Open Access Library Journal
2017, Volume 4, e4116
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Derivatives over Certain Finite Rings

Soud K. Mohamed

Department of Mathematics, School of Mathematical Sciences, University of Dodoma, Dodoma, Tanzania
Email: shkhalifa@hotmail.com

How to cite this paper: Mohamed, S.K. (2017) Derivatives over Certain Finite Rings. *Open Access Library Journal*, **4**: e4116.
https://doi.org/10.4236/oalib.1104116

Received: November 3, 2017
Accepted: December 17, 2017
Published: December 20, 2017

Abstract

We introduce a derivative of a relation over the ring of integers modulo an odd number which is based on the very fundamental concepts which helped in the evolution of derivative of a function over the real number field, namely slope. Then, for a prime field $GF(p)$, we use the derivatives to construct an algorithm that find all the directions, in the sense of Redei [1], of graphs of certain exponential relations over *R*.

Subject Areas

Algebra, Combinatorial Mathematics

Keywords

Relations, Derivatives, Directions

1. Introduction

Derivative plays a very fundamental role in the analysis of functions over the real and the complex number fields. In these fields, their properties and applications are well-studied, since they reflect well on our everyday lives. Over finite rings the notion of a derivative first appeared some 75 year ago in the paper by Hasse [2]. This derivative is the so called Hasse derivative, and has been successfully used in areas where finite fields play an important role, such as Coding Theory as reported by Massey, von Seeman, Schoeller [3].

Suppose that *R* is a commutative ring and let $f(x)=\sum_{n=1}^{n} a_i x^i$ be a polynomial over *R*. Then *r*th-Hasse derivative of $f(x)$ is $f^{[r]}(x)=\sum_{i=0}^{n}\binom{i}{r}a_i x^{i-r}$ with $\binom{i}{r}=0$ for $i<r$. It is well-known that over a finite field K all functions are polynomial. In fact, if $|K|=m$, then there are m^m functions over *K*. In addition, there is a 1-1 correspondence between a function $f:K\to K$ and poly-

nomial of degree less than *m*. So with Hasse derivatives one has every thing as far as a derivative of a function over *K*.

If R is a finite commutative ring, then only a fraction of functions on R are polynomials as shown by Frisch [4]. So for a function f on R which can not be represented by a polynomial over *R*, its Hasse derivative can not be determined. The aim of this paper is to introduce a derivative on a set of relations on certain rings.

Suppose that R is a finite ring and consider a relation ρ on R in a variable *x*, which shall be usually denoted by $\rho(x)$. Then the image of ρ may sometimes be an array, see de Souza, de Oliveira, de Souza, Vasconcelos [5]. For instance, the image of a function on R is an $s\times 1$-array. In Section 2 we will look into exponential relations and their arrays over the ring $R=\mathbb{Z}_n$ for an integer *n*, and then we give sufficient conditions for an exponential relation to be a function over *R*.

Let R be the finite ring $\mathbb{Z}_n$, where *n* is an odd integer. Given a relation ρ, and a point $a\in R$, what should be the derivative of ρ at *a*? In real analysis we take the slope of a tangent line at *a*, provided it exists. Moreover for a relation on the real number fields, we have at lest one slope at a point: one along each column (picture the derivative of $\sqrt{x}$). Over a finite field this is not possible, because a point has more than one tangent! In addition, slopes of tangents can be computed along a column of ρ as well as across it. In Section 3 we show that the slope of the closest secant to a point $x\in R$ along a column *k* is the best candidate for the derivative of ρ at *x*, which shall be denoted by $Dr_k^{(1)}(\rho(x))$ or simply $\rho_k^{(1)}(x)$, the *k*-th derivative of ρ at *x*. This derivative has similar properties as the derivative of the real number field, like: linearity; product and quotient rules and how it acts on polynomials and exponential relations. The definition of the derivative requires some ordering of the elements of *R*. In Section 1, we consider the ring R as cyclically ordered set, which is very natural since R is a finite set.

Let $R=\mathbb{F}_q$ be a finite field with *q* elements and let $\rho:R\to R$ be a relation. Define the set of directions of ρ (slopes of secants of the graph of ρ) by:

$$D(\rho):=\left\{\frac{\rho(a)-\rho(b)}{a-b}\mid a\neq b\in R\right\} \tag{1}$$

The problem of determining the bound on the size of $D(\rho)$ has be studied extensively both geometrically and combinatorically. The problem was first examined Blockhuis, Ball, Brouwer, Storme and Szonyi [6], then by Ball [7] [8] who has done an extensive investigation. However, there has not been any attempt on computing the directions themselves, so far.

