Aequat. Math. 89 (2015), 169–186

0001-9054/15/010169-18
published online September 20, 2014
DOI 10.1007/s00010-014-0306-2

Aequationes Mathematicae

On the functional equation $x + f(y + f(x)) = y + f(x + f(y))$, II

Jürg Rätz

Dedicated in friendship to Professor János Aczél on his 90th birthday

Abstract. For an abelian group $(G, +, 0)$ we consider the functional equation

$$f : G \to G, \;\; x + f(y + f(x)) = y + f(x + f(y)) \quad (\forall x, y \in G), \tag{1}$$

together with the condition

$$f(0) = 0. \tag{0}$$

The main question is that of existence of solutions of (1) $\wedge$ (0), specifically in the case when G is the direct sum $\mathbb{Z}_n^{(J)}$ of copies of a finite or infinite cyclic group (Theorems 3.2 and 4.20).

Mathematics Subject Classification. 39B12, 39B52.

Keywords. Abelian groups, composite functional equations.

1. Introduction, notation and preliminaries

This paper is a continuation of [17]. For the convenience of the reader, we repeat here some of the information on notation given in [17], section 1. The results were presented in [14–16].

Throughout the paper, $(G, +, 0)$ or $(G, +)$ or G denotes an abelian group. The set $S(G)$ of all solutions of (1) and

$$S_0(G) := \{f \in S(G);\; f(0) = 0\} \tag{2}$$

completely determine each other [17, p. 188/189, (B6′)], so we may confine ourselves to considering $S_0(G)$.

i_A denotes the identity mapping of the set A and $\underline{a}$ the constant mapping with value a. For $f : A \to A$ and $n \in \mathbb{N}$ ($n \in \mathbb{Z}$ if f is bijective) we denote by f^n the nth iterate of f.

For every abelian group G and every $n \in \mathbb{Z}$, the so-called canonical endomorphism $\omega_n : G \to G$ of G, defined by $\omega_n(x) := nx$ ($\forall x \in G$), is available. In order to keep the notation light, we refrain from using a second subscript like in $\omega_{n,G}$. It will be most times clear from the context to what G the respective ω_n belongs; if necessary, we write $\omega_n : G \to G$.

For every $z \in G$, let $t_z : G \to G$, $t_z(x) := x + z$ $(\forall x \in G)$ denote the translation of G by z. For $x \in G$, we let $\operatorname{ord} x$ stand for the order of x in G. We use $\cong$ as the symbol for groups (or rings) to be isomorphic. For every $m \in \mathbb{N}$, $G[m] := \{x \in G;\ mx = 0\}$ $(= \operatorname{Ker}\omega_m)$, $G[m]^* := \{x \in G;\ \operatorname{ord} x = m\}$. For a ring K with 1, $U(K)$ is the set of units of K.

For every $n \in \mathbb{N}$, we let $\mathbb{Z}_n$ stand for the cyclic group with n elements, most times written as $\{0, \ldots, n-1\}$. Whenever we find it helpful, we shall use the familiar ring structure on $\mathbb{Z}_n$ or $\mathbb{Z}$ with 1 as its identity element; for $\mathbb{Z}_1$ we have $1 = 0$. We put in addition $\mathbb{Z}_0 := \mathbb{Z}$ (cf. Remark 4.1). Accordingly, 0 and 1 stand for the integers zero and one as well as for the zero and the identity element of $\mathbb{Z}_n$ $(n \in \mathbb{N}^0)$. It will always be clear from the context what is meant.

For a list of fundamental properties of solutions of (1), stemming from M. Balcerowski [2], cf. [17, p. 188, (B1),…,(B9)].

Lemma 1.1. (a) *Every $f \in S_0(G)$ is bijective and satisfies*

$$f^2(x) + x = f(x) \quad (\forall x \in G). \tag{3}$$

(b) *If $\omega_2 : G \to G$ is injective, then every $f \in S_0(G)$ is additive, i.e., $S_0(G) \subset \operatorname{End}(G)$.*

(*cf.* [17, (B1′), (B3), (B8)]).

Lemma 1.2. *For $f \in S_0(G)$, $x \in G$, $\operatorname{ord} x = n \in \mathbb{N} \cup \{\infty\}$, we have $\operatorname{ord} f(x) = \operatorname{ord} x$. f shares this property with group isomorphisms, but here f need not be additive* ([17, p. 197–200, Example 3.14]).

Proof. Case 1: $n = \infty$. Then kx $(k \in \mathbb{N})$ are pairwise distinct, so are $f(kx)$ $(k \in \mathbb{N})$ by Lemma 1.1(a), and finally, by [17, p. 190, Theorem 2.5], so are $kf(x)$ $(k \in \mathbb{N})$. Therefore $\operatorname{ord} f(x) = \infty = n$. Case 2: $n \in \mathbb{N}$, so $nx = 0$. For $j \in \mathbb{N}$, we have $jx = 0 \Leftarrow_{[Lemma 1.1(a)]}\Rightarrow f(jx) = 0 \Leftarrow_{[17,\text{ Theorem 2.5}]}\Rightarrow jf(x) = 0$. Hence $\operatorname{ord} f(x) = \operatorname{ord} x$. □

Lemma 1.3. *If G_1 is an abelian group such that $G \cong G_1 \times G_1$, then $S_0(G) \neq \emptyset$, no matter if $S_0(G_1) \neq \emptyset$.*

Proof. Let

$$f : G_1 \times G_1 \to G_1 \times G_1,\ \ f(\xi_1, \xi_2) := (-\xi_2, \xi_1 + \xi_2)\ \ (\forall (\xi_1, \xi_2) \in G_1 \times G_1). \tag{4}$$

For $x = (\xi_1, \xi_2) \in G_1 \times G_1$, $y = (\eta_1, \eta_2) \in G_1 \times G_1$ arbitrary, we have $x + f(y + f(x)) = (\xi_1, \xi_2) + f((\eta_1, \eta_2) + (-\xi_2, \xi_1 + \xi_2)) = (\xi_1, \xi_2) + f(\eta_1 - \xi_2, \eta_2 + \xi_1 + \xi_2) = (\xi_1, \xi_2) + (-\eta_2 - \xi_1 - \xi_2, \eta_1 - \xi_2 + \eta_2 + \xi_1 + \xi_2) = (-\eta_2 - \xi_2, \eta_1 + \eta_2 + \xi_1 + \xi_2) =_{(4)} = f(y) + f(x)$. This expression is invariant under interchanging x and y. Hence (1) holds, and so does (0). I.e., $S_0(G_1 \times G_1) \neq \emptyset$. By [17, Remark 1.1] $S_0(G) \neq \emptyset$. □

If J is a set and G an abelian group, then $G^{(J)}$ denotes the direct sum of $\operatorname{card} J$ copies of G. For $\operatorname{card} J = 0$, we have $G^{(J)} = \{0\}$ [3, p. 22]. For $\operatorname{card} J = n \in \mathbb{N}$, $G^{(J)} := G^n := G \oplus \cdots \oplus G$ (n direct summands).

Lemma 1.4. *For any set J we have*

$$\operatorname{card} J \geq \aleph_0 \ \text{ or } \ \operatorname{card} J \in 2\mathbb{N}^0 \Longrightarrow S_0(G^{(J)}) \neq \emptyset, \ \ S(G^{(J)}) \neq \emptyset. \tag{5}$$

Proof. $S_0(\{0\}) = \{\underline{0}\}$ by [17, Lemma 2.1(a)], so the assertion holds for $\operatorname{card} J = 0$. For $\operatorname{card} J \in 2\mathbb{N}$ or $\operatorname{card} J \geq \aleph_0$, $G^{(J)}$ appears as the direct sum of copies of $G^2 = G \oplus G$ (cf. [17, p. 195, Proof of Lemma 3.7]). By Lemma 1.3 and [17, Lemma 2.3(a)], $S_0(G^{(J)}) \neq \emptyset$, so $S(G^{(J)}) \neq \emptyset$. □

Lemma 1.5. *For $f \in S_0(G)$ and $x \in G$, we obtain*

(a) *(i)* $f^2(x) = x \Leftrightarrow$ (ii) $f(x) = 2x \not\Longleftarrow\!\!\!\Longrightarrow$ (iii) $3x = 0$.
(b) $f^3(x) = x \Leftrightarrow 2x = 0$.

Proof. (a): (i) $\Leftrightarrow$ (ii) immediately follows from (3) in Lemma 1.1.—(ii) $\Rightarrow$ (iii): By [17, (B4)] $f^3(x) = -x$, so $ff^2(x) = -x$, hence by (i) $f(x) = -x$, and by (ii) $2x = -x$, so (iii) holds.—(iii) $\not\Rightarrow$ (i): Consider the function f in (4) for $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ and $x = (1,0)$. Then $3x = 0$, but $f^2(1,0) = f(0,1) = (-1,1) \neq (1,0)$, and by Lemma 1.3 $f \in S_0(\mathbb{Z}_3 \times \mathbb{Z}_3)$.
(b) $f^3(x) = x \Leftarrow_{(\mathrm{B4})}\Rightarrow -x = x \Leftrightarrow 2x = 0$. □

Lemma 1.6. *If $f \in S_0(G)$ and H is a subgroup of G such that $f(H) \subset H$, then the restriction $g : H \to H$ of f is in $S_0(H)$, and $f(H) = H$.*

Proof. $f(H) \subset H$ implies the existence of g and $g(0) = f(0) = 0$. Let $x, y \in H$ be arbitrary. Then $x+f(y)$, $y+f(x)$, $f(x+f(y))$, $f(y+f(x)) \in H$, and we have $x+g(y+g(x)) = x+f(y+f(x)) =_{(1)}= y+f(x+f(y)) = y+g(x+g(y))$. Since $x, y \in H$ were arbitrary, we have $g \in S_0(H)$. By Lemma 1.1(a) $g(H) = H$, so $f(H) = H$. □

2. Further general properties of solutions of (1)

Having Lemma 1.1(a) in mind, we first extend [17, p. 193, Lemma 3.2] to arbitrary abelian groups G.

