by $f(x) = x^n$. Since R^* is an abelian group, it follows that f is a group homomorphism. Therefore

$$\operatorname{im}(f) \cong R^* / \ker(f).$$

But $\ker(f) = \{x \in R^* : x^n = 1\}$ and $\operatorname{im}(f) = (R^*)^{(n)}$, so $|(R^*)^{(n)}| = |R^*|/u$, as required. □

As an application, let us apply Theorem 5.3 to finite fields. Note that if $\mathbb{F}$ is a finite field, then $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, so $\exp(\mathbb{F}^*) = |\mathbb{F}| - 1$. In addition, since the number of n-th root of unity in $\mathbb{F}$ is $\gcd(n, |\mathbb{F}| - 1)$, we obtain by Theorem 5.3 the following result

Corollary 5.4. *Suppose that $\mathbb{F}$ is a finite field and $n \geqslant 2$ is an integer. Then there exists an n-th MRF over $\mathbb{F}$ if and only if* $\gcd(n, |\mathbb{F}| - 1) = \gcd(n^2, |\mathbb{F}| - 1)$. *Furthermore, in this case, the n-th root function is given by*

$$\sqrt[n]{x} = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{\frac{|\mathbb{F}|-1}{u}}$ and $u = \gcd(n, |\mathbb{F}| - 1)$.

Example 5.5. Let p be an odd prime and consider the field $\mathbb{Z}_p$. By Corollary 5.4, there exists a multiplicative square-root function over $\mathbb{Z}_p$ if and only if $\gcd(2, p-1) = \gcd(4, p-1)$, that is, if and only if $2 = \gcd(4, p-1)$. Since either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$, it follows that there exists a multiplicative square-root function over $\mathbb{Z}_p$ if and only if $p \equiv 3 \pmod 4$.

In order to find the exponential form of this square function, we need to solve the congruence $2e \equiv 1 \pmod{\frac{p-1}{2}}$. Since

$$2\Big(\frac{p+1}{4}\Big) = \frac{p+1}{2} = \frac{p-1}{2} + 1 \equiv 1 \pmod{\frac{p-1}{2}},$$

it follows that $e = \frac{p+1}{4}$, so the desired square-root function is given by

$$\sqrt{x} = x^{\frac{p+1}{4}}.$$

As an illustrative example, if $p = 11$, then there exists a square-root function over $\mathbb{Z}_{11}$ and this square-root function is given by $\sqrt{x} = x^3$.

As another application of Theorem 5.3, we determine the conditions for the existence of n-th MRF's over the ring $\mathbb{Z}_m$. As Theorem 5.3 indicates, the group of units $\mathbb{Z}_m^*$ and its exponent are essential in determining the existence of such functions. Recall that $|\mathbb{Z}_m^*| = \varphi(m)$, where φ is the Euler's totient function, and the exponent of $\mathbb{Z}_m^*$ is denoted by $\lambda(m) = \exp(\mathbb{Z}_m^*)$. The function $\lambda(m)$ is called the *universal exponent* of m. By [9, p. 53], the values of λ can be computed as follows: $\lambda(1) = 1$, $\lambda(2) = 1$, $\lambda(4) = 2$ and $\lambda(2^a) = 2^{a-2}$, if $a \geqslant 3$. If p is an odd prime, then $\lambda(p^a) = p^{a-1}(p-1)$ for every $a \geqslant 1$. Finally, if $p_1, \ldots, p_s$ are distinct primes, then $\lambda(p_1^{a_1} \cdots p_s^{a_s}) = \operatorname{lcm}(\lambda(p_1^{a_1}), \ldots, \lambda(p_s^{a_s}))$. The first fifty values of λ are the following, as seen in Table 2:

Table 1 – Universal exponent for $1 \leqslant m \leqslant 50$

m	$\lambda(m)$	m	$\lambda(m)$	m	$\lambda(m)$	m	$\lambda(m)$	m	$\lambda(m)$
1	1	11	10	21	6	31	30	41	40
2	1	12	2	22	10	32	8	42	6
3	2	13	12	23	22	33	10	43	42
4	2	14	6	24	2	34	16	44	10
5	4	15	4	25	20	35	12	45	12
6	2	16	4	26	12	36	6	46	22
7	6	17	16	27	18	37	36	47	46
8	2	18	6	28	6	38	18	48	4
9	6	19	18	29	28	39	12	49	42
10	4	20	4	30	4	40	4	50	20

