Palestine Journal of Mathematics

Vol. 12(1)(2023) , 432–441

γ - DERIVATIONS IN RINGS

Aishwarya S., Kedukodi Babushri Srinivas and Kuncham Syam Prasad

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 16W25, 16N60; Secondary 12E20.

Keywords and phrases: derivation, commutativity, Lie product, Jordan product, Galois field.

The authors acknowledge Manipal Institute of Technology, Manipal Academy of Higher Education for their encouragement. The first author acknowledges Manipal Academy of Higher Education for Dr TMA Pai PhD scholarship.

Abstract. We introduce the notion of γ-derivations in rings and obtain commutativity results in a prime ring R admitting multiplicative γ-derivations. We show that the symmetry of γ with various conditions on Lie products and Jordan products gives rise to commutativity of R. We obtain (i) a characterization of Galois field of any characteristic by using Lie product and γ-derivation, and (ii) a characterization of Galois field of characteristic 2 by using Jordan product and γ-derivation.

1 Introduction

A derivation d on a ring R is a linear map on R which satisfies the Leibniz rule, that is, $d(xy) = xd(y) + d(x)y$ for all $x, y \in R$. Derivations on rings and nearrings have been widely studied in the literature. Posner [23] and Herstein [11, 12, 13] obtained some of the important early results on prime rings with derivations. Derivations and commutativity in prime and semiprime rings with different types of derivations have been widely investigated. Brešar [7] introduced the notion of generalized derivations. Argaç [2] generalized a well-known result of Posner [23] on commuting derivations to semiprime rings and obtained some sufficient conditions for a derivation to be commuting on a nonzero ideal of the ring. Recently, Gólbaşi and Öğirtici [9] obtained certain sufficient conditions for a multiplicative semiderivation on a semiprime ring to be commuting on an ideal of the ring. Mamouni and Tamekkante [20] studied commutativity in prime rings admitting two generalized derivations. Birkenmeier, Heatherly and Lee [6] studied the interconnections between different types of prime ideals in nearrings. Bhavanari, Kuncham and Kedukodi [5] introduced the graph of a nearring with respect to an ideal of the nearring and studied the relation between 3-primeness of the ideal and ideal symmetry of the corresponding graph. Kedukodi, Kuncham and Bhavanari [15] introduced equiprime, 3-prime and c-prime fuzzy ideals of nearrings, and subsequently, Koppula, Kedukodi and Kuncham [16] related the ideas to decision making. Koppula, Kedukodi and Kuncham [17] studied the notion of perfect ideals of seminearrings. Derivations in prime nearrings were first investigated by Bell and Mason [4] and several other results were obtained by Bell [3], Wang [24], Kamal and Shaalan [14], among others. Aishwarya, Kedukodi and Kuncham [1] obtained commutativity results in prime nearrings through permutation identities satisfied by certain subsets and gave a characterization of Galois field using permutation identities. It is well-known that Galois fields are extensively used in cryptography and coding theory (Lidl and Niederreiter [19], Mullen and Mummert [21], etc.). Different classes of codes based on Galois fields are used in various applications like error detection and correction, data transmission and storage, among many others. Gómez-Torrecillas, Lobillo, Navarro and Sánchez-Hernández [10] defined differential convolutional codes which are built from a derivation of the rational function field of a Galois field. In this paper, we introduce γ-derivation on a ring R as a generalization of derivations and provide natural examples of γ-derivations. The definition of γ-derivation extends the notion of derivation studied in Zhu and Xiong [25, 26], Li and Pan [18]. We obtain commutativity results in prime rings using multiplicative γ-derivations satisfying conditions on Lie and Jordan products. These results generalize the commutativity results obtained by Bell [3], Kamal and Shaalan [14]. Finally, we obtain a characterization of Galois fields of any characteristic and a characterization of Galois fields of characteristic 2 by using γ-derivations.

We would like to point out that one of the consequences of the results on γ-derivations is that the symmetry of Pascal's triangle arising due to the well-known discrete combinatorial formula ${}^nC_r = {}^nC_{n-r}$, naturally induces the commutativity of multiplication in complex numbers.

2 Preliminaries

Let $(R, +, \cdot)$ be a ring. For subsets A and B of R, the product of the sets A and B is $AB = \{ab \,|\, a \in A,\, b \in B\}$. If $A = \{a\}$ or $B = \{b\}$, we write AB simply as aB or Ab respectively. A non-empty subset K of R is called a subsemigroup of $(R, \cdot)$ if $KK \subseteq K$. A non-empty subset K of R is called a semigroup left ideal (resp. semigroup right ideal) of R if $RK \subseteq K$ (resp. $KR \subseteq K$) and a semigroup ideal of R if $RK \subseteq K$ and $KR \subseteq K$. An element x in R is said to centralize a subset K of R if $xk = kx$ for all $k \in K$. The set $\{x \in R \,|\, xr = rx \text{ for all } r \in R\}$ is called the multiplicative center of R, and is denoted by $Z(R)$. R is said to be a prime ring if for all $a, b \in R$, $aRb = \{0\}$ implies that either $a = 0$ or $b = 0$. For $a, b \in R$, $[a, b]$ denotes the Lie product $ab - ba$ and $a \circ b$ denotes the Jordan product $ab + ba$. For $A, B \subseteq R$, $[A, B]$ denotes the set $\{[a, b] \,|\, a \in A, b \in B\}$ and $A \circ B$ denotes the set $\{a \circ b \,|\, a \in A, b \in B\}$. If $A = \{a\}$ or $B = \{b\}$, $[A, B]$ is simply written as $[a, B]$ or $[A, b]$ respectively, and $A \circ B$ is written as $a \circ B$ or $A \circ b$ respectively. For a natural number t and $K \subseteq R$, we write $tK = \{\underbrace{k + k + \cdots + k}_{\text{t times}} \,|\, k \in K\}$. For more definitions and properties, we refer to Pilz [22], Ferrero and Ferrero [8].