Lemma 2.1. *Let $f \in S_0(G)$. Then:*

(a) $f^3 = -i_G$, $f^6 = i_G$.
(b) *G is the disjoint union of $C_0 := \{0\}$ and, for $G \neq \{0\}$, of the C_x ($x \in G \setminus \{0\}$) where C_x is the range of the cycle*

$$x \mapsto f(x) \mapsto -x + f(x) \mapsto -x \mapsto -f(x) \mapsto x - f(x) \mapsto x \quad \text{of } f.$$

(c) $\operatorname{card} C_x \in \{1,2,3,6\}$ ($\forall x \in G$), *i.e., f has only 1-,2-,3-, and/or 6-cycles.*

(d) $x, y \in G,\ y \in C_x \Rightarrow \operatorname{ord} y = \operatorname{ord} x$.
(e) *f has exactly one 1-cycle, namely* $\{0\}$.
(f) *1-cycles of f^3 only stem from 1- or 3-cycles of f.*
2-cycles of f^3 only stem from 2- or 6-cycles of f.

Proof. (a) follows from (B4). (b) On the basis of Lemma 1.1(a) we define

$$x, y \in G \Longrightarrow \left[x \sim_f y :\Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } y = f^k(x)\right].$$

Then $\sim_f$ is an equivalence relation on G, and the sets C_x $(x \in G)$ are the $\sim_f$-classes. By the aid of (3) and part (a), $f^2(x) = -x + f(x)$, $f^3(x) = -x$, $f^4(x) = f(-x) =_{(\mathrm{B4})}= -f(x)$, $f^5(x) = f^2(-x) =_{(\mathrm{B4})}= -f^2(x) = x - f(x)$, $f^6(x) = x$. (For $x = 0$, C_x becomes $\{0\}$). (c) By $f^6(x) = x$, the iterative order of every $x \in G$ is a positive divisor of 6, i.e., the possible lenghts of cycles of f are $1, 2, 3, 6$. (d) follows at once from Lemma 1.2. (e) is a consequence of [17, Lemma 2.4] and (0). (f) By (a), f^3 is involutorial, so f^3 has only 1- and/or 2-cycles. The rest follows, written in the usual cycle notation, from

$$\begin{aligned}&(u)^3 = (u),\ (u\,v\,w)^3 = (u)(v)(w);\ (u\,v)^3 = (u\,v),\ (u\,v\,w\,x\,y\,z)^3\\&\quad = (u\,x)(v\,y)(w\,z).\end{aligned} \tag{6}$$

□

Lemma 2.2. *If $\omega_2 : G \to G$ is injective and $f \in S_0(G)$, then f has no 3-cycles.*

Proof. By Lemma 1.5(b), the 1-cycles (x) of f^3 are characterized by $2x = 0$, i.e., by $\omega_2(x) = 0$, i.e., due to the hypothesis, by $x = 0$. If $(u\,v\,w)$ were a 3-cycle of f, then by (6) $(u\,v\,w)^3 = (u)(v)(w)$ with (see above) $u = v = w = 0$, a contradiction. So the assertion holds. □

Lemma 2.3. *If $\omega_2 : G \to G$ and $\omega_3 : G \to G$ are injective and $f \in S_0(G)$, then* $\operatorname{card} C_x = 6$ $(\forall x \in G \setminus \{0\})$.

Proof. Let $x \in G \setminus \{0\}$ be arbitrary. By [17, Lemma 2.4] and (0), $f(x) \neq x$. Injectivity of ω_2 and ω_3 implies $2x \neq 0$, $3x \neq 0$, so by Lemma 1.5(a), (b) $f^2(x) \neq x$, $f^3(x) \neq x$. $f^4(x) = x$ would imply $f^2(x) = f^2 f^4(x) = f^6(x) = x$, which is already excluded. If $f^5(x) = x$, then $f(x) = f f^5(x) = f^6(x) = x$, which is not true either. So

$$f^\nu(x) \neq x \quad (\nu = 1, 2, 3, 4, 5). \tag{7}$$

Assume that there are $\mu, \nu \in \{0, 1, 2, 3, 4, 5\}$ with $\mu < \nu$, $f^\mu(x) = f^\nu(x)$. Then, since f^μ is bijective, $x = f^{\nu-\mu}(x)$, where $\nu - \mu \in \{1, 2, 3, 4, 5\}$, which is a contradiction to (7). Therefore $x = f^0(x),\ f(x), \ldots, f^5(x)$ are pairwise distinct, i.e. $\operatorname{card} C_x = 6$. □

Corollary 2.4. *If $f \in S_0(G)$, each of the following conditions is sufficient for* $\operatorname{card} C_x = 6$ $(\forall x \in G \setminus \{0\})$*:*

(i) *G is torsion-free.*
(ii) *$\exists n \in \mathbb{N}$ with $2 \nmid n$, $3 \nmid n$, and $nG = \{0\}$.*

Proof. In Cases (i) and (ii), ω_2 and ω_3 turn out to be injective, and the assertion follows from Lemma 2.3. □

Bijectivity of all $f \in S(G)$ [17, (B1′)] is an invitation to the question as to whether f^{-1} must be in $S(G)$.

Theorem 2.5.
(a) *$f \in S_0(G) \Rightarrow f^{-1} = i_G - f \in S_0(G)$.*
(b) *If $S_0(G) \subset \mathrm{End}\,(G)$ and $f \in S(G)$, then $f^{-1} \in S(G)$.*
(c) *In* (b), *the condition $S_0(G) \subset \mathrm{End}\,(G)$ is essential.*

Proof. (a) By (B1′), f is bijective. Let $x \in G$ be arbitrary, $y := f^{-1}(x)$. By (3) $f^2(y) + y = f(y)$, so $f^2 f^{-1}(x) + f^{-1}(x) = f f^{-1}(x)$, i.e., $f(x) + f^{-1}(x) = x$. Since $x \in G$ was arbitrary, we have $f + f^{-1} = i_G$, i.e., $f^{-1} = i_G - f$. For the second part of the assertion, let $x, y \in G$ be arbitrary. By (B1′) there are unique $x', y' \in G$ with $x = f(x')$, $y = f(y')$, and we have $x + (i_G - f)(y + (i_G - f)(x)) = f(x') + (i_G - f)(f(y') + (i_G - f)(f(x'))) = f(x') + f(y') + (i_G - f)(f(x')) - f(f(y') + (i_G - f)(f(x'))) = f(x') + f(y') + f(x') - f^2(x') - f(f(y') + f(x') - f^2(x')) =_{(3)}= f(x') + f(y') + x' - f(f(y') + x') =_{(1)}= f(x') + f(y') + y' - f(f(x') + y')$. The expressions on both sides of "$=_{(1)}=$" are transformed into each other by interchanging x' and y'. The above calculation shows that the latter expression is $y + (i_G - f)(x + (i_G - f)(y))$. Since $x, y \in G$ were arbitrary, we get $(i_G - f) \in S(G)$. Since $(i_G - f)(0) = 0$, we have $(i_G - f) \in S_0(G)$ as asserted.

(b) Let $f \in S(G)$ be arbitrary. By [17, Remark 1.3] there exists $z \in G$ and $g \in S_0(G)$ with $f = g \circ t_z$, hence $f^{-1} = t_{-z} \circ g^{-1}$. By (a), $g^{-1} \in S_0(G)$, so $g^{-1} \in \mathrm{End}\,(G)$ by hypothesis. For arbitrary $x, y \in G$ we have $x + f^{-1}(y + f^{-1}(x)) = x + g^{-1}(y + g^{-1}(x) - z) - z =_{\mathrm{End}}= x + g^{-1}(y) + g^{-2}(x) - g^{-1}(z) - z =_{(3)}= g^{-1}(x) + g^{-1}(y) - g^{-1}(z) - z$. This last expression is invariant under interchanging x and y, so f^{-1} satisfies (1), i.e., $f^{-1} \in S(G)$.

For (c) cf. Remark 2.8 below. □

(B6) [17, p. 188] ensures that the membership of f in $S(G)$ is preserved under composition from the right with translations. How about composition from the left?

Theorem 2.6.
(a) *If $S_0(G) \subset \mathrm{End}\,(G)$, $f \in S(G)$, and $w \in G$, then $t_w \circ f \in S(G)$.*
(b) *In* (a), *the condition $S_0(G) \subset \mathrm{End}\,(G)$ is essential, even for $f \in S_0(G)$.*
(c) *If $S_0(G) \subset \mathrm{End}\,(G)$ and $f \in S(G)$, then there exists a unique $x_0 \in G$ with $f(x_0) = 0$, and for $g := f \circ t_{x_0}$ we have $g \in S_0(G)$ and $t_w \circ f = f \circ t_{g^{-1}(w)}$ for all $w \in G$.*

Proof. (a) Let $f \in S(G)$, $w \in G$ be arbitrary. By Theorem 2.5(b) $f^{-1} \in S(G)$. By (B6) $f^{-1} \circ t_{-w} \in S(G)$, and again by Theorem 2.5(b) $(f^{-1} \circ t_{-w})^{-1} \in S(G)$, i.e., $t_w \circ f \in S(G)$. (b) See Remark 2.7 below. (c) Existence and uniqueness of x_0 follow from (B1′). By (B6) $g \in S(G)$, and since $g(0) = f(x_0) = 0$, we even have $g \in S_0(G)$, so by hypothesis $g \in \mathrm{End}\,(G)$. Theorem 2.5(a) implies $g^{-1} = i_G - g$, so for all $x, w \in G$ we get $(f \circ t_{g^{-1}(w)})(x) = f(x + w - g(w)) = f(x + w + g(-w)) = f(x + w + f(-w + x_0)) =_{(1)}= w - x_0 + x + w + f(-w + x_0 + f(x+w))$, $(f \circ t_{g^{-1}(w)})(x) = w - x_0 + x + w + f(-w + x_0 + f(x+w))$ for all $x, w \in G$. Now the last term is $g(-w+f(x+w)) =_{\mathrm{End}}= g(-w)+g(f(x+w)) = f(-w + x_0) + f(x_0 + f(x + w))$, so

$$(f \circ t_{g^{-1}(w)})(x) = w - x_0 + x + w + f(-w + x_0) + f(x_0 + f(x+w)) \quad (\forall x, w \in G). \tag{8}$$

Next we put in (1) $x + w$, x_0 in place of x, y, respectively, and get $x + w + f(x_0 + f(x+w)) = x_0 + f(x+w+f(x_0)) = x_0 + f(x+w)$, so $f(x_0 + f(x+w)) = -x - w + x_0 + f(x + w)$, and (8) becomes

$$(f \circ t_{g^{-1}(w)})(x) = w + f(-w + x_0) + f(x + w) \quad (\forall x, w \in G). \tag{9}$$