Given a graph of a column of a relation ρ over *R*, the size s of the graph is the number of elements in the domain of ρ. Note that s is less than or equal to *q*. Now, ideally if one want to find all directions, one may have to compute up to $s(s-1)/2$ directions. The algorithm is as follow: you start at the first point and then find $s-1$ directions, then move to the second point and compute $s-2$

directions, and so on. Since $D(\rho)$ is a subset of *R*, as show by Ball [8] [9], there is a lot of unnecessary computations in this algorithm. In Section 4 we show that for some relations ρ over prime fields, the derivatives of ρ_k is all one needs to find all the directions of the graph of ρ.

2. Preliminaries

In this section we collect some of the preliminaries that will be needed in this paper. We fix the following notation: If *R* is a ring with unity, then R^* will denote the group of units of *R*. Unless otherwise specified, by order of an element $a \in R$ we mean the multiplicative order of *a*.

Throughout the paper, $\mathbb{Z}_n$ will denote the set all modulo integers $a \bmod n$, which is a class containg all integers *b* such that $n \mid (b-a)$. The $\gcd(a,b)$ denote the greatest common divisor of integers *a* and *b*, which is unique.

2.1. Immediate Successor and Predecessor

Most people are very familiar with linear ordering. However, cyclic order is not a household term. We give a formal definition of cyclic order and use it to define some terminologies as explained by Garcia-Colin, Montejano, Montejano, Oliveros [10].

Let *X* be a set of at least 3 elements. A ternary relation *C* is a subset of the Cartesian product $X \times X \times X$ which satisfies the following axioms:

1) *Cyclicity*: if $[a,b,c]$ is in *C*, then $[b,c,a]$ is in *C*.

2) *Asymmetry*: if $[a,b,c]$ is in *C*, then $[c,b,a]$ is not in *C*.

3) *Transitivity*: if $[a,b,c]$ and $[a,c,d]$ are in *C*, then $[a,b,d]$ is in *C*.

4) *Totality* or *Completeness*: if *a*, *b* and *c* are distinct, then either $[a,b,c]$ is in *C* or $[c,b,a]$ is in *C*.

If *C* satisfies the first three axioms, then it is called *partial cyclic ordering* on *X*, and consequently the pair (X,C) is a *partially cyclically ordered* set. If *C* satisfies all four axioms, it is called (*total*) *cyclic ordering* on *X*, as a result we get *cyclically ordered* set (X,C).

If a cyclically ordered set *X* is finite of cardinality *n*, then there is a 1-1 correspondence between *X* and the cyclically ordered set $\{1,2,\cdots,n,1\}$. We can use this correspondence to identify positions on *X*. Now, let *X* be a finite cyclically ordered set and let $x \in X$ be at position *i* (using the above correspondence), where *i* is an integer. Then the element in the position $i+1$ will be called an *immediate successor* of *x*, and will be denoted by x_+, while that in the position $i-1$ will be called *immediate predecessor* of *x* and will be denoted by x_-.

2.2. Unity Ordering

Let *G* be a finite group. The cyclic orderings on *G* which are of interest to us, are those that depend on generators of the group and the binary operation of the group. For example, for the additive group $\mathbb{Z}_5$, we have the orderings $\{1,2,3,4,0\}$, $\{3,1,4,2,0\}$, $\{2,4,1,3,0\}$ and $\{4,3,2,1,0\}$, while for the multiplicative group

$\mathbb{Z}_5^*$ we have orderings $\{2,4,3,1\}$ and $\{3,4,2,1\}$. Given a generator g of a finite cyclic group, if the group is additive, then the ordering determined by g will be referred to *g-additive cyclic ordering*, where as if the group is multiplicative, then the ordering will be referred to as *g-multiplicative cyclic ordering*.

Suppose that G is a finite cyclically ordered group of order $n \geq 3$ with a binary operation. Then G has at least one cyclic ordering, namely the one determined by each generator of *G*. For $a,b \in G$, define the *length* from *a* to *b*, denoted by $l(a,b)$, to be $b * a^{-1} \in G$, where a^{-1} is the inverse of *a*. For example, in the cyclically ordered set $\mathbb{Z}_5 = \{0,4,3,2,1\}$, we have that $l(0,3) = 3, l(2,2) = 0$, while for the multiplicative group $\mathbb{Z}_5^* = \{1,3,4,2\}$ modulo 5 which is cyclically ordered, we have $l(1,3) = 3$ and $l(3,2) = 4$.

Now, for our group G above, we have that every element $a \in G$ has an immediate predecessor and successor. Then the length $l(a,a^+)$ will be referred to as the least length of *a*, and will be denoted by $\delta(a)$. For example, for multiplicative cyclically ordered group $\mathbb{Z}_5^* = \{1,2,4,3\}$, we have that $\delta(x) = 3$ for all $x \in \mathbb{Z}_5^*$. The following fact can be easily proved.

Fact 1.1. *Let R be a ring with unity* 1_R *and isomorphic to the ring* $\mathbb{Z}_n$.

1) For any additive ordering on R the least length $\delta(a) = \delta$ is constant for all $a \in R$.