The following definition is from a communicated paper by Aishwarya, Kedukodi and Kuncham.

Definition 2.1. Let $\emptyset \neq K \subseteq R$. K is called *a* $\{0\}$*-weak semigroup left ideal (*$\{0\}$*-weak semigroup right ideal) of* R if there exists a nonzero subset I of K such that $RI \subseteq K$ (resp. $IR \subseteq K$).

Note that every non-zero semigroup left ideal (resp. nonzero semigroup right ideal) of R is a $\{0\}$-weak semigroup left ideal of R (resp. $\{0\}$-weak semigroup right ideal of R).

Definition 2.2. (Zhu and Xiong [26], Li and Pan [18]) A linear map d from a unital algebra $\mathcal{A}$ over a field F to an $\mathcal{A}$-bimodule $\mathcal{M}$ is called a generalized derivation if for all $a, b \in \mathcal{A}$, $d(ab) = d(a)b + ad(b) - ad(1)b$, where 1 is the unit of $\mathcal{A}$.

Proposition 2.3. *(Bell [3]) Let R be a prime ring. If $x \in Z(R) \setminus \{0\}$, then x is not a zero divisor.*

Proposition 2.4. *(Bell [3]) Let K be a nonzero semigroup left ideal of a prime ring R. If $x \in R$ is such that x centralizes K, then $x \in Z(R)$.*

Proposition 2.5. *(Bell [3]) Let R be a prime ring. If $Z(R)$ contains a nonzero semigroup left ideal or a nonzero semigroup right ideal, then R is commutative.*

3 γ - derivation

Definition 3.1. Let R be a ring and let $\gamma : R \times R \to R$. A function $d : R \to R$ is called a multiplicative γ-derivation on R if for all $x, y \in R$,

$$d(xy) = x\, d(y) + x\, \gamma(x, y)\, y + d(x)\, y.$$

We say that γ is symmetric if $\gamma(x, y) = \gamma(y, x)$ for all $x, y \in R$. It is clear that if $\gamma(x, y) = c$ for all $x, y \in R$ then γ is symmetric. When $\gamma(x, y) = 0$, we get $d(xy) = xd(y) + d(x)y$, that is, d is a (usual) multiplicative derivation.

Definition 3.2. Let R be a ring. A multiplicative γ-derivation d on R is called a γ-derivation on R if d is additive.

First, we give some examples to illustrate the concept and the idea involved.

Example 3.3. Let F be a field and let $F[x]$ be the polynomial ring over F. Let $f(x)$ be an element of $F[x]$ with degree at least 2 and let $R = F[x]/\langle f(x)\rangle$, the quotient ring of $F[x]$ by the principal ideal generated by $f(x)$. Define $d : R \to R$ by

$$d\left(p(x) + \langle f(x)\rangle\right) = x\,p(x) + \langle f(x)\rangle$$

and let $\gamma : R \times R \to R$ be defined by

$$\gamma\left(p(x) + \langle f(x)\rangle,\, q(x) + \langle f(x)\rangle\right) = -x + \langle f(x)\rangle.$$

For $a = p(x) + \langle f(x)\rangle$, $b = q(x) + \langle f(x)\rangle \in R$, we have

(i) $$\begin{aligned} d(a) + d(b) &= \left(x\,p(x) + \langle f(x)\rangle\right) + \left(x\,q(x) + \langle f(x)\rangle\right) \\ &= (x\,p(x) + x\,q(x)) + \langle f(x)\rangle \\ &= x\,(p(x) + q(x)) + \langle f(x)\rangle \\ &= d\left((p(x) + q(x)) + \langle f(x)\rangle\right) \\ &= d(a+b) \end{aligned}$$

(ii) $$\begin{aligned} ad(b) + a\gamma(a,b)b + d(a)b &= \left(p(x) + \langle f(x)\rangle\right)\left(x\,q(x) + \langle f(x)\rangle\right) \\ &\quad + \left(p(x) + \langle f(x)\rangle\right)\left(-x + \langle f(x)\rangle\right)\left(q(x) + \langle f(x)\rangle\right) \\ &\quad + \left(x\,p(x) + \langle f(x)\rangle\right)\left(q(x) + \langle f(x)\rangle\right) \\ &= \left(x\,p(x)q(x) + \langle f(x)\rangle\right) - \left(x\,p(x)q(x) + \langle f(x)\rangle\right) \\ &\quad + \left(x\,p(x)q(x) + \langle f(x)\rangle\right) \\ &= x\,p(x)q(x) + \langle f(x)\rangle \\ &= d\left(p(x)q(x) + \langle f(x)\rangle\right) \\ &= d(ab). \end{aligned}$$

By (i) and (ii), d is a γ-derivation on R.

