JOURNAL OF ALGEBRA **169**, 304–327 (1994)

Lie Isomorphisms in Prime Rings with Involution

K. I. BEIDAR

Moscow State University, 117234, Moscow, Russia

W. S. MARTINDALE 3RD

University of Massachusetts, Amherst, Massachusetts 01003

AND

A. V. MIKHALEV

Moscow State University, 117234, Moscow, Russia

Communicated by Susan Montgomery

Received January 20, 1993

Let R and R' be prime rings with involutions of the first kind and with respective Lie subrings of skew elements K and K'. Furthermore assume $(RC : C) \neq 1, 4, 9, 16, 25, 64$, where C is the extended centroid of R. It is shown that any Lie isomorphism of K onto K' can be extended uniquely to an associative isomorphism of $\langle K \rangle$ onto $\langle K' \rangle$, where $\langle K \rangle$ and $\langle K' \rangle$ are respectively the associative subrings generated by K and K'. © 1994 Academic Press, Inc.

1. INTRODUCTION

In his 1961 AMS Hour Talk, titled "Lie and Jordan Structures in Simple, Associative Rings," Herstein posed several problems he deemed worthy of attention [4]. Among these were the following questions (which we indicate in a rather loose fashion):

Problem 1. Is every Lie automorphism ϕ of a simple associative ring R given by (or "almost" given by) an automorphism σ or the negative of an antiautomorphism σ of R?

0021-8693/94 $6.00

Problem 2. If R is a simple ring with involution $*$ and K denotes the Lie ring of skew elements of R under $*$, is every Lie automorphism ϕ of K induced by (or "almost" induced by) an automorphism σ of R?

The qualification "almost" refers to the possibility that ϕ and σ may differ by an additive mapping τ of R into the center which sends commutators to 0.

The resolution of these problems in the classical case $R = M_n(F)$, F a field, has been well-known for a long time ([7, Chap. 10]). In 1951 Hua [6] solved Problem 1 for R a simple Artinian ring $M_n(D)$, D a division ring, $n \geq 3$. A more general situation for Problem 1 was subsequently considered by Martindale ([8, 9]) in which Lie isomorphisms ϕ: $R \rightarrow R'$ (R, R' primitive in [8] and prime in [9]) were investigated and in which the matrix condition $n \geq 3$ was replaced by the condition that R contains three orthogonal idempotents whose sum is 1 (in [9] only two idempotents were required). A close look at the results of these papers reveals the fact that the image of σ in general requires a "larger" ring than R' and that the image of τ requires a "larger" field than the center of R'. We note that it was precisely this necessity to enlarge certain rings that was the motivation for developing the notions of extended centroid and central closure which proved so useful in characterizing prime GPI rings [10]. The final breakthrough on Problem 1 was made only recently by Bresar [3]. Here, as a corollary to a general result on biadditive mappings in prime rings, he removed the assumption of orthogonal idempotents altogether and thereby settled Problem 1 in full generality.

THEOREM 1 (Bresar [3, Theorem 3]). *Let R and R' be prime rings of characteristic $\neq 2$, neither of which satisfies the standard identity S_4. Then any Lie isomorphism ϕ of R onto R' is of the form $\phi = \sigma + \tau$, where σ is either an isomorphism or the negative of an anti-isomorphism of R into the central closure of R' and τ is an additive mapping of R into the extended centroid of R' sending commutators to* 0.

The present paper is concerned with Problem 2. Let R be a prime ring with involution $*$, of characteristic $\neq 2, 3$, with $K = \{x \in R \mid x^* = -x\}$ the skew elements of R, and C the extended centroid of R (see [13] for details of these and various other notions we need). The involution $*$ induces an involution $c \rightarrow \bar{c}$ on the field C; we say that $*$ is of the first kind if $c \rightarrow \bar{c}$ is the identity mapping, otherwise $*$ is of the second kind. Throughout this paper all involutions are of the first kind. (For involutions of the second kind the feeling is that the solution of Problem 2 is inherently easier and should ultimately revert back to Theorem 1, partial results have been obtained by Rosen [14], and in a subsequent paper we plan to make a methodical study in this case). In a straightforward way $*$ may be extended to an involution of the central closure RC according to $rc \rightarrow r^*c$,

$r \in R$, $c \in C$. Up to now the main result concerning Problem 2 was the following theorem of Martindale [12] which we now state carefully, since it plays a crucial role in the present paper.

THEOREM 2 (Martindale [12, Theorem 3.1]). *Let R and R' be closed prime rings of characteristic $\neq 2$ with involutions of the first kind, with algebraicly closed extended centroids C and C', respectively, and with skew elements denoted respectively by K and K'. We assume furthermore that*

(a) $(R : C) \neq 1, 4, 9, 16, 25, 64$.

(b) *R contains two nonzero orthogonal symmetric idempotents e_1 and e_2 such that $e_1 + e_2 \neq 1$.*

(c) *For $i = 1, 2$, $e_1 \in \langle e_i\mathrm{R}e_i \cap [K, K]\rangle$, the associative subring generated by $e_iRe_i \cap [K, K]$.*

Then any Lie isomorphism of $[K, K]$ onto $[K', K']$ can be extended uniquely to an associative isomorphism of $\langle [K, K]\rangle$ onto $\langle [K', K']\rangle$.

Our aim in this paper is to eliminate the requirement of idempotents assumed in Theorem 2. We are now ready to state the main results of this paper.

THEOREM 3. *Let R and R' be prime rings with involutions of the first kind and of characteristic $\neq 2, 3$. Let K and K' denote respectively the skew elements of R and R' and let C and C' denote the extended centroids of R and R', respectively. Assume that $(RC : C) \neq 1, 4, 9, 16, 25, 64$. Then any Lie isomorphism α of K onto K' can be extended uniquely to an associative isomorphism of $\langle K\rangle$ onto $\langle K'\rangle$, the associative subrings generated by K and K', respectively.*

It is interesting to note that the possibility of the trace-like mapping τ: $R \to C'$ (which shows up in the statement of Theorem 1) appearing in the conclusion of Theorem 3 does not in fact occur. We also mention that counterexamples illustrating the dimension restrictions on $(RC : C)$ may be found in [12].

In view of our subsequent Remark 3 we have the following.

COROLLARY. *If in Theorem 3 R and R' are simple rings, then α can be extended uniquely to an isomorphism of R onto R'.*

Our plan of attack is to consider two cases: Case A in which R satisfies a generalized polynomial identity (briefly, R is GPI) and Case B in which R is not GPI. In Case A we are able to make use of Theorem 2. In Case B, inspired by Bresar's success with using bilinear mappings in proving Theorem 1, we set up a certain trilinear mapping $B : K^3 \to K$ intimately related to α. Then, making repeated use of a result (Lemma 1) on non-GPI prime rings which we believe may prove to be a useful technique in other situations, we are able to show (Theorem 4) that B is of a particularly useful form. The upshot is that both Theorem 2 in Case A and Theorem 4 in Case B enable us to prove that $(x^3)^\alpha = (x^\alpha)^3$ for all $x \in K$, which by Lemma 8 is precisely the criterion for lifting α to an isomorphism of $\langle K \rangle$ onto $\langle K' \rangle$. Our main result, Theorem 3, is thereby proved.

We close this introductory section by compiling various notions and results needed in the sequel. With the exception of Lemma 1 we state these results in the form of Remarks. Throughout we assume that R is prime; for Remarks 1 and 3 we assume $(RC : C) > 25$, for Remarks 6 and 8 we assume R is centrally closed, and for Remark 8 we assume that C is algebraically closed.

Remark 1. K is a prime Lie ring ([13, Corollary 5.12]) and its extended centroid $C(K)$ is equal to $C = C(R)$ ([1, p. 946, Theorem]).

Remark 2. $\langle K \rangle = K + K \circ K$, where $K \circ K$ is the additive span of all elements $xy + yx$, $x, y \in K$, or, equivalently, of all squares x^2, $x \in K$ ([5, proof of Theorem 2.3]).

Remark 3. Each of $\langle K \rangle$, $\langle [K, K] \rangle$, and $\langle S \rangle$ contains a nonzero ideal of R, where S is the symmetric elements of R ([5, proofs of Theorem 2.2, Theorem 2.13, and Theorem 1.6]).

Remark 4. Any involution of $M_n(C)$, C an algebraically closed field, is either transpose or symplectic.

Remark 5. If R has nonzero socle H and $\dim H \geq m$, then H contains a symmetric idempotent of rank $\geq m$ ([13, Corollary 2.9]).

Remark 6. If R_ℓ and R_r are respectively the rings of left and right multiplications of R, then $R_\ell R_r \cong R \otimes_C R^0$, where R^0 is the opposite ring of R ([9, Theorem 5]).

Remark 7. Let $f: R \to R$ be an additive mapping which is commuting in the sense that $[f(x), x] = 0$ for all $x \in R$. Then there exists $\lambda \in C$ and μ: $R \to C$ such that $f(x) = \lambda x + \mu(x)$, $x \in R$ ([2, Theorem 3.2]).