2) There is an additive ordering on R such that $\delta(a) = \delta = 1_R$.

The cyclic ordering of Fact 1.1 (2) on a ring R will be called the *unity ordering*.

For the rest of the paper, we impose the following assumption on our ring *R*:

Assumption 1.2. *R is the ring* $\mathbb{Z}_q$ *where q is an odd integer. Moreover, the ordering on R is the associated additive cyclic ordering.*

Remark 1.3. Under the above assumption our ring R will have a canonical cyclic ordering, which will be fundamental throughout the paper. Moreover, no matter what additive cyclic ordering one takes on *R*, the element $x_+ - x_- \in R$ will be a unit, since the ordering is determined by a generator of *R*.

3. Exponential and Hyperbolic Relations over *R*

In real analysis, exponential functions α^x are very fundamental, and they can easily be used to define other functions. Over finite ring, the mapping determined by α^x, for a unit α, is not necessarily a function. We have the following definition, which is motivated by de Souza, de Oliveira, Kauffman, Paschoal [5] and de Souza, de Oliveira, Kauffman, Paschoa [11].

Definition 2.1. Let $\alpha \in R$ be a unit of order *N*. Then, the exponential relation $\rho : R \to R$ is the relation $\rho(x) = \alpha^x$. The image of ρ is an $N \times t$-array $[\rho_i(x)]$ with the a-th row, $\rho(a) = \{\alpha^a, \alpha^{a+q}, \cdots, \alpha^{a+(t-1)q}\}$, where $t \leq N$. The k-th column of ρ, $\rho_k(x) = \alpha^{x+kq}$, where $x = 0,1,\cdots,N-1$, will be called the k-th exponential relation of ρ.

Example 1. We consider examples:

1) Let $R = \mathbb{Z}_7$ and consider the relation $\rho(x) = 2x \bmod 7$. Then the array of ρ is

$$\left[\rho_k(x)\right]=\begin{bmatrix}2^0 & 2^7 & 2^{14}\\ 2^1 & 2^8 & 2^{15}\\ 2^2 & 2^9 & 2^{16}\end{bmatrix}=\begin{bmatrix}2^0 & 2^1 & 2^2\\ 2^1 & 2^2 & 2^3\\ 2^2 & 2^3 & 2^1\end{bmatrix}=\begin{bmatrix}1 & 2 & 4\\ 2 & 4 & 1\\ 4 & 1 & 2\end{bmatrix}$$

2) If $R=\mathbb{Z}_9$ and our relation is $\rho(x)=2^x$, then the array of ρ is

$$\left[\rho_k(x)\right]=\begin{bmatrix}2^0 & 2^9 & 2^{18}\\ 2^1 & 2^{10} & 2^{19}\\ 2^2 & 2^{11} & 2^{20}\\ 2^3 & 2^{12} & 2^{21}\\ 2^4 & 2^{13} & 2^{22}\\ 2^5 & 2^{14} & 2^{23}\end{bmatrix}=\begin{bmatrix}1 & 8\\ 2 & 7\\ 4 & 5\\ 8 & 1\\ 7 & 2\\ 5 & 4\end{bmatrix}$$

Computation of the array of the relation in Example 1 (1.) looks easy, because along columns and rows one just increases the power by one. This is generally true for prime fields.

Lemma 2.2. *If R is a prime field, and* $\rho(x)=\alpha^x$ *is a relation on R, then the k-th relation of* ρ *is* $\rho_k(x)=\alpha^{x+k}$.

Proof. We have that

$kq \bmod N = kq-k+k \bmod N = k(q-1)+k \bmod N = k \bmod N$, since $N \mid q-1$. □

Consider the relation $\rho(x)=\alpha^x$, where $\alpha\in R$ has order *N*. Then $\rho_i(x)$ has *N* rows. However, as shown in the example above the number of columns may vary. If certain condition are satisfied, then the number of columns of the array of ρ can easily be obtained.

Theorem 2.3. *Let* α *be a unit in R of order N, and let* $\rho(x)=\alpha^x$ *be a relation.*

1) *If a perfect square is not a factor of q and* $\gcd(N,q)=1$, *then* $\left[\rho_i(x)\right]$ *is an* $N\times N$ *-array.*

2) *If* $q=p^m$ *for a prime p, where m is a positive integer, then there are* $\gcd(N,p-1)$ *columns in* $\left[\rho_i(x)\right]$.

Proof. Suppose that $\left[\rho_i(x)\right]$ is an $s\times t$ -array, and let the *a*-th row be $\rho(a)=\left\{\alpha^a,\alpha^{a+q},\alpha^{a+2q},\cdots,\alpha^{a+(t-1)q}\right\}$. Then $\rho(a)$ is a coset of the subgroup $H=\left\langle\rho^{iq}\right\rangle$ of R^* of order *t*. One can then observe that for both cases, $s=N$ and tN.