COROLLARY 5.6. *Suppose that $m > 1$ and $n \geqslant 2$ are integers and let $m = p_1^{a_1} \cdots p_s^{a_s}$ be the decomposition of m into distinct prime factors. Then there exists an n-th MRF over $\mathbb{Z}_m$ if and only if*

$$\max\{a_1, \ldots, a_s\} \leqslant n \quad \textit{and} \quad \gcd(n, \lambda(m)) = \gcd(n^2, \lambda(m)),$$

where λ is the universal exponent of m. Furthermore, in this case, the n-th root function is given by

$$\sqrt[n]{x} = x^e,$$

where e is the least positive integer such that $ne \equiv 1 \pmod{\frac{\varphi(m)}{u_n(m)}}$ and $u_n(m)$ is the number of n-th roots of unity in $\mathbb{Z}_m$.

Proof. In view of Theorem 5.3, it suffices to prove that $\mathbb{Z}_m^{(n)} \setminus \{0\}$ has no nilpotent elements if and only if $\max\{a_1, \ldots, a_s\} \leqslant n$.

Suppose that $\max\{a_1, \ldots, a_s\} \leqslant n$ and let $\overline{x} \in \mathbb{Z}_m$. If $\overline{x}$ is not nilpotent, then also $\overline{x}^n \in \mathbb{Z}_m^{(n)}$ is not nilpotent. If $\overline{x}$ is nilpotent, then there exists a positive integer k such that $\overline{x}^k = \overline{0}$. Thus $p_i \mid x^k$, and hence $p_i \mid x$ for each $1 \leqslant i \leqslant s$. Therefore, the decomposition of x into prime numbers is of the form $x = p_1^{b_1} \cdots p_s^{b_s} y$, where $\gcd(y, m) = 1$ and $b_i \geqslant 1$ for each $1 \leqslant i \leqslant s$. Thus

$$x^n = p_1^{nb_1} \cdots p_s^{nb_s} y^n$$

and since $a_i \leqslant n \leqslant nb_i$ for each $1 \leqslant i \leqslant s$, it follows that $m \mid x^n$, that is $\overline{x}^n = \overline{0}$. We conclude that $\mathbb{Z}_m^{(n)} \setminus \{0\}$ has no nilpotent elements.

Conversely, suppose that $\mathbb{Z}_m^{(n)} \setminus \{0\}$ has no nilpotent elements and assume by contradiction that $\max\{a_1, \ldots, a_s\} > n$. Thus, there exists $1 \leqslant i \leqslant s$ such that $a_i > n$. Let $x = p_1 \cdots p_s$. Clearly, $\overline{x}^n \in \mathbb{Z}_m^{(n)}$. Furthermore, $\overline{x}^n$ is a nilpotent element. Indeed, if $k = \max\{a_1, \ldots, a_s\}$, then $m \mid x^k$, so $(\overline{x}^n)^k = \overline{0}$.

But $\overline{x}^n \neq \overline{0}$ since otherwise $x^n \equiv 0 \pmod{m}$, so $x^n \equiv 0 \pmod{p_i^{a_i}}$. Thus $p_i^n \equiv 0 \pmod{p_i^{a_i}}$, which contradicts the fact that $n < a_i$. □

Corollary 5.7. *Let $m > 1$ be an integer. Then there exists a multiplicative square-root function over $\mathbb{Z}_m$ if and only if either $m = 2$ or $m = 4$ or the prime decomposition of m is of the form*

$$m = 2^{a_0} p_1^{a_1} \cdots p_s^{p_s},$$

where $a_0 \in \{0, 1, 2\}$, $s \geqslant 1$ and $p_i \equiv 3 \pmod 4$, $a_i \in \{1, 2\}$ for each $1 \leqslant i \leqslant s$. Furthermore, in this case, the square-root function is given by

$$\sqrt{x} = x^e,$$

where

$$e = \begin{cases} \frac{1}{2}\left(\frac{\varphi(m)}{2^s} + 1\right) & \textit{if } 4 \nmid m \\ \frac{1}{2}\left(\frac{\varphi(m)}{2^{s+1}} + 1\right) & \textit{if } 4 \mid m \end{cases}$$

and s is the number of odd prime divisors of m.

