International Electronic Journal of Algebra
Volume 38 (2025) 197-211
DOI: 10.24330/ieja.1611885

ON INVOLUTIONS OVER AMALGAMATED ALGEBRAS ALONG AN IDEAL

Brahim Boudine and Mohammed Zerra

Received: 23 June 2023; Accepted: 9 August 2024
Communicated by Tuğçe Pekacar Çalcı

Abstract. Let A and B be two associative rings, I be a two-sided ideal of B, and $f \in Hom(A, B)$. In this paper, we study the involutions on amalgamated algebras. Further, we construct a specific type of involutions on $A \bowtie^f I$ named amalgamated involutions. The paper investigates the Hermitian and skew-Hermitian elements of $A \bowtie^f I$ and determines the sets $H(A \bowtie^f I)$ and $S(A \bowtie^f I)$ for amalgamated involutions. Moreover, the paper derives several identities that establish the commutativity of $A \bowtie^f I$ when A is prime. This allows to construct non-prime rings in which these identities imply their commutativity.

Mathematics Subject Classification (2020): 16W10, 16N60
Keywords: Involution, amalgamated algebra, prime ring

1. Introduction

In this paper, every ring is considered associative and ideals are two-sided. An involution $*$ on a ring R is an additive map on R verifying: (1) $(x.y)^* = y^*.x^*$, and (2) $(x^*)^* = x$, for every $x, y \in R$. A ring that has an involution is known as a ring with involution or a $*$-ring. Involution holds significant importance in algebraic operations (see [1,12]) and finds recently numerous applications in coding theory and cryptography (see for instance [2,9,11]). In particular, involutions that possess only a limited number of fixed points are of interest in cryptography [2]. Fixed points of an involution on R are called Hermitian elements of R, and the set of Hermitian elements of R is denoted by $H(R)$. As well, an element x of R verifying $x^* = -x$ is called skew-Hermitian, and the set of skew-Hermitian elements is denoted by $S(R)$. Let $Z(R)$ be the center of R. If $Z(R) \subseteq H(R)$, then the involution is of the first kind. Otherwise, the involution is of the second kind, in this case, we have $S(R) \cap Z(R) \neq (0)$. Recall that R is called prime if the ideal (0) is prime. Also, a derivation on R is an additive map $d : R \to R$ such that $d(x.y) = d(x).y + x.d(y)$, for any $x, y \in R$. Involutions have been widely used to study the commutativity of prime rings, when some derivations identities hold (see for example [1,10]).

Assume that A and B are two rings, I is an ideal of B, and $f \in Hom(A, B)$. The amalgamated algebra of A and B along I with respect to f is the subring of $A \times B$ defined as follows:

$$A \bowtie^f I := \{(a, f(a) + i) \mid a \in A,\ i \in I\}.$$

In particular, if $A = B$ and $f = id_A$, the amalgamated algebra is called the amalgamated duplication denoted by $A \bowtie I$. It was introduced by D'Anna and Fontana [3,4], since then it knows several developments and applications (for more details see [6]). Due to its special structure, the amalgamated algebra $A \bowtie^f I$ covers many class of algebras (see for example [8]), this has made it interesting to study in recent years; especially, Ebadian and Jabbari [5] studied C^*-algebras defined by amalgamated duplication of C^*-algebras, and Idrissi and Oukhtite [7] studied derivations over amalgamated algebras.

In this paper, we give a complete description of involutions over amalgamated algebras. In particular, we show a special construction of involutions over $A \bowtie^f I$ from involutions over A and I, which we call amalgamated involutions. Further, we study Hermitian and skew-Hermitian elements of $A \bowtie^f I$, and we determine $H(A \bowtie^f I)$ and $S(A \bowtie^f I)$ in the case of amalgamated involutions. This allows us to characterize amalgamated involutions of the first kind and those of the second kind. Finally, we give some identities which imply the commutativity of $A \bowtie^f I$, when A is prime. This provides the possibility to construct non-prime rings in which those identities imply their commutativity.

2. Preliminaries

Throughout this paper, A and B are two rings, I is an ideal of B and $f \in Hom(A, B)$. Let ϕ be an additive map on $A \bowtie^f I$, π_1 and π_2 be projections over $A \bowtie^f I$, defined by $\pi_1 : (a, f(a) + i) \in A \bowtie^f I \mapsto a \in A$, and $\pi_2 : (a, f(a) + i) \in A \bowtie^f I \mapsto f(a) + i \in B$. We write $\phi_1(a) := \pi_1 \circ \phi(a, f(a))$, $\phi'_1(i) := \pi_1 \circ \phi(0, i)$, and $\phi_2(a) := \pi_2 \circ \phi(a, f(a))$, $\phi'_2(i) := \pi_2 \circ \phi(0, i)$; namely, $\phi(a, f(a) + i) = (\phi_1(a) + \phi'_1(i), \phi_2(a) + \phi'_2(i))$.

Recall that, for any $\theta, \beta \in Hom(A, B)$, an additive map $d : A \to B$ is called (β, θ)-derivation from A into B if $d(x, y) = d(x).\theta(y) + \beta(x).d(y)$ for any $x, y \in A$. Let us show the construction of derivations over $A \bowtie^f I$.

Lemma 2.1. [7, Theorem 1] *Let A and B be two rings, I be an ideal of B, and $f \in Hom(A, B)$. Suppose that d is an additive map on $A \bowtie^f I$. Then, the map d is a derivation on $A \bowtie^f I$ if and only if the following conditions hold:*

(1) *d_1 is a derivation on A,*
(2) *d_2 is an (f, f)-derivation from A into B,*
(3) *For all $a \in A$ and $i, i' \in I$, the map d'_1 verifies the following properties:*
- $d'_1(i.i') = 0$,
- $d'_1(f(a).i) = a.d'_1(i)$,
- $d'_1(i.f(a)) = d'_1(i).a$.