In particular, when F is a Galois field and $R = F[x]/\langle x^n - 1\rangle$ for some $n \geq 2$, the elements of R can be seen as codewords of length n over the field F. It is well-known that the ideals of R exactly correspond to the cyclic codes. The function d is the cyclic right shift operation on the set of codewords. The cyclic right shift operation is a γ-derivation on R.

Example 3.4. A generalized derivation d (refer Definition 2.2) from a unital algebra $\mathcal{A}$ over a field F to an $\mathcal{A}$-bimodule $\mathcal{M}$ is a γ-derivation on F when $\mathcal{A} = \mathcal{M} = F$, where $\gamma(x,y) = -d(1)$.

Example 3.5. Let R be a ring and let n be a natural number. Consider the ring

$$M_n(R) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \mid a_{ij} \in R,\ 1 \leq i,j \leq n \right\}$$

of all matrices of order $n \times n$ over R. For $c \in R$, define $d_1, d_2 : M_n(R) \to M_n(R)$ by

$$d_1\left(\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}\right) = \begin{pmatrix} c\,a_{11} & c\,a_{12} & \dots & c\,a_{1n} \\ c\,a_{21} & c\,a_{22} & \dots & c\,a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c\,a_{n1} & c\,a_{n2} & \dots & c\,a_{nn} \end{pmatrix}$$

and

$$d_2\left(\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}\right) = \begin{pmatrix} a_{11}\,c & a_{12}\,c & \dots & a_{1n}\,c \\ a_{21}\,c & a_{22}\,c & \dots & a_{2n}\,c \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}\,c & a_{n2}\,c & \dots & a_{nn}\,c \end{pmatrix}.$$

Let $\gamma : M_n(R) \times M_n(R) \to M_n(R)$ be defined by

$$\gamma(A,B) = \begin{pmatrix} -c & 0 & \dots & 0 \\ 0 & -c & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & -c \end{pmatrix}_{n\times n.}$$

Then d_1 and d_2 are multiplicative γ-derivations on $M_n(R)$.

Example 3.6. Consider the ring $M_2(\mathbb{R})$. For $\theta \in \mathbb{R}$, $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is the standard rotation matrix where θ denotes the polar angle of rotation.
Then $d : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ defined by

$$d(A) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} A$$

is a multiplicative γ-derivation on $M_2(\mathbb{R})$, where $\gamma : M_2(\mathbb{R}) \times M_2(\mathbb{R}) \to M_2(\mathbb{R})$ is defined by

$$\gamma(A,B) = \begin{pmatrix} \cos(\pi+\theta) & -\sin(\pi+\theta) \\ \sin(\pi+\theta) & \cos(\pi+\theta) \end{pmatrix} = \begin{pmatrix} -\cos\theta & \sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix},$$

the matrix corresponding to rotation by a polar angle $\pi+\theta$. Clearly, d rotates the column vectors of A by an angle θ in the anticlockwise direction.

Example 3.7. The identity map on a ring R is a (usual) derivation only when the multiplication in R is trivial. Such a severe restriction is not imposed by γ-derivations. For instance, if R is any ring with 1 then the identity map is a γ-derivation on R; where $\gamma(x,y) = -1$.

Example 3.8. Let R be a ring. Let $\gamma : R \times R \to R$ and let $f : R \to R$ be a γ-derivation on R. For an element $c \in Z(R)$, the functions $d_l : R \to R$ defined by $d_l(x) = f(x)\,c$ and $d_r : R \to R$ defined by $d_r(x) = c\,f(x)$ are a γ_l-derivation and a γ_r-derivation respectively on R, where $\gamma_l, \gamma_r : R \times R \to R$ are defined by $\gamma_l(x,y) = \gamma(x,y)\,c$ and $\gamma_r(x,y) = c\,\gamma(x,y)$. The γ_l-derivation d_l and the γ_r-derivation d_r are induced by the γ-derivation f on R.

In what follows, $\gamma : R \times R \to R$ and the image of γ is denoted by

$$\Gamma = \{\gamma(x,y) \mid x, y \in R\}.$$

Proposition 3.9. *Let K be a subsemigroup of $(R,\cdot)$ and let V be a non-empty subset of R such that $KV \subseteq K$. If d is a multiplicative γ-derivation on R such that $d([V,K]) = \{0\}$ (resp. $d(V \circ K) = \{0\}$) and $[V,K]\,\Gamma\,V = \{0\}$ (resp. $(V \circ K)\,\Gamma\,V = \{0\}$), then $[v,K]\,K\,d(v) = \{0\}$ $\forall$ $v \in V$.*

Proof. Let $k \in K$, $v \in V$. We have $kv \in K$ and hence

$$d([v,kv]) = d(v(kv) - (kv)v) = d((vk - kv)v) = d\big([v,k]\,v\big) = 0$$

$$\text{(resp. } d(v \circ (kv)) = d(v(kv) + (kv)v) = d((vk + kv)v) = d\big((v \circ k)\,v\big) = 0).$$

This gives

$$[v,k]\,d(v) + [v,k]\,\gamma([v,k],v)\,v + d([v,k])\,v = 0$$

$$\text{(resp. } (v \circ k)\,d(v) + (v \circ k)\,\gamma(v \circ k, v)\,v + d(v \circ k)\,v = 0).$$

Hence we get $[v,k]\,d(v) = 0$ (resp. $(v \circ k)\,d(v) = 0$). This implies that $vkd(v) = kvd(v)$ (resp. $vkd(v) = -kvd(v)$).