Proof. First suppose that $m = 2^a$, where $a \in \{1, 2\}$. Then $\max\{a\} \leqslant 2$ and since $\lambda(2^a) \in \{1, 2\}$, it follows by Corollary 5.6 that there exist multiplicative square-root functions over $\mathbb{Z}_2$ and over $\mathbb{Z}_4$.

If $m = 2^a$, where $a \geqslant 3$, then $\max\{a\} \nleqslant 2$, so by Corollary 5.6 a multiplicative square-root function over $\mathbb{Z}_{2^a}$ does not exist.

Next, suppose that $m > 2$ and let $m = 2^{a_0} p_1^{a_1} \cdots p_s^{p_s}$ be the prime decomposition of m, where $a_0 \geqslant 0$, $s \geqslant 1$, p_i is an odd prime number and $a_i \geqslant 1$ for every $1 \leqslant i \leqslant s$. By Corollary 5.6, there exists a multiplicative square-root function over $\mathbb{Z}_m$ if and only if $\gcd(2, \lambda(m)) = \gcd(4, \lambda(m))$, $a_0 \in \{0, 1, 2\}$ and $a_i \in \{1, 2\}$ for every $1 \leqslant i \leqslant s$. Since $\lambda(m)$ is even for every $m > 2$, it follows that $\gcd(2, \lambda(m)) = \gcd(4, \lambda(m))$ if and only if $2 \| \lambda(m)$. By noting that $\lambda(m) = \operatorname{lcm}(\lambda(2^{a_0}), \lambda(p_1^{a_1}), \ldots, \lambda(p_s^{a_s}))$ and that $\lambda(2^{a_0}) \in \{1, 2\}$, we deduce that $2 \| \lambda(m)$ if and only if $2 \| \lambda(p_i^{a_i})$ for each $1 \leqslant i \leqslant s$. Since the p_i's are odd, it follows that $2 \| \lambda(m)$ if and only if $2 \| p_i - 1$, that is, if and only if $p_i \equiv 3 \pmod 4$ for each i, as required.

By Corollary 5.6 the square-root function is given by $\sqrt{x} = x^e$, where e is a positive integer such that $2e \equiv 1 \pmod{\varphi(m)/u_2(m)}$ and $u_2(m)$ is the number of solutions of $x^2 = \overline{1}$ in $\mathbb{Z}_m$. Let s be the number of odd prime divisors of m. If $s = 0$, then by the first part of the theorem, either $m = 2$ or $m = 4$. In these cases, it is easy to see that $u_2(2) = 1$ and $u_2(4) = 2$. Suppose that $s \geqslant 1$. Since

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{2^{a_0}}^* \times \mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_s^{a_s}}^*,$$

we obtain that $u_2(m) = u_2(2^{a_0})u_2(p_1^{a_1})\cdots u_2(p_s^{a_s})$. Note that by [9, p. 58], if q has a primitive root, then the equation $x^2 = \overline{1}$ has $u_2(q) = \gcd(2, \varphi(q))$ solutions in $\mathbb{Z}_q$. Now, since $a_0 \in \{0,1,2\}$, it follows that 2^{a_0} has a primitive root, so

$$u_2(2^{a_0}) = \gcd(2, \varphi(2^{a_0})) = \begin{cases} 1 & \text{if } a_0 \in \{0,1\} \\ 2 & \text{if } a_0 = 2. \end{cases}$$

In addition, since the primes $p_1, \ldots, p_s$ are odd, it follows that $2 \mid \varphi(p_i)$, so

$$u_2(p_i^{a_i}) = \gcd(2, \varphi(p_i)) = 2$$

for every $1 \leqslant i \leqslant s$. Therefore

$$\begin{aligned} u_2(m) &= \begin{cases} 1 & s = 0 \text{ and } m = 2 \\ 2 & s = 0 \text{ and } m = 4 \\ 2^s & s \geqslant 1 \text{ and } 4 \nmid m \\ 2^{s+1} & s \geqslant 1 \text{ and } 4 \mid m \end{cases} \\ &= \begin{cases} 2^s & s \geqslant 0 \text{ and } 4 \nmid m \\ 2^{s+1} & s \geqslant 0 \text{ and } 4 \mid m. \end{cases} \end{aligned}$$

Since

$$e = \frac{1}{2}\Big(\frac{\varphi(m)}{u_2(m)} + 1\Big)$$

clearly satisfies the congruence $2e \equiv 1 \pmod{\frac{\varphi(m)}{u_2(m)}}$, our proof is complete. □

As Corollary 5.7 indicates, the first moduli m in which a multiplicative square-root function exists over $\mathbb{Z}_m$ are

$$2, 3, 4, 6, 7, 9, 11, 12, 14, 18, 19, 21, 22, 23, 28, 31, 33, 36, 38, 42, 43, 44, 46, 47, 49.$$

Note that Corollary 5.7 generalizes the result obtained in Example 5.5 regarding prime moduli.