Finally, $f(-w+x_0)+f(x+w) = f(-w+x_0)+f(x+w-x_0+x_0) = g(-w)+g(x+w-x_0) =_{\mathrm{End}}= g(-w)+g(w)+g(x-x_0) = f(x)$, so by (9) $(f \circ t_{g^{-1}(w)})(x) = w + f(x)$. Since $x \in G$ was arbitrary, we obtain $f \circ t_{g^{-1}(w)} = t_w \circ f \quad (\forall w \in G)$. □

Remark 2.7. Let $f_0 \in S_0(\mathbb{Z}_2^6) \setminus \mathrm{End}\,(\mathbb{Z}_2^6)$ be the specific function in [17, p. 197–200, Example 3.14] and $\{e_1, \ldots, e_6\}$ the basis used there, and let $g := f_0 + \underline{e_1}$. From the definition of f_0 [17, (32),(34),…,(54)] we obtain $g(e_1) = f_0(e_1) + e_1 = e_2 + e_1$, $g(e_3) = f_0(e_3) + e_1 = e_4 + e_1$. Then $e_1 + g(e_3 + g(e_1)) = e_1 + g(e_3 + e_2 + e_1) = e_1 + f_0(e_1 + e_2 + e_3) + e_1 =_{[17,(40)]}= e_2 + e_3 + e_6$, $e_3 + g(e_1 + g(e_3)) = e_3 + g(e_1 + e_4 + e_1) = e_3 + g(e_4) = e_3 + f_0(e_4) + e_1 =_{[17,\ (35)]}= e_3 + e_3 + e_4 + e_1 = e_1 + e_4 \neq e_2 + e_3 + e_6$, so g violates the functional equation (1), i.e., $t_{e_1} \circ f_0 = g \notin S(\mathbb{Z}_2^6)$, and Theorem 2.6(b) is proved.

Remark 2.8. Let f_0 and $\{e_1, \ldots, e_6\}$ be as in Remark 2.7 and let $h := f_0^{-1} \circ t_{e_1}$. By Theorem 2.5(a) $f_0^{-1} \in S_0(\mathbb{Z}_2^6)$, so by (B6) $h \in S(\mathbb{Z}_2^6)$. Then $h^{-1} = (f_0^{-1} \circ t_{e_1})^{-1} = t_{e_1}^{-1} \circ f_0 = t_{e_1} \circ f_0 \notin S(\mathbb{Z}_2^6)$ by Remark 2.7. Therefore we have proved Theorem 2.5(c).

Next we come to a variant of (B8) [17, p. 188].

Lemma 2.9. *If $\omega_2 : G \to G$ is surjective, then $S_0(G) \subset \mathrm{End}\,(G)$.*

Proof. Let $f \in S_0(G)$. By (B7) $2f(x + y) = 2f(x) + 2f(y)$ $(\forall x, y \in G)$, so by [17, p. 190, Theorem 2.5] $f(2(x + y)) = f(2x) + f(2y)$ $(\forall x, y \in G)$. For arbitrary $u, v \in G$, the surjectivity of ω_2 ensures the existence of $x, y \in G$ such that $u = 2x$, $v = 2y$, so $u + v = 2x + 2y = 2(x + y)$, and we have $f(u + v) = f(u) + f(v)$. As $u, v \in G$ were arbitrary, $f \in \mathrm{End}\,(G)$ holds. □

Lemma 2.3 in [17, p. 189] is a tool for building solutions of (1) on $\prod_{i\in I} G_i$ or $\bigoplus_{i\in I} G_i$ from those on G_i's. Our Lemma 2.10 proceeds in the opposite direction where appropriate care is necessary: $S_0(\mathbb{Z}_2^2) \neq \emptyset$, but $S_0(\mathbb{Z}_2) = \emptyset$ ([17, p. 194, Example 3.4(b), (c)]). Hypothesis (3) below takes care.

Lemma 2.10. *Hypotheses:*

(1) $I \neq \emptyset$, $(G_i)_{i\in I}$ *is a family of abelian groups.*
(2) *For every* $i \in I$ *there is* $n_i \in \mathbb{N}$ *such that* $n_i G_i = \{0\}$.
(3) $\gcd(n_i, n_j) = 1$ *for all* $i, j \in I$ *with* $i \neq j$.
(4) $G'_j := \{(x_i)_{i\in I} \in \prod_{i\in I} G_i;\ x_i = 0 \quad (\forall i \in I \setminus \{j\}\} \ (j \in I)$.
(5) $\chi_j : G_j \to G'_j$ *is the canonical bijection* $(\forall j \in I)$.

Then:

(a) $f \in S_0(\bigoplus_{i\in I} G_i) \Rightarrow f(G'_j) \subset G'_j$, $f|G'_j \in S_0(G'_j)$, *and* $f_j := \chi_j^{-1} \circ (f|G'_j) \circ \chi_j \in S_0(G_j)$ *for all* $j \in I$.
(b) *If* $f \in S_0(\bigoplus_{i\in I} G_i)$ *is additive, so are* $f|G'_j$ *and* f_j $(\forall j \in I)$, *and we have* $f = (\bigoplus_{j\in I} f_j) : (x_j)_{j\in I} \mapsto (f_j(x_j))_{j\in I} \quad (\forall (x_j)_{j\in I} \in \bigoplus_{j\in I} G_j)$.

Proof. (a) Let $j \in I$, $x = (z_i)_{i\in I} \in G'_j$ be arbitrary, say $z_i = 0 \quad (\forall i \in I \setminus \{j\})$, $z_j =: x_j \in G_j$. Since $\chi_j : G_j \cong G'_j$ we get $\operatorname{ord} x = \operatorname{ord} x_j$, so by Hypothesis (2) $\operatorname{ord} x \,|n_j$, and by Lemma 1.2

$$\operatorname{ord} f(x) \mid n_j. \tag{10}$$

Let $(y_i)_{i\in I} := f(x)$ and assume that $y_i \neq 0$ for $i \in I\setminus\{j\}$. $y_i \in G_i$ and Hypothesis 2) imply $1 \neq \operatorname{ord} y_i | n_i$. Because $\operatorname{ord} y_i | \operatorname{ord} f(x)$ and by (10) $\operatorname{ord} y_i | n_j$, so $1 \neq \operatorname{ord} y_i | \gcd(n_i, n_j)$ where $i \neq j$, in contradiction to Hypothesis (3). Therefore $y_i = 0$ $(\forall i \in I\setminus\{j\})$, i.e., $f(x) = (y_i)_{i\in I} \in G'_j$. Since $j \in I$ and $x \in G'_j$ were arbitrary, we have the first part of assertion (a), namely $f(G'_j) \subset G'_j$ $(\forall j \in I)$. So for every $j \in I$, $f|G'_j$ exists and is in $S_0(G'_j)$ by Lemma 1.6. Finally, $f_j \in S_0(G_j)$ $(\forall j \in I)$ by [17, Remark 1.1(a)].
(b) As a composite of additive mappings, f_j is additive for every $j \in I$. For the inclusion map $\psi_j : G'_j \hookrightarrow \bigoplus_{i\in I} G_i \quad (j \in I)$, we have

$$\psi_j \circ (f|G'_j) = f \circ \psi_j \quad (\forall j \in I). \tag{11}$$

Let $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} G_i$ and $j \in I$ be arbitrary. Then $x_j = \operatorname{pr}_j x \in G_j$, $\chi_j \operatorname{pr}_j x \in G'_j$, $\psi_j \chi_j \operatorname{pr}_j x \in \bigoplus_{i\in I} G_i$, and since x has finite support, we get

$$\sum_{j\in I} \psi_j \chi_j \operatorname{pr}_j x = \sum_{j\in I} (0, \dots, x_j, \dots, 0) = x \quad (\forall x \in \bigoplus_{i\in I} G_i). \tag{12}$$

Therefore $f(x) =_{(12)}= f(\sum_{j\in I} \psi_j \chi_j \operatorname{pr}_j x) = \sum_{j\in I} f(\psi_j \chi_j \operatorname{pr}_j x) =_{(11)}= \sum_{j\in I} \psi_j (f|G'_j) \chi_j \operatorname{pr}_j x = \sum_{j\in I} \psi_j \chi_j \chi_j^{-1} (f|G'_j) \chi_j \operatorname{pr}_j x =_{(a)}= \sum_{j\in I} \psi_j \chi_j f_j \operatorname{pr}_j x = \sum_{j\in I} \psi_j \chi_j f_j(x_j) = \sum_{j\in I} (0, \dots, f_j(x_j), \dots, 0) = (f_j(x_j))_{j\in I} = (\bigoplus_{j\in I} f_j)(x)$. Since $x \in \bigoplus_{j\in I} G_j$ was arbitrary, we have $f = \bigoplus_{j\in I} f_j$. □

3. Solutions of (1) for $G = \mathbb{Z}_n$

A few contributions to the subject of this section can be found in [17, pp. 191–192]. For $n \in \mathbb{N}$, the fact that $\omega_{n+k} : \mathbb{Z}_n \to \mathbb{Z}_n$ is identical with $\omega_k : \mathbb{Z}_n \to \mathbb{Z}_n$ [17, Remark 2.10] makes it natural to write $\omega_\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ for ω_k when $k \in \alpha \in \mathbb{Z}_n$. We are going to extend first those results towards a criterion for the existence of solutions of (1) (Theorem 3.2). Because of the agreement $\mathbb{Z}_0 := \mathbb{Z}$, the symbol $\mathbb{Z}_n$ is available for all $n \in \mathbb{N}^0$. We begin by a number-theoretic remark:

Remark 3.1. (a) For an odd integer $n > 1$, the following are equivalent:

(i) n has a positive divisor $d \equiv_6 5$.
(ii) n has a prime divisor $\equiv_6 5$.

(b) Every $n \in \mathbb{N}$ has a divisor $\equiv_6 5$, namely -1, but 3 has no prime divisor $\equiv_6 5$. So "positive" is essential in (i).