(4) *For all $a \in A$ and $i, i' \in I$, the map d'_2 verifies the following properties:*
- $d'_2(i.i') = d'_2(i).i' + i.d'_2(i')$,
- $d'_2(f(a).i) = d_2(a).i + f(a).d'_2(i)$,
- $d'_2(i.f(a)) = d'_2(i).f(a) + i.d_2(a)$.

Next, we show some results on the center of $A \bowtie^f I$.

Lemma 2.2. [7, Lemma 4] *Let A and B be two rings, I be an ideal of B and $f \in Hom(A, B)$. Then,*

$$Z(A \bowtie^f I) = (A \bowtie^f I) \cap (Z(A) \times Z(f(A) + I)).$$

In particular, $Z(A \bowtie^f I) = Z(A) \bowtie^f I$ if and only if $I \subseteq Z(f(A) + I)$.

We prove this result that we will need later.

Lemma 2.3. *Let A and B be two rings, I be an ideal of B and $f \in Hom(A, B)$. Then, the following statements are equivalent:*

(1) *$A \bowtie^f I$ is commutative if and only if A is commutative,*
(2) *$f(A) \subseteq Z_B(I) := \{b \in B \mid b.i = i.b, \forall i \in I\}$ and I is commutative.*

Proof. Let $(a, f(a), i), (a', f(a') + i') \in A \bowtie^f I$. Then, we have

$$(a, f(a) + i).(a', f(a') + i') = (a.a', f(a.a') + f(a).i' + i.f(a') + i.i'),$$

and

$$(a', f(a') + i').(a, f(a) + i) = (a'.a, f(a'.a) + f(a').i + i'.f(a) + i'.i).$$

It is easy to see that the commutativity of $A \bowtie^f I$ implies the commutativity of A. So, we can rewrite the first statement as “A is commutative implies that $A \bowtie^f I$ is commutative”.

(1) $\Rightarrow$ (2) Suppose that either $f(A) \nsubseteq Z_B(I)$ or I is not commutative. We distinguish it into two cases:

Case 1: If $f(A) \not\subseteq Z_B(I)$, then there exist $x \in A$ and $j \in I$ such that $f(x).j \neq j.f(x)$. Suppose that A is commutative, then we have:

$$(x, f(x)).(0, j) = (0, f(x).j) \neq (0, j.f(x)) = (0, j).(x, f(x)).$$

Then, $A \bowtie^f I$ is not commutative.

Case 2: If I is not commutative, then there exist $j, j' \in I$ such that $j'.j \neq j.j'$. Suppose that A is commutative, then we have:

$$(0, j).(0, j') = (0, j.j') \neq (0, j'.j) = (0, j').(0, j).$$

Then, $A \bowtie^f I$ is not commutative.

This proves the desired result.

(2) $\Rightarrow$ (1) Suppose that $f(A) \subseteq Z_B(I) := \{b \in B \mid b.i = i.b, \forall i \in I\}$ and I is commutative. If A is commutative, then we obtain

$$\begin{aligned}(a, f(a)+i).(a', f(a')+i') &= (a.a', f(a.a') + f(a).i' + i.f(a') + i.i'),\\ &= (a'.a, f(a'.a) + i'.f(a) + f(a').i + i'.i),\\ &= (a', f(a')+i').(a, f(a)+i).\end{aligned}$$

Therefore, $A \bowtie^f I$ is commutative. □

Let us recall this important result on the primeness of $A \bowtie^f I$.

Lemma 2.4. [7, Lemma 2] *Let A and B be two rings, I be an ideal of B and $f \in Hom(A, B)$. Then, the following statements are equivalent:*

(1) *$A \bowtie^f B$ is a prime ring,*
(2) *$f(A) + I$ is a prime ring and $f^{-1}(I) = \{0\}$.*

3. Characterization of involutions over $A \bowtie^f I$

In this section, we study the construction of involutions over $A \bowtie^f I$.

Lemma 3.1. *Let φ be an additive map of $A \bowtie^f I$ into $A \bowtie^f I$. Then, the following properties hold:*

- *$\varphi_2(a) - f(\varphi_1(a)) \in I$ for any $a \in A$,*
- *$\varphi'_2(i) - f(\varphi'_1(i)) \in I$ for any $i \in I$.*

Proof. Since $\varphi(a, f(a)+i) = \big(\varphi_1(a) + \varphi'_1(i), \varphi_2(a) + \varphi'_2(i)\big) \in A \bowtie^f I$, there exists $j \in I$ such that $\varphi_2(a)+\varphi'_2(i) = f(\varphi_1(a)+\varphi'_1(i))+j$; namely, $\varphi_2(a)+\varphi'_2(i)-f(\varphi_1(a)+\varphi'_1(i)) = j \in I$. In particular, if $i = 0$, then we get that $\varphi_2(a) - f(\varphi_1(a)) \in I$, and if $a = 0$, then we get that $\varphi'_2(i) - f(\varphi'_1(i)) \in I$. □

Theorem 3.2. *Let A and B be two rings, I be an ideal of B, and $f \in Hom(A,B)$. Suppose that inv is an additive map on $A \bowtie^f I$. Then, the map inv is an involution on $A \bowtie^f I$ if and only if the following conditions hold:*

(1) $inv_1(a.a') = inv_1(a').inv_1(a)$ *and* $inv_2(a.a') = inv_2(a').inv_2(a)$ *for every* $a, a' \in A$,