Example 5.8. Consider the ring $\mathbb{Z}_{33} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{32}\}$. In this case, $\mathbb{Z}_{33}^{(2)} = \{\overline{0}, \overline{1}, \overline{3}, \overline{4}, \overline{9}, \overline{12}, \overline{15}, \overline{16}, \overline{22}, \overline{25}, \overline{27}, \overline{31}\}$. Since $m = 33 = 3 \cdot 11$ and $3 \equiv 3 \pmod 4$, $11 \equiv 3 \pmod 4$ it follows by Corollary 5.7 that there exists a multiplicative square-root function over $\mathbb{Z}_{33}$. Furthermore, since m has $s = 2$ odd prime divisors, it follows that the square-root function is given by $\sqrt{x} = x^e$, where

$$e = \frac{1}{2}\Big(\frac{\varphi(33)}{2^2} + 1\Big) = \frac{1}{2}\Big(\frac{20}{4} + 1\Big) = 3$$

that is $\sqrt{x} = x^3$. Therefore

$$\begin{array}{rrrr}\sqrt{\overline{0}} = \overline{0} & \sqrt{\overline{1}} = \overline{1} & \sqrt{\overline{3}} = \overline{27} & \sqrt{\overline{4}} = \overline{31} \\ \sqrt{\overline{9}} = \overline{3} & \sqrt{\overline{12}} = \overline{12} & \sqrt{\overline{15}} = \overline{9} & \sqrt{\overline{16}} = \overline{4} \\ \sqrt{\overline{22}} = \overline{22} & \sqrt{\overline{25}} = \overline{16} & \sqrt{\overline{27}} = \overline{15} & \sqrt{\overline{31}} = \overline{25}.\end{array}$$

Acknowledgments. I wish to thank Prof. Marcel Herzog for his careful reading this paper's drafts.

REFERENCES

[1] J.L. Alperin, *A classification of n-abelian groups*. Canadian J. Math. **21** (1969), 1238–1244.

[2] B. Gilberto and F. Flamini, *Finite Commutative Rings and their Applications*. The Kluwer International Series in Engineering and Computer Science 680, Kluwer Academic Publishers, Boston, MA, 2002.

[3] P. Gładki, *Root selections and 2-th root selections in hyperfields*. Discuss. Math. Gen. Algebra Appl. **39** (2019), *1*, 43–53.

[4] P. Gładki, *n-th root selections in fields*. Ann. Math. Sil. **33** (2019), *1*, 106–120.

[5] M. Hall, *The Theory of Groups*. The Macmillan Company, New York, 1961.

[6] I.N. Herstein, *Topics in Algebra*, Second Edition. Xerox College Publishing, Lexington, Mass.-Toronto, Ont, 1975.

[7] J.M. Howie, *Fundamentals of Semigroup Theory*. London Mathematical Society Monographs. New Series, 12, The Clarendon Press, Oxford Univ. Press, New York, 1995.

[8] S. Lang, *Algebra*, Third Edition. Grad. Texts in Math. 211, Springer, New York, 2002.

[9] W.J. Leveq, *Topics in Number Theory,* Vol I. Dover Publications, Inc., Mineola, NY, 2002.

[10] S. Mac Lane and G. Birkhoff, *Algebra*, Third Edition. American Mathematical Society, 1999.

[11] H.F. Trotter, *Groups in which raising to a power is an automorphism*. Canad. Math. Bull. **8** (1965), 825–827.

[12] W.C. Waterhouse, *Square root as a homomorphism*. Amer. Math. Monthly **119** (2012), *3*, 235–239.

Received 18 April 2023

Department of Computer Science,
The Academic College of Tel-Aviv,
Rabenu Yeruham St., P.O.B 8401 Yaffo,
6818211, Israel
arctanx@gmail.com