Let $R_C\langle X, Y_1, Y_2, \ldots, Z_1, Z_2, \ldots \rangle$ be the free product over C of R and the free noncommutative algebra $C\langle X, Y_1, \ldots, Z_1, \ldots \rangle$. An additive subgroup W of R is said to satisfy a generalized polynomial identity over C with coefficients in R (briefly, W is GPI) if there is a nonzero element $f(X, Y_1, \ldots, Z_1, \ldots) \in R_C\langle X, Y_1, \ldots Z_1, \ldots \rangle$ such that $f(x, y_1, \ldots, z_1, \ldots) = 0$ for all $x, y_i, z_j \in W$.

Remark 8. R is GPI if and only if R has a minimal right ideal eR (i.e., the socle $H \neq 0$) and $eRe \cong C$ (since C is algebraically closed) ([10, Theorem 3]).

Remark 9. K is GPI if and only if R is GPI (follows from [11, Theorem 4.9]).

Our final result in this section provides a technique for specifically studying prime rings which are not GPI and may be of independent interest.

LEMMA 1. *Suppose R is not GPI. Let $T_i = \{f_{ij}(X) \in R_C\langle X\rangle \mid j = 1, 2, \ldots, n_i\}$, $i = 1, 2, \ldots, m$, be m given subsets of $R_C\langle X\rangle$, each of which is C-independent. Then there exists $x \in K$ such that, for each $i = 1, 2, \ldots, m$, $T_i(x) = \{f_{ij}(x) \mid j = 1, 2, \ldots, n_i\}$ is a C-independent subset of R.*

Proof. Suppose to the contrary that for each $x \in K$ there exists some i, $i = 1, 2, \ldots, m$, such that $T_i(x)$ is a C-dependent subset of R. Then the set $T_i(x, y_i) = \{f_{ij}(x)y_i \mid j = 1, 2, \ldots, n_i\}$ remains a C-dependent subset of R for all $y_i \in K$. We form the element

$$g = \prod_{i=1}^{m} S_{n_i}(f_{i1}(X)Y_i, f_{i2}(X)Y_i, \ldots, f_{in_i}(X)Y_i)Z_i \in R\langle X, Y_1, \ldots, Z_1, \ldots\rangle,$$

where S_{n_i} is the standard polynomial in n_i variables. Clearly $g \neq 0$ but, since $S_k(a_1, a_2, \ldots, a_k) = 0$ whenever $a_1, a_2, \ldots, a_k$ are C-dependent, g is a GPI on K. By Remark 9 we have a contradiction since R is assumed to be not GPI, and the lemma is proved.

2. TRILINEAR MAPPINGS

Throughout this section R is a closed prime ring over its extended centroid C, with an involution $*$ of the first kind and with characteristic $R \neq 2, 3$. Furthermore, we assume that R is not GPI. As usual K denotes the skew elements of R and note that K is a Lie algebra over C. Let V be a C-space. We say that a mapping $B: K^n \to V$ is n-linear if

(i) $B(x_1, x_2, \ldots, x_n) = B(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_n})$

for all $x_1, x_2, \ldots, x_n \in K$ and all permutations $\sigma \in S_n$.

(ii) $B(x_1, \ldots, x_i + y_i, \ldots, x_n) = B(x_1, \ldots, x_i, \ldots, x_n) + B(y_1, \ldots, y_i, \ldots, y_n)$

for $i = 1, 2, \ldots, n$, $x_1, \ldots, x_i, y_i, \ldots, x_n \in K$.

(iii) $B(x_1, \ldots, cx_i, \ldots, x_n) = cB(x_1, \ldots, x_i, \ldots, x_n)$

for all $i = 1, 2, 3, \ldots, n$, $x_1, x_2, \ldots, x_n \in K$, $c \in C$.

Consider then an n-linear mapping $B: K^n \to K$. The mapping $T: K \to K$ given by $T(x) = B(x, x, \ldots, x)$ is called the *trace* of B; T is said to be *commuting* if $[T(x), x] = 0$ for all $x \in K$. Our aim in this section is to prove the following.

THEOREM 4. *Under the conditions stated above, let $B: K^3 \to K$ be a trilinear mapping whose trace T is commuting. Then there exists $\lambda \in C$ and a bilinear mapping $\mu: K \times K \to C$ such that*

$$6B(x, y, z) = \lambda(xyz + xzy + yxz + yzx + zxy + zyx) + \mu(y, z)x + \mu(x, z)y + \mu(x, y)z,$$

for all $x, y, z \in K$.

This result is highly instrumental in the next section when we show that Lie isomorphisms preserve cubes. The proof of Theorem 4 follows from a series of observations and lemmas.

We begin by linearizing our given condition

$$[B(x, x, x), x] = 0, \qquad x \in K, \tag{1}$$

through various stages. By replacing x with $x + y$ in (1) we are led to

$$[B(x, x, x), y] + 3[B(x, x, y), x] + 3[B(x, x, y), y] + 3[B(x, y, y), x] + 3[B(x, y, y), y] + [B(y, y, y), x] = 0. \tag{2}$$

Replacing y with $-y$ and y with $2y$ in (2) we obtain

$$[B(x, x, x), y] + 3[B(x, x, y), x] = 0, \quad \text{i.e.,} \ [B(x, x, y), x] = -\tfrac{1}{3}[B(x, x, x), y]. \tag{3}$$

$$[B(x, x, y), y] = -[B(x, y, y), x]. \tag{4}$$

Substitution of x by $x + z$ in (3) then results in

$$2[B(x, y, z), x] + [B(x, x, y), z] + [B(x, x, z), y] = 0 \tag{5}$$

and finally replacement of x with $x + u$ in (5) leads to

$$[B(x, y, z), u] + [B(x, y, u), z] + [B(x, z, u), y] + [B(y, z, u), x] = 0 \tag{6}$$

for all $x, y, z, u \in K$.

Before proceeding to our first lemma it is convenient to *define* $\phi_{x^i}(y) = x^i y + x^{i-1}yx + \cdots + yx^i$, $x, y \in R$, $i = 0, 1, 2, \ldots$, (it is understood that

$\phi_{x^0}(y) = y$) and then to immediately note that

$$\phi_{x^i}[y, x] = [y, x^{i+1}]. \tag{7}$$

LEMMA 2. *If $x \in K$ is algebraic over C of degree $m + 1$ then $B(x, x, x) = \sum_{i=0}^{m} \beta_i x^i$, $\beta_i \in C$.*

Proof. We set $b = B(x, x, y)$, $y \in K$, $a = B(x, x, x)$, noting from (3) that $[b, x] = -\frac{1}{3}[a, y]$. From (7) we have $\phi_{x^i}[b, x] = [b, x^{i+1}]$, $i = 0, 1, 2, \ldots$ Writing $\sum_{i=0}^{m+1} \alpha_i x^i = 0$, $\alpha_i \in C$, $\alpha_{m+1} = 1$, we see $\sum_{i=0}^{m} \alpha_{i+1}\phi_{x^i}[b, x] = [b, \sum_{i=0}^{m} \alpha_{i+1} x^{i+1}] = [b, \sum_{j=0}^{m+1} \alpha_j x^j] = 0$, whence $\sum_{i=0}^{m} \alpha_{i+1}\phi_{x^i}[a, y] = 0$ for all $y \in K$. By Remark 9 the element $f(x) = \sum \alpha_{i+1}\phi_{x^i}[a, X]$ must be the zero element of $R_C\langle X\rangle$. This means in particular that

$$\sum_{i=0}^{m} \alpha_{i+1}\phi_{x^i}[a, y] = 0 \tag{8}$$

for all $y \in R$. With the help of Remark 6, Eq. (8) may be translated into the tensor product equation

$$\sum_{i=0}^{m} \alpha_{i+1} \sum_{j=0}^{i} (x^{i-j} \otimes x^j)(a \otimes 1 - 1 \otimes a) = 0. \tag{9}$$

Reversing the summation and rewriting (9), we have

$$\sum_{j=0}^{m} \left\{ \sum_{j \le i \le m} \alpha_{i+1} x^{i-j} a \right\} \otimes x^j - \sum_{j=0}^{m} \left\{ \sum_{j \le i \le m} \alpha_{i+1} x^{i-j} \right\} \otimes a x^j = 0. \tag{10}$$

For each summand of the tensor product in (10) let us agree to call the factor to the left of the tensor sign the coefficient of the factor to the right of the tensor sign. From our assumption that x is algebraic of degree $m + 1$ we know that $1, x, \ldots, x^m$ are C-independent. Suppose (to the contrary of what we are trying to prove) that $1, x, \ldots, x^m, a$ are independent. We make the important observation that the coefficient of a in (10) is $\sum_{i=0}^{m} \alpha_{i+1} x^i = x^m + \sum_{i=0}^{m-1} \alpha_{i+1} x^i$, a polynomial in x of degree m. For $j > 0$ the coefficient of ax^j in (10) is a polynomial in x of degree $<m$. For each $j > 0$, if ax^j is a linear combination of $1, x, \ldots, x^m, a, ax, \ldots, ax^{j-1}$ we rewrite (10) accordingly and note that the coefficient of a in the rewritten form of (10) remains a polynomial in x of degree m. A contradiction to $1, x, \ldots, x^m, a$ being independent is thereby reached, and so we may finally conclude that $a = B(x, x, x) = \sum_{i=0}^{m} \beta_i x^i$, $\beta_i \in C$.