(2) $inv_1'(i.i') = inv_1'(i').inv_1'(i)$ *and* $inv_2'(i.i') = inv_2'(i').inv_2'(i)$ *for every* $i, i' \in I$,

(3) *For all $a \in A$ and $i \in I$, we have the following properties:*
   - (a) $inv_1'(i.f(a)) = inv_1(a).inv_1'(i)$ *and* $inv_2'(i.f(a)) = inv_2(a).inv_2'(i)$,
   - (b) $inv_1'(f(a).i) = inv_1'(i).inv_1(a)$ *and* $inv_2'(f(a).i) = inv_2'(i).inv_2(a)$,
   - (c) $inv_1\big(inv_1(a)\big) = a - inv_1'\big(inv_2(a) - f(inv_1(a))\big)$ *and* $inv_2\big(inv_1(a)\big) = f(a) - inv_2'\big(inv_2(a) - f(inv_1(a))\big)$,
   - (d) $inv_1\big(inv_1'(i)\big) = inv_1'\big(f(inv_1'(i)) - inv_2'(i)\big)$ *and* $inv_2\big(inv_1'(i)\big) = i - inv_2'\big(inv_2'(i) - f(inv_1'(i))\big)$.

Proof. Let $(a, f(a)+i), (a', f(a')+i') \in A \bowtie^f I$. Then, we have

$$inv((a, f(a)+i).(a', f(a')+i')) = inv(a', f(a')+i').inv(a, f(a)+i).$$

It follows that

$$\begin{aligned}\pi_1 \circ inv((a, f(a)+i).(a', f(a')+i')) = \quad & inv_1(a').inv_1(a) + inv_1(a').inv_1'(i) \\ & + inv_1'(i').inv_1(a) + inv_1'(i').inv_1'(i).\end{aligned}$$

Also, we have:

$$inv((a, f(a)+i).(a', f(a')+i')) = inv(a.a', f(a.a') + f(a).i' + i.f(a') + i.i').$$

Taking $i = i' = 0$, we get that

$$inv_1(a.a') = inv_1(a').inv_1(a).$$

As well as, taking $a = a' = 0$, we get that

$$inv_1'(i.i') = inv_1'(i').inv_1'(i).$$

Further, if $a = 0$ and $i' = 0$, then we get:

$$inv_1'(i.f(a')) = inv_1(a').inv_1'(i).$$

And if $a' = 0$ and $i = 0$, then we get:

$$inv_1'(f(a).i') = inv_1'(i').inv_1(a).$$

By the same method, we get that

$$\begin{cases} inv_2(a.a') = inv_2(a').inv_2(a), \\ inv_2'(i.i') = inv_2'(i').inv_2'(i), \\ inv_2'(i.f(a')) = inv_2(a').inv_2'(i), \\ inv_2'(f(a).i') = inv_2'(i').inv_2(a). \end{cases}$$

Since $inv^2 = inv$, we get that

$$inv_1\big(inv_1(a) + inv_1'(i)\big) + inv_1'\big(inv_2(a) + inv_2'(i) - f(inv_1(a) + inv_1'(i))\big) = a,$$

and

$$inv_2\big(inv_1(a) + inv_1'(i)\big) + inv_2'\big(inv_2(a) + inv_2'(i) - f(inv_1(a) + inv_1'(i))\big) = f(a) + i.$$

Let $i = 0$, then we obtain

$$inv_1\big(inv_1(a)\big) + inv_1'\big(inv_2(a) - f(inv_1(a))\big) = a,$$

and

$$inv_2\big(inv_1(a)\big) + inv_2'\big(inv_2(a) - f(inv_1(a))\big) = f(a).$$

Then,

$$f\Big(inv_1\big(inv_1(a)\big) + inv_1'\big(inv_2(a) - f(inv_1(a))\big)\Big) = inv_2\big(inv_1(a)\big) + inv_2'\big(inv_2(a) - f(inv_1(a))\big).$$

Further, we obtain

$$inv_1\big(inv_1'(i)\big) = inv_1'\big(f(inv_1'(i)) - inv_2'(i)\big),$$

and

$$inv_2\big(inv_1'(i)\big) = inv_2'\big(f(inv_1'(i)) - inv_2'(i)\big) + i.$$

Conversely, we have

$$\begin{aligned} L &:= inv\Big((a, f(a) + i).(a', f(a') + i')\Big), \\ &= inv\Big(a.a', f(a.a') + f(a).i' + i.f(a') + i.i'\Big), \\ &= \big(inv_1(a.a') + inv_1'(f(a).i' + i.f(a') + i.i'), inv_2(a.a') + inv_2'(f(a).i' + i.f(a') + i.i')\big). \end{aligned}$$

Then,

$$\begin{aligned} \pi_1(L) &= inv_1(a.a') + inv_1'(f(a).i') + inv_1'(i.f(a')) + inv_1'(i.i'), \\ &= inv_1(a').inv_1(a) + inv_1'(i').inv_1(a) + inv_1(a').inv_1'(i) + inv_1'(i').inv_1'(i), \\ &= \big(inv_1(a') + inv_1'(i')\big).\big(inv_1(a) + inv_1'(i)\big), \\ &= \pi_1\Big(inv(a', f(a') + i').inv(a, f(a) + i)\Big). \end{aligned}$$

As well as, we have

$$\begin{aligned} \pi_2(L) &= inv_2(a.a') + inv_2'(f(a).i') + inv_2'(i.f(a')) + inv_2'(i.i'), \\ &= inv_2(a').inv_2(a) + inv_2'(i').inv_2(a) + inv_2(a').inv_2'(i) + inv_2'(i').inv_2'(i), \\ &= \big(inv_2(a') + inv_2'(i')\big).\big(inv_2(a) + inv_2'(i)\big), \\ &= \pi_2\Big(inv(a', f(a') + i').inv(a, f(a) + i)\Big). \end{aligned}$$

