# Polyfunctions over Commutative Rings 

Ernst Specker ${ }^{1}$, Norbert Hungerbühler ${ }^{2}$, and Micha Wasem ${ }^{3}$<br>${ }^{1}$ Dedicated to the memory of the first author<br>2 Department of Mathematics, ETH Zürich, Rämistrasse 101, 8092 Zürich, Switzerland<br>${ }^{3}$ HTA Freiburg, HES-SO University of Applied Sciences and Arts Western Switzerland, Pérolles 80, 1700 Freiburg, Switzerland

September 7, 2022


#### Abstract

A function $f: R \rightarrow R$, where $R$ is a commutative ring with unit element, is called polyfunction if it admits a polynomial representative $p \in R[x]$. Based on this notion we introduce ring invariants which associate to $R$ the numbers $s(R)$ and $s\left(R^{\prime} ; R\right)$, where $R^{\prime}$ is the subring generated by 1 . For the ring $R=$ $\mathbb{Z} / n \mathbb{Z}$ the invariant $s(R)$ coincides with the number theoretic Smarandache or Kempner function $s(n)$. If every function in a ring $R$ is a polyfunction, then $R$ is a finite field according to the Rédei-Szele theorem, and it holds that $s(R)=|R|$. However, the condition $s(R)=|R|$ does not imply that every function $f: R \rightarrow R$ is a polyfunction. We classify all finite commutative rings $R$ with unit element which satisfy $s(R)=|R|$. For infinite rings $R$, we obtain a bound on the cardinality of the subring $R^{\prime}$ and for $s\left(R^{\prime} ; R\right)$ in terms of $s(R)$. In particular we show that $\left|R^{\prime}\right| \leqslant s(R)$ !. We also give two new proofs for the Rédei-Szele theorem which are based on our results.


## 1 Introduction

For a commutative ring $R$ with unit element, a function $f: R \rightarrow R$ is said to be a polyfunction if there exists a polynomial $p \in R[x]$ such that $f(x)=p(x)$ for all $x \in R$ (see [11, 9], and also [1, 2] for a discussion on polyfunctions from
$\left.\mathbb{Z}_{m} \rightarrow \mathbb{Z}_{n}\right)$. The set of polyfunctions over $R$ equipped with pointwise addition and multiplication forms a subring

$$
G(R):=\{f: R \rightarrow R, \exists p \in R[x] \forall x \in R \Longrightarrow p(x)=f(x)\}
$$

of $R^{R}$ and will be called the ring of polyfunctions over $R$. The polynomials in $R[x]$ which represent the zero element in $G(R)$ are called null-polynomials (see [13]). If $S$ is a subring of $R$, then

$$
G(S ; R):=\{f: R \rightarrow R, \exists p \in S[x] \forall x \in R \Longrightarrow p(x)=f(x)\},
$$

is a natural subring of $G(R)$. In particular, the subring $R^{\prime}$ generated by the unit element 1 in $R$ gives rise to the integer polyfunctions $G\left(R^{\prime} ; R\right)$. Instead of restricting the ring of allowed coefficients as in the construction for $G(S ; R)$, one obtains other rings of polyfunctions by restricting the domain: The ring

$$
\{f: S \rightarrow R, \exists p \in R[x] \forall x \in S \Longrightarrow p(x)=f(x)\}
$$

e.g. contains $G(R)$ as a subring.

If $S$ is a subring of $R$, a characteristic number connected to $S$ and $R$ is the minimal degree $m$ such that the function $x \mapsto x^{m}$ can be represented by a polynomial in $S[x]$ of degree strictly smaller than $m$. Then, in particular, every function in $G(S ; R)$ has a polynomial representative of degree strictly less than $m$. We set

$$
s(S ; R):=\min \left\{m \in \mathbb{N}, \exists p \in S[x], \operatorname{deg}(p)<m, \forall x \in R \Longrightarrow p(x)=x^{m}\right\}
$$

and $s(R):=s(R ; R)$ for brevity. We set $s(S ; R):=\infty$ if no function $x \mapsto x^{m}$ can be represented by a polynomial of degree strictly smaller than $m$.

