Differential Identities with Automorphisms and Antiautomorphisms, I

CHEN-LIAN CHUANG

Department of Mathematics, National Taiwan University,
Taipei, Taiwan 10764, Republic of China

Communicated by Nathan Jacobson
Received January 2, 1989

Let \( R \) be a prime associative ring with the extended centroid \( C \). Assume that \( R \) satisfies a nontrivial differential identity with automorphisms and antiautomorphisms. It is shown here that \( R \) must satisfy a nontrivial ordinary generalized polynomial identity (without derivations, automorphisms, and antiautomorphisms). When this is combined with Martindale's result on generalized polynomial identities, it follows that the central closure \( RC \) of \( R \) is a primitive ring with nonzero socle and its skew field is finite dimensional over \( C \).

Our primary objective of this paper is to prove the following

**Main Theorem.** A prime ring satisfying a nontrivial differential identity with automorphisms and antiautomorphisms must also satisfy a nontrivial ordinary generalized polynomial identity (without derivations, automorphisms, and antiautomorphisms).

Applying the main result in [11], we have the following immediate

**Corollary.** If a prime ring \( R \) satisfies a nontrivial differential identity with automorphisms and antiautomorphisms, then the central closure \( RC \) of \( R \), where \( C \) is the extended centroid of \( R \), is a primitive ring with nonzero socle and with its skew field finite dimensional over \( C \).

In addition to allowing (anti)automorphisms in our differential identities, we work in the more general context of Utumi quotient rings instead of Martindale quotient rings. We mention the following two slight improvements:

1. All coefficients in our differential identities are assumed to be in the left Utumi quotient ring of the given prime ring.
2. All derivations occurring in our differential identities are assumed to be of the two-sided Utumi quotient ring of the given prime ring.
Our result has been conjectured in [13, p. 116] and is basically a generalization of [6, 7, 2, 10]. Our method here is essentially a refinement of that in [7] mixed with a computation in [11] (or in [10]).

The material of this paper is organized as follows: In Section 0, we define precisely all the basic notions, especially the nontriviality of differential identities. We give the proof of our main theorem in Section I and leave the proof of our crucial lemma (Lemma 2) to Section II. Our notation is mostly adopted from [6–8].

0. PRELIMINARIES

Utumi Quotient Rings

Our rings here are always associative but not necessarily with the multiplication identity 1. A ring \( R \) is said to be right faithful if \( Ra = 0 \) implies \( a = 0 \) for any \( a \in R \) [3, p. 67]. Left faithfulness is defined analogously. Throughout this paper, rings of our main concern are always prime and hence are both right and left faithful. A left ideal \( \lambda \) of a right faithful ring \( R \) is said to be (left) dense if for any given \( x, 0 \neq y \in R \), there exists \( r \in R \) such that \( rx \in \lambda \) and \( ry \neq 0 \) [3, Proposition 2, p. 58]. A ring \( U \) satisfying the following axioms is called a left Utumi quotient ring of \( R \) (see, for example, [9, Lemma 3, p. 97]):

Axiom 1. \( R \subseteq U \).

Axiom 2. For each \( a \in U \), there exists a nonzero dense left ideal \( \lambda \) of \( R \) such that \( \lambda a \subseteq R \).

Axiom 3. If \( \lambda \) is a dense left ideal of \( R \) and if \( \xi: R\lambda \to R \) is a left \( R \)-module homomorphism, then there exists a unique \( a \in U \) such that \( \xi(x) = xa \) for all \( x \in \lambda \). Simply speaking, the ring \( U \) is merely the ring of left quotients of \( R \) relative to the filter of nonzero dense left ideals of \( R \). By [3, Theorem 6, p. 59], the left Utumi quotient ring \( U \) for a right faithful ring \( R \) exists uniquely up to within an isomorphism fixing \( R \).

The uniqueness of \( a \) in Axiom 3 is equivalent to the property: If \( a \in U \) and \( \lambda a = 0 \) for some dense left ideal \( \lambda \) of \( R \), then \( a = 0 \). This uniqueness property also implies the right faithfulness of any dense left ideal of \( R \), including \( R \) itself. In this sense, the right faithfulness of a given ring is necessary and sufficient for the existence of its left Utumi quotient ring.

We generalize the notion of (left) density as follows: Assume that \( R \) is right faithful and \( U \) is its left Utumi quotient ring. A left \( R \)-submodule \( A \) of \( U \) is said to be (left) dense if and only if for any given \( x, 0 \neq y \in R \), there exists \( r \in R \) such that \( rx \in A \) and \( ry \neq 0 \). It is obvious that the intersection
of two dense left $R$-submodules of $U$ is still dense. In particular, if $A$ is a
dense left $R$-submodule of $U$, then $R \cap A$ is a dense left ideal of $R$. Conver-
sely, if the left $R$-submodule $A$ of $U$ includes a dense left ideal of $R$, then
$A$ itself must also be dense. Thus a left $R$-submodule $A$ of $U$ is left dense
if and only if it includes a dense left ideal of $R$. In the following fact, the
first statement strengthens the defining property of (left) density for left
$R$-submodules of $U$ and the second statement strengthens the defining
axiom 3 for Utumi quotient rings.

**FACT 0.** Assume that $R$ is a right faithful ring and $U$ is its left Utumi
quotient ring.

(0) If a left $R$-submodule $A$ of $U$ is (left) dense, then for any $a \in U$, the
set

$$\Lambda a^{-1} \overset{\text{def}}{=} \{ u \in U : ua \in A \}$$

also forms a dense left $R$-submodule of $U$.

(1) A left $R$-submodule $A$ of $U$ is dense if and only if for any dense left
ideal $\lambda$ of $R$ and for any given $x, 0 \neq y \in U$, there exists $r \in \lambda$ such that $rx \in A$ and $ry \neq 0$.

(2) Let $A$ be a dense left $R$-submodule of $U$ and let $\lambda$ be a dense left ideal
of $R$. If $\xi : \lambda A \to \lambda U$ is a left $\lambda$-module homomorphism, then there exists a
unique $a \in U$ such that $\xi(x) = xa$ for all $x \in A$.

**Proof.** (0) Assume that $x, 0 \neq y \in R$ are given. The left ideal $\lambda = \{ r \in R :
(\text{rx}) \in R \}$ includes a dense left ideal of $R$ by Axiom 2 and hence must be
dense itself. Since $y \neq 0$, $\lambda y \neq 0$ by the uniqueness assertion of Axiom 3.
Pick $r \in \lambda$ such that $ry \neq 0$. By applying the density of the left $R$-module $A$
to the pair $\lambda x, 0 \neq ry \in R$, there exists $r' \in R$ such that $r'\lambda x \in A$ and
$r'ry \neq 0$. We have succeeded in finding $r' \in R$ such that $r'\lambda x \in A^{-1}$ and
such that $r'ry \neq 0$. So $\Lambda a^{-1}$ is dense, as desired.