Therefore, we obtain

$$inv\Big((a, f(a)+i).(a', f(a')+i')\Big) = inv(a', f(a')+i').inv(a, f(a)+i).$$

On the other hand, we have

$$\begin{aligned} M \quad &:= inv\Big(inv\big((a, f(a)+i)\big)\Big),\\ &= inv\Big(inv_1(a)+inv'_1(i), inv_2(a)+inv'_2(i)\Big),\\ &= inv\Big(inv_1(a)+inv'_1(i), f(inv_1(a)+inv'_1(i))+inv_2(a)-f(inv_1(a))+inv'_2(i)-f(inv'_1(i))\Big). \end{aligned}$$

Then, we get that

$$\begin{aligned} \pi_1(M) = \quad & inv_1\big(inv_1(a)+inv'_1(i)\big)+inv'_1\Big(inv_2(a)-f\big(inv_1(a)\big)+inv'_2(i)-f\big(inv'_1(i)\big)\Big),\\ = \quad & inv_1(inv_1(a))+inv_1(inv'_1(i))+inv'_1\Big(inv_2(a)-f\big(inv_1(a)\big)\Big)+inv'_1\Big(inv'_2(i)-f\big(inv'_1(i)\big)\Big),\\ = \quad & \Big(inv_1(inv_1(a))+inv'_1\Big(inv_2(a)-f\big(inv_1(a)\big)\Big)\Big)+\Big(inv_1(inv'_1(i))+inv'_1\Big(inv'_2(i)-f\big(inv'_1(i)\big)\Big)\Big),\\ = \quad & a. \end{aligned}$$

As well as, we have

$$\begin{aligned} \pi_2(M) = \quad & inv_2\big(inv_1(a)+inv'_1(i)\big)+inv'_2\Big(inv_2(a)-f\big(inv_1(a)\big)+inv'_2(i)-f\big(inv'_1(i)\big)\Big),\\ = \quad & inv_2(inv_1(a))+inv_2(inv'_1(i))+inv'_2\Big(inv_2(a)-f\big(inv_1(a)\big)\Big)+inv'_2\Big(inv'_2(i)-f\big(inv'_1(i)\big)\Big),\\ = \quad & \Big(inv_2(inv_1(a))+inv'_2\Big(inv_2(a)-f\big(inv_1(a)\big)\Big)\Big)+\Big(inv_2(inv'_1(i))+inv'_2\Big(inv'_2(i)-f\big(inv'_1(i)\big)\Big)\Big),\\ & = f(a)+i. \end{aligned}$$

Therefore, we obtain

$$inv\big(inv(a, f(a)+i)\big) = (a, f(a)+i).$$

Thus, *inv* is an involution on $A \bowtie^f I$. □

Corollary 3.3. *Let A be a ring and I be an ideal of A. Suppose that inv is an additive map on the amalgamated duplication $A \bowtie I$. Then, the map inv is an involution on $A \bowtie I$ if and only if the following conditions hold:*

1. $inv_1(a.a') = inv_1(a').inv_1(a)$ *and* $inv_2(a.a') = inv_2(a').inv_2(a)$ *for every* $a, a' \in A$,
2. $inv'_1(i.i') = inv'_1(i').inv'_1(i)$ *and* $inv'_2(i.i') = inv'_2(i').inv'_2(i)$ *for every* $i, i' \in I$,
3. *For all $a \in A$ and $i \in I$, we have the following properties:*
   - $inv'_1(i.a) = inv_1(a).inv'_1(i)$ *and* $inv'_2(i.a) = inv_2(a).inv'_2(i)$,
   - $inv'_1(a.i) = inv'_1(i).inv_1(a)$ *and* $inv'_2(a.i) = inv'_2(i).inv_2(a)$,
   - $inv_1\big(inv_1(a)\big) = a - inv'_1\big(inv_2(a) - inv_1(a)\big)$ *and* $inv_2\big(inv_1(a)\big) = a - inv'_2\big(inv_2(a) - inv_1(a)\big)$,
   - $inv_1\big(inv'_1(i)\big) = inv'_1\big(inv'_1(i) - inv'_2(i)\big)$ *and* $inv_2\big(inv'_1(i)\big) = i - inv'_2\big(inv'_2(i) - inv'_1(i)\big)$.

Next, we show a special construction of involutions over $A \bowtie^f I$, which we call amalgamated involutions.

Theorem 3.4. *Let A and B be two rings, I be an ideal of B, and $f \in Hom(A, B)$. Suppose that $*$ is an involution on A and ι is an involution on I such that $\iota(i.f(a)) = f(a^*).\iota(i)$ and $\iota(f(a).i) = \iota(i).f(a^*)$ for every $a \in A$ and $i \in I$. Then, there exists an involution inv on $A \bowtie^f I$, where:*

- $inv_1 = *$,
- $inv'_1 = 0$,
- $inv_2(a) = f(a^*)$ *for every* $a \in A$,
- $inv'_2 = \iota$.

In this case, the involution inv is called the amalgamated involution on $A \bowtie^f I$ associated to $*$ and ι.

Proof. We verify that all the properties of Theorem 3.2 hold.
Let $a, a' \in A$ and $i, i' \in I$.