LEMMA 3. *If $z \in K$ is not algebraic of degree ≤ 6 then $B(z, z, z) = \alpha z^5 + \beta z^3 + \gamma z$, $\alpha, \beta, \gamma \in C$.*

Proof. Replacing x by z^3 in (5) we have

$$2[B(z^3, y, z), z^3] + [B(z^3, z^3, y), z] + [B(z^3, z^3, z), y] = 0, \quad (11)$$

for all $y \in K$, Applying (7) to the first summand of (11) we obtain

$$\phi_{z^2} 2[B(z^3, y, z), z] + [B(z^3, z^3, y), z] + [B(z^3, z^3, z), y] = 0,$$

which in view of (5) again may be rewritten as

$$\begin{aligned} &-\phi_{z^2}[B(z, z, z^3), y] - \phi_{z^2}[B(z, z, y), z^3] \\ &+ [B(z^3, z^3, y), z] + [B(z^3, z^3, z), y] = 0. \end{aligned} \quad (12)$$

Using (7) in connection with the second summand in (12) we then have

$$\begin{aligned} &-\phi_{z^2}[B(z, z, z^3), y] - \phi_{z^2}^2[B(z, z, y), z] \\ &+ [B(z^3, z^3, y), z] + [B(z^3, z^3, z), y] = 0. \end{aligned} \quad (13)$$

An application of (3) to the second summand of (13) results in

$$\begin{aligned} &-\phi_{z^2}[B(z, z, z^3), y] + \tfrac{1}{3}\phi_{z^2}^2[B(z, z, z), y] \\ &+ [B(z^3, z^3, y), z] + [B(z^3, z^3, z), y] = 0. \end{aligned} \quad (14)$$

We then apply ϕ_{z^2} to (14) and use (7) to obtain

$$\begin{aligned} &-\phi_{z^2}^2[B(z, z, z^3), y] + \tfrac{1}{3}\phi_{z^2}^3[B(z, z, z), y] \\ &+ [B(z^3, z^3, y), z^3] + \phi_{z^2}[B(z^3, z^3, z), y] = 0. \end{aligned} \quad (15)$$

Using (3) on the third summand of (15) we have

$$\begin{aligned} &-\phi_{z^2}^2[B(z, z, z^3), y] + \tfrac{1}{3}\phi_{z^2}^3[B(z, z, z), y] \\ &- \tfrac{1}{3}[B(z^3, z^3, z^3), y] + \phi_{z^2}[B(z^3, z^3, z), y] = 0 \end{aligned} \quad (16)$$

Multiplication of (16) by -3 and rearrangement of terms yields

$$\begin{aligned} &[B(z^3, z^3, z^3), y] - 3\phi_{z^2}[B(z^3, z^3, z), y] \\ &+ 3\phi_{z^2}^2[B(z, z, z^3), y] - \phi_{z^2}^3[B(z, z, z), y] = 0. \end{aligned} \quad (17)$$

For simplification of notation we rewrite (17) as

$$[d, y] - 3\phi_{z^2}[c, y] + 3\phi_{z^2}^2[b, y] - \phi_{z^2}^3[a, y] = 0, \qquad y \in K, \quad (18)$$

where $a = B(z, z, z)$, $b = B(z^3, z, z)$, $c = B(z^3, z^3, z)$, $d = B(z^3, z^3, z^3)$. By Remark 9 $f(X) = [d, X] - 3\phi_{z^2}[c, X] + 3\phi_{z^2}^2[b, X] - \phi_{z^2}^3[a, X]$ must be the zero element of $R_C\langle X\rangle$ and so in particular

$$[d, y] - 3\phi_{z^2}[c, y] + 3\phi_{z^2}^2[b, y] - \phi_{z^2}^3[a, y] = 0. \tag{19}$$

for all $y \in R$. Using Remark 6 we may translate (19) into the tensor product equation

$$\begin{aligned} d \otimes 1 - 1 \otimes d &- 3(z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)(c \otimes 1 - 1 \otimes c) \\ &+ 3(z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^2(b \otimes 1 - 1 \otimes b) \\ &- (z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^3(a \otimes 1 - 1 \otimes a) = 0. \end{aligned} \tag{20}$$

Two side calculations yield

$$(z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^2 = z^4 \otimes 1 + 2z^3 \otimes z + 3z^2 \otimes z^2 + 2z \otimes z^3 + 1 \otimes z^4 \tag{21}$$

$$\begin{aligned} (z^2 \otimes 1 + z \otimes z + 1 \otimes z^2)^3 = z^6 \otimes 1 + 3z^5 \otimes z + 6z^4 \otimes z^2 + 7z^3 \otimes z^3 \\ + 6z^2 \otimes z^4 + 3z \otimes z^5 + 1 \otimes z^6. \end{aligned} \tag{22}$$

Inserting (21) and (22) in (20) and then expanding in full we see that

$$\begin{aligned} d \otimes 1 - 1 \otimes d &- 3\{z^2c \otimes 1 + zc \otimes z + c \otimes z^2 - z^2 \otimes c - z \otimes cz \\ &- 1 \otimes cz^2\} + 3\{z^4b \otimes 1 + 2z^3b \otimes z + 3z^2b \otimes z^2 + 2zb \otimes z^3 \\ &+ b \otimes z^4 - z^4 \otimes b - 2z^3 \otimes bz - 3z^2 \otimes bz^2 - 2z \otimes bz^3 \\ &- 1 \otimes bz^4\} - \{z^6a \otimes 1 + 3z^5a \otimes z + 6z^4a \otimes z^2 + 7z^3a \otimes z^3 \\ &+ 6z^2a \otimes z^4 + 3za \otimes z^5 + a \otimes z^6 \\ &- z^6 \otimes a - 3z^5 \otimes az - 6z^4 \otimes az^2 - 7z^3 \otimes az^3 - 6z^2 \otimes az^4 \\ &- 3z \otimes az^5 - 1 \otimes az^6\} = 0. \end{aligned} \tag{23}$$

Systematically rearranging the terms of (23) we have

$$\begin{aligned} (d - 3z^2c + 3z^4b - z^6a) \otimes 1 &+ (-3zc + 6z^3b - 3z^5a) \otimes z \\ &+ (-3c + 9z^2b - 6z^4a) \otimes z^2 + (6zb - 7z^3a) \otimes z^3 \\ &+ (3b - 6z^2a) \otimes z^4 - 3za \otimes z^5 - a \otimes z^6 + z^6 \otimes a \\ &+ 3z^5 \otimes az + 6z^4 \otimes az^2 + 7z^3 \otimes az^3 + 6z^2 \otimes az^4 + 3z \otimes az^5 \\ &+ 1 \otimes az^6 - 3z^4 \otimes b - 6z^3 \otimes bz - 9z^2 \otimes bz^2 - 6z \otimes bz^3 \\ &- 3 \otimes bz^4 + 3z^2 \otimes c + 3z \otimes cz + 3 \otimes cz^2 - 1 \otimes d = 0. \end{aligned} \tag{24}$$

Since z is not algebraic of degree ≤ 6 we may speak of the degree of polynomials in z whose powers of z do not exceed 6. We know that 1, $z, \ldots, z^6$ are independent. Suppose (contrary to what we are trying to prove) that $1, z, \ldots, z^6, a$ are independent. In a similar fashion to the proof of Lemma 2 we note that the coefficient of a in (24) is z^6 whereas the coefficients of $az, az^2, \ldots, az^6, b, bz, \ldots, bz^4, c, cz, cz^2, d$ in (24) are all polynomials in z of degree <6. Consequently, writing if necessary any of the above elements as linear combinations of preceding elements and then rewriting (24) accordingly, it follows that the coefficient of a in the rewritten form of (24) remains a polynomial in z of degree 6. That is a contradiction to $1, z, \ldots, z^6, a$ being assumed independent and so $a = B(z, z, z) = \sum_{i=0}^{6} \beta_i z^i$. Since $B(z, z, z)$ is skew we finally have $B(z, z, z) = \alpha z^5 + \beta z^3 + \gamma z$, $\alpha, \beta, \gamma \in C$, as desired.