1) Now $\alpha^a=\alpha^{a+tq}$ means that $tq=0 \bmod N$ which is implies that $N\mid tq$. But since *N* does not divide *q*, it must divide *t*. Hence $t=N$.

2) We have that $H\le\langle\alpha\rangle$, since *H* contains power of α. Let *K* be a subgroup of R^* of order $p-1$. Since $\gcd\left(p^{n-1},p-1\right)=1$, then $R^* \square \mathbb{Z}_{p^{n-1}}\oplus\mathbb{Z}_{p-1}$, and hence *K* is unique. From this we infer that if $\beta\in R^*$ is such that $\beta^{p-1}=1$, then $\beta\in K$. Now we have that $\left(\alpha^{iq}\right)^{p-1}=\left(\alpha^{\phi(q)}\right)^{ip}=1$ for $i=1,\cdots,t$, so that $H\le K$. Hence $t\mid N$ and $t\mid p-1$, which implies that $t\le\gcd(N,p-1)=d$. If $d<t$, then $\alpha^{dq}=\alpha^{sNq+r(p-1)q}=1$, so that $|H|<t$, a contradiction. □

The following corollary gives a sufficient condition for an exponential relation on *R* to be a function.

Corollary 2.4. *Suppose that* $\alpha\in R$ *is unit of order N.*

1) *If a perfect square is not a factor of q and* $N\mid q$, *then the relation* $\rho(x)=\alpha^x$

is a function.

2) *If* $q = p^m$ *for a prime p and* α *has order* p^i *for* $i = 1,\cdots,m-1$, *then the relation* $\rho(x) = \alpha^x$ *is a function.*

Proof. 1) For all $a \in R$ and some positive integer *t*, we have that $\rho(a) = \left\{\alpha^a, \alpha^{a+q}, \cdots, \alpha^{a+(t-1)q}\right\} = \left\{\alpha^a\right\}$, since $N \mid q$.

2) Follows from Theorem 2.3, since $\gcd\left(p^i, p-1\right) = 1$ for $i = 1,\cdots,m-1$. □

Let $\alpha \in R$ be a unit of order *N*, and consider the relation $\rho(x) = \alpha^x$. Then ρ is periodic of period *N*. More precisely, for a positive integer *s* each subset $S_j = \left\{jN, jN+1,\cdots,(j+1)N-1\right\}$ of the domain of ρ, where $j = 0,1,\cdots,s-1$, determines the same image $\rho\left(S_j\right) = \left\{\rho(jN), \rho(jN+1),\cdots,\rho\left((j+1)N-1\right)\right\}$. The subset S_j is referred to as the *j*-th *steps* of ρ. As expected, starting at a point in *R*, there are only a finite number of steps of ρ before one gets back to the same point.

Proposition 2.5. *Let* $\alpha \in R$ *be a unit of order N, and consider the relation* $\rho(x) = \alpha^x$. *If* $\gcd(N,q) = d$, *then* ρ *has* q/d *steps.*

Proof. Let ν be the least positive integer with the property that the set $T = \left\{0, N, 2N,\cdots,(\nu-1)N\right\}$ taken $\bmod q$ has distinct elements. Observe that find number of steps of ρ is the same as finding the cardinality ν of *T*. Also note that $\nu \le q/d$. If $\nu > q/d$, then $|T| < \nu$, a contradiction. □

Corollary 2.6. *Let* $\alpha \in R$ *be a unit of order N, and consider the relation* $\rho(x) = \alpha^x$. *Then the map* $\pi = \rho_{|S_j} : S_j \to \operatorname{Im}\rho$ *is a permutation.*

Proof. Only need to show that π is 1-1. Suppose that $\pi(jN) = \pi(jN+k)$ for $k \ne 0 \bmod N$. Then $\alpha^{jN} = \alpha^{jN+k}$ which is equivalent to $k = 0 \bmod N$, a contradiction. □

We now define hyperbolic relations over *R*.

Definition 2.7. Let $\alpha \in R$ be a unit of order $N \ge 3$. Then

1) The *k*-th *hyperbolic sine and cosine relations to the base* α over *R*, denoted by $\cosh_{\alpha,k}(x)$ and $\sinh_{\alpha,k}(x)$ are respectively

$$\cosh_{\alpha,k}(x) := \frac{\alpha^{x+kq} + \alpha^{-(x+kq)}}{x_+ - x_-}; \sinh_{\alpha,k}(x) := \frac{\alpha^{x+kq} - \alpha^{-(x+kq)}}{x_+ - x_-}. \tag{2}$$

2) The *hyperbolic since and cosine relations to the base* α, denoted by $\cosh_\alpha(x)$ and $\sinh_\alpha(x)$ are the relations with images the $N \times t$ -arrays made by the columns $\cosh_{\alpha,k}(x)$ and $\sinh_{\alpha,k}(x)$, respectively, where $t < N$.