Trivially, we have $s(S ; R) \geqslant s(T ; R) \geqslant s(R)$ whenever $S \subset T$ are subrings of $R$. On the other hand, we will see in Section 3, that $s\left(R^{\prime} ; R\right)<\infty$ is bounded in terms of $s(R)$ if $s(R)<\infty$.

Clearly, if two rings $R_{1}, R_{2}$ are isomorphic, then $s\left(R_{1}\right)=s\left(R_{2}\right)$ and $s\left(R_{1}^{\prime}, R_{1}\right)=$ $s\left(R_{2}^{\prime}, R_{2}\right)$. In other words, $R \mapsto s(R)$ and $R \mapsto s\left(R^{\prime}, R\right)$ are ring invariants.

The function $s$, which associates to a given ring $R$ the number $s(R) \in \mathbb{N} \cup\{\infty\}$ has been introduced in [5] and is called Smarandache function. This naming stems from the fact, that for all $2 \leqslant n \in \mathbb{N}$, the map $n \mapsto s(\mathbb{Z} / n \mathbb{Z})$ coincides with the well-known number theoretic Smarandache or Kempner function $s$ (see [5, Theorem 2]) defined by

$$
\begin{equation*}
s(n):=\min \{k \in \mathbb{N}, n \mid k!\} \tag{1}
\end{equation*}
$$

(see Lucas [8], Neuberg [10] and Kempner [6]). In fact, Legendre has already studied aspects of the function $s(n)$ : In [7] he showed that if $n=p^{\mu}$ for some prime $p$ and $1 \leqslant \mu \in \mathbb{N}$, then $s(n)$ verifies

$$
s(n)=\mu(p-1)+a_{0}+a_{1}+\ldots+a_{k}
$$

where the numbers $a_{i}$ are the digits of $s(n)$ in base $p$. i.e. $s(n)=a_{k} p^{k}+\ldots+a_{0}$ and $0 \leqslant a_{i}<p$. We refer to Dickson [3, p. 263-265] for the history of the function $s(n)$.

In a finite field $F$, every function is a polyfunction as a polynomial respresentative of a function $f: F \rightarrow F$ is, e.g., given by the Lagrange interpolation polynomial for $f$. This representation property characterizes finite fields among commutative rings with unit element (see [12]):

Theorem 1 (Rédei, Szele). If $R$ is a commutative ring with unit element then $R$ is a finite field if and only if every function $f: R \rightarrow R$ can be represented by $a$ polynomial in $R[x]$.

We will include two short alternative proofs of this theorem in Section 4. For finite fields $F$, one has $s(F)=|F|$, so in view of Theorem 1 , it is natural to ask what can be said about commutative rings $R$ with unit element for which $s(R)=|R|$ holds true. Note that if $R$ is a finite ring, it trivially holds that $s(R) \leqslant|R|$, as the polynomial

$$
p(x)=\prod_{y \in R}(x-y)
$$

is a normed null-polynomial of degree $|R|$.
The following theorem (which will be restated below for the reader's convenience as Theorem 3), answers the above question and classifies all finite commutative rings $R$ with unit element that satisfy $s(R)=|R|$ :

Theorem. Let $R$ be a finite commutative ring with unit element. Then, $s(R)=$ $|R|$ holds if and only if $R$ is one of the following:
(a) $R$ is a finite field, or
(b) $R$ is $\mathbb{Z}_{4}$, or
(c) $R$ is the ring $\rho$ with four elements $\{0,1, a, 1+a\}$ with $1+1=0$ and $a^{2}=0$.

## Remarks:

1. The ring $\rho$ is not a field since it has zero divisors, and since it is of characteristic 2 , it is not isomorphic to $\mathbb{Z}_{4}$.
2. Observe the similarity between this result and the fact that for $n \geqslant 2$, the usual Smarandache function satisfies $s(n)=n$ if and only if $n$ is prime or $n=4$.

Section 2 is devoted to the proof of this theorem. In Section 3 we discuss infinite rings and show that for an infinite commutative ring $R$ with unit element and $s(R)<\infty$, we obtain an upper bound for $\left|R^{\prime}\right|$ and for $s\left(R^{\prime} ; R\right)$ in terms of $s(R)$, where $R^{\prime}$ is the subring of $R$ generated by 1. Finally, in Section 4 we give two proofs of Theorem 1 - a direct one and one that is based on Theorem 3.