Proof of (a). (ii) $\Rightarrow$ (i) is trivial. (i) $\Rightarrow$ (ii): Let $d \in \mathbb{N}$, $d|n$, $d \equiv_6 5$. There exist $r \in \mathbb{N}$; $p_1, \ldots, p_r \in \mathbb{P}$ (not necessarily pairwise distinct) with $d = p_1 \cdot \ldots \cdot p_r$. Oddness of n enforces $p_\nu \in \{3\} \cup (6\mathbb{N} + 1) \cup (6\mathbb{N}^0 + 5)$ $(\nu = 1, \ldots, r)$. As $d \equiv_6 5$, we have $3 \nmid d$. If $p_1, \ldots, p_r$ were in $6\mathbb{N} + 1$, then $d \in 6\mathbb{N} + 1$, which is a contradiction to the definition of d. So at least one p_ν is in $6\mathbb{N}^0 + 5$, and this is a prime divisor of n, i.e., (ii) holds. □

Theorem 3.2. *For* $n \in \mathbb{N}^0$ *and*

$$\mathbb{M} := \{m \in \mathbb{N};\ m \textit{ odd, } m \textit{ has no positive divisor } \equiv_6 5, \textit{ and } m \textit{ contains the prime factor } 3 \textit{ at most once}\}, \tag{13}$$

the following statements are equivalent:

(i) $S_0(\mathbb{Z}_n) \neq \emptyset$,
(ii) $n \in \mathbb{M}$,
(iii) *There exists* $\alpha \in \mathbb{Z}_n$ *such that* $\alpha^2 - \alpha + 1 = 0$.

Proof. For $n = 0$, (i) is false [17, Example 2.7], (ii) is false by (13), and (iii) is false since $\alpha^2 - \alpha + 1$ is odd ($\forall \alpha \in \mathbb{Z}_0 = \mathbb{Z}$). So the assertion holds for $n = 0$. In the following, let $n \in \mathbb{N}$.
(i)$\Rightarrow$(ii). Let $S_0(\mathbb{Z}_n) \neq \emptyset$. By [17, Corollary 2.6] $S_0(\mathbb{Z}_n) \subset \mathrm{End}\,(\mathbb{Z}_n)$. By [17, Remark 2.10] $\mathrm{End}\,(\mathbb{Z}_n) = \{\omega_0, \ldots, \omega_{n-1}\}$. If n were even, then by [17, Corollary 2.11] $S_0(\mathbb{Z}_n) = \emptyset$, contradicting (i). Therefore

$$n \text{ is odd.} \tag{14}$$

Assume that there exist $d \in \mathbb{N}$ with $d|n$, $d \equiv_6 5$. Then $\gcd(d, 2) = 1$ and $\gcd(d, 3) = 1$, so $\omega_2 : \mathbb{Z}_d \to \mathbb{Z}_d$ and $\omega_3 : \mathbb{Z}_d \to \mathbb{Z}_d$ are injective.

Assume that $f \in S_0(\mathbb{Z}_d)$. By Lemma 2.3, every cycle C_x ($x \in \mathbb{Z}_d \setminus \{0\}$) of f has cardinality 6. By Lemma 2.1(b), $\mathbb{Z}_d$ is the disjoint union of one 1-cycle and some 6-cycles, therefore $d = \operatorname{card} \mathbb{Z}_d \equiv_6 1$, contradicting $d \equiv_6 5$. So f cannot exist, i.e., $S_0(\mathbb{Z}_d) = \emptyset$.

Now by (i) $S_0(\mathbb{Z}_n) \neq \emptyset$, say, by [17, (14)] $\omega_k \in S_0(\mathbb{Z}_n)$ for a suitable $k \in \mathbb{Z}$, where $n|m_k$. Since $d|n$, we get $d|m_k$, so again by [17, (14)] $(\omega_k : \mathbb{Z}_d \to \mathbb{Z}_d) \in S_0(\mathbb{Z}_d)$, a contradiction to $S_0(\mathbb{Z}_d) = \emptyset$. This means that d cannot exist, i.e.,

$$n \text{ has no positive divisor } \equiv_6 5. \tag{15}$$

By inspection we find that $9 \not| m_k$ $(k \in \{0, \dots, 8\})$, so by [17, (14)] $S_0(\mathbb{Z}_9) = \emptyset$. Let us realize (i) again by the assumption $\omega_k \in S_0(\mathbb{Z}_n)$, so again as above $n|m_k$. If $9|n$, then $9|m_k$, so by [17, (14)] $(\omega_k : \mathbb{Z}_9 \to \mathbb{Z}_9) \in S_0(\mathbb{Z}_9)$, which is impossible. Therefore $9 \not| n$, so

$$3^s|n \quad \text{only if} \quad s = 0 \quad \text{or} \quad s = 1. \tag{16}$$

By (14), (15), (16) $n \in \mathbb{M}$, i.e., (ii) holds.
(ii)⇒(i). Let $n \in \mathbb{M}$. Then there exist $s \in \{0, 1\}$, $n' \in \mathbb{N}$ such that $n = 3^s n'$, $\gcd(3, n') = 1$. $n \in \mathbb{M}$ implies $n' \in \mathbb{M}$.
Case 1: $n' = 1$. So $n \in \{1, 3\}$, and since $S_0(\mathbb{Z}_1) = \{\omega_0\}$, $S_0(\mathbb{Z}_3) = \{\omega_2\}$ [17, Example 2.12], (i) holds. – Case 2: $n' > 1$. (This means in fact that $n' \geq 7$). Since $3 \not| n'$, all prime divisors of n' are in $6\mathbb{N} + 1$. Therefore -3 is a quadratic residue modulo all prime divisors of n' [4, p. 75, Theorem 96]; Gauss's Lemma is involved here. It follows from [10, p. 63, Theorem 5-1] that

$$-3 \text{ is a quadratic residue modulo } n'. \tag{17}$$

$\mathbb{Z}_{n'}$ is a commutative ring with $1 \neq 0$. Oddness of n' guarantees that $\gcd(n', 4) = 1$, so $4 \in U(\mathbb{Z}_{n'})$, and for any $x \in \mathbb{Z}_{n'}$ we have

$$x^2 - x + 1 = 0 \Leftrightarrow 4x^2 - 4x + 4 = 0 \Leftrightarrow (2x - 1)^2 = -3. \tag{18}$$

By (17), $(2x - 1)^2 = -3$ is solvable in $\mathbb{Z}_{n'}$, and so is $x^2 - x + 1 = 0$, i.e., there exists $\alpha \in \mathbb{Z}_{n'}$ such that $\alpha^2 - \alpha + 1 = 0$. If $\pi : \mathbb{Z} \to \mathbb{Z}_{n'}$ is the canonical ring epimorphism, then there exists $k \in \mathbb{Z}$ with $\pi(k) = \alpha$. Then $\pi(k^2 - k + 1) = \alpha^2 - \alpha + 1 = 0$ whence $n'|(k^2 - k + 1)$, so by [17, (14)]

$$\omega_k \in S_0(\mathbb{Z}_{n'}), \quad \text{i.e., } S_0(\mathbb{Z}_{n'}) \neq \emptyset. \tag{19}$$

Case 2a: $s = 0$. Then $n = n'$, so by (19) $S_0(\mathbb{Z}_n) \neq \emptyset$. Case 2b: $s = 1$. Then $\mathbb{Z}_n \cong \mathbb{Z}_3 \times \mathbb{Z}_{n'}$, and from $S_0(\mathbb{Z}_3) \neq \emptyset$, (19), and [17, Lemma 2.3(a)] we get again $S_0(\mathbb{Z}_n) \neq \emptyset$. So (i) holds in both cases.
(i)⇔ (iii). For the canonical ring epimorphism $\pi : \mathbb{Z} \to \mathbb{Z}_n$ (remember $\pi(0) = 0$, $\pi(1) = 1$ by our notational agreement) we have (i)$\Leftarrow_{[17,\ (14)]}\Rightarrow$ $\exists k \in \{0, \dots, n-1\}$ with $n|(k^2-k+1) \Leftrightarrow \exists k \in \{0, \dots, n-1\}$ with $\pi(k^2-k+1) = 0 \Leftarrow_{\pi \text{ surjective}}\Rightarrow$ $\exists \alpha \in \mathbb{Z}_n$ with $\alpha^2 - \alpha + 1 = 0$ (iii). □

Remark 3.3. The last part of the proof above shows that for the canonical epimorphism $\pi : \mathbb{Z} \to \mathbb{Z}_n$, we have

$$S_0(\mathbb{Z}_n) = \{\omega_k;\ k \in \{0, \dots, n-1\},\ (\pi(k))^2 - \pi(k) + 1 = 0\} \quad (\forall n \in \mathbb{N}). \tag{20}$$

Theorem 3.2 characterizes those $n \in \mathbb{N}^0$ for which $S_0(\mathbb{Z}_n) \neq \emptyset$ by $n \in \mathbb{M}$. So for all $n \in \mathbb{N}^0 \setminus \mathbb{M}$, $\operatorname{card} S_0(\mathbb{Z}_n) = 0$. What is $\operatorname{card} S_0(\mathbb{Z}_n)$ for $n \in \mathbb{M}$?

It becomes visible from (13) that the prime number 3 plays a singular role in the present characterization problem. This will be observed many more times in what follows.

Lemma 3.4. *If $n \in \mathbb{M}$, $3 \nmid n$, and if n has σ distinct prime divisors, then* $\operatorname{card} S_0(\mathbb{Z}_n) = 2^\sigma$.