(1) We have $inv_1(a.a') = (a.a')^* = (a')^*.a^* = inv_1(a').inv_1(a)$. As well,

$$inv_2(a.a') = f((a.a')^*) = f((a')^*.a^*) = f((a')^*).f(a^*) = inv_2(a').inv_2(a).$$

(2) It is obvious that $inv'_1(i.i') = inv'_1(i').inv'_1(i) = 0$. Moreover,

$$inv'_2(i.i') = \iota(i.i') = \iota(i').\iota(i) = inv'_2(i').inv'_2(i).$$

(3) (a) Obviously, we have $inv'_1(i.f(a)) = inv_1(a).inv'_1(i) = 0$. Moreover,

$$inv'_2(i.f(a)) = \iota(i.f(a)) = f(a^*).\iota(i) = inv_2(a).inv'_2(i).$$

(b) Similarly, we get $inv'_1(f(a).i) = inv'_1(i).inv_1(a)$ and $inv'_2(f(a).i) = inv'_2(i).inv_2(a)$.

(c) We have $inv_1(inv_1(a)) = (a^*)^* = a$, and

$$a - inv'_1(inv_2(a) - f(inv_1(a))) = a - 0 = a.$$

Then, $inv_1(inv_1(a)) = a - inv'_1(inv_2(a) - f(inv_1(a)))$.
Also, we have $inv_2(inv_1(a)) = f\big((a^*)^*\big) = f(a)$, and

$$f(a) - inv'_2\big(inv_2(a) - f(inv_1(a))\big) = f(a) - \iota\big(f(a^*) - f(a^*)\big) = f(a).$$

Therefore, $inv_2(inv_1(a)) = f(a) - inv'_2\big(inv_2(a) - f(inv_1(a))\big)$.

(d) It is obvious that $inv_1\big(inv'_1(i)\big) = inv'_1\big(f(inv'_1(i)) - inv'_2(i)\big) = 0$. Moreover, it is clear that $inv_2(inv'_1(i)) = 0$, and we have

$$i - inv'_2\big(inv'_2(i) - f(inv'_1(i))\big) = i - \iota\big(\iota(i)\big) = i - i = 0.$$

Therefore, $inv_2(inv'_1(i)) = i - inv'_2\big(inv'_2(i) - f(inv'_1(i))\big)$.

By Theorem 3.2, we conclude that inv is an involution on $A \bowtie^f I$. □

4. Hermitian and skew-Hermitian elements of $A \bowtie^f I$

In this section, we study Hermitian and skew-Hermitian elements of $A \bowtie^f I$. We leave the proof of these following easy lemmas to the reader.

Lemma 4.1. *Let A and B be two rings, I be an ideal of B, and $f \in Hom(A, B)$. Suppose that inv is an involution on $A \bowtie^f I$ and $(a, f(a)+i) \in A \bowtie^f I$. Then, we have the following statements:*

- *$(a, f(a)+i)$ is Hermitian if and only if $inv_1(a)+inv'_1(i) = a$ and $inv_2(a)+inv'_2(i) = f(a)+i$,*
- *$(a, f(a)+i)$ is skew-Hermitian if and only if $inv_1(a)+inv'_1(i) = -a$ and $inv_2(a)+inv'_2(i) = -f(a)-i$.*

Lemma 4.2. *Let A and B be two rings, I be an ideal of B, and $f \in Hom(A, B)$. Suppose that inv is an involution on $A \bowtie^f I$. Then, the involution inv is of the first kind if and only if for any $(a, f(a)+i) \in Z(A \bowtie^f I)$, we have $inv_1(a)+inv'_1(i) = a$ and $inv_2(a)+inv'_2(i) = f(a)+i$.*

Let us show Hermitian and skew-Hermitian elements of $A \bowtie^f I$ in the case of amalgamated involutions.

Theorem 4.3. *Let A and B be two rings, I be an ideal of B, and $f \in Hom(A, B)$. Suppose that inv is an amalgamated involution on $A \bowtie^f I$. Then,*

$$H(A \bowtie^f I) = H(A) \bowtie^f H(I) \text{ and } S(A \bowtie^f I) = S(A) \bowtie^f S(I).$$

Proof. Let $*$ be the involution on A and ι be the involution on I such that inv is associated to $*$ and ι. Let $(a, f(a)+i) \in H(A \bowtie^f I)$. Then, $inv(a, f(a)+i) = (a, f(a)+i)$. It follows from Lemma 4.1 that

$$\begin{cases} inv_1(a)+inv'_1(i) = a, \\ inv_2(a)+inv'_2(i) = f(a)+i, \end{cases}$$

namely, we get

$$\begin{cases} a^* = a, \\ f(a^*)+\iota(i) = f(a)+i. \end{cases}$$

Thus, a is Hermitian in A and i is Hermitian in I; namely, $(a, f(a)+i) \in H(A) \bowtie^f H(I)$. This shows that $H(A \bowtie^f I) \subseteq H(A) \bowtie^f H(I)$. Let now $(a, f(a)+i) \in H(A) \bowtie^f H(I)$. Then, $a \in H(A)$ and $i \in H(I)$; namely, $a^* = a$ and $\iota(i) = i$.

Therefore,

$$\begin{aligned} inv(a, f(a)+i) &= (inv_1(a)+inv_1'(i), inv_2(a)+inv_2'(i)), \\ &= (a^*, f(a^*)+\iota(i)), \\ &= (a, f(a)+i). \end{aligned}$$