Under certain assumption on *R*, hyperbolic relations on *R* behave like those over the real.

Proposition 2.8. *Suppose that R has the unity ordering, and let* $\alpha \in R$ *be a unit of order* $N \ge 3$. *Then for* $k = 0,1,\cdots,N-1$:

1) *the identity* $\cosh^2_{\alpha,k}(x) - \sinh^2_{\alpha,k}(x) = 1_R$ *holds,*

2) $\cosh_{\alpha,k}(-x) = \cosh_{\alpha,k}(x)$ *and* $\sinh_{\alpha,k}(-x) = -\sinh_{\alpha,k}(x)$

Proof. Follows from the definition. □

4. Derivatives and Their Properties

Denote the set of relations from *R* to *R* whose image are $s \times t$ -arrays by $Rel_{st}(R)$, and by $Fun(R)$ the set of all functions from R to R.

Let q be the order of the ring R and let $x\in R$. For a positive integer k and a relation $\rho\in Rel_{st}(R)$, define a map $Dr_k^{(1)}:Rel_{st}(R)\to Rel_{st}(R)$ on the k-th relation ρ_k of ρ by

$$Dr_k^{(1)}(\rho)(x):=\frac{\rho_k(x_++kq)-\rho_k(x_-+kq)}{x_+-x_-}. \tag{3}$$

If the context is clear, then $Dr_k^{(1)}(\rho)(x)$ will be just denoted by $\rho_k^{(1)}(x)$.

If one looks closely at the this map one will notice that its value at a point $x\in R$ is the slope of the closest secant to the point x along ρ_k. It can be also interpreted as the average of the two closest slopes to x along ρ_k. The result below show that the transformation has good properties too.

Theorem 3.1. *Let* $\rho,\gamma\in Rel_{st}(R), x\in R$ *and let* $c\in\mathbb{Z}$. *Then*

1) *the transformation* $Dr_k^{(1)}$ *is linear.*

2) *Product Rule*:

$$(\rho_k\gamma_k)^{(1)}(x)=\rho_k(x_-+kq)\gamma_k^{(1)}(x)+\gamma_k(x_++kq)\rho_k^{(1)}(x) \tag{4}$$

$$=\rho_k(x_++kq)\gamma_k^{(1)}(x)+\gamma_k(x_-+kq)\rho_k^{(1)}(x). \tag{5}$$

3) *Quotient rule*: *If* $\gamma_k(x)\neq 0$ *for all* $x\in R$, *then*

$$\left(\frac{\rho_k}{\gamma_k}\right)^{(1)}=\frac{\gamma_k(x_-+kq)\rho_k^{(1)}(x)-\rho_k(x_-+kq)\gamma_k^{(1)}(x)}{\gamma(x_++kq)\gamma_k(x_-+kq)} \tag{6}$$

Proof. 1) Follows easily.

2) We use the elementary + tricks.

$$(\rho_k\gamma_k)^{(1)}(x)=\frac{(\rho_k\gamma_k)(x_++kq)-(\rho_k\gamma_k)(x_-+kq)}{x_+-x_-} \tag{7}$$

$$=\frac{\rho_k(x_++kq)\gamma_k(x_++kq)-\rho_k(x_-+kq)\gamma_k(x_-+kq)}{x_+-x_-} \tag{8}$$

$$=\rho_k(x_-+kq)\gamma_k^{(1)}(x)+\gamma_k(x_++kq)\gamma_k^{(1)}(x) \tag{9}$$

3) Exercise. □

Remark 3.2. If R is a prime field, then (3) and its subsequent formulas in Theorem 3.1 become much easier, by the use of Lemma 2.2.

Example 2. Let us look into examples:

1) Let p be an odd prime number and consider the ring $\mathbb{Z}_p$ with the associated additive cyclic ordering. Let $f(x)=ax \bmod p$. Then for each $x\in\square_p,\rho(x)=1\in\square_p$, so that $x_+-x_-=2$ is a unit in $\mathbb{Z}_p$. So, $f^{(1)}(x)=\dfrac{a(x+1)-a(x-1)}{2}=a$. For $g(x)=bx^2 \bmod p$, we have that $g^{(1)}(x)=2bx$.

2) Let $R=\mathbb{Z}_9$ has the unity ordering, and consider the relation $\rho\in Rel(R)$ given by $\rho(x)=2x$. Then the image of ρ is 6×2-array with columns $\rho_0(x)=\{2^0,21,2^2,2^3,2^4,2^4\}$ and $\rho_1(x)=\{2^3,2^4,2^5,2^0,2^1,2^2\}$. One can verify

that $\rho_0^{(1)}(x)=\{3,6,3,6,3,6\}$ and $\rho_1^{(1)}(x)=\{6,3,6,3,6,3\}$ for $x \in R$.