Now let $l \in K$. We have $lk \in K$ and hence $vlkd(v) = lkvd(v)$ (resp. $vlkd(v) = -lkvd(v)$). As $vkd(v) = kvd(v)$ (resp. $vkd(v) = -kvd(v)$), we get $vlkd(v) = lvkd(v) = 0$ (resp. $vlkd(v) = -l(-vkd(v)) = 0$). Therefore $vlkd(v) = lvkd(v)$. This gives $(vl - lv)kd(v) = [v,l]\,k\,d(v) = \{0\}$. Hence $[v,K]\,K\,d(v) = \{0\}$.

□

Theorem 3.10. *Let $S := \{c \in R \,|\, xcy = ycx \;\forall\, x \in Z(R),\, y \in R\}$. Then S is a subgroup of $(R, +)$ containing $Z(R)$. If R is prime and $Z(R) \neq \{0\}$ then $S = Z(R)$.*

Proof. As $0 \in S$, the set S is non-empty. Let $a, b \in S$. Let $x \in Z(R)$ and $y \in R$. We have $x(a-b)y = x(ay-by) = xay - xby = yax - ybx = y(ax - bx) = y(a-b)x$, showing that $a - b \in S$. Hence S is a subgroup of $(R, +)$. Now we will show that $Z(R) \subseteq S$. Let $b \in Z(R)$. Let $x \in Z(R)$ and $y \in R$. We have $x(by) = x(yb) = (yb)x$. Hence $b \in S$, which implies $Z(R) \subseteq S$. Suppose R is prime and $Z(R) \neq \{0\}$. Let $a \in S$. Let $x \in Z(R) \setminus \{0\}$ and $y \in R$. We have $xay = yax$, which implies that $xay - yax = 0$. This gives $ayx - yax = (ay - ya)x = 0$. By Proposition 2.3, we get $ay - ya = 0$, that is, $ay = ya$. Hence $a \in Z(R)$, showing that $S \subseteq Z(R)$. Hence $S = Z(R)$. □

The following result generalizes the well-known result by Wang [24]: If $x \in Z(R)$, then $d(x) \in Z(R)$.

Proposition 3.11. *Let γ be symmetric and let $\Gamma \subseteq S$. Let d be a multiplicative γ-derivation on R. If $x \in Z(R)$, then $d(x) \in Z(R)$.*

Proof. Let $y \in R$. We have $d(xy) = xd(y) + x\,\gamma(x, y)\,y + d(x)y$ and $d(yx) = d(y)x + y\,\gamma(y, x)\,x + yd(x)$. As $xy = yx$, we get

$$xd(y) + x\,\gamma(x, y)\,y + d(x)y = d(y)x + y\,\gamma(y, x)\,x + yd(x).$$

This gives $d(x)y = yd(x)$, and hence $d(x) \in Z(R)$. □

4 γ - derivation and commutativity of prime rings

In this section, R denotes a prime ring unless specified otherwise.

Proposition 4.1. *Let K be a $\{0\}$-weak semigroup right (resp. left) ideal of R. If $x \in R$ is such that $Kx = \{0\}$ (resp. $xK = \{0\}$), then $x = 0$.*

Proof. Suppose that K is a $\{0\}$-weak semigroup right (resp. left) ideal of R. Let I be a nonzero subset of K such that $IR \subseteq K$ (resp. $RI \subseteq K$). Suppose $Kx = \{0\}$ (resp. $xK = \{0\}$). Then $(IR)x = \{0\}$ (resp. $x(RI) = \{0\}$), which implies that $(I \setminus \{0\})Rx = \{0\}$ (resp. $xR(I \setminus \{0\}) = \{0\}$). As R is prime and I is nonzero, we get $x = 0$. □

The following result generalizes Proposition 4.2 of Kamal and Shaalan [14] for rings.

Proposition 4.2. *Let K be a nonzero semigroup left ideal of R and let V be a nonzero semigroup left ideal of R such that $VK \subseteq V$ (resp. let V be a semigroup right ideal and a $\{0\}$-weak semigroup left ideal of R such that $KV \subseteq V$). If $vk = -kv \;\forall\, v \in V,\, k \in K$, then R is commutative and is of characteristic 2.*

Proof. Let $v \in V$, $k, l \in K$. We have $kl \in K$ and hence $v(kl) = -(kl)v = (-k)(lv) = (-k)(-vl) = k(vl)$, that is, $(vk)l = (kv)l$. This implies $(vk - kv)l = 0$. By Proposition 4.1, $vk = kv$. Now by Lemma 4.1 (iii) in Kamal and Shaalan [14], R is commutative. We have $vk \in V$ and hence $-l(vk) = (vk)l = v(kl) = -(kl)v$ because $kl \in K$. As $lv \in V$, we have $-(kl)v = -k(lv) = (lv)k$, and hence $-lvk = lvk$. This gives $lvk + lvk = (lv + lv)k = (2lv)k = 0$. Hence $(2lv)K = \{0\}$. By Proposition 4.1, $2lv = (2l)v = 0$, hence $(2l)V = \{0\}$. Again by Proposition 4.1, $2l = \{0\}$. Hence $2K = \{0\}$. By Proposition 2.8 in Kamal and Shaalan [14], $2R = \{0\}$, that is, R is of characteristic 2. □