LEMMA 4. *If $a \in K$ is not algebraic of degree 6 then $B(a, a, a) = \lambda a^3 + \mu a$ for some $\lambda, \mu \in C$.*

Proof. If a is algebraic of degree ≤ 5 then by Lemma 2 $B(a, a, a) = \sum_{i=0}^{m} \beta_i a^i$ for some $m \leq 4$. But $B(a, a, a)$ is skew and so $B(a, a, a) = \beta_3 a^3 + \beta_1 a$. Therefore we may assume a is not algebraic of degree ≤ 6. In the free product $R_C\langle X\rangle$ we consider the following sets of elements:

$\{M_i(a, X) \mid i = 1, 2, \ldots, n\}$, the set of all monomials of the form $a^{j_0} X^{k_1} a^{j_1} \cdots X^{k_s} a^{j_s}$, where $j_0 + j_1 + \cdots + j_s \leq 6$ and $k_1 + k_2 + \cdots + k_s \leq 6$

$\{(X + a)^i \mid i = 0, 1, \ldots, 6\}$

$\{(X - a)^i \mid i = 0, 1, \ldots, 6\}$.

Since $1, a, \ldots, a^6$ are independent, each of the above three sets is an independent subset of $R_C\langle X\rangle$. By Lemma 1 there exists $x \in K$ such that each of the sets $\{M_i(a, x)\}$, $\{(x + a)^i\}$, $\{(x - a)^i\}$ is an independent subset of R. We let V denote the C-span of the set $\{M_i(a, x)\}$. Since none of the elements $a, x, a + x, x - a$ are algebraic of degree ≤ 6 Lemma 3 implies that the traces $T(a)$, $T(x)$, $T(x + a)$, $T(x - a)$ are all elements of V and in fact are of "degree" ≤ 5 in x and "degree" ≤ 5 in a. It then follows from the equations

$$T(x + a) = T(x) + T(a) + 3B(x, x, a) + 3B(x, a, a)$$

$$T(x - a) = T(x) - T(a) - 3B(x, x, a) + 3B(x, a, a)$$

that $B(x, x, a)$ and $B(x, a, a)$ are also elements of V of degree ≤ 5 in both x and a. Using (3), we may then conclude from

$$[B(x, x, x), a] = -3[B(x, x, a), x]$$

that $B(x, x, a)$ is of degree 1 in a. Next, using (4), from

$$[B(x, x, a), a] = -[B(x, a, a), x]$$

we see that $B(x, a, a)$ is of degree ≤ 2 in a. As a result it follows from

$$[B(x, a, a), a] = -\tfrac{1}{3}[B(a, a, a), x]$$

that $B(a, a, a)$ has degree ≤ 3 in a. Since $B(a, a, a)$ is skew we then have $B(a, a, a) = \lambda a^3 + \mu a$, $\lambda, \mu \in C$, as desired.

LEMMA 5. *If $a \in K$ is algebraic of degree 6 there exist $\lambda, \mu \in C$ such that $B(a, a, a) = \lambda a^3 + \mu a$.*

Proof. In the free product $R_C\langle X\rangle$ we consider the following five sets:

$\{M_i(a, X) \mid i = 1, 2, \dots, n\}$, the set of all monomials of degree ≤ 6 in X and of degree ≤ 5 in a

$\{X^i \mid i = 0, 1, \dots, 6\}$
$\{(X - a)^i \mid i = 0, 1, \dots, 6\}$
$\{(X + a)^i \mid i = 0, 1, \dots, 6\}$
$\{(X + 2a)^i \mid i = 0, 1, \dots, 6\}$.

Each of these sets is a C-independent subset of $R_C\langle X\rangle$, so by Lemma 1 there exists $x \in K$ such that each of the five sets $\{M_i(a, x)\}$, $\{x^i\}$, $\{(x - a)^i\}$, $\{(x + a)^i\}$, $\{(x + 2a)^i\}$ is an independent subset of R. We let W denote the C-span of the set $\{M_i(a, x)\}$ and let W' denote the subspace of W whose elements are of degree ≤ 3 in x. Since none of the elements x, $x - a$, $x + a$, $x + 2a$ are algebraic of degree 6, Lemma 4 implies that the traces $T(x)$, $T(x - a)$, $T(x + a)$, $T(x + 2a)$ all belong to W'. By adding the equations

$$T(x + a) = T(x) + T(a) + 3B(x, x, a) + 3B(x, a, a)$$
$$T(x - a) = T(x) - T(a) - 3B(x, x, a) + 3B(x, a, a),$$

we have $6B(x, a, a) = T(x + a) + T(x - a) - 2T(x)$, and so $B(x, a, a) \in W'$. Next, from the equations

$$T(x + 2a) = T(x) + 8T(a) + 6B(x, x, a) + 12B(x, a, a)$$
$$8T(x + a) = 8T(x) + 8T(a) + 24B(x, x, a) + 24B(x, a, a),$$

we obtain

$$8T(x + a) - T(x + 2a) = 7T(x) + 18B(x, x, a) + 12B(x, a, a)$$

and so $B(x, x, a) \in W'$. In W we have the equation

$$[B(x, x, x), a] = -3[B(x, x, a), x]$$

from which we may conclude that $B(x, x, a)$ has degree 1 in a. We therefore see from

$$[B(x, x, a), a] = -[B(x, a, a), x]$$

that $B(x, a, a)$ has degree ≤ 2 in a. Since a is algebraic of degree 6 we know from Lemma 2 that $B(a, a, a) = \sum_{i=0}^{5} \gamma_i a^i$, $\gamma_i \in C$, and so $[B(a, a, a), x] \in W$. Therefore from the equation

$$[B(a, a, a), x] = -3[B(x, a, a), a]$$

we see that $B(a, a, a)$ is of degree ≤ 3 in a, and the proof of the lemma is complete.

Together Lemma 4 and Lemma 5 imply

LEMMA 6. *For all $a \in K$ there exist λ, $\mu \in C$ such that $B(a, a, a) = \lambda a^3 + \mu a$.*

We next show that λ is independent of a.

LEMMA 7. *There exists $\lambda \in C$ such that for all $a \in K$ $B(a, a, a) = \lambda a^3 + \mu(a)a$, $\mu(a) \in C$.*

Proof. Let a, b be any elements of K, neither of which is algebraic of degree ≤ 3. In the free product $R_C\langle X\rangle$ we consider the two sets

$\{M_i(a, X) \mid i = 1, 2, \ldots, n\}$, the set of all monomials of degree ≤ 6 in X and of degree ≤ 3 in a.

$\{M_i(b, X) \mid i = 1, 2, \ldots, m\}$, the set of all monomials of degree ≤ 6 in X and of degree ≤ 3 in b.

These are each independent subsets of $R_C\langle X\rangle$ and so by Lemma 1 there exists $x \in K$ such that the sets $\{M_i(a, x)\}$ and $\{M_i(b, x)\}$ are both independent subsets of R. Let U denote the C-span of the set $\{M_i(a, x)\}$, and let U' denote the subspace of U where elements are of degree ≤ 3 in x. By Lemma 6 $T(x)$, $T(a)$, $T(x + a)$, $T(x - a)$ all belong to U' and so from the equations

$$\begin{aligned} T(x + a) &= T(x) + T(a) + 3B(x, x, a) + 3B(x, a, a) \\ T(x - a) &= T(x) - T(a) - 3B(x, x, a) + 3B(x, a, a) \end{aligned} \tag{25}$$

we conclude that $B(x, x, a)$ and $B(x, a, a)$ both lie in U'. From

$$[B(x, x, x), a] = -3[B(x, x, a), x]$$

we see that $B(x, x, a)$ is of degree 1 in a, hence from

$$[B(x, x, a), a] = -[B(x, a, a), x]$$

we see that $B(x, a, a)$ has degree ≤ 2 in a. Next from

$$[B(x, a, a), a] = -\tfrac{1}{3}[B(a, a, a), x]$$

we see that $B(x, a, a)$ has degree 1 in x, hence from

$$[B(x, x, a), a] = -[B(x, a, a), x]$$

we see that $B(x, x, a)$ has degree ≤ 2 in x. Returning to Eq. (25) and using Lemma 6 we write

$$\begin{aligned}\lambda_1(a + x)^3 + \mu_1(a + x) = \lambda_2 a^3 + \mu_2 a + \lambda_3 x^3 + \mu_3 x \\ + 3B(x, x, a) + B(x, a, a)\end{aligned} \tag{26}$$

for suitable $\lambda_i, \mu_i \in C$. Since the degrees of $B(x, x, a)$ and $B(x, a, a)$ either in x or in a do not exceed 2 we conclude from (26) that $\lambda_1 = \lambda_2$ and $\lambda_1 = \lambda_3$, whence $\lambda_2 = \lambda_3$. In a similar fashion, writing $B(b, b, b) = \lambda_2' b^3 + \mu_2' b$, our argument shows that $\lambda_2' = \lambda_3$ and therefore $\lambda_2 = \lambda_2' = \lambda$. In case $y \in K$ is algebraic of degree ≤ 3 we know by Lemma 2 that $B(y, y, y) = \mu y$, so, writing $y^3 = \gamma y$, we have $B(y, y, y) = \lambda y^3 + \mu y - \lambda y^3 = \lambda y^3 + (\mu - \gamma\lambda)y$. The proof of Lemma 7 is now complete.