3) Consider the ring $\mathbb{Z}_{35}$, and let $R=5\mathbb{Z}_{35}=\{0,5,10,15,20,25,30\}$. Then *R* is a ring modulo 35 whose unity $1_R=15$. If one considers the given cyclic ordering on *R*, then for each $x \in R$, $\delta(x)=\delta=5$ and $x_+ - x_- = 2\delta = 10$ which is a unit in *R*. Consider the relation $\rho(x)=25^{5x} \bmod 35$ on *R*. Then the image of ρ is a 3×3-array, and we have that $\rho_0^{(1)}(x)=\{25,15,30\}$, $\rho_1^{(1)}(x)=\{15,30,25\}$ and $\rho_2^{(1)}(x)=\{30,25,15\}$ for $x \in R$.

The computation in Example 2.3 (1) and (2) would not be very clear as far as $\rho_k^{(1)}(0)$ is concerned. But we used the following result.

Lemma 3.3. *Suppose* $\rho \in R$ *is a unit of order* $N \geq 3$, *and let* $\rho(x)=\alpha^x$ *be a relation on R. Then* $\rho(k)=\rho(sN+j)$, *for all integers* j,s. *In particular,* $\rho(0)=\rho(N)$, $\rho(-1)=\rho(N=1)$ *and* $\rho(N+1)=\rho(1)$.

Proof. We have that $\rho(j)=\alpha^j=\alpha^{sN+j}=\rho(sN+j)$. □

From the above theorem we see that the transformation $\rho_k^{(1)}$ looks indeed like a derivative on $Rel_{st}(R)$. For, when applied to a constant function it vanishes, and when applied to a polynomial of degree two it gives a polynomial of degree one, and so on. Also, when the transformation is applied to an exponential relation over *R*, it produces the relation times a constant. The above behavior are similar to those seen in the derivative transformation of real functions.

Definition 3.4. Let ρ be a relation on *R* and let $x \in R$. If $\rho_k^{(1)}(x)$ is defined, then it will be called the k-th derivative of the relation ρ at *x*, and will be denoted by $\rho_k^{(1)}(x)$.

In the real analysis case we are used to very nice derivative formulas for functions. The situation here is the similar, and we have the following result.

Corollary 3.5. *Let R has unity* 1_R *and let* δ *be the least length. If* $\alpha \in R$ *is a unit and n is a nonnegative integer greater than* 1, *then*

$$\left(\alpha^x\right)_k^{(1)}(x)=\frac{\left(\alpha^{2\delta}-1_R\right)}{2\delta\alpha^{\delta}}\alpha^{x+kq} \tag{10}$$

$$\left(x^n\right)^{(1)}(x)=\sum_{i=0}^{s}\binom{n}{2i+1}x^{n-(2i+1)}\delta^{2i}; \quad s=\begin{cases}\frac{n}{2}-1 & n \text{ even}\\ \frac{n-1}{2} & n \text{ odd}\end{cases} \tag{11}$$

$$\left(\sinh_{\alpha,h}(x)\right)^{(1)}(x)=\frac{\left(\alpha^{2\delta}-1_R\right)}{2\delta\alpha^{\delta}}\cosh_{\alpha,h}(x) \tag{12}$$

$$\left(\cosh_{\alpha,h}(x)\right)^{(1)}(x)=\frac{\left(\alpha^{2\delta}-1_R\right)}{2\delta\alpha^{\delta}}\sinh_{\alpha,h}(x) \tag{13}$$

Proof. One just uses the definition of the derivative. □

Remark 3.6. 1) If the ordering of *R* in Corollary 3.5 is the unity ordering, then $\delta=1_R$ and the formulas become much simpler.

2) Theorem 3.1 and Corollary 3.5 can be used to find *k*-th derivatives of all relations which are linear combinations or products of the set of *k*-th relations $\left\{x^n,\alpha_k^x,\sinh_{\alpha,k}(x),\cosh_{\alpha,k}(x)\right\}$ for a unit $\alpha \in R$.

3) The derivative of a monomial function whose degree is divisible q is not zero in *R*.

The derivative is a linear transformation on $Rel_{st}(R)$. So it can be applied on a relation ρ more that once and still preserve the linearity property. The following result, which is a consequence of Theorem 3.1 and Corollary 3.5, gives formulas for computing *k*-th derivatives of certain relations ρ, *t* times, which will be called (t,k)-th *derivative* of ρ. If the array of ρ has only one column, then the $(t,0)$-th derivative will be just called *t*-th *derivative*.