Throughout the article, $n \geqslant 2$ will denote a natural number, and $\mathbb{Z}_{n}=\mathbb{Z} / n \mathbb{Z}$ is the ring of integers modulo $n$, and we write $a \mid b$ if $b$ is an integer multiple of $a$.

## 2 Polyfunctions over Finite Rings

Theorem 1 answered the question, when a ring $R$ has the property, that every function $f: R \rightarrow R$ can be represented by a polynomial in $R[x]$. For finite rings a necessary (but not sufficient) condition for this property to hold is

$$
\begin{equation*}
s(R)=|R|, \tag{2}
\end{equation*}
$$

(see Theorem 3 below). In this section, we want to address the question for which finite rings, equation (2) holds. The first step to answer this, is the following proposition:

Proposition 2. If $R$ is a commutative ring with unit element and with zero divisors then either
(a) there exist $a, b \in R \backslash\{0\}$ with $a \neq b$ and $a b=0$, or
(b) $R$ is $\mathbb{Z}_{4}$, or
(c) $R$ is the ring $\rho$ with four elements $\{0,1, a, 1+a\}$ with $1+1=0$ and $a^{2}=0$.

## Proof

Let us assume that in $R$ the implication holds: if $u, v \in R \backslash\{0\}$ and $u v=0$ then it follows $u=v$. Let $a \in R \backslash\{0\}$ be a zero divisor: $a^{2}=0$. Thus, if $x$ is an element
in $R$ with $a x=0$, we have either $x=0$ or $x=a$. Notice that for all $u \in R$ we have

$$
a(a u)=0
$$

and hence for all $u \in R$

$$
a u=0 \text { or } a(u-1)=0 .
$$

Hence, we have only the four cases $u=0$ or $u=a$ or $u=1$ or $u=1+a$. If $1+1=a$, then $R=\mathbb{Z}_{4}$, if $1+1=0$, then $R$ is the $\operatorname{ring} \rho$ in (c).

We can now prove the main result of this section:
Theorem 3. Let $R$ be a finite commutative ring with unit element. Then, $s(R)=$ $|R|$ holds if and only if $R$ is one of the following:
(a) $R$ is a finite field, or
(b) $R$ is $\mathbb{Z}_{4}$, or
(c) $R$ is the ring $\rho$ with four elements $\{0,1, a, 1+a\}$ with $1+1=0$ and $a^{2}=0$.

## Proof

If $R$ is not a field and not $\mathbb{Z}_{4}$ and not the ring $\rho$, then, according to Proposition 2 , $R$ is a ring with $a, b \in R \backslash\{0\}$ such that $a b=0$ and with $a \neq b$. Then

$$
(x-a)(x-b) \prod_{z \in R \backslash\{a, b, 0\}}(x-z)
$$

is a normed null-polynomial of degree $|R|-1$. Therefore $s(R)<|R|$.
To prove the opposite direction, we go through the three cases:
(a) If $R$ is a field, then a polynomial of degree $n$ has at most $n$ roots. Hence, $s(R)=|R|$.
(b) If $R$ is $\mathbb{Z}_{4}$, then (by [5, Theorem 2]) $s\left(\mathbb{Z}_{4}\right)=s(4)=4=\left|\mathbb{Z}_{4}\right|$.
(c) If $R$ is the ring $\rho$ with elements $\{0,1, a, 1+a\}$ and with $1+1=0$ and $a^{2}=0$, we have to prove that $s(R)=4$. Assume by contradiction, that $p(x) \in R[x]$ is a normed null-polynomial of degree 3 . Since $p(0)=p(1)=0, p(x)$ must be of the form

$$
p(x)=x(x+1)(\xi+x) .
$$

From $p(a)=0$, it follows that $a \xi=0$ and from $p(a+1)=0$ it subsequently follows that $a=0$ which is a contradiction.