Proof of Theorem 4. By Lemma 7 there exists $\lambda \in C$ such that

$$B(x, x, x) = \lambda x^3 + \gamma(x)x, \qquad \gamma(x) \in C, \tag{27}$$

for all $x \in K$. We proceed to linearize (27) in the usual fashion. Replacement of x by $x + y$ in (27) results in

$$3B(x, x, y) + 3B(x, y, y) = \lambda(x^2y + yxy + yx^2 + xy^2 + yxy + y^2x) + h_1 \tag{28}$$

for all $x, y \in K$, where h_1 is a linear term in x and y. Replacement of y by $-y$ in (28) then quickly leads to

$$3B(x, y, y) = \lambda(xy^2 + yxy + y^2x) + h_2, \tag{29}$$

where h_2 is linear in x and y. Replacement of y by $y + z$ in (29) then results in

$$6B(x, y, z) = \lambda(xyz + xzy + yxz + yzx + zxy + zyx) + h \tag{30}$$

for all $x, y \in K$, where

$$h(x, y, z) = \alpha(x, y, z)x + \beta(x, y, z)y + \gamma(x, y, z)z. \tag{31}$$

We note from (30) that $h: K^3 \to K$ is a trilinear mapping. We define a mapping $\mu: K \times K \to C$ in the following fashion. Given $(y, z) \in K \times K$ choose $x \in K$ such that x does not lie in the span of y and z (such x exist since K is infinite dimensional over C). Now write

$$h(x, y, z) = \alpha x + \beta y + \gamma z$$

and define $\mu(y, z) = \alpha$. To show that μ is well-defined let $u \in K$ such that $u \notin \text{span}\{y, z\}$. Suppose first that $u = \tau_1 x + \tau_2 y + \tau_3 z$ (necessarily $\tau_1 \neq 0$). Then

$$\begin{aligned} h(u, y, z) &= \tau_1 h(x, y, z) + \tau_2 h(y, y, z) + \tau_3 h(z, y, z) \\ &= \tau_1(\alpha x + \beta y + \gamma z) + \tau_2(\beta_2 y + \gamma_2 z) + \tau_3(\beta_3 y + \gamma_3 z) \\ &= \alpha(\tau_1 x + \tau_2 y + \tau_3 z) + \beta_4 y + \gamma_4 z = \alpha u + \beta_4 y + \gamma_4 z. \end{aligned}$$

We may thus assume that u, x are independent modulo span $\{y, z\}$. In this case we write

$$h(x, y, z) + h(u, y, z) = h(x + u, y, z)$$

whence

$$\alpha x + \beta y + \gamma z + \alpha_1 u + \beta_1 y + \gamma_1 z = \alpha_2(x + u) + \beta_2 y + \gamma_2 z. \tag{32}$$

It follows from (32) that $\alpha = \alpha_2$ and $\alpha_1 = \alpha_2$ and so $\alpha = \alpha_1$ as desired.

We next show that μ is bilinear. Let $y, y', z \in K$, $\tau \in C$, and choose $x \in K$ such that $x \notin \text{span}\{y, y', z\}$. The equations

$$\begin{aligned} &h(x, y, z) = \alpha x + \beta y + \gamma z = h(x, z, y) \\ &h(x, y + y', z) = \mu(y + y', z)x + \beta_1(y + y') + \gamma_1 z \\ = {}&h(x, y, z) + h(x, y', z) = \mu(y, z)x + \beta_2 y + \gamma_2 z + \mu(y', z)x + \beta_3 y' + \gamma_3 z \\ &h(x, \tau y, z) = \mu(\tau y, z)x + \beta_4 \tau y + \gamma_4 z \\ = {}&\tau h(x, y, z) = \tau\mu(y, z)x + \beta y + \gamma z \end{aligned}$$

clearly imply that μ is bilinear.

Now let $x, y, z \in K$ be independent. From

$$\begin{aligned} &h(x, y, z) = \mu(y, z)x + \beta y + \gamma z \\ = {}&h(y, x, z) = \mu(x, z)y + \beta_1 x + \gamma_1 z \\ = {}&h(z, x, y) = \mu(x, y)z + \beta_2 x + \gamma_2 y \end{aligned}$$

we then conclude that

$$h(x, y, z) = \mu(y, z)x + \mu(x, z)y + \mu(x, y)z.$$

Next suppose y, z are independent but $x \in \text{span}\{y, z\}$. Choose $u \notin \text{span}\{y, z\}$. Then $x + u \notin \text{span}\{y, z\}$ and we have

$$\begin{aligned} h(x, y, z) &= h(x + u, y, z) - h(u, y, z) \\ &= \mu(y, z)(x + u) + \mu(x + u, z)y + \mu(x + u, y)z \\ &\quad - \mu(y, z)u - \mu(u, z)y - \mu(u, y)z \\ &= \mu(y, z)x + \mu(x, z)y + \mu(x, y)z. \end{aligned}$$

Finally, if $\text{span}\{x, y, z\}$ is one-dimensional, we choose $u \notin \text{span}\{x, y, z\}$ and write

$$\begin{aligned} h(x, y, z) &= h(x, y, z + u) - h(x, y, u) \\ &= \mu(y, z + u)x + \mu(x, z + u)y + \mu(x, y)(z + u) \\ &\quad - \mu(y, u)x - \mu(x, u)y - \mu(x, y)u \\ &= \mu(y, z)x + \mu(x, z)y + \mu(x, y)z \end{aligned}$$

making use of the preceding case. This completes the proof of Theorem 4.

3. Lie Isomorphisms

Throughout this section R and R' are prime rings with involutions of the first kind, of characteristic $\neq 2, 3$, with respective skew elements K and K', and with respective extended centroids C and C'. We also make the assumption that $(RC : C) \neq 1, 4, 9, 16, 25, 64$. For W a subset of R we denote by $\langle W \rangle$ the associative subring of R generated by W. Finally, under the above conditions, we suppose that α is a Lie isomorphism of K onto K' given by $x \to x^\alpha$, $x \in K$. The main result of this paper is then to prove that α can be extended uniquely to an associative isomorphism of $\langle K \rangle$ onto $\langle K' \rangle$.

We begin by showing that without loss of generality R and R' may be assumed to be closed prime rings with C and C' algebraically closed fields. Indeed, since $(RC : C) \neq 16$, we know from Remark 1 that $C = C(K)$ where $C(K)$ is the extended centroid of the prime Lie ring K. From the Lie isomorphism α we see that K' is also a prime Lie ring, in which case it follows that $C' = C(K')$. The Lie isomorphism α then induces an isomorphism $c \to \bar{c}$ of C onto C' and α may be extended to a Lie isomorphism ϕ: $KC \to K'C'$ given by $\Sigma x_i c_i \to \Sigma x_i^\alpha \bar{c}_i$, $x_i \in K$, $c_i \in C$ (see [12,

p. 934] for details). Therefore without loss of generality we may assume that R and R' are already centrally closed. Now let F be an algebraic closure of C and let F' be an algebraic closure of C' such that the isomorphism $c \to \bar{c}$ of C onto C' is extended to an isomorphism $\lambda \to \bar{\lambda}$ of F onto F'. We then form $\tilde{R} = R \otimes_C F$ and $\tilde{R}' = R' \otimes_C F'$ (see [13, Theorem 2.11]), noting that $\tilde{R}$ and $\tilde{R}'$ are closed prime rings with involutions, with respective extended centroids F and F', and with respective skew elements $K \otimes_C F$ and $K' \otimes_{C'} F'$. Now we extend α to a Lie isomorphism ϕ: $K \otimes_C F \to K' \otimes_{C'} F'$ via $x \otimes \lambda \to x^\alpha \otimes \bar{\lambda}$, $x \in K$, $\lambda \in F$. This mapping is well-defined (the crucial observation being that $(xc)^\alpha \otimes_{C'} \bar{\lambda} = x^\alpha \bar{c} \otimes_{C'} \bar{\lambda} = x^\alpha \otimes_{C'} \bar{c}\bar{\lambda} = x^\alpha \otimes_{C'} (\overline{c\lambda})$, $x \in K$, $c \in C$, $\lambda \in F$). We leave it for the reader to verify the straightforward details that ϕ is a Lie isomorphism. Clearly we have the conditions that $(\tilde{R} : F) \neq 1, 4, 9, 16, 25, 64$. Therefore we may assume to begin with that $R = \tilde{R}$ and $R' = \tilde{R}'$ are closed prime rings with algebraically closed extended centroids.

We next present a criterion for extending α to an associative isomorphism of $\langle K \rangle$ onto $\langle K' \rangle$.