Corollary 3.7. *Let* $\alpha \in R$ *be a unit, and let* δ *is the least length. Then for a nonnegative integer t*:

$$\left(x^n\right)^{(t)} = \sum_{i=0}^{s} \binom{2}{2i+1} \left(x^{n(2i+1)}\right)^{(t-1)} \delta^{2i}; \quad s = \begin{cases} \frac{n}{2} - 1 & n \text{ even} \\ \frac{n-1}{2} & n \text{ odd} \end{cases} \tag{14}$$

$$\left(\alpha^x\right)_k^{(t)} = \left(\frac{\alpha^{2\delta} - 1_R}{2\delta\alpha^{\delta}}\right)^t \alpha^{x+kq} \tag{15}$$

Proof. 1) Follows from (2) and Theorem 3.1.

2) Exercise. □

Over the real the derivative transformation is not necessarily periodic for exponential functions. Over prime fields the derivative transformation on an exponential relation is periodic forall of the bases.

Theorem 3.8. *Let* $R = GF(q)$ *for a prime number q, and let* $\alpha \in R$ *be a unit which is not a square root of unity. If* $\rho(x) = \alpha^x$, *then*

$$\rho_h^{(t)}(x) = \rho_h(x) \text{ for some positive integer } t.$$

Proof. By the assumption $\alpha^2 - 1 \neq 0 \in R$, so that $\frac{\alpha^2 - 1}{2\alpha} \in R^*$, which implies that $\left(\frac{\alpha^2 - 1}{2\alpha}\right)^t = 1$ some positive integer *t*. □

The Exponential Values *e*

In real analysis the exponential relation $\exp(x) = e^x$ is characterized by its derivative, in the sense that it is the only relation with derivative equals the relation itself. Given a finite ring with additive cyclically ordering, do we have an analog of the exponential relation with respect the derivative we have defined? The answer is not necessarily! But some rings have indeed got a pair of *e*s. The result below gives a sufficient condition for that to happen.

Theorem 3.9. *Let* $R = GF(q)$, *where* $q \geq 3$ *is prime. If* 2 *is a quadratic residue in R, then the elements* $e = 1 \pm \sqrt{2}$ *has the property that* $\rho_k^{(1)}(x) = \rho_k(x)$, *where* ρ_k *is the k-th relation of the relation* $\rho(x) = e^x$.

Proof. Consider the relation $\rho(x) = e^x$, where *e* is in *R*. Suppose that $\rho(x)$ has the property that $\rho_k^{(1)}(x) = \rho_k(x)$ for all *k*. Then one has that $e^2 - 2e - 1 = 0 \in R$, which means $e = 1 \pm \sqrt{2}$. □

5. Finding Directions

Throughout this section $R = GF(q)$ for an odd prime *q*, and the ordering of *R* is the unity ordering. Recall that for a relation $\rho : R \to R$, the set of directions of ρ is denoted by $D(\rho)$ (see (1)). Let us denote the set of all (i,k)-th derivatives of ρ by $Dr_k^{(i)}(\rho)$ *i.e.*

$$Dr_k^i(\rho) = \left\{ \rho_k^{(i)}(x) \mid x \in R \right\} \tag{16}$$

From the definition of derivative we see that $Dr_k^{(i)}(\rho) \subseteq D(\rho)$ for all i,k.

For a relation $\rho : R \to R$, the bound on the size of $D(\rho)$ has be well studied. But there are only few relations ρ over *R* whereby the exact size of $D(\rho)$ is known. So far these are the known ones: Redei [1] shows that for linear functions f, $|D(f)| = 1$, while Ball [8] establihed that functions of the form $f(x) = x(q+1)/2$ have $|D(f)| = (q+3)/2$. We will try to add to this collection. We need the following lemma.

Lemma 4.1. *Let* $\alpha \in R$ *be a unit of order* $N \geq 3$, *and consider the relation* $\rho(x) = \alpha^x$. *Then for all* $x \in R$, $\rho_k^{(i)}(x) \neq 0 \in R$ *for all* i,k.

Proof. For $x \in R$ such that $jN + 1 \leq x \leq (j+1)N - 1$, we have that $\rho_k^{(i)}(x) \neq 0$ for all j,k, by Corollary 2.6. One can easily verify that $\rho_k^{(i)}(jN) \neq 0$, for all i,j,k. □

Suppose that $\alpha \in R$ is a unit, and let $\rho(x) = \alpha^x$ be a relation. Then by Theorem 3.9, applying the derivative transformation repeatedly gives back $\rho(x)$. We have two cases for $\beta = \frac{\alpha^2 - 1}{2\alpha}$:

Case 1: If β is in $\langle \alpha \rangle$, then we get a permutation of $\langle \alpha \rangle$ whose order it the order of subgroup generated by β.

Case 2: If β is not in $\langle \alpha \rangle$, then the collection $\left\{ Dr_k^{(i)}(\rho) \right\}$ partitions a bigger subgroup of R^* containing $\langle \alpha \rangle$. If this happens, then we say that α *partitions* the subgroup.

We have the following result.