(1) The “if” part is obvious. We show the “only-if” part. Assume that
$x, 0 \neq y \in U$ are given. Let $\lambda$ be the given dense left ideal of $R$. By (0) of this
fact, $\lambda x^{-1}$ is dense. Hence their intersection $\lambda' = \lambda x^{-1} \cap \lambda$ is also left dense.
By the uniqueness assertion of Axiom 3, $\lambda' y \neq 0$, since $y \neq 0$. Pick $r \in \lambda'$
such that $ry \neq 0$. Since $r \in \lambda' \subseteq \lambda x^{-1}$, $rx \in A$. We have succeeded in finding
$r \in \lambda$ with $rx \in A$ and $ry \neq 0$, as asserted.

(2) First, we claim that $\xi : \lambda A \to \lambda U$ is an $R$-module homomorphism:
Assume on the contrary that $\xi(rx) - r\xi(x) \neq 0$ for some $r \in R$ and $x \in A$. By
applying the density of $\lambda$ to the pair $r, 0 \neq \xi(rx) \in U$ and using (1)
of this fact, there exists $r_0 \in \lambda$ such that $r_0r \in \lambda$ and $r_0(\xi(rx) - r\xi(x)) \neq 0$. 

Since $r_0, r_0r \in \lambda$ and since $\xi$ is assumed to be a $\lambda$-module homomorphism, we compute
\[
 r_0(\xi(rx) - r\xi(x)) = \xi(r_0rx) - (r_0r) \xi(x) = \xi(r_0rx) - \xi((r_0r)x) = 0,
\]
a contradiction. So the map $\xi : \lambda A \to \lambda U$ is a left $R$-module homomorphism, as claimed. Set $A_0 = \{x \in \lambda : \xi(x) \in R\}$. Since $\xi$ is a left $R$-module homomorphism, $A_0$ is a left $R$-module. We show that $A_0$ is left dense: For given $x, 0 \neq y \in R$, pick $r \in \lambda$ such that $rx \in A$ and $ry \neq 0$. Since $rx \in A, \xi(rx)$ is defined. Since $\xi(rx) \in U$, by Axiom 2, there exists a dense left ideal $\lambda'$ such that $\lambda' \xi(rx) \subseteq R$. By the uniqueness assertion of Axiom 3, $\lambda'ry \neq 0$, since $ry \neq 0$. Pick $r' \in \lambda'$ such that $r'ry \neq 0$. For this $r'$, we also have that $\xi(r'rx) = r'\xi(rx) \in \lambda' \xi(rx) \subseteq R$ and hence $r'rx \in A_0$. We have succeeded in finding $r'x \in R$ such that $r'rx \in A_0$ and $r'ry \neq 0$. So $A_0$ is dense, as desired. By applying Axiom 3 of $U$ to the left $R$-module homomorphism map $x \in A_0 \mapsto \xi(x) \in U$, there exists $a \in U$ such that $\xi(x) = xa$ for all $x \in A_0$. We show that $\xi(x) = xa$ for all $x \in \lambda$: Assume on the contrary that $\xi(x) - xa \neq 0$ for some $x \in \lambda$. By applying the density of $A_0$, as strengthened in (1) of this fact, to the pair $x, 0 \neq \xi(x) - xa$, there exists $r \in R$ such that $rx \in A_0$ and $0 \neq r(\xi(x) - xa)$. Since $rx \in A_0, \xi(rx) - (rx)a - 0$ by our choice of $a$. Since $\xi$ is a left $R$-module homomorphism, $r(\xi(x) - xa) = \xi(rx) - (rx)a = 0$, a contradiction. So $\xi(x) = xa$ for all $x \in \lambda$. The uniqueness of $a$ follows easily from Axiom 3 and our proof of (2) is completed.

The second statement of Fact 0 also implies that the left Utumi quotient ring of any right faithful ring is also the left Utumi quotient ring of any of its dense left ideals.

The dense right ideals and the right Utumi quotient ring of a left faithful ring $R$ are defined analogously. Assume that $R$ is both right and left faithful and that $U$ is its left Utumi quotient ring. The subset $Q$ of $U$ defined by
\[
 Q = \{a \in U : ap \subseteq R \text{ for some dense right ideal } p \text{ of } R\}
\]
forms a subring of $U$, called the two-sided Utumi quotient ring of $R$. Essentially, $Q$ can be regarded as the intersection of the left and the right Utumi quotient rings of $R$. The center of $Q$, denoted by $C$, is called the extended centroid of $R$. The extended centroid $C$ of a prime ring $R$ coincides with the center of $U$ and is always a commutative field. For a given prime ring $R$, both $U$ and $Q$ are also prime (see [3, Proposition 10, p. 74]).

**Derivations**

By a derivation of an arbitrary ring $R$, we mean a map $\delta : R \to R$ satisfy $(x+y)^\delta = x^\delta + y^\delta$ and $(xy)^\delta = x^\delta y + xy^\delta$ for all $x, y \in R$. For a given ring $R$, we use $\text{Der}(R)$ to denote the set of all derivations of $R$. 
The following simple fact is a generalization of a result due to Tewari (see [9, Exercise 10, p. 101]:

**FACT 1.** A mapping \( \delta \) from a right faithful ring \( R \) into its left Utumi quotient ring \( U \) satisfying

\[
(x + y)^{\delta} = x^{\delta} + y^{\delta}, \\
(xy)^{\delta} = x^{\delta}y + xy^{\delta}
\]

for all \( x, y \in R \)

can be extended uniquely to a derivation of \( U \).

**Proof.** For given \( a \in U \), let \( \lambda \) be a dense left ideal of \( R \) such that \( \lambda a \subseteq R \).

Define the map \( \xi: \lambda \rightarrow U \) by setting \( \xi(x) = (xa)^{\delta} - x^{\delta}a \) for \( x \in \lambda \). We verify that \( \xi \) is a left \( R \)-module homomorphism from \( \lambda \) into \( U \): For \( r \in R \) and \( x \in \lambda \), we have \( rx \in \lambda \) and compute

\[
\xi(rx) = (rxa)^{\delta} - (rx)^{\delta}a = (r(xa))^{\delta} - (r^{\delta}x + rx^{\delta})a \\
= (r^{\delta}xa + r(xa)^{\delta}) - (r^{\delta}x + rx^{\delta})a = r((xa)^{\delta} - x^{\delta}a) = r\xi(x),
\]

as desired. Hence, by (2) of Fact 0, there exists a unique \( a' \in U \) such that \( \xi(x) = xa' \) for all \( x \in \lambda \). It is easy to verify that the map \( a \in U \mapsto a' \in U \), where \( a' \) is defined from \( a \) as above, is a derivation of \( U \) extending \( \delta \). The uniqueness of such an extension of \( \delta \) to \( U \) is also obvious.