Thus, $(a, f(a)+i) \in H(A \bowtie^f I)$. Hence, $H(A \bowtie^f I) = H(A) \bowtie^f H(I)$. Suppose now that $(a, f(a)+i) \in S(A \bowtie^f I)$. Then, $inv(a, f(a)+i) = (-a, -f(a)-i)$. By Lemma 4.1, we get that

$$\begin{cases} inv_1(a)+inv_1'(i) = -a, \\ inv_2(a)+inv_2'(i) = -f(a)-i, \end{cases}$$

so that

$$\begin{cases} a^* = -a, \\ f(a^*)+\iota(i) = f(-a)-i. \end{cases}$$

Thus, a is skew-Hermitian in A and i is skew-Hermitian in I; namely, $(a, f(a)+i) \in S(A) \bowtie^f S(I)$. This proves that $S(A \bowtie^f I) \subseteq S(A) \bowtie^f S(I)$. On the other hand, if $(a, f(a)+i) \in S(A) \bowtie^f S(I)$, then $a \in S(A)$ and $i \in S(I)$; namely, $a^* = -a$ and $\iota(i) = -i$. Therefore,

$$\begin{aligned} inv(a, f(a)+i) &= (inv_1(a)+inv_1'(i), inv_2(a)+inv_2'(i)), \\ &= (a^*, f(a^*)+\iota(i)), \\ &= (-a, f(-a)-i). \end{aligned}$$

It follows that $(a, f(a)+i) \in S(A \bowtie^f I)$. Hence, $S(A \bowtie^f I) = S(A) \bowtie^f S(I)$. □

So, we can now characterize amalgamated involutions of the first kind and of the second kind.

Theorem 4.4. *Let A and B be two rings, I be an ideal of B such that $I \subseteq Z(f(A)+I)$, and $f \in Hom(A, B)$. Suppose that inv is an amalgamated involution on $A \bowtie^f I$ associated to $*$ and ι. Then, inv is an involution of the first kind if and only if the following statements hold:*

- *the involution $*$ is of the first kind,*
- *$\iota = id_I$. In this case, I is commutative.*

Proof. By Lemma 2.2, we have $Z(A \bowtie^f I) = Z(A) \bowtie^f I$ and by Theorem 4.3, we have $H(A \bowtie^f I) = H(A) \bowtie^f H(I)$. Therefore, $Z(A) \subseteq H(A)$ and $I \subseteq H(I)$; namely, the involution $*$ is of the first kind and every element in I is Hermitian. It follows that $\iota(i) = i$, for every $i \in I$. So that $\iota = id_I$. Since ι is an involution on I, for every elements $i, j \in I$, we have $x.y = \iota(x.y) = \iota(y).\iota(x) = y.x$. Thus I is commutative. □

By Theorem 4.4, it is easy to get the following result:

Corollary 4.5. *Let A and B be two rings, I be an ideal of B such that $I \subseteq Z(f(A)+I)$, and $f \in Hom(A,B)$. Suppose that inv is an amalgamated involution on $A \bowtie^f I$ associated to $*$ and ι. Then, inv is an involution of the second kind if and only if one of the following statements holds:*

- *the involution $*$ is of the second kind,*
- *$\iota \neq id_I$.*

5. On the commutativity of $A \bowtie^f I$ when A is prime

In this section, we investigate the commutativity of $A \bowtie^f I$ with amalgamated involutions provided by derivations satisfying some algebraic identities. Recall that a ring A is called 2-torsion free, if for any $x \in A$, we have

$$x + x = 0 \Rightarrow x = 0.$$

Theorem 5.1. *Let A be a 2-torsion free prime ring and B be a ring, I be a commutative ideal of B, and $f \in Hom(A,B)$ such that $f(A) \subseteq Z_B(I)$. Suppose that $*$ is an involution of second kind over A, inv is an amalgamated involution on $A \bowtie^f I$ associated to $*$ and ι and d is a derivation over $A \bowtie^f I$. If one of the following statements holds:*

1. *$[d(a,f(a)+i), inv(a,f(a)+i)] \in Z(A \bowtie^f I)$ for every $(a,f(a)+i) \in A \bowtie^f I$,*
2. *$d(a,f(a)+i).d(inv(a,f(a)+i)) = \pm(a,f(a)+i).inv(a,f(a)+i)$ for every $(a,f(a)+i) \in A \bowtie^f I$,*
3. *$[d(a,f(a)+i), d(inv(a,f(a)+i))] \pm [(a,f(a)+i), inv(a,f(a)+i)] \in Z(A \bowtie^f I)$ for every $(a,f(a)+i) \in A \bowtie^f I$,*

then $A \bowtie^f I$ is commutative.

Proof. By Lemma 2.1, we have d_1 is a derivation on A. Let $i \in I$. Since I is commutative and $f(A) \subseteq Z_B(I)$, for every $j \in I$ and $a \in A$, we get that

$$i.(f(a)+j) = i.f(a) + i.j = f(a).i + j.i = (f(a)+j).i;$$

namely, $I \subseteq Z(f(A)+I)$. Then, by Lemma 2.2, we get that $Z(A \bowtie^f I) = Z(A) \bowtie^f I$. Let $a \in A$.

(1) Set $E_1 = [d(a,f(a)), inv(a,f(a))]$. Then, we obtain

$$\begin{aligned}
E_1 &= d(a,f(a)).inv(a,f(a)) - inv(a,f(a)).d(a,f(a)),\\
&= \big(d_1(a),d_2(a)\big).\big(a^*,f(a^*)\big) - \big(a^*,f(a^*)\big).\big(d_1(a),d_2(a)\big),\\
&= \big(d_1(a).a^*, d_2(a).f(a^*\big) - \big(a^*.d_1(a), f(a^*).d_2(a)\big),\\
&= \big([d_1(a),a^*],[d_2(a),f(a^*)]\big).
\end{aligned}$$

Since $E_1 \in Z(A \bowtie^f I)$, we get that $[d_1(a), a^*] \in Z(A)$. Then, Theorem 3.7 in [12] proves that A is commutative. Thus, Lemma 2.3 shows that $A \bowtie^f I$ is commutative.