Proposition 4.3. *Let K be a semigroup left (resp. right) ideal and a $\{0\}$-weak semigroup right (resp. left) ideal of R. If $x, y \in R$ are such that $xKy = \{0\}$, then $x = 0$ or $y = 0$.*

Proof. Suppose $xKy = \{0\}$. As $RK \subseteq K$ (*resp.* $KR \subseteq K$), $xRKy = \{0\}$ (*resp.* $xKRy = \{0\}$). As R is prime, we get $x = 0$ or $Ky = \{0\}$ (*resp.* $xK = \{0\}$ or $y = 0$). By Proposition 4.1, $x = 0$ or $y = 0$. □

The following theorem extends Theorem 2.1 of Bell [3] and Theorem 3.4 of Kamal and Shaalan [14] for rings.

Theorem 4.4. *Let K be a nonzero semigroup left (resp. right) ideal of R. Let γ be such that $[K, R\Gamma K] = \{0\}$ (resp. $[K, K\Gamma R] = \{0\}$). If d is a multiplicative γ-derivation on R such that $\{0\} \neq d(K) \subseteq Z(R)$, then R is commutative.*

Proof. Suppose K is a nonzero semigroup left ideal of R and $[K, R\Gamma K] = \{0\}$. Let $a \in K$ be such that $d(a) \neq 0$. Note that $d(a) \in Z(R)$. Let $k, l \in K$. Then $kl \in K$ and hence $d(kl)\, l = l\, d(kl)$. This gives

$$k\, d(l)\, l + k\, \gamma(k, l)\, l^2 + d(k)\, l^2 = l\, k\, d(l) + l\, k\, \gamma(k, l)\, l + l\, d(k)\, l.$$

As $d(K) \subseteq Z(R)$ and $[K, R\Gamma K] = \{0\}$, we get

$$k\, l\, d(l) + k\, \gamma(k, l)\, l^2 + d(k)\, l^2 = l\, k\, d(l) + k\, \gamma(k, l)\, l^2 + d(k)\, l^2.$$

This gives $k\, l\, d(l) = l\, k\, d(l)$, that is, $(kl - lk)d(l) = 0$. Taking $l = a$, we get $(ka - ak)d(a) = 0$. Now by Proposition 2.3, $ka = ak$. Hence a centralizes K.

As $ka \in K$, we have $d(ka)\, l = l\, d(ka)$, that is,

$$k\, d(a)\, l + k\, \gamma(k, a)\, a\, l \,+\, d(k)\, a\, l = l\, k\, d(a) \,+\, l\, k\, \gamma(k, a)\, a \,+\, l\, d(k)\, a.$$

This gives

$$k\, l\, d(a) + l\, k\, \gamma(k, a)\, a + d(k)\, l\, a = l\, k\, d(a) + l\, k\, \gamma(k, a)\, a + d(k)\, l\, a.$$

Hence we get $k\, l\, d(a) = l\, k\, d(a)$, that is, $(kl - lk)\, d(a) = 0$. By Proposition 2.3, $kl = lk$, that is, $kl - lk = [k, l] = 0$. Therefore $[K, K] = \{0\}$.

Let $x \in R$. As $xa \in K$, we have $d(xa)\, l = l\, d(xa)$, that is,

$$x\, d(a)\, l + x\, \gamma(x, a)\, a\, l \,+\, d(x)\, a\, l = l\, x\, d(a) \,+\, l\, x\, \gamma(x, a)\, a \,+\, l\, d(x)\, a,$$

which gives

$$x\, l\, d(a) + x\, \gamma(x, a)\, a\, l + l\, d(x)\, a = l\, x\, d(a) + x\, \gamma(x, a)\, a\, l + l\, d(x)\, a$$

because K is a semigroup left ideal of R. Thus we have $x\, l\, d(a) = l\, x\, d(a)$, and hence $(xl - lx)d(a) = 0$. By Proposition 2.3, $xl = lx$. Hence $K \subseteq Z(R)$. Now by Proposition 2.5, R is commutative.

The proof is analogous for the other case. □

Theorem 4.5. *Let K be a nonzero semigroup ideal of R and let A be a nonzero semigroup left (resp. right) ideal of R. Let γ be symmetric, $\Gamma \subseteq Z(R)$ and $[A, K]\Gamma = \{0\}$. If d is a multiplicative γ-derivation on R such that $d([A, K]) = \{0\}$ and $d(A) \neq \{0\}$, then R is commutative.*

Proof. As $[A, K]\Gamma = \{0\}$, we get $[A, K]\Gamma A = \{0\}$. Let $a \in A$ be such that $d(a) \neq 0$. By Proposition 3.9, we have $[a, K]\, K d(a) = \{0\}$. Now using Proposition 4.3, we get $[a, K] = \{0\}$, that is, a centralizes K. By Proposition 2.4, we have $a \in Z(R)$. As γ is symmetric, by Proposition 3.11 we get $d(a) \in Z(R)$. Let $y \in A$, $k \in K$. We have $ka \in K$ and hence $d([y, ka]) = 0$. This gives

$$d(yka - kay) = d(yka - kya) = d((yk - ky)a) = d([y, k]\, a) = 0.$$

Therefore,

$$d([y, k]\, a) = [y, k]\, d(a) + [y, k]\, \gamma([y, k], a)\, a + d([y, k])\, a = 0.$$