## 3 Infinite Rings

In this section $R$ is a commutative ring with unit element and $R^{\prime}$ the subring of $R$ which is generated by 1 . We will need the following lemma, which is a corollary of [5, Lemma 4, p.4]:
Lemma 4. For all $k, n \in \mathbb{N} \cup\{0\}, k \leqslant n$ we have

$$
\sum_{j=0}^{n}(-1)^{n-j}\binom{n}{j} j^{k}=\delta_{k n} n!
$$

(with the convention $0^{0}:=1$ ).
Proposition 5. If $s(R)<\infty$ then $R^{\prime}$ is a finite ring and $\left|R^{\prime}\right| \mid s(R)$ !.
Remark: We notice, that $s(R)<\infty$ may hold even if $R$ is an infinite ring. As an example consider the ring

$$
R=\mathbb{Z}_{2}\left[x_{1}, x_{2}, \ldots\right] /\left\{x_{1}^{2}, x_{2}^{2}, \ldots\right\}
$$

in which all $u \in R$ satisfy the relation $u^{4}=u^{2}$. On the other hand, if $R$ is finite, we trivially have $s(R) \leqslant|R|$.

## Proof of Proposition 5

By assumption, for $n=s(R)$ there exist coefficients $a_{i} \in R, i \in\{0,1, \ldots n-1\}$, such that for all $u \in R$ we have

$$
\begin{equation*}
u^{n}-\sum_{i=0}^{n-1} a_{i} u^{i}=0 . \tag{3}
\end{equation*}
$$

We denote

$$
\underbrace{1+1+\ldots+1}_{m \text { times }} \in R^{\prime}
$$

by $\bar{m}$. Then, by Lemma 4 , we have for $k \leqslant n$

$$
\begin{equation*}
\sum_{j=0}^{n} \overline{(-1)^{n-j}\binom{n}{j} j^{k}}=\overline{\delta_{k n} n!} \tag{4}
\end{equation*}
$$

Hence, it follows from (3) that

$$
\begin{aligned}
0 & =\sum_{j=0}^{n} \overline{(-1)^{n-j}\binom{n}{j}}\left(\bar{j}^{n}-\sum_{i=0}^{n-1} a_{i} \bar{j}^{i}\right)= \\
& =\sum_{j=0}^{n} \overline{(-1)^{n-j}\binom{n}{j} j^{n}}-\sum_{i=0}^{n-1} a_{i} \sum_{j=0}^{n} \overline{(-1)^{n-j}\binom{n}{j} j^{i}}=\overline{n!}
\end{aligned}
$$

where the last equality follows from (4).

Remark: As the example $R=\mathbb{Z}_{n}$ ! shows, the estimate on the size of $R^{\prime}$ emerging from Proposition $5,\left|R^{\prime}\right| \leqslant s(R)$ !, cannot be improved in general.

Lemma 6. If $n:=s(R)<\infty$ then there exists a bound $\Lambda=n!^{(2 n)^{n} n}$ for the cardinality of the orbits of the elements of $R$, i.e., for all $u \in R$ there holds

$$
\left|\left\{u^{k}, k \in \mathbb{N}\right\}\right| \leqslant \Lambda .
$$

## Proof

As in the previous proof, we adopt (3). For $k \in \mathbb{N}$ let

$$
\begin{aligned}
M_{k} & :=\left\{\prod_{i=0}^{n-1} a_{i}^{\varepsilon_{i}}, \varepsilon_{i} \in\{0,1, \ldots, k\}\right\} \\
N_{k} & :=\left\{\sum_{\mu \in M_{k}} \overline{r_{\mu}} \mu, r_{\mu} \in\{0,1, \ldots, n!-1\}\right\} .
\end{aligned}
$$

Observe that $\left|M_{k}\right| \leqslant(k+1)^{n}$ and $\left|N_{k}\right| \leqslant n!!^{\left|M_{k}\right|}$. By Proposition 5 it follows that for $a, b \in N_{k}$, the sum $a+b$ also belongs to $N_{k}$. On the other hand, by applying (3) to $u=a_{j}^{2}, j \in\{0,1, \ldots, n-1\}$, we obtain

$$
a_{j}^{2 n}=\sum_{i=0}^{n-1} a_{i} a_{j}^{2 i}
$$

and hence, $N_{k}=N_{k-1}$ for $k \geqslant 2 n$. It follows for all $u \in R$ and all $k \in \mathbb{N}$ that $u^{k}$ is of the form

$$
u^{k}=\sum_{i=0}^{n-1} \mu_{i}(k) u^{j}
$$

for certain coefficients $\mu_{i}(k) \in N_{2 n-1}$ and hence $\left|\left\{u^{k}, k \in \mathbb{N}\right\}\right| \leqslant\left|N_{2 n-1}\right|^{n} \leqslant \Lambda$.