Lemma 4.2. *Let* α *be a unit in R, and let* $\rho(x) = \alpha^x$ *be a relation. Then the order of* $Dr_k^{(i)}(\rho)$ *divides* $q - 1$ *for all* i,k. *In particular, if* α *is a generator of* R^*, *then* $\left| Dr_k^{(i)}(\rho) \right| = q - 1$ *for all* i,k.

Proof. We know that the set $Dr_k^{(i)}(\rho)$ is a coset of $\langle \alpha \rangle$ in R^* for all i,k. Then the result follows, since all cosets of a subgroup have the same size. □

Now we have our main result of this section, which establishes a connection between $D(\rho)$ and $Dr^{(i)}(\rho)$ for exponential relations $\rho(x)$.

Theorem 4.3. *Suppose that* α *is a unit in R of order* $N3$, *consider the relation* $\rho(x) = \alpha^x$, *and let s be the order of* $\frac{\alpha^2 - 1}{2\alpha}$.

1) If α partitions R^*, then for all *k*

$$D(\rho) = Dr_k^{(1)}(\rho) \sqcup Dr_h^{(2)}(\rho) \sqcup \cdots \sqcup Dr_h^{(s)} \sqcup \{0\} \tag{17}$$

2) If α is a generator of R^*, then

$$D(\rho) = Dr_k^{(1)}(\rho) \sqcup \{0\} \tag{18}$$

Proof. 1) Let $T = Dr_k^{(1)}(\rho) \sqcup Dr_h^{(2)}(\rho) \sqcup \cdots \sqcup Dr_h^{(s)}$. Then $|T| = q-1$, since α partitions R^*. We also have that 0 is not in $Dr_k^{(i)}(\rho)$ for all i,k, by Lemma 4.1. Since $Dr_k^{(i)}(\rho) \subseteq D(\rho)$ and $|D(\rho)| \le q$ for all *i*, the result follows.

2) By Lemma 4.2 we have that $|Dr_k^{(i)}(\rho)| = q-1$ and $\notin Dr_k^{(i)}(\rho)$ by Lemma 4.1, for all i,k. Since $Dr_k^{(i)}(\rho) \subset D(\rho)$ for all i,k, and $|D(\rho)| \le q$, the result follows. □

6. Conclusion

The notion of derivatives over certain finite ring is developed and is used to find the number of directions of exponential relations in the sence of Redei [1]. The developed theory is limited to finite rings of the form $\mathbb{Z}_n$ for an odd integer *n*. It is an open problem to develop the notion of derivatives to fit other finite algebraic setting.

References

[1] Redei, L. (1973) Luchenhafte Polynome Uber Endkichen Korper. Birkhauser Verlag, Basel.

[2] Hasse, H. (1936) Theorie der Hoheren Differentiale in Einem Algebraischen Funktionenkorper mit Vollkommenen Konstantenkorper bei Beliebiger Charakteristik. *Journal für die reine und angewandte Mathematik*, **175**, 50-54.

[3] Massey, J.L., von Seeman, N. and Schoeller, P. (1986) Hasse Derivatives and Repeated-Root Cyclic Codes. IEEE International Symposium on Information Theory, USA.

[4] Frisch, S. (1999) Polynomial Functions on Finite Commutative Rings. *Lecture Notes in Pure and Appl. Mathematics*, **205**, 323-336.

[5] de Souza, M.M.C., de Oliveira, H.M., de Souza, R.M.C. and Vasconcelos, M.M. (2004) The Discrete Cosine Transform over Prime Finite Fields. *LNCS*, **3124**, 37-59. https://doi.org/10.1007/978-3-540-27824-5_65

[6] Blockhuis, A., Ball, S., Brouwer, A.E., Storme, L. and Szonyi, T. (1999) On the Number of Slopes of the Fraph of a Function Defined on a Finite Field. *Journal of Combinatorial Theory, Series A*, **86**, 187-196. https://doi.org/10.1006/jcta.1998.2915

[7] Ball, S. (2003) The Number of Directions Determined by a Function over Finite Field. *Journal of Combinatorial Theory, Series A*, **104**, 341-435. https://doi.org/10.1016/j.jcta.2003.09.006

[8] Ball, S. (2011) Lacunary Polynomials over Finite Fields. Unpublished.

[9] Ball, S. (2007) Functions over Finite Fields That Fetermine Few Directions. *Electronic Notes in Discrete Mathematics*, **29**, 185-188. https://doi.org/10.1016/j.endm.2007.07.032

[10] Garcia-Colin, N., Montejano, A., Montejano, L. and Oliveros, D. (2017) Transitive Oriented 3-Hypergraphs of Cyclic Orders. https://arxiv.org/pdf/1210.6828.pdf

[11] Campello de Souza, R.M., de Oliveira, H.M., Kauffman, A.N. and Paschoal, A.J.A. (1998) Trigonometry in Finite Fields and a New Hartley Transform. ISIT, Cambridge. https://doi.org/10.1109/ISIT.1998.708898