Proof. For $n = 1$ we have $S_0(\mathbb{Z}_n) = \{\omega_0\}$ and $\sigma = 0$, so the assertion holds. Let $n > 1$. Then by (13) we have that n is odd and $n \geq 7$, so $\gcd(4, n) = 1$, and 4 is a unit of the ring $\mathbb{Z}_n$. For any $\alpha \in \mathbb{Z}_n$ we get (cf. (18)) (i) $\alpha^2 - \alpha + 1 = 0 \Leftrightarrow$ (ii) $(2\alpha - 1)^2 = -3$. Since n is odd and $\gcd(n, -3) = 1$, (ii) has 2^σ solutions in $\mathbb{Z}_n$ ([10, p. 65, Theorem 5-2]). As $\alpha \mapsto 2\alpha - 1$ is bijective from $\mathbb{Z}_n$ into itself, (i) has 2^σ solutions, too, so by (20) $\operatorname{card} S_0(\mathbb{Z}_n) = 2^\sigma$. □

Theorem 3.5. *If $n \in \mathbb{M}$ and $3 \nmid n$, then $3n \in \mathbb{M}$ and there exists $q \in \mathbb{N}^0$ with $n = 6q + 1$, furthermore*

$$S_0(\mathbb{Z}_{3n}) = \{\omega_{(6q+1)\cdot 2 + 3\cdot(4q+1)t};\ \omega_t \in S_0(\mathbb{Z}_n)\}, \tag{21}$$

$$\operatorname{card} S_0(\mathbb{Z}_{3n}) = \operatorname{card} S_0(\mathbb{Z}_n). \tag{22}$$

Proof. For $n = 1$ we have $S_0(\mathbb{Z}_n) = \{\omega_0\}$, $S_0(\mathbb{Z}_{3n}) = \{\omega_2\}$, $q = 0$, $t = 0$, so $(6q+1)\cdot 2 + 3(4q+1)t = 2$, i.e., (21) and (22) hold. Let in the following $n > 1$. Then by (13) $3n \in \mathbb{M}$, n is odd and $n \geq 7$, and all prime divisors of n are $\equiv_6 1$. So there exists $q \in \mathbb{N}$ with $n = 6q + 1$. Since $\gcd(3, n) = 1$, we have a ring isomorphism $\varphi : \mathbb{Z}_{3n} \cong \mathbb{Z}_3 \times \mathbb{Z}_n$,

$$\varphi : 3n\mathbb{Z} + \ell \mapsto (3\mathbb{Z} + \ell, n\mathbb{Z} + \ell) \quad (\forall \ell \in \mathbb{Z}). \tag{23}$$

If $\omega_t \in S_0(\mathbb{Z}_n)$, then by [17, Lemma 2.3(a)] $\omega_2 \times \omega_t \in S_0(\mathbb{Z}_3 \times \mathbb{Z}_n)$. The elements $3n\mathbb{Z} + 1$, $3\mathbb{Z} + 1$, $n\mathbb{Z} + 1$ are generators of $\mathbb{Z}_{3n}$, $\mathbb{Z}_3$, $\mathbb{Z}_n$, respectively.

$$\begin{array}{ccccccc} \mathbb{Z}_{3n} & \xrightarrow{\varphi} & \mathbb{Z}_3 \times \mathbb{Z}_n & \xrightarrow{\omega_2 \times \omega_t} & \mathbb{Z}_3 \times \mathbb{Z}_n & \xrightarrow{\varphi^{-1}} & \mathbb{Z}_{3n} \\ 3n\mathbb{Z} + 1 & \longmapsto & (3\mathbb{Z} + 1, n\mathbb{Z} + 1) & \longmapsto & (3\mathbb{Z} + 2, n\mathbb{Z} + t) & \longmapsto & 3n\mathbb{Z} + s \end{array}$$

In this diagram, s is to be determined. $\varphi^{-1}(3\mathbb{Z} + 2, n\mathbb{Z} + t) = 3n\mathbb{Z} + s$ implies $\varphi(3n\mathbb{Z} + s) = (3\mathbb{Z} + 2, n\mathbb{Z} + t)$, so by (23) $(3\mathbb{Z} + s, n\mathbb{Z} + s) = (3\mathbb{Z} + 2, n\mathbb{Z} + t)$, i.e., $3\mathbb{Z} + s = 3\mathbb{Z} + 2$, $n\mathbb{Z} + s = n\mathbb{Z} + t$, so $s \equiv_3 2$ and $s \equiv_n t$. From the Chinese remainder theorem we obtain $s = (6q+1)\cdot 2 + 3(4q+1)t$. Therefore, $\varphi^{-1} \circ (\omega_2 \times \omega_t) \circ \varphi = \omega_{(6q+1)\cdot 2 + 3(4q+1)t}$, so (21) holds. (22) follows from [17, Lemma 2.3(a)] and $\operatorname{card} S_0(\mathbb{Z}_3) = 1$ or from (21) and
$t \equiv_n t' \Leftrightarrow (6q+1)\cdot 2 + 3(4q+1)t \equiv_{3n} (6q+1)\cdot 2 + 3(4q+1)t' \quad (\forall t, t' \in \mathbb{Z})$. □

Example 3.6. $n = 21$, so $n \in \mathbb{M}$. $S_0(\mathbb{Z}_3) = \{\omega_2\}$, $S_0(\mathbb{Z}_7) = \{\omega_3, \omega_5\}$ [17, Example 2.12]. So by Theorem 3.5 with $q = 1$: $S_0(\mathbb{Z}_{21}) = \{\omega_{7\cdot 2 + 3\cdot 5t};\ t \in \{3, 5\}\} = \{\omega_{14+15\cdot 3};\ \omega_{14+15\cdot 5}\} = \{\omega_{59}, \omega_{89}\} =_{(\text{on } \mathbb{Z}_{21})}= \{\omega_{17}, \omega_5\}$. By the way,

ω_{17} and ω_5 in $S_0(\mathbb{Z}_{21})$ are inverses of each other and $\omega_{17} + \omega_5 = \omega_1 = i_{\mathbb{Z}_{21}}$ as it must be by Theorem 2.5(a).

Remark 3.7. If $n \in \mathbb{M}$ and $n > 3$, then part (ii)$\Rightarrow$(i) Case 2, of the proof of Theorem 3.2 shows that -3 is a quadratic residue mod n (cf. (17)). So there exists $\gamma_1 \in \mathbb{Z}_n$ such that $\gamma_1^2 = -3$ in $\mathbb{Z}_n$. For $\gamma_2 := -\gamma_1$, we also have $\gamma_2^2 = -3$. Assume that $\gamma_2 = \gamma_1$. Then $-\gamma_1 = \gamma_1$, so $2\gamma_1 = 0$, and the oddness of n implies $\gamma_1 = 0$, a contradiction to $\gamma_1^2 = -3$. Therefore $\gamma_1 \neq \gamma_2$. Let $\alpha_1, \alpha_2 \in \mathbb{Z}_n$ such that $2\alpha_\nu - 1 = \gamma_\nu$ $(\nu = 1, 2)$. Since $2 \in U(\mathbb{Z}_n)$, $\alpha_1 \neq \alpha_2$, and $2\alpha_1 = 1 + \gamma_1$, $2\alpha_2 = 1 + \gamma_2 = 1 - \gamma_1$. Therefore $2\alpha_1 + 2\alpha_2 = 2$, $2\alpha_1 \cdot 2\alpha_2 = 1 - \gamma_1^2 = 1 + 3 = 4$. $2, 4 \in U(\mathbb{Z}_n)$ imply

$$\alpha_1 + \alpha_2 = 1, \quad \alpha_1 \cdot \alpha_2 = 1, \tag{24}$$

and by (18) $\alpha_{1,2}^2 - \alpha_{1,2} + 1 = 0$. So for $n \in \mathbb{M}$, $n > 3$, pairs of mutually inverse functions in $S_0(\mathbb{Z}_n)$ stem from pairs $(\gamma_1, -\gamma_1)$ with $\gamma_1^2 = -3$.

Remark 3.8. The proof of Theorem 3.2 shows that solving (1) over $\mathbb{Z}_n$ is dependent on solving $X^2 = -3$ in $\mathbb{Z}_n$. The situation is satisfactory as long as only solvability is concerned. On the other hand, it is unpleasant that there is no general systematic calculation method for the solutions of $X^2 = -3$ in $\mathbb{Z}_n$, not even when n is a prime number. Enjoyable exceptional cases are $n \in \mathbb{P}$, $n \equiv_6 1$ and ($n \equiv_4 3$ or $n \equiv_8 5$) (cf. [5, p. 42], [9, p. 133], [18, p. 287]). For proceeding from the solutions over $\mathbb{Z}_{p^{\ell-1}}$ to those over $\mathbb{Z}_{p^\ell}$ $(p \in \mathbb{P})$ cf, e.g., [1, p. 182] or [19, p. 240/241].

4. Solutions of (1) for $G = K^\ell$

We first put together some auxiliary facts for later purposes.

Remark 4.1. The rings $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{0, \dots, n-1\}$ $(n \in \mathbb{N})$ and $\mathbb{Z}_0 := \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ constitute the complete list of all prime rings of rings with identity element 1; $\mathbb{Z}_1 = \mathbb{Z}/1\mathbb{Z} = \{0\}$ is the only trivial ring among them: $1 = 0$ in $\mathbb{Z}_1$. The list of all prime fields consists of $\mathbb{Q}$ and all $\mathbb{Z}_n$ with $n \in \mathbb{P}$ [7, pp. 108–109, 213].

Remark 4.2. For every set J and every $n \in \mathbb{N}^0$ there is exactly one way to make the abelian group $\mathbb{Z}_n^{(J)}$ (for this notation cf. the paragraph before Lemma 1.4) into a free unitary $\mathbb{Z}_n$-module; for $n = 1$, $\mathbb{Z}_n^{(J)}$ degenerates to $\{0\}$. All these modules are dimensional in the sense that any two of their bases are of the same cardinality, and one defines

$$\dim_{\mathbb{Z}_n} \mathbb{Z}_n^{(J)} := \operatorname{card} J \ (n \in \mathbb{N}^0 \setminus \{1\}), \quad \dim_{\mathbb{Z}_1} \mathbb{Z}_1^{(J)} := 0,$$

([3, p. 150–151]), also valid for $J = \emptyset$. For any fixed $n \in \mathbb{N}^0$, $\dim_{\mathbb{Z}_n} M$ characterizes the free $\mathbb{Z}_n$-module M up to isomorphism. The analogue holds for $\mathbb{Q}$-vector spaces.

Lemma 4.3. (a) *For $K \in \{\mathbb{Q}, \mathbb{Z}_n;\ n \in \mathbb{N}^0\}$, the set* $\mathrm{End}\,(K^{(J)})$ *of additive mappings $f : K^{(J)} \to K^{(J)}$ is precisely the set* $\mathrm{Hom}_K(K^{(J)}, K^{(J)})$ *of K-linear mappings from $K^{(J)}$ into itself.*

(b) *If K is a commutative ring with identity $1 \neq 0$ and $\ell \in \mathbb{N}$, then, with respect to every ordered basis Φ of K^ℓ, $f \in \mathrm{Hom}_K(K^\ell, K^\ell)$ has a matrix representation exactly as in the case of a scalar field: The basis Φ induces a K-algebra isomorphism Ω_Φ from* $\mathrm{Hom}_K(K^\ell, K^\ell)$ *to the K-algebra $K^{\ell\times\ell}$ of all $\ell \times \ell$-matrices over K.*

Proof. (a) K is a prime ring (field), and the homogeneity ring $H_f := \{\alpha \in K;\ f(\alpha x) = \alpha f(x)\ (\forall x \in K^{(J)})\}$ of every $f \in \mathrm{End}\,(K^{(J)})$ is a subring of K; if K is a field, so is H_f [13, Lemma 1]. As K has no proper subring (subfield), we get $H_f = K$, so f is K-linear.