Theorem 7. If $n:=s(R)<\infty$ then $s\left(R^{\prime} ; R\right) \leqslant \operatorname{lcm}(\Lambda)+\Lambda$, where $\Lambda=n!(2 n)^{n} n$.

## Remarks:

(a) Here $\operatorname{lcm}(n)$ denotes the least common multiple of the numbers in the set $\{1,2, \ldots, n\}$.
(b) Since $R^{\prime}$ is contained in every subring $T$ (with 1 ) of $R$, the given bound also holds for $s(T ; R)$.

## Proof of Theorem 7

By Lemma 6, there exist for arbitrary $u \in R$ integers $l<k \leqslant \Lambda+1$ such that $u^{k}=u^{l}$. Thus, we have

$$
u^{\operatorname{lcm}(\Lambda)+\Lambda}=u^{\operatorname{lcm}(\Lambda)+\Lambda-\frac{\operatorname{lcm}(\Lambda)}{k-l}(k-l)}=u^{\Lambda} .
$$

We conclude this section by an example of a ring $R$ which has the property, that $s(R)<s\left(R^{\prime}, R\right)$.
Example: Let $R=\mathbb{Z}_{2}[x] /\left\{x^{3}+x^{4}\right\}$.
The following lemma shows that for this particular ring $s(R) \leqslant 4$.
Lemma 8. For all polynomials $P \in \mathbb{Z}_{2}[x]$ we have that

$$
x P+(1+x) P^{2}+P^{4} \equiv 0 \quad \bmod \left(x^{3}+x^{4}\right) .
$$

## Proof

We first consider the special case $P(x)=x^{m}$. We have to show, that

$$
x x^{m}+(1+x) x^{2 m}+x^{4 m}=x^{m+1}+x^{2 m}+x^{2 m+1}+x^{4 m} \equiv 0 \quad \bmod \left(x^{3}+x^{4}\right) .
$$

This is readily checked:

$$
\begin{array}{lrl}
m=0: & x+1+x+1 \equiv 0 & \bmod \left(x^{3}+x^{4}\right) \\
m=1: & x^{2}+x^{2}+x^{3}+x^{4} \equiv 0 & \bmod \left(x^{3}+x^{4}\right) \\
m \geqslant 2: & x^{3}+x^{3}+x^{3}+x^{3} \equiv 0 & \bmod \left(x^{3}+x^{4}\right)
\end{array}
$$

Now, for arbitrary $P$, the claim follows by additivity in $\mathbb{Z}_{2}[x]$ :

$$
x\left(P_{1}+P_{2}\right)+(1+x)\left(P_{1}+P_{2}\right)^{2}+\left(P_{1}+P_{2}\right)^{4}=\sum_{i=1}^{2} x P_{i}+(1+x) P_{i}^{2}+P_{i}^{4}
$$

Remark: We leave it to the reader to verify, that in fact $s(R)=4$.
Now, we show that $s\left(R^{\prime} ; R\right) \geqslant 6$.
Lemma 9. Let $a_{i} \in \mathbb{Z}_{2}$ be such that $\sum_{i=0}^{5} a_{k} u^{k}=0$ in $R$ for all $u \in R$. Then $a_{0}=\cdots=a_{5}=0$.

## Proof

First, by choosing $u$ to be the class of $x$ in $R$ (which we denote by $\bar{x}$ ), we obtain

$$
a_{0}+a_{1} \bar{x}+a_{2} \bar{x}^{2}+\left(a_{3}+a_{4}+a_{5}\right) \bar{x}^{3}=0 \quad \text { in } R
$$

and hence, we conclude that $a_{0}=a_{1}=a_{2}=0$ and $a_{3}+a_{4}+a_{5}=0$. Next, we choose $u$ to be the class of $1+x$ in $R$. Observing that

$$
\begin{aligned}
& (1+\bar{x})^{3}=1+\bar{x}+\bar{x}^{2}+\bar{x}^{3} \text { in } R \\
& (1+\bar{x})^{4}=1+\bar{x}^{4}=1+\bar{x}^{3} \text { in } R \\
& (1+\bar{x})^{5}=1+\bar{x}
\end{aligned} \quad \text { in } R \text { }
$$