(2) Set $E_2 = d(a, f(a)).d(inv(a, f(a))) \pm (a, f(a)).inv(a, f(a))$. Then, we obtain

$$\begin{aligned} E_2 &= d(a, f(a)).d(inv(a, f(a))) \pm (a, f(a)).inv(a, f(a)), \\ &= \big(d_1(a), d_2(a)\big).\big(d_1(a^*), d_2(a^*)\big) \pm (a, f(a)).(a^*, f(a^*)), \\ &= \big(d_1(a).d_1(a^*), d_2(a).d_2(a^*)\big) \pm \big(a.a^*, f(a).f(a^*)\big), \\ &= \big(d_1(a).d_1(a^*) \pm a.a^*, d_2(a).d_2(a^*) \pm f(a.a^*)\big). \end{aligned}$$

Since $E_2 = (0, 0)$, we get that $d_1(a).d_1(a^*) \pm a.a^* = 0$. Then, Theorem 2.6 in [1] proves that A is commutative. Thus, Lemma 2.3 shows that $A \bowtie^f I$ is commutative.

(3) Set $E_3 = [d(a, f(a)), d(inv(a, f(a)))] \pm [(a, f(a)), inv(a, f(a))]$. Then, we obtain

$$\begin{aligned} E_3 = \;& [d(a, f(a)), d(inv(a, f(a)))] \pm [(a, f(a)), inv(a, f(a))], \\ = \;& [(d_1(a), d_2(a)), (d_1(a^*), d_2(a^*))] \pm [(a, f(a)), (a^*, f(a^*))], \\ = \;& (d_1(a), d_2(a)).(d_1(a^*), d_2(a^*)) - (d_1(a^*), d_2(a^*)).(d_1(a), d_2(a)) \\ & \pm\big((a, f(a)).(a^*, f(a^*)) - (a^*, f(a^*)).(a, f(a))\big), \\ = \;& (d_1(a).d_1(a^*), d_2(a).d_2(a^*)) - (d_1(a^*)d_1(a), d_2(a^*).d_2(a)) \\ & \pm\big((a.a^*, f(a.a^*)) - (a^*.a, f(a^*.a))\big), \\ = \;& \big([d_1(a), d_1(a^*)], [d_2(a), d_2(a^*)]\big) \pm \big[a, a^*], [f(a), f(a^*)]\big), \\ = \;& \big([d_1(a), d_1(a^*)] \pm [a, a^*], [d_2(a), d_2(a^*)] \pm [f(a), f(a^*)]\big). \end{aligned}$$

Since $E_3 \in Z(A \bowtie^f I)$, we get that $[d_1(a), d_1(a^*)] \pm [a, a^*] \in Z(A)$. Then, Theorem 3.1 in [12] proves that A is commutative. Thus, Lemma 2.3 shows that $A \bowtie^f I$ is commutative. □

Remark 5.2. If $f(A) + I$ is not prime or $f^{-1}(I) \neq \{0\}$, then Lemma 2.4 shows that $A \bowtie^f I$ is not prime. In this case, we get an example in which the identities of Theorem 5.1 imply the commutativity of a non-prime ring.

Theorem 5.3. *Let A be a prime ring such that $char(A) \neq 2$ and B be a ring, I be a commutative ideal of B, and $f \in Hom(A, B)$ such that $f(A) \subseteq Z_B(I)$. Suppose that $*$ is an involution of second kind over A, inv is an amalgamated involution on $A \bowtie^f I$ associated to $*$ and ι, and d is a derivation over $A \bowtie^f I$. If one of the following statements holds:*

(1) $d\big([(a, f(a) + i), inv(a, f(a) + i)]\big) = (0, 0)$ *for every* $(a, f(a) + i) \in A \bowtie^f I$,

(2) $d(a, f(a) + i).d(inv(a, f(a) + i)) \pm (a, f(a) + i).inv(a, f(a) + i) = (0, 0)$ *for every* $(a, f(a) + i) \in A \bowtie^f I$,

(3) $d(a, f(a)+i).d(inv(a, f(a)+i)) \pm inv(a, f(a)+i).(a, f(a)+i) = (0,0)$ *for every* $(a, f(a)+i) \in A \bowtie^f I$,

(4) $d\big((a, f(a)+i).inv(a, f(a)+i)\big) \pm (a, f(a)+i).inv(a, f(a)+i) = (0,0)$ *for every* $(a, f(a)+i) \in A \bowtie^f I$,

(5) $d\big((a, f(a)+i).inv(a, f(a)+i)\big) \pm inv(a, f(a)+i).(a, f(a)+i) = (0,0)$ *for every* $(a, f(a)+i) \in A \bowtie^f I$,

then $A \bowtie^f I$ *is commutative.*

Proof. Let $a \in A$.

(1) Set $F_1 = d\big([(a, f(a)), inv(a, f(a))]\big)$. Then

$$\begin{aligned} F_1 = (0,0) \quad &\Rightarrow d\big([(a, f(a)), (a^*, f(a^*))]\big) = (0,0), \\ &\Rightarrow d\big((a.a^*, f(a.a^*)) - (a^*.a, f(a^*.a))\big) = (0,0), \\ &\Rightarrow d\big([a, a^*], [f(a), f(a^*)]\big) = (0,0), \\ &\Rightarrow d_1\big([a, a^*]\big) = 0. \end{aligned}$$

By Theorem 2.2 in [1], we get that A is commutative. Thus, Lemma 2.3 shows that $A \bowtie^f I$ is commutative.