As remarked before, the left Utumi quotient ring of a right faithful ring is also the left Utumi quotient ring of any of its dense left ideals. Hence Fact 1 above can be immediately strengthened to the following:

**FACT 1'.** A mapping \( \delta \) from a dense left ideal \( \lambda \) of a right faithful ring \( R \) into its left Utumi quotient ring \( U \) satisfying

\[
(x + y)^{\delta} = x^{\delta} + y^{\delta}, \\
(xy)^{\delta} = x^{\delta}y + xy^{\delta}
\]

for all \( x, y \in \lambda \)

can be extended uniquely to a derivation of \( U \).

Suppose that \( Q \) is an arbitrary algebra over an arbitrary commutative ring \( C \). For \( \delta, \mu \in \text{Der}(Q) \) and \( x \in C \), we define

\[
x^{(\delta \mu)} = \mu(x^{\delta}), \\
x^{[\delta, \mu]} = (x^{\delta})^\mu - (x^\mu)^\delta
\]

for \( x \in Q \).

Obviously, \( \delta \mu \) and \([\delta, \mu]\) thus defined above are also derivations of \( Q \). In this manner, \( \text{Der}(Q) \) is a right \( C \)-module and forms a Lie ring under the
binary operation \([\delta, \mu]\). For \(a \in Q\), the map \(\text{ad}(a): x \in Q \mapsto ax - xa \in Q\) defines a derivation of \(Q\), called the inner derivation defined by \(a\). A derivation \(\delta\) of \(Q\) is said to be inner if \(\delta = \text{ad}(a)\) for some \(a \in Q\). The set of all inner derivations of \(Q\), denoted by \(\text{Der}_i(Q)\), obviously forms a \(C\)-submodule of \(\text{Der}(Q)\).

Recall the following basic terminology from module theory: Let \(M\) be a module over a commutative ring \(C\) and let \(M_0\) be a \(C\)-submodule of \(M\). A subset \(X\) of \(M\) is said to be \(C\)-independent modulo \(M_0\) if for any \(x_1, ..., x_n \in C\) and for any \(m_1, ..., m_n \in X\), \(\sum_{i=1}^{n} m_i x_i \in M_0\) implies \(x_1 = \cdots = x_n = 0\). This is equivalent to the \(C\)-independence of the subset \(\{m + M_0 : m \in X\}\) of the difference module \(M \setminus M_0\). An independent subset \(X\) of \(M\) is called a basis of \(M\) modulo \(M_0\) if the set \(\{m + M_0 : m \in X\}\) forms a \(C\)-basis for the difference \(C\)-module \(M \setminus M_0\).

For a given prime ring, we apply these concepts to the \(C\)-algebra \(Q\), where \(Q\) is its two-sided Utumi quotient ring and \(C\) is its extended centroid. The set \(\text{Der}(Q)\) forms a right \(C\)-vector space with the \(C\)-subspace \(\text{Der}_i(Q)\). A subset \(M\) of \(\text{Der}(Q)\) is said to be independent modulo \(\text{Der}_i(Q)\) if for any \(x_1, ..., x_n \in C\) and for any \(\delta_1, ..., \delta_n \in M\), \(\sum_{i=1}^{n} \delta_i x_i \in \text{Der}_i(Q)\) implies \(x_1 = \cdots = x_n = 0\). A subset \(M\) of \(\text{Der}(Q)\) is called a basis of \(\text{Der}(Q)\) modulo \(\text{Der}_i(Q)\) if the set \(\{\delta + \text{Der}_i(Q) : \delta \in M\}\) forms a \(C\)-basis for the quotient vector space \(\text{Der}(Q)/\text{Der}_i(Q)\). This is equivalent to the condition that the set \(M\) forms a maximal independent subset of \(\text{Der}(Q)\) modulo \(\text{Der}_i(Q)\). An independent subset \(M\) of \(\text{Der}(Q)\) modulo \(\text{Der}_i(Q)\) endowed with a linear order <, denoted by \((M, <)\), is called an ordered independent subset of \(\text{Der}(Q)\) modulo \(\text{Der}_i(Q)\). If \(M\) happens to be a basis of \(\text{Der}(Q)\) modulo \(\text{Der}_i(Q)\), then \((M, <)\) is called an ordered basis of \(\text{Der}(Q)\) modulo \(\text{Der}_i(Q)\). For an ordered independent subset \((M, <)\) of \(\text{Der}(Q)\) modulo \(\text{Der}_i(Q)\), by a regular derivation word in \((M, <)\), we mean a derivation word \(\Delta\) of the form

\[
\Delta = \delta_1^{s_1} \delta_2^{s_2} \cdots \delta_m^{s_m},
\]

where

1. \(\delta_i \in M\) for \(i = 1, ..., m\),
2. \(\delta_1 < \delta_2 < \cdots < \delta_m\), and
3. \(0 < s_i < p\) for \(i = 1, ..., m\), if the characteristic of \(Q\) (or, equivalently, of \(R\)) is some prime number \(p \geq 2\).

We let \(\Omega(M, <)\) denote the set consisting of all regular derivation words in \((M, <)\). We also extend the linear order \(<\) on \(M\) to the set \(\Omega(M, <)\) by assuming that a longer word is greater than a shorter one and that words of the same length are ordered lexicographically. Note that the order \(<\) thus defined on \(\Omega(M, <)\) is also a linear order. It is important to observe that
if $M$ is finite, then the linear order $<$ on $\Omega(M, <)$ is a well order. That is, there does not exist $\Delta_i \in \Omega(M, <)$ ($i = 1, 2, \ldots$) such that $\Delta_{i+1} < \Delta_i$ for $i = 1, 2, \ldots$. Finally, for a subset $\overline{M}$ of $M$, let $\Omega(\overline{M}, <)$ be the set $\overline{M}$ endowed with the restriction of the order $<$ on $M$. Note that the linear order $<$ on $\Omega(\overline{M}, <)$ is also the restriction of the linear order $<$ on $\Omega(M, <)$.

Automorphisms and Antiautomorphisms

By an automorphism of an arbitrary ring $R$, we mean a bijective map $\sigma: R \rightarrow R$ satisfying $(x + y)\sigma = x\sigma + y\sigma$ and $(xy)\sigma = x\sigma y\sigma$ for all $x, y \in R$. The set of all automorphisms of $R$, denoted by $\text{Aut}(R)$, forms a group under composition. By an antiautomorphism of an arbitrary ring $R$, we mean a bijective map $\nu: R \rightarrow R$ satisfying $(x + y)\nu = x\nu + y\nu$ and $(xy)\nu = y\nu x\nu$ for all $x, y \in R$. The set of all antiautomorphisms of $R$ will be denoted by $\text{Ant}(R)$. The set $G(R) = \text{Aut}(R) \cup \text{Ant}(R)$, consisting of all automorphisms and all antiautomorphisms of $R$, forms a group under composition and contains $\text{Aut}(R)$ as a normal subgroup. The analogue of Fact 1 for automorphisms is the following:

**Fact 2.** Any automorphism of a right faithful ring can be extended uniquely to an automorphism of its left Utumi quotient ring. If the ring is also left faithful, the automorphism of the given ring, thus extended to its left Utumi quotient ring, induces an automorphism of its two-sided Utumi quotient ring.