we have

$$
\begin{aligned}
0 & =a_{3} u^{3}+a_{4} u^{4}+a_{5} u^{5}= \\
& =\left(a_{3}+a_{4}+a_{5}\right)+\left(a_{3}+a_{5}\right) \bar{x}+a_{3} \bar{x}^{2}+\left(a_{3}+a_{4}\right) \bar{x}^{3} \text { in } R
\end{aligned}
$$

which immediately implies that $a_{3}=a_{4}=a_{5}=0$. This completes the proof.

Finally we prove that $s\left(R^{\prime} ; R\right)=6$.
Lemma 10. For all $u \in R$ it holds that $u^{3}+u^{4}+u^{5}+u^{6}=0$ in $R$.

## Proof

Let $u$ be the class of a polynomial $P \in \mathbb{Z}_{2}[x]$ in $R$.
First case: $P(0)=0$. In this case, we have

$$
\begin{aligned}
P(x) & =x Q(x) \\
P^{2}(x) & \equiv x^{2} Q^{2}(x) \quad \bmod \left(x^{3}+x^{4}\right) \\
P^{3}(x) & \equiv x^{3} Q^{3}(x) \equiv x^{3} Q(1) \quad \bmod \left(x^{3}+x^{4}\right) \\
P^{4}(x) & \equiv x^{4} Q^{4}(x) \equiv x^{3} Q(1) \quad \bmod \left(x^{3}+x^{4}\right)
\end{aligned}
$$

and hence $P^{3}(x) \equiv P^{4}(x) \bmod \left(x^{3}+x^{4}\right)$. This proves the claim in this case.
Second case: $P(0)=1$. In this case, we have

$$
\begin{aligned}
P(x) & =1+x Q(x) \\
P^{2}(x) & \equiv 1+x^{2} Q^{2}(x) \quad \bmod \left(x^{3}+x^{4}\right) \\
P^{3}(x) & \equiv(1+x Q(x))\left(1+x^{2} Q^{2}(x)\right) \equiv \\
& \equiv 1+x Q(x)+x^{2} Q^{2}(x)+x^{3} Q(1) \quad \bmod \left(x^{3}+x^{4}\right) \\
P^{4}(x) & \equiv 1+x^{4} Q^{4}(x) \equiv 1+x^{3} Q(1) \quad \bmod \left(x^{3}+x^{4}\right) \\
P^{5}(x) & \equiv(1+x Q(x))\left(1+x^{3} Q(1)\right) \equiv 1+x Q(x) \equiv P(x) \quad \bmod \left(x^{3}+x^{4}\right)
\end{aligned}
$$

which allows to verify the claim easily.

## 4 Two Alternative Proofs of the Rédei-Szele Theorem

We start with a short direct proof of Theorem 1 Let $R$ be a commutative ring with unit element. One implication is immediate:

Assume that $R$ is a finite field and $f: R \rightarrow R$. Then the Lagrange interpolation polynomial

$$
p(x)=\sum_{y \in R} f(y) p_{y}(x),
$$

where

$$
p_{y}(x)=\prod_{z \in R \backslash\{y\}}(x-z)\left(\prod_{z \in R \backslash\{y\}}(y-z)\right)^{-1},
$$

represents $f$.
For the opposite implication, we assume that every function $f: R \rightarrow R$ can be represented by a polynomial in $R[x]$. In particular, for the function

$$
f(x):=\left\{\begin{aligned}
-1, & \text { if } x=0 \\
0, & \text { if } x \neq 0
\end{aligned}\right.
$$

there exists a representing polynomial

$$
\sum_{k=0}^{n} a_{k} x^{k}=f(x) \quad \text { for all } x \in R
$$

Since $a_{0}=f(0)=-1$, it follows that

$$
x \underbrace{\sum_{k=1}^{n} a_{k} x^{k-1}}_{=x^{-1}}=\sum_{k=1}^{n} a_{k} x^{k}=1 \quad \text { for all } x \in R \backslash\{0\} .
$$

Hence, $R$ is a field. Moreover, for all $x \in R$

$$
\begin{equation*}
0=x f(x)=\sum_{k=0}^{n} a_{k} x^{k+1} \tag{5}
\end{equation*}
$$

The right hand side of (5) is a polynomial of degree $n+1$ which (in the field $R$ ) has at most $n+1$ roots. Hence, $|R| \leqslant n+1$.