(b) [20, p. 293, Theorem 29.2]. □

Lemma 4.4. *If K is a commutative ring with $1 \neq 0$, if $\ell \in \mathbb{N}$, and if $f \in \mathrm{Hom}_K(K^\ell, K^\ell)$, $A := \Omega_\Phi(f) \in K^{\ell\times\ell}$, then*

$$f \in S_0(K^\ell) \Leftrightarrow A^2 - A + I = 0 \tag{M}$$

where $I \in K^{\ell\times\ell}$ is the identity matrix and $0 \in K^{\ell\times\ell}$ the zero matrix.

Proof. Since $\mathrm{Hom}_K(K^\ell, K^\ell) \subset \mathrm{End}\,(K^\ell)$, (B5) implies $f \in S_0(K^\ell) \Leftrightarrow$ (3) $f^2 - f + i_{K^\ell} = \underline{0}$, and by Lemma 4.3(b) this latter is equivalent to $A^2 - A + I = 0$. □

Remark 4.5. By (M) the quadratic matrix equation

$$A^2 - A + I = 0 \quad (A \in K^{\ell\times\ell},\ \ell \in \mathbb{N}), \tag{3'}$$

where K is a commutative ring with $1 \neq 0$, becomes of central importance. The following consequences of (3') for $A \in K^{\ell\times\ell}$ are easily established:

(a) $A^3 = -I$,
(b) A is invertible, $A^{-1} = I - A$,
(c) $(A^{-1})^2 - A^{-1} + I = 0$,
(d) $B \in K^{\ell\times\ell}$ is invertible $\Rightarrow (B^{-1}AB)^2 - B^{-1}AB + I = 0$.

They reflect properties of solutions of (1)$\wedge$(0): (a), (B4); (b), Theorem 2.5(a); (c), Theorem 2.5(a); (d), [17, Remark 1.1(a)].

We consider Eq. (3') now for some other class of rings than prime rings.

Lemma 4.6. *For a commutative ring K with 1 and the property $2 := 1 + 1 \in U(K)$, for $\ell \in \mathbb{N}$ and $A \in K^{\ell\times\ell}$, the following statements are equivalent:*

(i) $A^2 - A + I = 0$,
(ii) $(2A - I)^2 = -3I$.

[Here K can be, e.g., $\mathbb{Z}_n$ ($n \in \mathbb{N}$ is odd, $n > 1$) or $\mathbb{Q}$, but neither $\mathbb{Z}_1$ (=$\{0\}$) nor $\mathbb{Z}_n$ ($n \in \mathbb{N}^0$ is even)].

Proof. Since $2 \in U(K)$, also $4 \in U(K)$, and we have (i) $A^2 - A + I = 0 \Leftrightarrow 4A^2 - 4A + 4I = 0 \Leftrightarrow 4A^2 - 4A + I = -3I \Leftrightarrow$ (ii) $(2A - I)^2 = -3I$. □

Remark 4.7. The equivalence of (i) and (ii) in Lemma 4.6 is based upon the possibility of successfully completing the square and proceeding as in the classical case of a scalar quadratic equation over a field. For contrasting situations, where the matrices involved in the equation do not commute, cf. [8, Section 3.2].

Lemma 4.8. *If K is a totally ordered commutative ring with* 1 *and the property* $2 \in U(K)$, *and if* $\ell \in \mathbb{N}$ *is odd, then there is no* $A \in K^{\ell\times\ell}$ *such that* $A^2 - A + I = 0$.

Proof. Assume that there exists $C \in K^{\ell\times\ell}$ with $C^2 = -3I$. Then (cf. [11, p. 166] and [21, p. 688,691]) $0 \le (\det C)^2 = \det(C^2) = \det(-3I) = (-3)^\ell = -3^\ell < 0$, a contradiction. So C cannot exist, and by Lemma 4.6, neither can A. □

Several subsequent statements concern the case $\ell \in \mathbb{N}$ is odd. For even $\ell \in \mathbb{N}^0$, we recall Lemma 1.4 where $S_0(G^\ell) \neq \emptyset$ is ensured.

Corollary 4.9. $S_0(\mathbb{Q}^\ell) = \emptyset$ *for odd* $\ell \in \mathbb{N}$. *(For* $\ell = 1$ *cf.* [17, Example 2.13]*).*

Proof. Injectivity of $\omega_2 : \mathbb{Q}^\ell \to \mathbb{Q}^\ell$ and (B8) imply $S_0(\mathbb{Q}^\ell) \subset \mathrm{End}\,(\mathbb{Q}^\ell) =_{\text{Lemma 4.3(a)}} = \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}^\ell, \mathbb{Q}^\ell)$. Now (M) in Lemma 4.4 is available for $K = \mathbb{Q}$, so $S_0(\mathbb{Q}^\ell) = \emptyset$ follows from Lemma 4.8. □

Next we extend [17, Corollary 2.2] from $\mathbb{R}^1$ to higher dimensions. In this context, $\mathbb{R}^\ell$ ($\ell \in \mathbb{N}^0$) is supposed to be furnished with the unique $\mathbb{R}$-linear Hausdorff topology, i.e., the topology of, e.g., the euclidean norm on $\mathbb{R}^\ell$ [22, p. 192, Theorem 1].

Theorem 4.10. *If* $\ell \in \mathbb{N}^0$, *then*

(a) *Every continuous* $f \in S_0(\mathbb{R}^\ell)$ *is* $\mathbb{R}$*-linear.*
(b) *For odd* $\ell \in \mathbb{N}$, *there are no continuous functions in* $S_0(\mathbb{R}^\ell)$.
(c) $S_0(\mathbb{R}^\ell) \neq \emptyset$.

Proof. (a) Let $f \in S_0(\mathbb{R}^\ell)$ be continuous. Since $\omega_2 : \mathbb{R}^\ell \to \mathbb{R}^\ell$ is injective, $f \in \mathrm{End}\,(\mathbb{R}^\ell)$ by (B8). By [13, Lemma 1], f is $\mathbb{Q}$-linear. Let $x \in \mathbb{R}^\ell$, $\lambda \in \mathbb{R}$ be arbitrary. Then there are $\alpha_n \in \mathbb{Q}$ ($n \in \mathbb{N}$) with $\alpha_n \to \lambda$ ($n \to \infty$). So $\alpha_n x \to \lambda x$ ($n \to \infty$). Continuity of f implies $f(\alpha_n x) \to f(\lambda x)$ ($n \to \infty$). But $f(\alpha_n x) = \alpha_n f(x) \to \lambda f(x)$. Uniqueness of limits in $\mathbb{R}^\ell$ ensures $f(\lambda x) = \lambda f(x)$. Since $x \in \mathbb{R}^\ell$, $\lambda \in \mathbb{R}$ were arbitrary, f is $\mathbb{R}$-homogeneous, so in the total $\mathbb{R}$-linear. (b) Assume that f were in $S_0(\mathbb{R}^\ell)$ and continuous. By (a) f would be $\mathbb{R}$-linear. (M) in Lemma 4.4 is available for $K = \mathbb{R}$. By Lemma 4.8, f cannot exist. (c) For every $\ell \in \mathbb{N}^0$, $\mathbb{R}^\ell$ is a $\mathbb{Q}$-vector space of dimension 0 (for $\ell = 0$) or $2^{\aleph_0}$, and the assertion follows from (5) in Lemma 1.4. By virtue of (b), $S_0(\mathbb{R}^\ell)$ consists of discontinuous functions if $\ell \in \mathbb{N}$ is odd. For $\ell = 1$ cf. [2, p. 300, Corollary 4]. □

As a further essential contrast to Theorem 4.10(b) we have:

Lemma 4.11. *For $\ell \in \mathbb{N}^0$ there do exist continuous functions f in $S_0(\mathbb{R}^{2\ell})$.*

Proof. For $\ell = 0$ we have $f := \underline{0} \in S_0(\{0\})$. For $\ell = 1$ we take $f_1 \in S_0(\mathbb{R}^2)$ given by (4) in Lemma 1.3, and for $\ell \geq 2$ the ℓ-fold direct sum $f_1 \oplus \cdots \oplus f_1$ of f_1 with itself, which is in $S_0(\mathbb{R}^{2\ell})$ by [17, Lemma 2.3(a)]. All these functions are $\mathbb{R}$-linear and, since $\mathbb{R}^{2\ell}$ is finite-dimensional over $\mathbb{R}$, continuous. □

Corollary 4.12. *For every $\ell \in \mathbb{N}^0$ there are continuous functions in $S_0(\mathbb{C}^\ell)$. (For $\ell = 1$ cf.* [2, p. 301, Corollary 5]*).*

Proof. The isomorphism of topological groups $\varphi : \mathbb{R}^{2\ell} \cong \mathbb{C}^\ell$, $\varphi : (\xi_1, \ldots, \xi_\ell, \eta_1, \ldots, \eta_\ell) \mapsto (\xi_1 + i\eta_1, \ldots, \xi_\ell + i\eta_\ell)$ transforms continuous functions f in $S_0(\mathbb{R}^{2\ell})$ into continuous functions $g = \varphi \circ f \circ \varphi^{-1}$ in $S_0(\mathbb{C}^\ell)$ [17, Remark 1.1.(a)]. The assertion follows from Lemma 4.11. □

Finally, we deal with the problem of existence of solutions of (1) for $G = \mathbb{Z}_n^\ell$ ($n \in \mathbb{N}^0$, $\ell \in \mathbb{N}^0$).