**Proof** Assume that $R$ is a given right faithful ring and $U$ is its left Utumi quotient ring. Let $\sigma \in \text{Aut}(R)$ be given. For $a \in U$, pick a dense left ideal $\lambda$ of $R$ such that $\lambda a \subseteq R$. Define $\xi: \lambda \nu R$ by setting $\xi(x\sigma) = (xa)\sigma$ for $x \in \lambda$. Then $\xi$ is a left $R$-module homomorphism from $\lambda\sigma$ into $R$. Hence there exists $a' \in U$ such that $\xi(x) = xa'\sigma$ for any $x \in \lambda$. The map $a \in U \mapsto a' \in U$ (as defined above) obviously extends $\sigma$, which we will also denote by $\sigma$. (Hence $a' = a\sigma$.) We verify that the map $a \in U \mapsto a\sigma \in U$ is an automorphism of $U$ as follows: For $a, b \in U$, $(a + b)\sigma = a\sigma + b\sigma$ and $(ab)\sigma = a\sigma b\sigma$ hold obviously. For $a \in U$, let $\lambda$ be a dense left ideal of $R$ such that $\lambda a \subseteq R$. For $x \in \lambda$, we have $xa = ((xa)\sigma)^{-1} = (x\sigma a\sigma)^{-1} = x(a\sigma)^{-1}$ and hence $(a\sigma)^{-1} = a$. We can show similarly that $(a^{-1}\sigma)^{-1} = a$ for all $a \in U$. From these, the surjectivity and the injectivity of the map $\sigma: a \in U \mapsto a\sigma \in U$ follow. So $\sigma$ thus extended is indeed an automorphism of $U$, as desired. The uniqueness of such an extension is obvious.

Assume that $R$ is also left faithful and $Q$ is its two-sided Utumi quotient ring. For $a \in Q$, there exists a dense right ideal $\rho$ of $R$ such that $a\rho \subseteq R$. By applying the automorphism $\sigma$ thus extended, $a\sigma^\rho \sigma \subseteq R = R$. But $\rho\sigma$ is also a dense right ideal of $R$. Hence $a\sigma$ is also an element of the two-sided Utumi quotient ring of $R$, as asserted.
The following is the analogue of Fact 2 for anti-automorphisms:

**FACT 3.** Any anti-automorphism of a right and left faithful ring \( R \) can be extended uniquely to an anti-automorphism of its two-sided Utumi quotient ring.

**Proof.** Assume that the given ring \( R \) is left and right faithful and \( Q \) is its two-sided Utumi quotient ring. Let \( v \in \text{Ant}(R) \). For \( a \in Q \), pick a dense right ideal \( \rho \) of \( R \) such that \( a \rho \subseteq R \). Define the map \( \xi: \rho^* \rightarrow R \) by setting \( \xi(x^r) = (ax)^r \) for \( x \in \rho \). For \( r \in R \), we compute \( \xi((xr)^r) = \xi((ax) r)^r = (a(xr))^r = r (ax)^r = r^* \xi(x^r) \). So \( \xi \) is a left \( R \)-module homomorphism from \( \rho^* \) into \( R \). But as \( \rho \) is a dense right ideal of \( R \), \( \rho^* \) is a dense left ideal of \( R \). Hence there exists \( a' \in U \) such that \( \xi(x^r) = x^r a' \). The map \( a \in Q \rightarrow a' \in U \) obviously extends \( v \) and will also be denoted by \( v \). So \( \xi(x^r) = (ax)^r = x^r a' = x^r a^r \). We verify easily that \( (a + b)^r = a^r + b^r \) and \( (ab)^r = b^r a^r \) hold for \( a, b \in Q \). For \( a \in Q \), pick a dense left ideal \( \lambda \) of \( R \) such that \( \lambda a \subseteq R \). Note that \( \lambda^* \) is a dense right ideal of \( R \) and \( a^r \lambda^* = (\lambda a)^r \subseteq R \). So \( a^r \in Q \). Hence \( v \), thus extended, maps \( Q \) into \( Q \). As in the case of automorphisms, the surjectivity and the injectivity of \( v \) on \( Q \) can be shown by considering \( v^{-1} \). Hence \( v \), thus extended, is indeed an anti-automorphism of \( Q \). The uniqueness of such an extension of \( v \) is obvious.

By these two facts, for a prime ring \( R \), we have \( G(R) \subseteq G(Q) \) and \( \text{Aut}(R) \subseteq \text{Aut}(Q) \subseteq \text{Aut}(U) \), where \( Q \) and \( U \) are respectively the two-sided and the left Utumi quotient rings of \( R \). Thereafter, all (anti)automorphisms of \( R \) will be implicitly assumed to be defined on \( Q \) and \( U \).

An automorphism \( \sigma \in \text{Aut}(R) \) is said to be the **inner automorphism defined by an invertible element** \( a \in R \) if and only if \( x^a = a^{-1} xa \) for all \( x \in R \). The set of all inner automorphisms defined by invertible elements of \( R \) is denoted by \( \text{Aut}_i(R) \). Assume that \( R \) is a prime ring. Set \( G_i(R) = G(R) \cap \text{Aut}_i(Q) \), where \( Q \) is its two-sided Utumi quotient ring.

Note that, in general, anti-automorphisms of \( R \) **cannot** be extended to be defined on the left Utumi quotient ring \( U \) of \( R \), especially for those prime rings which are most interesting to us. The reason is as follows: We are interested in prime rings satisfying nontrivial differential identities with (anti)automorphisms and we aim to show that such prime rings must also satisfy nontrivial GPIs. So the prime rings interesting to us are those satisfying nontrivial GPIs. By the main theorem of [11], the central closures of such rings must be primitive with nonzero socle. By [9, Proposition 7, p. 98], the left Utumi quotient ring of a primitive ring with nonzero socle is the ring consisting of all linear transformations of a left vector space over a division ring. But the left Utumi quotient ring of a prime ring obviously coincides with the left Utumi quotient ring of its central closure. So the left Utumi quotient ring of the prime ring which we are
really interested in is the ring consisting of all linear transformations of a left vector space over a division ring. The following says that such rings cannot have antiautomorphisms in general:

**Fact 4.** The ring consisting of all linear transformations of a left vector space $V$ over a division ring $D$ has an antiautomorphism if and only if the dimension of $V$ over $D$ is finite.