This gives $[y, k]\, d(a) = 0$. Now by Proposition 2.3, we get $[y, k] = 0$. Hence y centralizes K. Now by Proposition 2.4, $y \in Z(R)$, and hence $A \subseteq Z(R)$. By Proposition 2.5, R is commutative. □

Example 4.6. Let n be a natural number. The function d on the ring of complex numbers $\mathbb{C}$ defined by $d(0) = 0$ and $d(re^{i\theta}) = r(\log r)^n e^{i\theta}$ for $r \neq 0$, is a multiplicative γ-derivation on $\mathbb{C}$, where $\gamma : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ is defined by

$$\gamma(r_1 e^{i\theta_1}, r_2 e^{i\theta_2}) = \begin{cases} \sum\limits_{k=1}^{n-1} {}^nC_k \, (\log r_1)^{n-k} \, (\log r_2)^k & \text{if } n \geq 2,\ r_1 \neq 0 \text{ and } r_2 \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

For $n \geq 2$, the coefficients of powers of $\log r_1$, $\log r_2$ are binomial coefficients which can be computed as the interior part of the well-known Pascal's triangle as shown in Figure 1. It follows easily from the symmetry of Pascal's triangle that γ is symmetric. The ring $\mathbb{C}$ is prime and all conditions of Theorem 4.5 hold with $K = A = \mathbb{C}$. Using Theorem 4.5, we conclude that symmetry of γ induces commutativity of $\mathbb{C}$ through the derivation d.

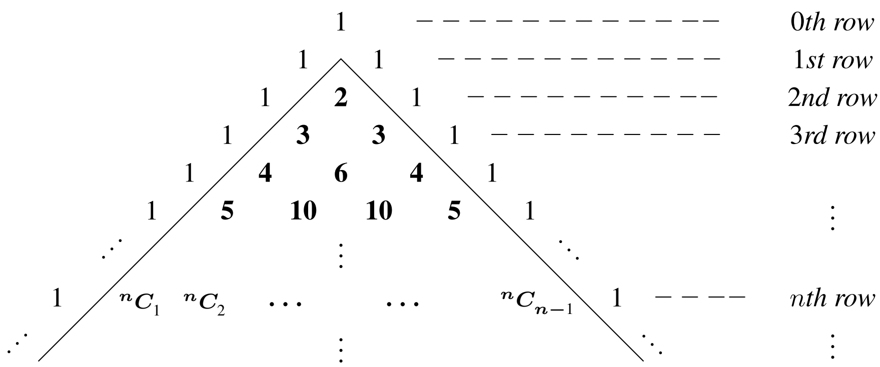

Figure 1. Symmetry of γ (symmetry of Pascal's triangle) induces commutativity of $\mathbb{C}$

Now we give a characterization of Galois fields in terms of Lie product and γ-derivation.

Theorem 4.7. *Suppose*

(1) R is finite;

(2) there exist a nonzero semigroup ideal K of R, a nonzero semigroup left (resp. right) ideal A of R, a function $\gamma : R \times R \to R$ and a multiplicative γ-derivation d on R such that

(a) γ is symmetric, $\Gamma \subseteq Z(R)$ and $[A, K]\,\Gamma = \{0\}$;

(b) $d([A, K]) = \{0\}$ and $d(A) \neq \{0\}$.

Then R is a Galois field. Conversely, if R is a Galois field, then the conditions (1), (2a), (2b) hold in R.

Proof. Let conditions *(1)*, *(2a)*, *(2b)* hold. By Theorem 4.5, R is a commutative ring. Let $a, b \in R$ be such that $ab = 0$. Then for $r \in R$, $arb = abr = 0r = 0$. This gives $aRb = \{0\}$. As R is prime, we get either $a = 0$ or $b = 0$. Hence R is an integral domain. As R is finite, R is a Galois field.

Conversely, suppose that R is a Galois field with $q = p^n$ elements. Then we have $R = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$, where α is a root of a primitive polynomial and $\alpha^{q-1} = 1$. Hence the condition *(1)* holds. It is clear that as R has no nonzero zero divisors, R is prime. Consider the map $d : R \to R$ defined by $d(0) = 0$ and $d(\alpha^k) = \alpha^{k-1}$ for $1 \leq k \leq q-1$. Define $\gamma : R \times R \to R$ by $\gamma(x, y) = -\alpha^{-1}$. Let $x, y \in R$. *(i)* Let $x = 0$ or $y = 0$. Then we have $xd(y) + x\gamma(x, y)y + d(x)y = 0 + 0 + 0 = 0 = d(0) = d(xy)$. *(ii)* Let $x \neq 0$ and $y \neq 0$. Then $x = \alpha^r$ and $y = \alpha^s$ for some r, s where $1 \leq r, s \leq q-1$. This gives $xd(y) + x\gamma(x, y)y + d(x)y = \alpha^r\alpha^{s-1} + \alpha^r(-\alpha^{-1})\alpha^s + \alpha^{r-1}\alpha^s = \alpha^{r+s-1} - \alpha^{r+s-1} + \alpha^{r+s-1} = \alpha^{r+s-1} = d(\alpha^{r+s}) = d(\alpha^r\alpha^s) = d(xy)$. Hence d is a multiplicative γ-derivation on R. Note that γ is symmetric and $\Gamma \subseteq R = Z(R)$. By choosing $K = A = R$, we have $[A, K]\Gamma = \{0\}\Gamma = \{0\}$, $d([A, K]) = d(\{0\}) = \{0\}$ and $d(A) = d(R) \neq \{0\}$. Hence the conditions *(2a)*, *(2b)* hold. $\square$