LEMMA 8. *α can be extended to an isomorphism β: $\langle K \rangle \to \langle K' \rangle$ if and only if $(x^3)^\alpha = (x^\alpha)^3$ for all $x \in K$.*

Proof. The "only if" part being obvious, we assume

$$(x^3)^\alpha = (x^\alpha)^3 \tag{33}$$

for all $x \in K$. By Remark 2 $\langle K \rangle = K \oplus K \circ K$. Replacement of x by $x \pm y$ in (33) results in

$$2(xy^2 + yxy + y^2x)^\alpha = 2x^\alpha(y^\alpha)^2 + 2y^\alpha x^\alpha y^\alpha + 2(y^\alpha)^2 x^\alpha \tag{34}$$

for all x, $y \in K$. Also we have

$$\begin{aligned}(xy^2 - 2yxy + y^2x)^\alpha &= [[x, y], y]^\alpha = [[x^\alpha, y^\alpha], y^\alpha] \\ &= x^\alpha(y^\alpha)^2 - 2y^\alpha x^\alpha y^\alpha + (y^\alpha)^2 x^\alpha.\end{aligned} \tag{35}$$

Adding (34) and (35) and then dividing by 3, we see that

$$(xy^2 + y^2x)^\alpha = x^\alpha(y^\alpha)^2 + (y^\alpha)^2 x^\alpha \tag{36}$$

for all x, $y \in K$. We now define a mapping β: $\langle K \rangle \to \langle K' \rangle$ according to

$$x \oplus \Sigma y_i^2 \to x^\alpha \oplus \Sigma (y_i^\alpha)^2, \qquad x, y_i \in K.$$

To show that β is well-defined it suffices to show that if $\Sigma y_i^2 = 0$ then $\Sigma (y_i^\alpha)^2 = 0$. Indeed, for $x \in K$ we have $\Sigma y_i^2 x + \Sigma x y_i^2 = 0$ whence by (36) we see that $\Sigma (y_i^\alpha)^2 x^\alpha + x^\alpha \Sigma (y_i^\alpha)^2 = 0$. But a nonzero symmetric element of R'

can only anticommute with all skew elements of R' when K' is one-dimensional, a condition which is ruled out by $(R : C) > 4$. Therefore we conclude that $\Sigma(y_i^{\alpha})^2 = 0$ and thus β is a well-defined additive mapping of $\langle K\rangle$ onto $\langle K'\rangle$.

From the identity $xy = \frac{1}{2}\{(x + y)^2 - x^2 - y^2 + [x, y]\}$ we see from the definition of β that for $x, y \in K$,

$$\begin{aligned}(xy)^{\beta} &= \tfrac{1}{2}\{[(x + y)^2]^{\beta} - (x^2)^{\beta} - (y^2)^{\beta} + [x, y]^{\beta}\} \\ &= \tfrac{1}{2}\{(x^{\alpha} + y^{\alpha})^2 - (x^{\alpha})^2 - (y^{\alpha})^2 + [x^{\alpha}, y^{\alpha}]\} \\ &= x^{\alpha}y^{\alpha} = x^{\beta}y^{\beta}.\end{aligned} \tag{37}$$

From the identity $x^2y = \frac{1}{2}\{x \circ [x, y] + x^2 \circ y\}$ we obtain

$$\begin{aligned}(x^2y)^{\beta} &= \tfrac{1}{2}\{(x \circ [x, y])^{\beta} + (x^2 \circ y)^{\alpha}\} \\ &= \tfrac{1}{2}\{x^{\alpha} \circ [x^{\alpha}, y^{\alpha}] + (x^{\alpha})^2 \circ y^{\alpha}\} \\ &= (x^{\alpha})^2y^{\alpha} = (x^2)^{\beta}y^{\beta},\end{aligned} \tag{38}$$

making use of (36). Together (37) and (38) imply

$$(ux)^{\beta} = u^{\beta}x^{\beta}, \qquad u \in \langle K\rangle, x \in K, \tag{39}$$

and, since $\langle K\rangle$ is generated by K, it follows from (39) that β is a homomorphism of $\langle K\rangle$ onto $\langle K'\rangle$. By symmetry the Lie isomorphism $x^{\alpha} \to x$ of K' onto K can be extended to a homomorphism γ: $\langle K'\rangle \to \langle K\rangle$. Since $\beta\gamma$ is the identity on K and $\gamma\beta$ is the identity on K' it is clear that β is an isomorphism.

At this point we divide our analysis of α into two separate cases.

Case A: R is *GPI*.

Case B: R is not *GPI*.

Case A. By Remark 8 R has nonzero socle H. Since $(R : C) \geq 36$ we know from Remark 5 that H contains a symmetric idempotent e of rank $n \geq 6$. Then $eRe \cong M_n(C)$ and by Remark 4 eRe has either the transpose or the symplectic involution. In either of these cases it is well-known that eRe contains orthogonal symmetric idempotents e_1 and e_2 each of rank 2. It is then easy to check that for $i = 1, 2$ e_i lies in the subring generated by $[K, K] \cap e_iRe_i$. Finally, α clearly induces a Lie isomorphism α_0 from $[K, K]$ onto $[K', K']$, and so the conditions of Theorem 2 have now been met. We may therefore conclude that α_0 can be extended to an associative isomorphism σ: $T \to T'$, where $T = \langle [K, K]\rangle$ and $T' = \langle [K', K']\rangle$. It is easily seen that $(K \cap T)^{\sigma} = K' \cap T'$. Indeed, this follows from writing $x \in K \cap T$ as $x = \Sigma\,(u_1u_2 \cdots u_n + (-1)^{n+1}u_n \cdots u_1)$, $u_i \in [K, K]$, and then applying the isomorphism σ. Similarly, $(S \cap T)^\sigma = S' \cap T'$, where S and S' are respectively the symmetric elements of R and R'. We also claim that α agrees with σ on $K \cap T$. Indeed, for $x \in K \cap T$, $y \in [K, K]$, we have $[x^\alpha, y^\alpha] = [x, y]^\alpha = [x, y]^\sigma - [x^\sigma, y^\sigma] = [x^\sigma, y^\sigma]$, whence $x^\alpha - x^\sigma$ commutes with $[K', K']$ and so by Remark 3 $x^\alpha - x^\sigma$ is central. But we have already seen that x^σ (as well as x^α) must be skew, and so $x^\alpha - x^\sigma = 0$.

Since R is GPI the socle H of R is nonzero by Remark 8 and so by Remark 3 $H \subseteq T$. We note that H itself is a simple ring. If $I \neq 0$ is an ideal of T then $I \cap H \neq 0$ is an ideal of H and so $I \cap H = H$, i.e., $I \supseteq H$. It follows that H is also the socle of T. It is easy to show via σ that R' must also be GPI with socle H^σ.

We now fix $\tau \in K$. We claim first of all that

$$[u, t]^\sigma = [u^\sigma, t^\alpha], \qquad u \in H. \tag{40}$$

Indeed, since $\langle H \cap K\rangle = H$ by Remark 3 and the simplicity of H we may assume without loss of generality that $u = x_1x_2 \cdots x_n$, $x_i \in H \cap K$. For $n = 1$ $[x_1, t]^\sigma = [x_1, t]^\alpha = [x_1^\alpha, t^\alpha] = [x_1^\sigma, t^\alpha]$. Inductively we have

$$\begin{aligned}[x_1x_2 \cdots x_n, t]^\sigma &= \{x_1[x_2 \cdots x_n, t] + [x_1, t]x_2 \cdots x_n\}^\sigma \\ &= x_1^\sigma[x_2 \cdots x_n, t]^\sigma + [x_1, t]^\sigma(x_2 \cdots x_n)^\sigma \\ &= x_1^\sigma[(x_2 \cdots x_n)^\sigma, t^\alpha] + [x_1^\sigma, t^\alpha](x_2 \cdots x_n)^\sigma \\ &= [x_1^\sigma(x_2 \cdots x_n)^\sigma, t^\alpha] = [(x_1x_2 \cdots x_n)^\sigma, t^\alpha],\end{aligned}$$

and so our claim is established.

From $[u \circ t, u] = [t, u] \circ u$ we see, making use of (40), that

$$[(u \circ t)^\sigma, u^\sigma] = [t^\alpha, u^\sigma] \circ u^\sigma = [u^\sigma \circ t^\alpha, u^\sigma]$$

for all $u \in H$. In other words, ψ_t: $u^\sigma \to (u \circ t)^\sigma - u^\sigma \circ t^\alpha$ is an additive commuting function on the ring H^σ. By Remark 7 there exists $\lambda \in C'$ and μ: $H^\sigma \to C'$ such that

$$(u \circ t)^\sigma - u^\sigma \circ t^\alpha = \lambda u^\sigma - \mu(u^\sigma), \qquad u \in H. \tag{41}$$

Choosing $u \in H \cap K$ we see that $\lambda = 0$ by comparing the skew and symmetric parts of (41). Next, choosing $u \in S \cap H$, we see from (41) that $\mu(u^\sigma) = 0$; that is

$$(u \circ t)^\sigma = u^\sigma \circ t^\alpha, \qquad u \in S \cap H. \tag{42}$$

Together (40) and (42) imply that

$$(ut)^\sigma = u^\sigma t^\alpha, \qquad u \in S \cap H,$$

whence

$$(u_1u_2 \cdots u_nt)^\sigma = u_1^\sigma u_2^\sigma \cdots u_n^\sigma t^\alpha, \qquad u_i \in S \cap H. \tag{43}$$

But $\langle S \cap H\rangle = H$ by Remark 3 and so (43) implies

$$(ut)^\sigma = u^\sigma t^\alpha, \qquad u \in H, t \in K.$$

Similarly $(tv)^\sigma = t^\alpha v^\sigma$, $v \in H$, $t \in K$ and so

$$\begin{aligned} u^\sigma(t^3)^\alpha v^\sigma &= (ut^3)^\sigma v^\sigma = (ut^3v)^\sigma = \{(ut)t(tv)\}^\sigma \\ &= [(ut)t]^\sigma (tv)^\sigma = (ut)^\sigma t^\alpha v^\sigma = u^\sigma (t^\alpha)^3 v^\sigma \end{aligned}$$

for all $u, v \in H$, $t \in K$. Therefore $U^\sigma[(t^3)^\alpha - (t^\alpha)^3]U^\sigma = 0$ whence $(t^3)^\alpha = (t^\alpha)^3$ for all $t \in K$. Lemma 8 is thereby applicable and so we have succeeded in showing in Case A that α can be extended to an isomorphism of $\langle K\rangle$ onto $\langle K'\rangle$.