**Proof.** Let $R$ denote the ring of all linear transformations of $V$. Let $b$ be the dimension of $V$ over the division ring $D$. First, assume that $b$ is finite and that the division ring $D$ has an antiautomorphism $\varphi: d \in D \mapsto d' \in D$. Then $R$ is just the ring of all $b \times b$ matrices over $D$. Let $e_{ij}$ $(i, j = 1, \ldots, b)$ be the matrix unit with 1 in the $(i, j)$-entry and 0 elsewhere. Define the map $*: R \to R$ as follows: For $a = \sum_{i,j} a_{ij} e_{ij}$, where $a_{ij} \in D$, set $a^* = \sum_{i,j} \bar{a}_{ij} e_{ij}$. It is easy to verify that the map $*$ is an antiautomorphism of $R$.

Assume that $R$ has an antiautomorphism $\ast$. Obviously, the ring $R$ is prime with nonzero socle. It is well known that all right irreducible modules of a prime ring with nonzero socle are isomorphic. Using this fact and by [4, Theorem 1, p. 821], the antiautomorphism $\ast$ of the ring $R$ can be represented as follows: The division ring $D$ has an antiautomorphism $\varphi: d \in D \mapsto d'$ and using this antiautomorphism of the division ring $D$, the left $D$-vector space $_DV$ can be interpreted as a right $D$-vector space $V_D$ by setting $vd = dv$ for $d \in D$ and $v \in V$. On this pair of the left vector space $D_V$ and the right vector space $V_D$, there exists a bilinear form $(\cdot, \cdot): D_V \times V_D \to D$ such that the given antiautomorphism $\ast$ is merely the adjoint operation on $R$. Let $f$ be a linear functional on $D_V$. Pick arbitrary $v_0, w_0 \in V$ such that $(v_0, w_0) \neq 0$. Consider the linear transformation $a \in R$ defined by $va = f(v)v_0$ for $v \in V$ and let $a^*$ be the adjoint of $a$ with respect to the bilinear form $(\cdot, \cdot)$ on $D_V \times V_D$. (By the representation theorem just quoted, $a^*$ is also the image of $a$ under the antiautomorphism $\ast$.) Hence

$$f(v)(v_0, w_0) = (f(v)v_0, w_0) = (va, w_0) = (v, w_0 a^*) \quad \text{for any } v \in V.$$ 

As $(v_0, w_0)$ is chosen to be nonzero, $f(v) = (v, w_0 a^*)(v_0, w_0)^{-1} = (v, w_0 a^*(v_0, w_0)^{-1})$. We have thus shown that any linear functional of $D_V$ is of the form $v \in V \mapsto (v, w)$ for some fixed $w \in V$. Hence the dual space $V^*$ consisting of all linear functionals of $D_V$ is isomorphic to $V_D$ as right $D$-vector spaces. In particular, the dimension of $V^*$ is also equal to $b$. Assume on the contrary that $b$ is infinite. By [5, Theorem 2, p. 247], the dimension of $V^*$ over $D$ is $d^b$, where $d$ is the cardinality of the division ring $D$. Since $d \geq 2$, the well-known Cantor theorem says $d^b > b$, a contradiction. Hence $b$ must be finite, as desired.
Note that, for a prime ring satisfying a nontrivial GPI, its left Utumi quotient ring is the ring of all linear transformations of a finite dimensional vector space over a division ring if and only if the ring satisfies an ordinary polynomial identity. Also, in this case, its two-sided Utumi quotient ring must coincide with its left Utumi quotient ring. In this sense, Fact 3 is the best possible.

Recall the following basic terminology from group theory: Let $G$ be a group with a normal subgroup $N$. A subset $\mathcal{A}$ of $G$ is said to be independent modulo $N$ if for any $g_1, g_2 \in \mathcal{A}$, $g_1 g_2^{-1} \in N$ implies $g_1 = g_2$. This is equivalent to saying that elements of $\mathcal{A}$ belong to distinct cosets of the quotient group $G/N$. A subset $\mathcal{B}$ of $G$ is called a basis of $G$ modulo $N$ if $\mathcal{B}$ is maximal with respect to the property of being independent modulo $N$. This is equivalent to saying that $\mathcal{B}$ is a set of representatives of the quotient group $G/N$. All these concepts will be applied to the group $G(R)$ and its normal subgroup $G_i(R)$ for a given prime ring $R$.

**Differential Polynomials and Identities**

Let $Q$ be the two-sided Utumi quotient ring of a given prime ring $R$. The set of all endomorphisms of the abelian additive group $(Q, +)$ forms a ring under pointwise addition and composition multiplication. Elements of $\text{Der}(Q)$ and $G(R)$ obviously preserve the addition of $R$ and hence are endomorphisms of the abelian additive group $(Q, +)$. Let $\delta(R)$ be the subring generated by $\text{Der}(Q)$ and $G(R)$ in the ring of endomorphisms of $(Q, +)$. Intuitively speaking, a differential polynomial (or identity respectively) with automorphisms and anti-automorphisms is merely a GP (or a GPI respectively) involving noncommutative indeterminates acted on by elements of $\delta(R)$.

**DEFINITION.** Assume that $R$ is a prime ring and that $Q$ is its two-sided Utumi quotient ring and $U$ is its left Utumi quotient ring.

(1) By a *differential polynomial with automorphisms and anti-automorphisms* of the ring $R$, we mean an expression of the form $\phi(x^\varepsilon)$, where $\varepsilon_j \in \delta(R)$ and where $\phi(z^\varphi)$ is an ordinary generalized polynomial in distinct indeterminates $z^\varphi$ and with coefficients in $U$.

(2) Let $\phi$ be a differential polynomial with automorphisms and anti-automorphisms. The expression $\phi = 0$ is said to be a *differential identity with automorphisms and anti-automorphisms* of $R$, if $\phi$ assumes the constant value 0 for any assignment of values from $R$ to its indeterminates.

(3) For brevity, we introduce the following abbreviations: DP for differential polynomial; DI for differential identity; DP($M$) (or DI($M$) respectively) for DP (or DI respectively) with automorphisms and
antiautomorphisms. Here the letter “M” suggests “-morphism” in the two key words “automorphism” and “antiautomorphism.”

(4) Ordinary generalized polynomials (or generalized polynomial identities respectively) are merely DP(M)s (or DI(M)s respectively) without derivations, automorphisms, and antiautomorphisms, and, as usual, are abbreviated as GPs (or GPIs respectively).

Basic Identities

As in [7, 8], the following basic DIs hold in any arbitrary algebra $Q$ over a commutative ring $C$:

1. $(x + y)^\delta = x^\delta + y^\delta$, where $\delta \in \text{Der}(Q)$.
2. $(xy)^\delta = x^\delta y + xy^\delta$, where $\delta \in \text{Der}(Q)$.
3. $x^{\delta_1 + \delta_2 + \delta_3} = x_1(x^{\delta_1}) + x_2(x^{\delta_2})$, where $\delta_1, \delta_2 \in \text{Der}(Q)$ and $x_1, x_2 \in C$.
4. $x^\delta = ax - xa$, where $\delta \in \text{Der}(Q)$ is the inner derivation $\text{ad}(a)$ defined by $a \in Q$.
5. $x^{[\mu, \delta]} = (x^\mu)^\delta - (x^\delta)^\mu$, where $\mu, \delta \in \text{Der}(Q)$ and $[\mu, \delta]$ is their commutator.