The following results extend Theorem 4.3 and Corollary 4.4 of Kamal and Shaalan [14] for rings.

Proposition 4.8. *Let K be a semigroup left ideal and a $\{0\}$-weak semigroup right ideal of R. Let A be a non-empty subset of R such that $KA \subseteq K$. If d is a multiplicative γ-derivation on R such that $d(A \circ K) = (A \circ K)\,\Gamma = \{0\}$ and $d(A) \neq \{0\}$, then $A \subseteq Z(R)$. Further, if A is a nonzero semigroup left (resp. right) ideal of R, then R is commutative.*

Proof. As $(A \circ K)\,\Gamma = \{0\}$, we get $(A \circ K)\,\Gamma A = \{0\}$. Let $a \in A$ be such that $d(a) \neq 0$. By Proposition 3.9, we have $[a, K]\,K\,d(a) = \{0\}$. Then by Proposition 4.3, we get $[a, K] = \{0\}$, that is, a centralizes K. By Proposition 2.4, $a \in Z(R)$. Let $y \in A$, $k \in K$. We have $ka \in K$ and hence $d(y \circ ka) = 0$. This gives $d(yka+kay) = d(yka+kya) = d((yk+ky)a) = d((y \circ k)a) = 0$. Thus we have

$$(y \circ k)\,d(a) + (y \circ k)\,\gamma(y \circ k, a)\,a + d(y \circ k)\,a = 0,$$

which gives

$$(y \circ k)\,d(a) = 0. \tag{1}$$

Let $l \in K$. Then we have $lk \in K$. Using Equation (1), we get $(y \circ lk)\,d(a) = 0$. This gives

$$ylk\,d(a) = -lky\,d(a) = (-l)(ky)d(a) = -l(-ykd(a)) = lyk\,d(a).$$

Therefore, we have

$$(ylk - lyk)\,d(a) = (yl - ly)\,k\,d(a) = 0.$$

Hence $(yl - ly)\,K\,d(a) = \{0\}$. As $d(a) \neq 0$, by Proposition 4.3, we get $yl - ly = 0$. Hence y centralizes K. Now by Proposition 2.4, $y \in Z(R)$ and hence $A \subseteq Z(R)$. Suppose A is a nonzero semigroup left (resp. right) ideal of R. By Proposition 2.5, R is commutative.

□

Theorem 4.9. *Let K be a nonzero semigroup left (resp. right) ideal of R and let $\emptyset \neq A$ be a nonzero subset of R such that $KA \subseteq K$. Let γ be symmetric and $\Gamma \subseteq S$. If d is a multiplicative γ-derivation on R such that $d(A \circ K) = (A \circ K)\,\Gamma = \{0\}$ and $d(A) \neq \{0\}$, then R is of characteristic 2. Further, if A is a nonzero semigroup left (resp. right) ideal of R, then R is commutative.*

Proof. By Proposition 4.8, we have $A \subseteq Z(R)$. Let $a \in A$ be such that $d(a) \neq 0$. Let $y \in A \backslash \{0\}$ and $k \in K$. By Equation (1) in the proof of Proposition 4.8, we have $(y \circ k)\,d(a) = 0$. Also we have $a \in Z(R)$. Hence by Proposition 3.11, $d(a) \in Z(R)$. By Proposition 2.3, we get $y \circ k = 0$ because $d(a) \neq 0$. Hence $yk + ky = 0$. As $y \in Z(R)$, we get

$$ky + ky = (k + k)y = 0.$$

Now Proposition 2.3 gives $k + k = 2k = 0$. Hence $2K = \{0\}$. By Proposition 2.8 in Kamal and Shaalan [14], we get $2R = \{0\}$. Hence R is of characteristic 2. Suppose A is a nonzero semigroup left (resp. right) ideal of R. As $A \subseteq Z(R)$ by Proposition 4.8, R is commutative by Proposition 2.5.

□

Now we give a characterization of Galois fields of characteristic 2 in terms of Jordan product and γ-derivation.

Theorem 4.10. *Suppose*

(1) R is finite;

(2) there exist a nonzero semigroup left (resp. right) ideal K of R, a nonzero semigroup left (resp. right) ideal A of R, a function $\gamma : R \times R \to R$ and a multiplicative γ-derivation d on R such that

(a) $KA \subseteq K$;

(b) γ is symmetric, $\Gamma \subseteq S$ and $(A \circ K)\,\Gamma = \{0\}$;

(c) $d(A \circ K) = \{0\}$ *and* $d(A) \neq \{0\}$.