Case B. We begin by pointing out that necessarily R' is not GPI. Indeed, since R is not GPI it follows that $(K : C) = \infty$, whence $(K' : C') = \infty$. If R' is GPI we have already seen in our discussion of Case A (with α^{-1} now playing the role of α) that α^{-1} may be lifted to an isomorphism of σ' of $\langle K'\rangle$ onto $\langle K\rangle$. Using σ' we easily reach the contradiction that R must be GPI.

We define a C'-trilinear mapping B: $(K')^3 \to K'$ as

$$B(x^\alpha, y^\alpha, z^\alpha) = \tfrac{1}{6}(xyz + xzy + yxz + yzx + zxy + zyx)^\alpha$$

for all $x, y, z \in K$. Its trace $B(x^\alpha, x^\alpha, x^\alpha)$ is obviously commuting since $B(x^\alpha, x^\alpha, x^\alpha) = (x^3)^\alpha$ and $[(x^3)^\alpha, x^\alpha] = 0$ for all $x \in K$. Thus by Theorem 4 there exists $\lambda \in C'$ and a C'-bilinear mapping μ: $K' \times K' \to C'$ such that

$$\begin{aligned} &(xyz + xzy + yxz + yzx + zxy + zyx)^\alpha \\ &\quad = \lambda(x^\alpha y^\alpha z^\alpha + x^\alpha z^\alpha y^\alpha + y^\alpha x^\alpha z^\alpha + y^\alpha z^\alpha x^\alpha + z^\alpha x^\alpha y^\alpha + z^\alpha y^\alpha x^\alpha) \qquad (44) \\ &\quad\quad + \mu(y, z)x^\alpha + \mu(x, z)y^\alpha + \mu(x, y)z^\alpha, \end{aligned}$$

for all $x, y, z \in K$, where for notational ease we are simply writing $\mu(x, y)$ for $\mu(x^\alpha, y^\alpha)$. Our aim, of course, is to show that $\lambda = 1$ and that $\mu = 0$, whence $(x^3)^\alpha = (x^\alpha)^3$, and Lemma 8 may accordingly be invoked to obtain the desired conclusion that α may be extended to an isomorphism of $\langle K\rangle$ onto $\langle K'\rangle$.

We now proceed to draw some consequences from (44). First setting $x = z$ in (44) and dividing by 2, we obtain

$$(x^2y + xyx + yx^2)^\alpha = \lambda\{(x^\alpha)^2y^\alpha + x^\alpha y^\alpha x^\alpha + y^\alpha(x^\alpha)^2\} + \mu(x, y)x^\alpha + \tfrac{1}{2}\mu(x, x)y^\alpha. \tag{45}$$

Now, setting $x = y$ in (45), we have

$$(x^3)^\alpha = \lambda(x^\alpha)^3 + \tfrac{1}{2}\mu(x, x)x^\alpha. \tag{46}$$

From $3xyx = x^2y + xyx + yx^2 - [[y, x], x]$ we conclude using (45) that

$$\begin{aligned} 3(xyx)^\alpha &= \lambda[(x^\alpha)^2y^\alpha + x^\alpha y^\alpha x^\alpha + y^\alpha(x^\alpha)^2] + \mu(x, y)x^\alpha + \tfrac{1}{2}\mu(x, x)y^\alpha \\ &\quad - [(x^\alpha)^2y^\alpha - 2x^\alpha y^\alpha x^\alpha + y^\alpha(x^\alpha)^2] \\ &= (\lambda + 2)x^\alpha y^\alpha x^\alpha + (\lambda - 1)[(x^\alpha)^2y^\alpha + y^\alpha(x^\alpha)^2] \\ &\quad + \mu(x, y)x^\alpha + \tfrac{1}{2}\mu(x, x)y^\alpha, \end{aligned}$$

whence

$$(xyx)^\alpha = (\lambda + 2)/3x^\alpha y^\alpha x^\alpha + (\lambda - 1)/3[(x^\alpha)^2y^\alpha + y^\alpha(x^\alpha)^2] + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha. \tag{47}$$

LEMMA 9. $\lambda = 1$, *i.e.*, $(xyx)^\alpha = x^\alpha y^\alpha x^\alpha + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha$.

Proof. Choose $x^\alpha \in K'$ such that x^α is not algebraic of degree ≤ 6 (such x^α exist since otherwise K' would be PI). In the free product $R'_{C'}\langle Y\rangle$ consider the C'-independent subset $\{M_i(x^\alpha, Y) \mid i = 1, 2, \ldots, n\}$ of all monomials of the form $(x^\alpha)^{j_0}Y^{i_1}(x^\alpha)^{j_1} \cdots Y^{i_k}(x^\alpha)^{j_k}$ where $j_0 + j_1 + \cdots + j_k \leq 6$ and $i_1 + i_2 + \cdots + i_k \leq 6$. By Lemma 1 there exists $y^\alpha \in K'$ such that $\{M_i(x^\alpha, y^\alpha)\}$ is an independent subset of R'. We compute $(x^3yx^3)^\alpha$ in two ways and compare the results, being only interested in the coefficients of $(x^\alpha)^6y^\alpha$ and $(x^\alpha)^5y^\alpha x^\alpha$. On the one hand,

$$(x^3yx^3)^\alpha = \frac{\lambda + 2}{3}[\ ]y^\alpha[\ ] + \frac{\lambda - 1}{3}\{[\ ]^2y^\alpha + y^\alpha[\ ]^2\} + \tfrac{1}{3}\mu(x^3, y)[\ ] + \tfrac{1}{6}\mu(x^3, x^3)y^\alpha, \tag{48}$$

where $[\ ] = \lambda(x^\alpha)^3 + \tfrac{1}{2}\mu(x, x)x^\alpha$. Using $[\ ]^2 = \lambda^2(x^\alpha)^6 + \lambda\mu(x, x)(x^\alpha)^4 + \tfrac{1}{4}\mu(x, x)^2(x^\alpha)^2$ we may write (48) as

$$(x^3yx^3)^\alpha = \frac{\lambda - 1}{3}\lambda^2(x^\alpha)^6y^\alpha + 0(x^\alpha)^5y^\alpha x^\alpha + \cdots. \tag{49}$$

On the other hand,

$$(x^3yx^3)^\alpha = [x(x^2yx^2)x]^\alpha$$
$$= \frac{\lambda+2}{3}\{\ \}x^\alpha + \frac{\lambda-1}{3}(x^\alpha)^2\{\ \} + \frac{\lambda-1}{3}\{\ \}(x^\alpha)^2 \tag{50}$$
$$+ \tfrac{1}{3}\mu(x, x^2yx^2)x^\alpha + \tfrac{1}{6}\mu(x, x)\{\ \},$$

where

$$\{\ \} = (x^2yx^2)^\alpha = [x(xyx)x]^\alpha$$
$$= \frac{\lambda+2}{3}x^\alpha[\ ]x^\alpha + \frac{\lambda-1}{3}(x^\alpha)^2[\ ] + \frac{\lambda-1}{3}[\ ](x^\alpha)^2$$
$$+ \tfrac{1}{3}\mu(x, xyx)x^\alpha + \tfrac{1}{6}\mu(x, x)[\ ]$$

where in turn

$$[\ ] = (xyx)^\alpha = \frac{x+2}{3}x^\alpha y^\alpha x^\alpha + \frac{\lambda-1}{3}(x^\alpha)^2y^\alpha + \frac{\lambda-1}{3}y^\alpha(x^\alpha)^2$$
$$+ \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha.$$

Therefore

$$(x^3yx^3)^\alpha = \left(\frac{\lambda-1}{3}\right)^3(x^\alpha)^6y^\alpha$$
$$+\left[\frac{\lambda+2}{3}\left(\frac{\lambda-1}{3}\right)^2 + \frac{\lambda-1}{3}\,\frac{\lambda+2}{3}\,\frac{\lambda-1}{3}\right.$$
$$\left. + \left(\frac{\lambda-1}{3}\right)^2\frac{\lambda+2}{3}\right](x^\alpha)^5y^\alpha x^\alpha \tag{51}$$
$$+ \cdots$$
$$= \left(\frac{\lambda-1}{3}\right)^3(x^\alpha)^6y^\alpha + \frac{(\lambda+2)(\lambda-1)^2}{9}(x^\alpha)^5y^\alpha x^\alpha + \cdots.$$

Equating the coefficients of $(x^\alpha)^6y^\alpha$ and $(x^\alpha)^5y^\alpha x^\alpha$ in (49) and (51) we have

$$\left(\frac{\lambda-1}{3}\right)^3 = \left(\frac{\lambda-1}{3}\right)\lambda^2 \tag{52}$$

$$\frac{(\lambda + 2)(\lambda - 1)^2}{9} = 0. \tag{53}$$

From (52) we find that $\lambda = 1$ or $\lambda^2 = ((\lambda - 1)/3)^2$, whence $\lambda = 1, -\frac{1}{2}$, or $\frac{1}{4}$. From (53) we have $\lambda = 1$ or $\lambda = -2$. It follows that $\lambda = 1$ and the lemma is proved.