The characteristic of a ring $R$ is defined to be the maximum for the addition orders of its elements if such maximum exists, and is defined to be infinity if no such maximum exists.

Assume that the characteristic $p$ of $Q$ is either a prime number $\geq 2$ or $\infty$. This is always the case when $R$ is prime.

\[ p\text{-times} \]

6. \[ (\cdots (x^\delta)^\delta \cdots) = x^{(p\delta)}, \]

where $\delta \in \text{Der}(Q)$, if the characteristic of $Q$ is the prime number $p \geq 2$. If the characteristic of $Q$ is $\infty$, then this identity assumes the form $x = x$.

The following are basic identities for automorphisms and antiautomorphisms of a given ring $R$:

7. $(x + y)^g = x^g + y^g$ for $g \in G(R)$.
8. $(xy)^\sigma = x^\sigma y^\sigma$ for $\sigma \in \text{Aut}(R)$.
9. $(xy)^v = y^v x^v$ for $v \in \text{Ant}(R)$.
10. $x^\sigma = a^{-1}xa$, where $\sigma \in G_1(R)$ is the inner automorphism defined by the invertible element $a \in U$.

Assume that $R$ is right and left faithful and $Q$ is its two-sided Utumi quotient ring. By Facts 2 and 3, all elements of $G(R)$ can be assumed to be defined on the whole $Q$. For $g \in G(R)$ and $\delta \in \text{Der}(Q)$, we define $\delta^g$ by

\[ x^{(\delta^g)} = ((x^g)^\delta)^{-1} \quad \text{for} \quad x \in Q. \]
It is easy to verify that $\delta^g \in \text{Der}(Q)$. Also, for $\delta \in \text{Der}(Q)$, if $\delta = \text{ad}(a)$ for some $a \in Q$, then $\delta^g = \text{ad}(a^g)$. Hence, if $\delta \in \text{Der}_i(Q)$, then $\delta^g \in \text{Der}_i(Q)$.

Our last basic identity is the following:

11. $x^{g\delta} = x^{(\delta^g)g}$, where $\delta \in \text{Der}(Q)$ and $g \in G(R)$.

An immediate generalization of 11 is the following

11'. $(x^g)^{\delta_1\delta_2\cdots\delta_n} = x^{(\delta_1^g\delta_2^g\cdots\delta_n^g)g}$, where $\delta_1, \delta_2, \ldots, \delta_n \in \text{Der}(Q)$ and $g \in G(R)$.

We have thus finished our list of basic DIs.

**Reduced DP(M)s and Nontrivial DI(M)s**

**Definition.** Assume that $R$ is a prime ring and that $Q$ is its two-sided Utumi quotient ring, and $U$ is its left Utumi quotient ring. Let $(M, <)$ be an ordered independent subset of $\text{Der}(Q)$ modulo $\text{Der}_i(Q)$ and let $\mathcal{R}$ be an independent subset of $G(R)$ modulo $G_i(R)$.

1. A DP(M) $\varphi$ is said to be reduced, with respect to $(M, <)$ and $\mathcal{R}$, if $\varphi$ assumes the form

$$\varphi = \psi(x_i^{\Delta_i g_k}),$$

where $\Delta_i \in \Omega(M, <)$, $g_k \in \mathcal{R}$ and where $\psi(z_{ijk})$ is an ordinary generalized polynomial in distinct indeterminates $z_{ijk}$ with coefficients in $U$.

2. A reduced DP(M) $\varphi = \psi(x_i^{\Delta_i g_k})$ with respect to $(M, <)$ and $\mathcal{R}$, as described above, is said to be nontrivial if the corresponding ordinary generalized polynomial $\psi(z_{ijk})$ is nontrivial.

3. A DI(M) $\varphi = 0$ is said to be reduced with respect to $(M, <)$ and $\mathcal{R}$ if the DP(M) $\varphi$ is reduced with respect to $(M, <)$ and $\mathcal{R}$.

4. A reduced DI(M) $\varphi = 0$ is said to be nontrivial if the reduced DP(M) $\varphi$ is nontrivial.

The following important fact is implicit in Kharchenko's path-breaking work [7]:

**Fact 5.** Assume that $R$ is a prime ring with the extended centroid $C$ and $Q$ is its two-sided Utumi quotient ring. Let $(M, <)$ be an ordered basis of $\text{Der}(Q)$ modulo $\text{Der}_i(Q)$ and let $\mathcal{R}$ be a basis of $G(R)$ modulo $G_i(R)$. Then by means of the basic identities 1–11 for the $C$-algebra $Q$, any arbitrary DP(M) $\varphi$ can be transformed into a reduced DP(M) with respect to $(M, <)$ and $\mathcal{R}$.

**Proof.** An element $\omega \in \mathcal{S}(R)$ is called a word if $\omega$ assumes the form $\omega = \varepsilon_1^{\varepsilon_2\cdots\varepsilon_n}$, where $\varepsilon_i \in \text{Der}(Q) \cup G(R)$ for $i = 1, \ldots, n$. If all $\varepsilon_i$ are derivations in $\text{Der}(Q)$, then $\omega$ is particularly called a derivation word. Also, we
interpret \( x \in C \) as an endomorphism of the abelian group \((Q, +)\) via right multiplication. We describe a procedure as follows:

**Step 1.** Any derivation word can be written in the form \( \sum_s A_s A'_{s} a_s \), where \( a_s \in A, A'_{s} \) are compositions of inner derivations in \( \text{Der}_i(Q) \), and \( A_s \) are regular derivation words in \((M, \prec)\). Let \( \omega \) be a given derivation word, say \( \omega = \varepsilon_1 \cdots \varepsilon_n \), where each \( \varepsilon_i \in \text{Der}(Q) \). We proceed by induction on the length \( n \) of \( \omega \) to show that \( \omega \) can be written in the desired form. Express each \( \varepsilon_i \) as a right \( C \)-linear combination of derivation words in \( M \) and an inner derivation in \( \text{Der}_i(Q) \). If \( n = 1 \), we are done. So we assume that \( n > 1 \) and, as our induction hypothesis, we also assume that the assertion holds for derivation words of length less than \( n \). Observe the identity: 

\[
x^b = x^b + b x^a,
\]