(2) Set $F_2 = d(a, f(a)).d(inv(a, f(a))) \pm (a, f(a)).inv(a, f(a))$. Then,

$$\begin{aligned} F_2 = (0,0) \quad &\Rightarrow \big(d_1(a), d_2(a)\big).\big(d_1(a^*), d_2(a^*)\big) \pm (a, f(a)).(a^*, f(a^*) = (0,0), \\ &\Rightarrow \big(d_1(a).d_1(a^*, d_2(a).d_2(a^*)\big) \pm (a.a^*, f(a.a^*) = (0,0), \\ &\Rightarrow \big(d_1(a).d_1(a^*) \pm a.a^*, d_2(a).d_2(a^*) \pm f(a.a^*)\big) = (0,0), \\ &\Rightarrow d_1(a).d_1(a^*) \pm a.a^* = 0. \end{aligned}$$

By Theorem 2.6 in [1], we get that A is commutative. Thus, Lemma 2.3 shows that $A \bowtie^f I$ is commutative.

(3) Set $F_3 = d(a, f(a)).d(inv(a, f(a))) \pm inv(a, f(a)).(a, f(a))$. By the same method in the proof of (2), we get $F_3 = (0,0) \quad \Rightarrow d_1(a).d_1(a^*) \pm a^*.a = 0$. By Theorem 2.7 in [1], we get that A is commutative. Thus, Lemma 2.3 shows that $A \bowtie^f I$ is commutative.

(4) Set $F_4 = d\big((a, f(a)).inv(a, f(a))\big) \pm (a, f(a)).inv(a, f(a))$. Then,

$$\begin{aligned} F_4 = (0,0) \quad &\Rightarrow d\big(a.a^*, f(a.a^*)\big) \pm (a.a^*, f(a.a^*) = (0,0), \\ &\Rightarrow \big(d_1(a.a^*), d_2(a.a^*)\big) \pm (a.a^*, f(a.a^*) = (0,0), \\ &\Rightarrow \big(d_1(a.a^*) \pm a.a^*, d_2(a.a^*) - f(a.a^*)\big) = (0,0), \\ &\Rightarrow d_1(a.a^*) \pm a.a^* = 0. \end{aligned}$$

By Theorem 2.4 in [1], we get that A is commutative. It follows by Lemma 2.3 that $A \bowtie^f I$ is commutative.

(5) Set $F_5 = d\big((a, f(a)).inv(a, f(a))\big) \pm inv(a, f(a)).(a, f(a))$. By the same method in the proof of (4), we get $F_5 = (0, 0) \Rightarrow d_1(a.a^*) \pm a^*.a = 0$. By Theorem 2.5 in [1], we get that A is commutative. It follows by Lemma 2.3 that $A \bowtie^f I$ is commutative. □

Remark 5.4. If $f(A) + I$ is not prime or $f^{-1}(I) \neq \{0\}$, then Lemma 2.4 shows that $A \bowtie^f I$ is not prime. In this case, we get an example in which the identities of Theorem 5.3 imply the commutativity of a non-prime ring.

Acknowledgement. The authors would like to thank the referee for the valuable suggestions and comments.

Declarations. There is no funding source. The authors declare no conflicts of interest. No data set is associated with this article.

References

[1] S. Ali, N. A. Dar and M. Asci, *On derivations and commutativity of prime rings with involution*, Georgian Math. J., 23(1) (2016), 9-14.

[2] P. Charpin, S. Mesnager and S. Sarkar, *Involutions over the Galois field* $\mathbb{F}_{2^n}$, IEEE Trans. Inform. Theory, 62(4) (2016), 2266-2276.

[3] M. D'Anna and M. Fontana, *An amalgamated duplication of a ring along an ideal: the basic properties*, J. Algebra Appl., 6(3) (2007), 443-459.

[4] M. D'Anna and M. Fontana, *The amalgamated duplication of a ring along a multiplicative-canonical ideal*, Ark. Mat., 45(2) (2007), 241-252.

[5] A. Ebadian and A. Jabbari, *C^*-algebras defined by amalgamated duplication of C^*-algebras*, J. Algebra Appl., 20(2) (2021), 2150019 (15 pp).

[6] A. El Khalfi, H. Kim and N. Mahdou, *Amalgamation extension in commutative ring theory: a survey*, Moroc. J. Algebra Geom. Appl., 1(1) (2022), 139-182.

[7] M. A. Idrissi and L. Oukhtite, *Derivations over amalgamated algebras along an ideal*, Comm. Algebra, 48(3) (2020), 1224-1230.

[8] H. Javanshiri and M. Nemati, *Amalgamated duplication of the Banach algebra $\mathfrak{A}$ along a $\mathfrak{A}$-bimodule $\mathcal{A}$*, J. Algebra Appl., 17(9) (2018), 1850169 (21 pp).

[9] G. Luo, X. Cao and S. Mesnager, *Several new classes of self-dual bent functions derived from involutions*, Cryptogr. Commun., 11(6) (2019), 1261-1273.

[10] A. Mamouni, L. Oukhtite and M. Zerra, *Certain algebraic identities on prime rings with involution*, Comm. Algebra, 49(7) (2021), 2976-2986.

[11] S. Mesnager, M. Yuan and D. Zheng, *More about the corpus of involutions from two-to-one mappings and related cryptographic S-boxes*, IEEE Trans. Inform. Theory, 69(2) (2023), 1315-1327.

[12] B. Nejjar, A. Kacha, A. Mamouni and L. Oukhtite, *Commutativity theorems in rings with involution*, Comm. Algebra, 45(2) (2017), 698-708.

Brahim Boudine (Corresponding Author)
Department of Mathematics
Faculty of Sciences Meknes
Moulay Ismail University
30000 Fez, Morocco
e-mail: brahimboudine.bb@gmail.com

Mohammed Zerra
Department of Mathematics
Faculty of Sciences and Technology
Sidi Mohamed Ben Abdellah University
30000 Fez, Morocco
e-mail: mohamed.zerra@gmail.com