LEMMA 10. $\mu = 0$.

Proof. Let $x^\alpha \neq 0$ be arbitrary but fixed in K'. In the free product $R'_{C'}\langle Y\rangle$ we define the independent set $\{M_i(x, Y) \mid i = 1, 2, \dots, n\}$ to be the set of all monomials of the form $(x^\alpha)^{j_0}Y^{i_1}(x^\alpha)^{j_1} \cdots Y^{i_k}(x^\alpha)^{j_k}$, where $i_1 + i_2 + \cdots + i_k \leq 3$, $i_q \leq 3$, $j_0 + j_1 + \cdots + j_k \leq 4$, and

$$j_q \leq 3 \text{ if } x \text{ is not algebraic of degree} \leq 3 \tag{54}$$

$$j_1 \leq 2 \text{ if } x \text{ is algebraic of degree 3} \tag{55}$$

$$j_1 \leq 1 \text{ if } x \text{ is algebraic of degree 2.} \tag{56}$$

In case of (55) we can replace $(x^\alpha)^3$ by βx^α, $\beta \in C'$, and in case of (56) we can replace $(x^\alpha)^2$ by $\gamma \in C'$ and hence $(x^\alpha)^3$ by γx^α. By Lemma 1 there exists $y^\alpha \in K'$ such that the set $\{M_i(x^\alpha, y^\alpha)\}$ is an independent subset of R'. We compute $(xyxyxyx)^\alpha$ in two ways and compare the results, being only interested in the coefficients of $(y^\alpha)^2x^\alpha y^\alpha x^\alpha$.

On the one hand, making use of Lemma 9, we have

$$\begin{aligned}
[(xyx)y(xyx)]^\alpha &= (xyx)^\alpha y^\alpha (xyx)^\alpha + \tfrac{1}{3}\mu(y, xyx)(xyx)^\alpha + \tfrac{1}{6}\mu(xyx, xyx)y^\alpha \\
&= [x^\alpha y^\alpha x^\alpha + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha]y^\alpha[x^\alpha y^\alpha x^\alpha \\
&\quad + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha] \\
&\quad + \tfrac{1}{3}\mu(y, xyx)[x^\alpha y^\alpha x^\alpha + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha] \\
&\quad + \tfrac{1}{6}\mu(xyx, xyx)y^\alpha \\
&= x^\alpha y^\alpha x^\alpha y^\alpha x^\alpha y^\alpha x^\alpha + \tfrac{1}{6}\mu(x, x)(y^\alpha)^2x^\alpha y^\alpha x^\alpha + \cdots .
\end{aligned} \tag{57}$$

On the other hand, again using Lemma 9, we have

$$\begin{aligned}
[x(yxyxy)x]^\alpha &= x^\alpha(yxyxy)^\alpha x^\alpha + \tfrac{1}{3}\mu(x, yxyxy)x^\alpha + \tfrac{1}{6}\mu(x, x)(yxyxy)^\alpha \\
&= x^\alpha\{y^\alpha(xyx)^\alpha y^\alpha + \tfrac{1}{3}\mu(y, xyx)y^\alpha + \tfrac{1}{6}\mu(y, y)(xyx)^\alpha\}x^\alpha \\
&\quad + \tfrac{1}{3}\mu(x, yxyxy)x^\alpha \\
&\quad + \tfrac{1}{6}\mu(x, x)\{y^\alpha(xyx)^\alpha y^\alpha + \tfrac{1}{3}\mu(y, xyx)y^\alpha + \tfrac{1}{6}\mu(y, y)(xyx)^\alpha\}
\end{aligned}$$

$$\begin{aligned}
&= x^\alpha y^\alpha\{x^\alpha y^\alpha x^\alpha + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha\}y^\alpha x^\alpha \\
&\quad + \tfrac{1}{3}\mu(y, xyx)x^\alpha y^\alpha x^\alpha \\
&\quad + \tfrac{1}{6}\mu(y, y)x^\alpha\{x^\alpha y^\alpha x^\alpha + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha\}x^\alpha \\
&\quad + \tfrac{1}{3}\mu(x, yxyxy)x^\alpha \qquad (58)\\
&\quad + \tfrac{1}{6}\mu(x, x)y^\alpha\{x^\alpha y^\alpha x^\alpha + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha\}y^\alpha \\
&\quad + \tfrac{1}{18}\mu(x, x)\mu(y, xyx)y^\alpha \\
&\quad + \tfrac{1}{36}\mu(x, x)\mu(y, y)\{x^\alpha y^\alpha x^\alpha + \tfrac{1}{3}\mu(x, y)x^\alpha + \tfrac{1}{6}\mu(x, x)y^\alpha\}.
\end{aligned}$$

It is understood that (58) will be further rewritten by replacing $(x^\alpha)^3$ by βx^α in case (55) holds and replacing $(x^\alpha)^2$ by γ and $(x^\alpha)^3$ by γx^α in case (56) holds. Now, comparing the coefficients of $(y^\alpha)^2 x^\alpha y^\alpha x^\alpha$ in (57) and (58) we see that $\mu(x, x) = \mu(x^\alpha, x^\alpha) = 0$ for all $x^\alpha \in K'$. Linearizing we have $\mu(x^\alpha, y^\alpha) = 0$ for all $x^\alpha, y^\alpha \in K'$ and the proof of Lemma 10 is complete.

Together Lemma 9 and Lemma 10 imply that $(x^3)^\alpha = (x^\alpha)^3$ for all $x \in K$ and so by Lemma 8 we have succeeded in showing in Case B that α can be extended uniquely to an isomorphism of $\langle K\rangle$ onto $\langle K'\rangle$. Our analyses of Case A and Case B combine to immediately give us the proof of our main result, Theorem 3, a complete statement of which is given in Section 1.

REFERENCES

1. W. E. BAXTER AND W. S. MARTINDALE, 3rd, The extended centroid in semiprime rings with involution, *Comm. Algebra* **13** (1985), 945–985.
2. M. BRESAR, Centralizing mappings and derivations in prime rings, *J. Algebra*, to appear.
3. M. BRESAR, Commuting traces of biadditive mappings, commutativity preserving mappings, and Lie mappings, *Trans. Amer. Math. Soc.*, to appear.
4. I. N. HERSTEIN, Lie and Jordan structures in simple, associative rings, *Bull. Amer. Math. Soc.* **67** (1961), 517–531.
5. I. N. HERSTEIN, "Topics in Ring Theory," Univ. of Chicago Press, Chicago, 1969.
6. L. HUA, "A theorem on matrices over an sfield and its applications," *J. Chinese Math. Soc. (N.S.)* **1** (1951), 110–163.
7. N. JACOBSON, "Lie Algebras," Intersciences Tracts in Pure and Applied Math., Vol. 10, Interscience, New York, 1962.
8. W. S. MARTINDALE 3RD, "Lie isomorphisms of primitive rings," *Proc. Amer. Math. Soc.* **14** (1963), 909–916.
9. W. S. MARTINDALE 3RD, Lie isomorphisms of prime rings, *Trans. Amer. Math. Soc.* **142** (1969), 437–455.
10. W. S. MARTINDALE 3RD, Prime rings satisfying a generalized polynomial identity, *J. Algebra* **12** (1969), 576–584.
11. W. S. MARTINDALE 3RD, Prime rings with involution and generalized polynomial identities, *J. Algebra* **22** (1972), 502–516.

12. W. S. MARTINDALE 3RD, Lie isomorphisms of the skew elements of a prime ring with involution, *Comm. Algebra* **4** (1976), 929–977.
13. W. S. MARTINDALE 3RD AND C. R. MIERS, Herstein's Lie theory revisited, *J. Algebra* **98** (1986), 14–37.
14. M. P. ROSEN, Isomorphisms of a certain class of prime Lie rings, *J. Algebra* **89** (1984), 291–317.