for \( b \in M \cup \text{Der}_i(Q) \), and derivation words of length less than \( n \). Derivation words of length less than \( n \) are done by the induction hypothesis. It suffices to prove the assertion for derivation words of the form \( \delta_1 \cdots \delta_n \), where \( \delta_i \in M \cup \text{Der}_i(Q) \), and derivation words of length less than \( n \). Derivation words of length less than \( n \) are done by the induction hypothesis. Without loss of generality, we may assume that the given derivation word \( \omega \) is of this form. The basic identity 5 says that \( \mu \delta = \delta \mu + [\mu, \delta] \) for \( \mu, \delta \in \text{Der}(Q) \). Note that \([\mu, \delta]\) is itself a derivation and hence, as a derivation word, is of length 1. By using this basic identity 5 repeatedly, we can permute the derivations in a given derivation word modulo a sum of shorter derivation words. Applying this to the derivation word \( \omega \), we may assume

\[
\omega = \delta_1 \cdots \delta_s \delta_{s+1} \cdots \delta_n + \text{derivation words of length less than } n,
\]

where \( \delta_1, \ldots, \delta_s \in M, \delta_1 < \cdots < \delta_s \), and \( \delta_{s+1}, \ldots, \delta_n \in \text{Der}_i(Q) \). By the induction hypothesis, it suffices to look at the derivatin word \( \omega' = \delta_1 \cdots \delta_s \). If \( s < n \), we are done, again by the induction hypothesis. So we may assume \( s = n \). By collecting equal terms, we may write \( \omega' = \mu_1^{s_1} \cdots \mu_m^{s_m} \), where \( \mu_1, \ldots, \mu_m \in M, \mu_1 < \cdots < \mu_m, s_1, \ldots, s_m > 0, \) and \( s_1 + \cdots + s_m = n \). If the characteristic of the given prime ring \( R \) is \( \infty \), \( \omega' \) is already a regular derivation word with respect to \( M \) and we are done. So assume that the characteristic of \( R \) is a prime \( p \geq 2 \). If \( s_i < p \) for all \( i = 1, \ldots, m \), then \( \omega' \) is again a regular derivation word with respect to \( M \) and again we are done. So assume some \( s_i \geq p \). By the basic identity 6, \( \delta = \mu_i^p \) is also a derivation in \( \text{Der}(Q) \). But then

\[
\omega' = \mu_1^{s_1} \cdots \mu_i^{s_i - p} \mu_i^p \cdots \mu_m^{s_m} = \mu_1^{s_1} \cdots \mu_i^{s_i - p} \delta \cdots \mu_m^{s_m}.
\]

The last expression shows that the derivation word \( \omega' \) is of length \( n - p + 1 \), which is strictly less than \( n \). We are done by the induction hypothesis.
Step 2. For any word \( \omega \in \mathcal{E}(R) \), the DP(M) \( x^\omega \) can be written in the form

\[
x^\omega = \sum_s \sum_t a_s^{(t)} x^d_s g h_s^{(t)},
\]

where \( \Delta_s \in \Omega(M, \prec) \), \( g \in \mathcal{R} \), and \( a_s^{(t)}, h_s^{(t)} \in Q \): Let \( \omega \in \mathcal{E}(R) \) be a word. By means of the basic identity 11, the (anti)automorphisms \( g \in G(R) \) occurring in the expression of \( \omega \) can be pushed outside of the derivations occurring in the expression of \( \omega \). Hence we can write

\[
\omega = \delta_1 \cdots \delta_m h_1 \cdots h_n,
\]

where \( \delta_i \in \text{Der}(Q) \) \((i = 1, \ldots, m)\) and \( h_i \in G(R) \) \((i = 1, \ldots, n)\). Using the procedure of Step 1, the derivation word \( \delta_1 \cdots \delta_m \) can be written, by means of the basic identities 1–6, in the form \( \delta_1 \cdots \delta_m = \sum_s \Delta_s \Delta'_s \alpha_s \), where \( \alpha_s \in C \), \( \Delta'_s \) are compositions of inner derivations in \( \text{Der}_1(Q) \), and \( \Delta_s \) are regular derivation words in \( (M, \prec) \). Set \( h = h_1 \cdots h_n \in G(R) \) and write \( h = gg' \), where \( g \in \mathcal{R} \) and \( g' \in G_i(R) \). For an indeterminate \( x \), we have

\[
x^\omega = x^{\delta_1 \cdots \delta_m h_1 \cdots h_n} = \sum_s x^{(\Delta_s \Delta'_s \alpha_s)} g g'.
\]

Note that \( (\Delta'_s)^{(g^{-1})} \) is still also a composition of inner derivations in \( \text{Der}_1(Q) \). By means of the basic identities 4 and 10, \( (\Delta'_s)^{(g^{-1})} \) and \( g' \) can be expressed in terms of elements of \( Q \). Hence \( x^\omega \) can be written in the reduced form

\[
x^\omega = \sum_s \sum_t a_s^{(t)} x^d_s g h_s^{(t)},
\]

where \( \Delta_s \in \Omega(M, \prec) \), \( g \in \mathcal{R} \), and \( a_s^{(t)}, h_s^{(t)} \in Q \), as desired.

Step 3. DP(M)s of the form \( x^\epsilon \), where \( \epsilon \in \mathcal{E}(R) \): Any element \( \epsilon \in \mathcal{E}(R) \) is a sum of words in \( \mathcal{E}(R) \), say \( \epsilon = \sum \omega_s \), where \( \omega_s \in \mathcal{E}(R) \) are words. For an indeterminate \( x \), the DP(M) \( x^\epsilon = \sum x^\omega \). By Step 2, each DP(M) \( x^\omega \) can be transformed into the reduced form and hence so does the DP(M) \( x^\epsilon \).

Step 4. General case: Now consider an arbitrary DP(M) \( \phi(x^\epsilon) \). Express each \( x^\epsilon \) in reduced forms as explained in Step 3 and substitute these reduced expressions into \( \phi(x^\epsilon) \). Expanding the resulting expression, we obtain our desired reduced form of \( \phi(x^\epsilon) \).

The following definition is crucially important:
DEFINITION. A DP(M) \( \varphi \) is said to be nontrivial if and only if, by means of the basic identities 1–11, the given DP(M) \( \varphi \) gives rise to a nontrivial reduced DP(M) with respect to some ordered basis \((M, <)\) of \(\text{Der}(Q)\) modulo \(\text{Der},(Q)\) and some basis \(R\) of \(G(R)\) modulo \(G,(R)\). A DI(M) \( \varphi = 0 \) is said to be nontrivial if and only if \( \varphi \) is a nontrivial DP(M).

Remark. For a given prime ring \(R\), let \((M, <)\) be an ordered basis of \(\text{Der}(Q)\) modulo \(\text{Der},(Q)\) and let \(R\) be a basis of \(G(R)\) modulo \(G,(R)\). Note that, in the reduced DP(M)s defined in [7], where only automorphisms are involved, automorphisms are put on the left-hand side of derivations instead of on the right-hand side of derivations as we do here. Let us call the reduced DP(M)s defined here, where elements \(g\) of \(R\) are put on the right-hand side of derivation words \(\Delta \in \Omega(M, <)\), right reduced. Alternatively, we may also define a left reduced DP(M) by putting elements \(g\) of \(R\) on the left-hand side of derivation words \(\Delta \in \Omega(M, <)\) as in [7]. By means of the basic identities 1–11, any DP(M) can be similarly transformed into a left reduced DP(M) thus defined. Now the natural question to ask is:

1. With respect to given \((M, <)\) and \(R\), is the nontriviality of a DP(M) independent of the definition of reduced DP(M)s used: right reduced forms as here, or left reduced forms as in [7]?