Then R is a Galois field of characteristic 2. Conversely, if R is a Galois field of characteristic 2, then the conditions (1), (2a), (2b), (2c) hold in R.

Proof. Let conditions *(1)*, *(2a)*, *(2b)*, *(2c)* hold. By Theorem 4.9, R is a commutative ring of characteristic 2. Now as in the proof of Theorem 4.7, R is a Galois field. Conversely, suppose that R is a Galois field of characteristic 2 with q elements. Then $q = 2^n$ for some $n \geq 1$. As R is of characteristic 2, for any $a, b \in R$, the Jordan product of a and b coincides with the Lie product of a and b. That is, $a \circ b = ab + ba = ab - ba = [a, b]$. Now, the rest of the proof follows from Theorem 4.7. □

References

[1] S. Aishwarya, B. S. Kedukodi and S. P. Kuncham, Commutativity in 3-prime nearrings through permutation identities, *Asian-Eur. J. Math.***15**(06), 2250109 (2022).

[2] N. Argaç, On prime and semiprime rings with derivations, *Algebra Colloq.* **13**(3), 371–380 (2006).

[3] H. E. Bell, On derivations in near-rings-II, In *Proceedings of Nearrings, Nearfields and K-Loops*, pages 191–197, Kluwer Acad. Publ. (1997).

[4] H. E. Bell and G. Mason, On derivations in near-rings, In *Proceedings of Near-rings and Near-Fields*, pages 31–35, North-Holland Mathematics Studies (1987).

[5] S. Bhavanari, S. P. Kuncham and B. S. Kedukodi, Graph of a nearring with respect to an ideal, *Comm. Algebra* **38**(5), 1957–1967 (2010).

[6] G. Birkenmeier, H. Heatherly and E. Lee, Prime ideals in near-rings, *Results Math.* **24**(1-2), 27–48 (1993).

[7] M. Brešar, On the distance of the composition of two derivations to the generalized derivations, *Glasg. Math. J.* **33**(1), 89–93 (1991).

[8] C. C. Ferrero and G. Ferrero, *Near-Rings: Some developments linked to semi-groups and groups*, Kluwer Acad. Publ. (2002).

[9] Ö. Gólbaşi and Ö.Öğirtici, Multiplicative semiderivations on ideals of semiprime rings, *Palest. J. Math.* **9**(2), 792–800 (2020).

[10] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro and J. P. Sánchez-Hernández, Peterson-Gorenstein-Zierler algorithm for differential convolutional codes, *Appl. Algebra Engrg. Comm. Comput.* **32**(3), 321–344 (2021).

[11] I. N. Herstein, Jordan derivations of prime rings, *Proc. Amer. Math. Soc.* **8**(6), 1104–1110 (1957).

[12] I. N. Herstein, A note on derivations, *Canad. Math. Bull.* **21**(3), 369–370 (1978).

[13] I. N. Herstein, A note on derivations II, *Canad. Math. Bull.* **22**(4), 509–511 (1979).

[14] A. A. M. Kamal and K. H. Al-Shaalan, Commutativity of near-rings with derivations by using algebraic substructures, *Indian J. Pure Appl. Math.* **43**(3), 211–225 (June 2012).

[15] B. S. Kedukodi, S. P. Kuncham and S. Bhavanari, Equiprime, 3-prime and c-prime fuzzy ideals of nearrings, *Soft Comput.* **13**(10), 933–944 (2009).

[16] K. Koppula, B. S. Kedukodi and S. P. Kuncham, Markov frameworks and stock market decision making, *Soft. Comput.* **24**(21), 16413–16424 (2020).

[17] K. Koppula, B. S. Kedukodi and S. P. Kuncham, On perfect ideals of seminearrings, *Beitr. Algebra Geom.* **62**(4), 823–842 (2021).

[18] J. Li and Z. Pan, Annihilator-preserving maps, multipliers, and derivations, *Linear Algebra Appl.* **432**(1), 5–13 (2010).

[19] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications (2nd ed.)*, Cambridge University Press (1994).

[20] A. Mamouni and M. Tamekkante, Commutativity of prime rings involving generalized derivations, *Palest. J. Math.* **10**(2), 407–413 (2021).

[21] G. L. Mullen and C. Mummert, *Finite Fields and Applications*, Student Mathematical Library (AMS) (2007).

[22] G. Pilz, *Near-rings and Near-fields, Handbook of Algebra, Vol I*, Elsevier Science Publishers (1996).

[23] E. C. Posner, Derivations in prime rings, *Proc. Amer. Math. Soc.* **8**(6), 1093–1100 (1957).

[24] X. K. Wang, Derivations in prime nearrings, *Proc. Amer. Math. Soc.* **121**(2), 361–366 (1994).

[25] J. Zhu and C. Xiong, Generalized derivable mappings at zero point on nest algebras, *Acta Math. Sinica (Chin. Ser.)* **45**(4), 783–788 (2002).

[26] J. Zhu and C. Xiong, Generalized derivable mappings at zero point on some reflexive operator algebras, *Linear Algebra Appl.* **397**, 367–379 (2005).

Author information

Aishwarya S., Kedukodi Babushri Srinivas and Kuncham Syam Prasad, Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, Karnataka, India.
E-mail: `babushrisrinivas.k@manipal.edu`

Received: July 27th, 2021
Accepted: December 31st, 2021