A second alternative proof uses the characterization of the rings for which $s(R)=$ $|R|$ (see Theorem 3 ). This condition is necessary for the property, that all functions from $R$ to $R$ have a polynomial representative. In order to rule out the case $R=\mathbb{Z}_{4}$, we use the following formula from [4, Theorem $6, \mathrm{p} .9$ ]: If $p$ is a prime number and $m \in \mathbb{N}$, the number of polyfunctions over $\mathbb{Z}_{p^{m}}$ is given by

$$
\Psi\left(p^{m}\right):=\left|G\left(\mathbb{Z}_{p^{m}}\right)\right|=\exp _{p}\left(\sum_{k=1}^{m} s\left(p^{k}\right)\right)
$$

Here $s$ denotes the usual number theoretic Smarandache function (see equation (1)), and $\exp _{p}(q):=p^{q}$ for better readability. It follows that there are $\Psi(4)=\Psi\left(2^{2}\right)=$ $2^{2+4}=64$ polyfunctions over $\mathbb{Z}_{4}$, but the number of functions from $\mathbb{Z}_{4}$ to $\mathbb{Z}_{4}$ equals $4^{4}=256$. The case $R=\rho$ is ruled out by explicit verification that

$$
f(x)= \begin{cases}0 & \text { for } x \neq 0 \text { and } \\ 1 & \text { for } x=0\end{cases}
$$

is not a polyfunction over $\rho$ : Since $s(\rho)=4$, it is enough to show that no polynomial $p \in \rho[x]$ of degree $\leqslant 3$ represents $f$. Suppose there is

$$
p(x)=\sum_{k=0}^{3} a_{k} x^{k}
$$

representing $f$. Then $p(0)=a_{0}=1$ and $p(a)=1+a_{1} a=0$, which implies that $a_{1} a=1$ which is impossible since $a$ does not have a multiplicative inverse.

## References

[1] M. Bhargava: Congruence preservation and polynomial functions from $\mathbb{Z}_{n}$ to $\mathbb{Z}_{m}$. Discrete Math. 173 (1997), no. 1-3, 15-21.
[2] Z. Chen: On polynomial functions from $\mathbb{Z}_{n}$ to $\mathbb{Z}_{m}$. Discrete Math. 137 (1995), no. 1-3, 137-145.
[3] L. E. Dickson: History of the Theory of Numbers, vol. 1. Carnegie Institution of Washington Publication, 1919.
[4] N. Hungerbühler, E. Specker: A generalization of the Smarandache function to several variables. Integers 6 (2006): Paper A23, 11 p.
[5] N. Hungerbühler, E. Specker, M. Wasem: The Ring of Polyfunctions over $\mathbb{Z} / n \mathbb{Z}$. Comm. Algebra, Published online: 17 July 2022, DOI: https://doi.org/10.1080/00927872.2022.2092628.
[6] A. J. Kempner: Concerning the smallest integer $m$ ! divisible by a given integer $n$. Amer. Math. Monthly 25 (1918), 204-210.
[7] A. M. Legendre: Essai sur la théorie des nombres, 2nd edition, Paris: Courcier, 1808.
[8] E. Lucas: Question $\times 288$. Mathesis 3 (1883), 232.
[9] G. Mullen, H. Stevens: Polynomial functions $(\bmod m)$. Acta Math. Hungar. 44 (1984), no. 3-4, 237-241.
[10] J. Neuberg: Solutions de questions proposées, ${ }^{\times}$Question 288. Mathesis 7 (1887), 68-69.
[11] L. Rédei, T. Szele: Algebraisch-zahlentheoretische Betrachtungen über Ringe. I. Acta Math. 79, (1947), 291-320.
[12] L. Rédei, T. Szele: Algebraisch-zahlentheoretische Betrachtungen über Ringe. II. Acta Math. 82, (1950), 209-241.
[13] D. Singmaster: On polynomial functions $(\bmod m)$. J. Number Theory 6 (1974), 345-352.