Lemma 4.13. $S_0(\mathbb{Z}^\ell) = \emptyset$ *($\forall \ell \in \mathbb{N}$ is odd). (Remember $\mathbb{Z} = \mathbb{Z}_0$). (For $\ell = 1$ cf.* [17, p. 192, Example 2.7]*).*

Proof. Let $\ell \in \mathbb{N}$ be odd and assume $f \in S_0(\mathbb{Z}^\ell)$. Injectivity of $\omega_2 : \mathbb{Z}^\ell \to \mathbb{Z}^\ell$ and (B8) imply $f \in \operatorname{End}(\mathbb{Z}^\ell)$. By Lemma 4.3(a) $f \in \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}^\ell, \mathbb{Z}^\ell)$, and by Lemma 4.4 there exists $A \in \mathbb{Z}^{\ell \times \ell}$ with $A^2 - A + I = 0$. We put $A = (\alpha_{ij})$, $B = (\beta_{ij}) := A^2 - A + I$. For every $i \in \{1, \ldots, \ell\}$, $\beta_{ii} = \sum_j \alpha_{ij}\alpha_{ji} - \alpha_{ii} + 1 = \alpha_{ii}^2 + \sum_{j \neq i} \alpha_{ij}\alpha_{ji} - \alpha_{ii} + 1$. Now $\sum_i \sum_{j \neq i} \alpha_{ij}\alpha_{ji} = \sum_i (\sum_{j<i} \alpha_{ij}\alpha_{ji} + \sum_{j>i} \alpha_{ij}\alpha_{ji}) = \sum_{i,j;\, j<i} \alpha_{ij}\alpha_{ji} + \sum_{i,j;\, j>i} \alpha_{ij}\alpha_{ji} = 2\sum_{i,j;\, j<i} \alpha_{ij}\alpha_{ji} \in 2\mathbb{Z}$, furthermore $\alpha_{ii}^2 - \alpha_{ii} \in 2\mathbb{Z}$, so $\operatorname{tr} B = \sum_i \beta_{ii} \in 2\mathbb{Z} + \ell$, and the oddness of ℓ prevents $\operatorname{tr} B$ from being 0, a contradiction to $B = 0$. So f cannot exist, and the assertion holds. □

Lemma 4.14. $S_0(\mathbb{Z}_n^\ell) = \emptyset$ *($\forall n \in \mathbb{N}$ is even, $\forall \ell \in \mathbb{N}$ is odd). (For $\ell = 1$ cf.* [17, Corollary 2.11]*; Lemma 4.13 is the case $n = 0$).*

Proof. $\mathbb{Z}_n^\ell[2]^* := \{x \in \mathbb{Z}_n^\ell;\ \operatorname{ord} x = 2\}$ consists of all ℓ-tuples of elements 0 and $n/2$ of $\mathbb{Z}_n$ except $(0, \ldots, 0)$ (ℓ times). Therefore

$$\operatorname{card} \mathbb{Z}_n^\ell[2]^* = 2^\ell - 1. \tag{25}$$

Assume that $f \in S_0(\mathbb{Z}_n^\ell)$. By Lemma 1.2, $f(\mathbb{Z}_n^\ell[2]^*) \subset \mathbb{Z}_n^\ell[2]^*$, and the bijectivity of f (Lemma 1.1) enforces $f(\mathbb{Z}_n^\ell[2]^*) = \mathbb{Z}_n^\ell[2]^*$. By Lemma 1.5(b)

$$f^3(x) = x \quad (\forall x \in \mathbb{Z}_n^\ell[2]^*). \tag{26}$$

There is no $y \in \mathbb{Z}_n^\ell[2]^*$ with $f^2(y) = y$: Otherwise $f^2(y) =_{(26)}= f^3(y)$, so by the bijectivity of f: $y = f(y)$, in contradiction to $y \neq 0$, $f(0) = 0$ and [17, Lemma 2.4]. So f has no 2-cycle in $\mathbb{Z}_n^\ell[2]^*$ and by (26) no 6-cycle in $\mathbb{Z}_n^\ell[2]^*$. By Lemma 2.1(c), f has therefore only 3-cycles in $\mathbb{Z}_n^\ell[2]^*$, so by (25) $3|(2^\ell - 1)$.

But since ℓ is odd, say $\ell = 2v+1 \quad (\exists v \in \mathbb{N}^0)$, $2^\ell - 1 = 2^{2v+1} - 1 = 4^v \cdot 2 - 1 \equiv_3 2 - 1 = 1$, which is a contradiction. So f cannot exist, and the assertion holds. □

[For even ℓ, we do have $3|(2^\ell - 1)$, so that the latter contradiction does not arise, as it must be by (5) in Lemma 1.4.]

Lemma 4.15. *If $n \in \mathbb{N}$ and $\ell \in \mathbb{N}$ are odd and if there exists $d \in \mathbb{N}$ with $d|n$ and $d \equiv_6 5$, then $S_0(\mathbb{Z}_n^\ell) = \emptyset$.*

Proof. By the hypothesis on d and Remark 3.1(a), n has a prime divisor $p \equiv_6 5$. For $H := (\frac{n}{p}) \cdot \mathbb{Z}_n$ we have $H = \mathbb{Z}_n[p] := \{\xi \in \mathbb{Z}_n;\ p\xi = 0\}$ and $\operatorname{card} H = p$ ([6, p. 34, Exercise 4]). Since $p \in \mathbb{P}$, we have moreover $H = \{0\} \dot\cup \mathbb{Z}_n[p]^*$, and $H^\ell[p]^*$ consists of all ℓ-tuples of elements of H except $(0, \dots, 0)$ (ℓ times), so

$$\operatorname{card} H^\ell[p]^* = p^\ell - 1. \tag{27}$$

Assume that $f \in S_0(\mathbb{Z}_n^\ell)$. By Lemma 1.2 $f(H^\ell[p]^*) \subset H^\ell[p]^*$, and the bijectivity of f (Lemma 1.1) guarantees that $f(H^\ell[p]^*) = H^\ell[p]^*$. Since $pH^\ell = \{0\}$ and $2\not| p$, $3\not| p$, Corollary 2.4(ii) ensures that $H^\ell[p]^*$ consists of 6-cycles only. Therefore by (27) $6|(p^\ell - 1)$. On the other hand, since $p \equiv_6 5$ and ℓ is odd, say $\ell = 2u+1 \quad (\exists u \in \mathbb{N}^0)$, we have $p^\ell - 1 = p^{2u+1} - 1 = p^{2u}p - 1 \equiv_6 p - 1 \equiv_6 4$, a contradiction. So f cannot exist, and the assertion holds. □

(For even ℓ, $p^\ell - 1 \equiv_6 0$, so that no contradiction occurs, as it must be by Lemma 1.4).

The singular role of the prime number 3 (cf. (13)) requires a special procedure in the investigation of $S_0(\mathbb{Z}_{3^k}^\ell)$ for $k \in \mathbb{N}$, $k \geq 2$. Lemma 4.16 was inspired by [12].

Lemma 4.16. *For odd $\ell \in \mathbb{N}$, $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p|a$, $p^2\not| a$, $k \in \mathbb{N}$, $k \geq 2$ there is no $X \in \mathbb{Z}^{\ell\times\ell}$ with $X^2 \equiv aI \pmod{p^k}$, where $I \in \mathbb{Z}^{\ell\times\ell}$ is the identity matrix. ($U \equiv V \pmod{p^k}$ for $U, V \in \mathbb{Z}^{\ell\times\ell}$ means that $[U]_{ij} \equiv_{p^k} [V]_{ij}$ for all $i, j \in \{1, \dots, \ell\}$).*

Proof. We first note that

$$\text{if } B \in \mathbb{Z}^{\ell\times\ell},\ m \in \mathbb{Z},\ B \equiv pmI \pmod{p^2}, \text{ then there exists } Q \in \mathbb{Z}^{\ell\times\ell} \text{ such that } B = pQ \text{ and } Q \equiv mI \pmod{p}. \tag{28}$$

$p|a$ implies the existence of $m \in \mathbb{Z}$ with $a = pm$, and $p^2\not| a$ enforces $a \neq 0$. Therefore $m \neq 0$, so $\gcd(m, p) \in \{1, p\}$; but $\gcd(m, p) = p$ would mean $p|m$, so $p^2|mp$, i.e., $p^2|a$, contradicting the hypothesis. So

$$\gcd(m, p) = 1. \tag{29}$$

Suppose that there exists $X \in \mathbb{Z}^{\ell\times\ell}$ with $X^2 \equiv aI \pmod{p^2}$, i.e., $X^2 \equiv pmI \pmod{p^2}$. By (28) there exists $Q \in \mathbb{Z}^{\ell\times\ell}$ with $X^2 = pQ$ and $Q \equiv mI \pmod{p}$. Therefore

$$\det Q \equiv_p \det(mI) \equiv_p m^\ell. \tag{30}$$

(29) implies $\gcd(m^\ell, p) = 1$, so by (30)

$$\gcd(\det Q, p) = 1. \tag{31}$$

Clearly $p^\ell | \det(pQ)$. Assume $p^{\ell+1} | \det(pQ)$, say $p^{\ell+1}v = \det(pQ) = p^\ell \det Q$, i.e., $pv = \det Q$, i.e., $p | \det Q$, a contradiction to (31). Therefore, since $X^2 = pQ$ and $\det(X^2) = (\det X)^2$,

$$p^\ell | (\det X)^2 \quad \text{and} \quad p^{\ell+1} \not| (\det X)^2. \tag{32}$$

By the second formula of (32), $(\det X)^2 \neq 0$, and the oddness of ℓ makes (32) impossible. So

$$\text{there is no } X \in \mathbb{Z}^{\ell\times\ell} \text{ with } X^2 \equiv aI \pmod{p^2}, \tag{33}$$

and since $p^2 | p^k$, (33) implies the assertion of Lemma 4.16. □

Lemma 4.17. *For odd $\ell \in \mathbb{N}$, $k \in \mathbb{N}$, $k \geq 2$ there is no $C \in \mathbb{Z}_{3^k}^{\ell\times\ell}$ with $C^2 = -3I$, where $I \in \mathbb{Z}_{3^k}^{\ell\times\ell}$ is the identity matrix.*

Proof. Every element α of $\mathbb{Z}_{3^k}$ $(= \mathbb{Z}/3^k\mathbb{Z})$ is of the form $a' + 3^k\mathbb{Z}$ with $a' \in \mathbb{Z}$, and in every set $a' + 3^k\mathbb{Z}$ there is exactly one $a \in \{0, \ldots, 3^k - 1\}$; we define

$$\psi : \mathbb{Z}_{3^k} \longrightarrow \mathbb{Z}, \quad \psi : a' + 3^k\mathbb{Z} \longmapsto a. \tag{34}$$

If $\pi : \mathbb{Z} \to \mathbb{Z}_{3^k}$ is the canonical ring epimorphism, then $\pi \circ \psi = i_{\mathbb{Z}_{3^k}}$, so ψ is a lifting for $\mathbb{Z}_{3^k}$. The following properties of ψ are easily established:

$$\psi(0 + 3^k\mathbb{Z}) = 0, \quad \psi(1 + 3^k\mathbb{Z}) = 1, \tag{35}$$

$$\psi(\alpha + \beta) \equiv_{3^k} \psi(\alpha) + \psi(\beta) \quad (\forall \alpha, \beta \in \mathbb{Z}_{3^k}), \tag{36}$$

$$\psi(\alpha \cdot \beta) \equiv_{3^k} \psi(\alpha) \cdot \psi(\beta) \quad (\forall \alpha, \beta \in \mathbb{Z}_{3^k}), \tag{37}$$

$$(\psi \circ \pi)(a) \equiv_{3^k} a \quad (\forall a \in \mathbb{Z}). \tag{38}$$

We assume on the contrary that there exists $C = (\gamma_{ij}) \in \mathbb{Z}_{3^k}^{\ell\times\ell}$ with $C^2 = -3I$. A useful notation is $L := \{m \in \mathbb{N};\ 1 \leq m \leq \ell\}$. From $C : L \times L \to \mathbb{Z}_{3^k}$ we construct $X : L \times L \to \mathbb{Z}$ by $X = (\xi_{ij}) := \psi \circ C$, i.e. $\xi_{ij} = \psi(\gamma_{ij}) \quad (\forall (i,j) \in L \times L)$. For arbitrary $(i,j) \in L \times L$ we get $[X^2]_{ij} = \sum_\nu [X]_{i\nu}[X]_{\nu j} = \sum_\nu \xi_{i\nu}\xi_{\nu j} = \sum_\nu \psi(\gamma_{i\nu}) \cdot \psi(\gamma_{\nu j}) \equiv_{(36),(37)} \equiv_{3^k} \psi(\sum_\nu \gamma_{i\nu}\gamma_{\nu j}) = \psi([C^2]_{ij}) = \psi([-3I]_{ij}) = \psi(-3\delta_{ij} + 3^k\mathbb{Z}) \equiv_{(35),(38)} \equiv_{3^k} -3\delta_{ij}$. Since $(i,j) \in L \times L$ was arbitrary, we have $X^2 \equiv -3I \pmod{3^k}$, and because ℓ is odd, $a = -3$, $p = 3$, $p|a$, $p^2 \not| a$, and $k \in \mathbb{N}$, $k \geq 2$, Lemma 4.16 denies the existence of such an X in $\mathbb{Z}^{\ell\times\ell}$. So C cannot exist either. □

Lemma 4.18. *For odd $\ell \in \mathbb{N}$, $k \in \mathbb{N}$, $k \geq 2$, we have $S_0(\mathbb{Z}_{3^k}^\ell) = \emptyset$.*

Proof. $\mathbb{Z}_{3^k}$ is a commutative ring with 1, and $2 \in U(\mathbb{Z}_{3^k})$. By Lemma 4.17 there is no $C \in \mathbb{Z}_{3^k}^{\ell\times\ell}$ with $C^2 = -3I$, so by Lemma 4.6

$$\text{there is no } A \in \mathbb{Z}_{3^k}^{\ell\times\ell} \text{ with } A^2 - A + I = 0. \tag{39}$$

Assume that $f \in S_0(\mathbb{Z}_{3^k}^\ell)$. Injectivity of $\omega_2 : \mathbb{Z}_{3^k}^\ell \to \mathbb{Z}_{3^k}^\ell$ and (B8) imply $f \in \mathrm{End}\,(\mathbb{Z}_{3^k}^\ell)$. By Lemma 4.3(a) $f \in \mathrm{Hom}_{\mathbb{Z}_{3^k}}(\mathbb{Z}_{3^k}^\ell, \mathbb{Z}_{3^k}^\ell)$, and by Lemma 4.4 there exists $A \in \mathbb{Z}_{3^k}^{\ell\times\ell}$ with $A^2 - A + I = 0$, which is a contradiction to (39). So f cannot exist, i.e., the assertion holds. □

Remark 4.19. Because $0 \notin \mathbb{M}$, $2\mathbb{N} \cap \mathbb{M} = \emptyset$, $\{n \in \mathbb{N};\ \exists d \in \mathbb{N},\ d|n,\ d \equiv_6 5\} \cap \mathbb{M} = \emptyset$, $3^k \notin \mathbb{M}$ ($k \in \mathbb{N}$, $k \geq 2$) (cf. (13)), Lemmas 4.13, 4.14, 4.15, and 4.18 confirm, for $\ell = 1$, Theorem 3.2.

Theorem 4.20. *For $n, \ell \in \mathbb{N}^0$ we have* (i) $S_0(\mathbb{Z}_n^\ell) = \emptyset \Leftrightarrow$ (ii) *ℓ is odd and $n \notin \mathbb{M}$.*

Proof. (i) $\Rightarrow$ (ii). If ℓ were even, then by Lemma 1.4 $S_0(\mathbb{Z}_n^\ell) \neq \emptyset$, contradicting (i). So ℓ is odd. Assume $n \in \mathbb{M}$. Then by Theorem 3.2, $S_0(\mathbb{Z}_n) \neq \emptyset$, so by [17, Lemma 2.3(a)] $S_0(\mathbb{Z}_n^\ell) \neq \emptyset$, which is impossible. Therefore $n \notin \mathbb{M}$.
(ii) $\Rightarrow$ (i). Let ℓ be odd and $n \notin \mathbb{M}$. Case 1: $n \in 2\mathbb{N}^0$. Then (i) holds by Lemma 4.13 or 4.14. Case 2: n is odd. By (13)
Case 2a: $\exists d \in \mathbb{N}$ with $d|n$, $d \equiv_6 5$ and/or
Case 2b: $\exists k \in \mathbb{N}$ with $k \geq 2$, $3^k|n$.
In Case 2a, (i) holds by Lemma 4.15.
In Case 2b, $S_0(\mathbb{Z}_{3^k}^\ell) = \emptyset$ by Lemma 4.18. Without loss of generality, let $k \geq 2$ such that $3^{k+1} \nmid n$. Then there exists $q \in \mathbb{N}$ with $n = 3^k q$ and $\gcd(3^k, q) = 1$. It follows that $\mathbb{Z}_n \cong \mathbb{Z}_{3^k} \times \mathbb{Z}_q$, hence $\mathbb{Z}_n^\ell \cong (\mathbb{Z}_{3^k} \times \mathbb{Z}_q)^\ell \cong \mathbb{Z}_{3^k}^\ell \times \mathbb{Z}_q^\ell$. Assume $S_0(\mathbb{Z}_n^\ell) \neq \emptyset$. By Lemma 2.10(a) we obtain $S_0(\mathbb{Z}_{3^k}^\ell) \neq \emptyset$, a contradiction to Lemma 4.18. Therefore $S_0(\mathbb{Z}_n^\ell) = \emptyset$, i.e., (i) holds. □

References

[1] Bachmann, P.: Niedere Zahlentheorie. Teubner, Leipzig (1902)
[2] Balcerowski, M.: On the functional equation $x + f(y + f(x)) = y + f(x + f(y))$. Aequ. Math. **75**, 297–303 (2008)
[3] Bourbaki, N.: Eléments de Mathématique, Livre II: Algèbre. chapitre 2. Hermann, Paris (1962)
[4] Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 5th edn. Clarendon Press, Oxford (1979)
[5] Hua, L.K.: Introduction to Number Theory. Springer, New York (1982)
[6] Jacobson, N.: Lectures in Abstract Algebra, vol. I. Van Nostrand, Princeton (1966)
[7] Jacobson, N.: Basic Algebra I. Freeman, New York (1985)
[8] Jivulescu, M.A., Napoli, A., Messina, A.: Elementary symmetric functions of two solvents of a quadratic matrix equation. Rep. Math. Phys. **62**, 369–387 (2008)
[9] Lehmer, D.H.: Computer technology applied to the theory of numbers. In: Studies in Number Theory, pp. 117–151. The Mathematical Association of America (1969)
[10] LeVeque, W.J.: Topics in Number Theory, vol. I. Addison-Wesley, Reading (1965)
[11] MacLane, S., Birkhoff, G.: Algebra. Macmillan, New York (1968)
[12] Pall, G., Taussky, O.: Scalar matrix quadratic residues. Mathematika **12**, 94–96 (1965)
[13] Rätz, J.: On the homogeneity of additive mappings. Aequ. Math. **14**, 67–71 (1976)

[14] Rätz, J.: On the functional equation $x + f(y + f(x)) = y + f(x + f(y))$, II. Report of meeting. Aequ. Math. **84**, 301–302 (2012)
[15] Rätz, J.: On the functional equation $x + f(y + f(x)) = y + f(x + f(y))$, III. Report of meeting. Aequ. Math. **86**, 305 (2013)
[16] Rätz, J.: On the functional equation $x + f(y + f(x)) = y + f(x + f(y))$, IV. Report of meeting. Aequ. Math. (to appear)
[17] Rätz, J.: On the functional equation $x + f(y + f(x)) = y + f(x + f(y))$. Aequ. Math. **86**, 187–200 (2013)
[18] Riesel, H.: Prime Numbers and Computer Methods for Factorization. Birkhäuser, Boston (1985)
[19] Sierpiński, W.: Elementary theory of numbers (A. Schinzel, ed.). Polish Scientific Publishers, Warszawa (1987)
[20] Warner, S.: Modern Algebra, vol. I. Prentice-Hall, Englewood Cliffs (1965)
[21] Warner, S.: Modern Algebra, vol. II. Prentice-Hall, Englewood Cliffs (1965)
[22] Wilansky, A.: Functional Analysis. Blaisdell, New York (1964)

Jürg Rätz
Mathematisches Institut der Universität Bern
Sidlerstrasse, 3012 Bern
Switzerland
e-mail: math@math.unibe.ch

Received: April 14, 2014