Actually the following two, more fundamental questions were ignored in Kharchenko’s work [6, 7] and have also been deliberately avoided in this paper:

2. With respect to \((M, <)\) and \(R\), does a DP(M) give rise to a unique right (or left) reduced DP(M)?

3. Is the nontriviality of a DP(M) independent of the choice of \((M, <)\) and \(R\)?

In fact, all three questions have affirmative answers. We can give a free product treatment of DP(M)s and prove all three questions. But, since this sort of universal mapping argument is rather lengthy (as usual) and does not seem immediately relevant to our main theme here, these matters will be taken up elsewhere. Assuming these affirmative answers, it really does not matter whether left or right reduced DP(M)s are used, as far as only the nontriviality of a DI(M) is concerned, which is exactly what our main theorem needs. Actually, our argument given here also works for left reduced DP(M)s as well. However, for deeper theorems about DI(M)s, such as Theorem 3 of [7], Theorem 2 of [8], or the main theorem of [2], we must consider right reduced DP(M)s. A counterexample is constructed in [2] to show the falsity of Theorem 7 of [10], where the involution * is put on the left-hand side of derivations. For left reduced multilinear
As in [7, p. 156], for $a \in U$ and $\beta = \sum r_i \otimes r'_i \in Q \otimes Z Q'$, where $r_i \in Q$ and $r'_i \in Q'$, we define $a \cdot \beta = \sum r_i a r_i'$. For $a \in U$, let $a^\perp = \{ \beta \in B : a \cdot \beta = 0 \}$. For $V \subseteq B$, let $V^\perp = \{ a \in U : a \cdot V = 0 \}$ [6, p. 134].

Suppose that $E$ is an endomorphism of the additive group $(Q, +)$. For $p = \sum r_i \otimes r'_i \in B$, where $r_i \in Q$ and $r'_i \in Q'$, we define $E \cdot \beta = \sum r_i E r_i'$. For $a \in U$, $\sigma \in \text{Aut}(R)$ and $\beta \in B$, we have $a \cdot \beta = a \cdot (\sigma \cdot \beta)$. Let $f(x)$ be a linear expression in the variable $x$ only. If $p = 1$, $r_i \otimes r_i' \in B$, where $r_i \in R$ and $r_i' \in R'$, then we define $f(x) \cdot \beta = x a f(r, x)$. Clearly, if $f(x)$ assumes the constant value 0 on $R$, then so does $f(x) \cdot \beta$. Let $\Delta = \delta_1 \delta_2 \cdots \delta_m$ be a regular derivation word in the ordered basis $(A, <)$ of $\text{Der}(Q)$ modulo $\text{Der}_i(Q)$. Assume that $\delta_1 = \delta_2 = \cdots = \delta_s \neq \delta_{s+1}$. Note that, by the definition of regular derivation words, if the characteristic of $R$ is a prime number $p \geq 2$, then $0 < s < p$. For $\sigma \in \text{Aut}(R)$ and $\beta \in B$, we have

$$
(ax^{A\sigma} b) \cdot \beta = (a \cdot \beta^\sigma) x^{A \sigma} b + s(a \cdot \beta^{\delta_1}) x^{\delta_1 \cdots \delta_m} b + \cdots,
$$

where the dots denote a sum of terms $dx^{A \sigma} b$ in which $A' < A$. If $\sigma$ is the identity 1 of $\text{Aut}(R)$, then (1) assumes the simpler form

$$
(ax^{A} b) \cdot \beta = (a \cdot \beta) x^{A} b + s(a \cdot \beta^{\delta_1}) x^{\delta_1 \cdots \delta_m} b + \cdots.
$$

(1')
Martindale Quotient Rings

The original results in Kharchenko’s path-breaking work [6–8] and the later generalization to differential identities with involution are all formulated in terms of Martindale quotient rings. It might be proper here to explain the connection between Kharchenko’s formulation and ours. Let us recall the definitions needed and then give a precise formulation of these cited results.

Assume that $R$ is both right and left faithful. A two-sided ideal of $R$ is said to be two-sided dense if it is both left dense as a left ideal and right dense as a right ideal. It is easy to see that a two-sided ideal $I$ of $R$ is two-sided dense if and only if for any $a \in R$, $aI = 0$ or $Ia = 0$ implies $a = 0$. For a semiprime ring, a two-sided ideal is two-sided dense if and only if it intersects nontrivially any nonzero two-sided ideal of the given ring. Such two-sided ideals are also said to be essential. For a prime ring, a two-sided ideal is two-sided dense if and only if it is nonzero. The ring consisting of all left quotients of $R$ relative to the filter of two-sided dense two-sided ideals of $R$ is called the left Martindale quotient ring of $R$ and will be denoted by $U$, (see [11] for the definition and the construction in the prime case). The left Martindale quotient ring $U_0$ can also be characterized axiomatically as follows (see [8] for the semiprime case):

Axiom 1. $R \subseteq U_0$.

Axiom 2. For each $a \in U_0$, there exists a two-sided dense two-sided ideal $I$ of $R$ such that $Ia \subseteq R$.

Axiom 3. If $I$ is a two-sided dense two-sided ideal of $R$ and if $\xi : R_I \rightarrow R$ is a left $R$-module homomorphism, then there exists a unique $a \in U_0$ such that $\xi(x) = xa$ for all $x \in I$.

The left Martindale quotient ring $U_0$ can be naturally embedded as a subring of the left Utumi quotient ring $U$ of $R$. Analogous to the definition of the two-sided Utumi quotient ring $Q$ of $R$, the subset $Q_0$ of $U_0$ defined by

$$Q_0 = \{x \in U_0 : xI \subseteq R \text{ for some two-sided dense two-sided ideal } I \text{ of } R\}$$

forms a subring of the left Martindale quotient ring $U_0$ and is called the two-sided Martindale quotient ring of $R$. The ring $Q_0$ is essentially the intersection of the left and the right Martindale quotient rings of $R$. Obviously, $Q_0$ can be naturally embedded as a subring of $Q$. Also, both the center of $Q_0$ and the center of $U_0$ are equal to the extended centroid $C$ of $R$.

By an $R$-valued derivation of a two-sided dense two-sided ideal $I$ of $R$, we mean a map $\delta : I \rightarrow R$ satisfying: $(x + y)^\delta = x^\delta + y^\delta$ and $(xy)^\delta = x^\delta y + xy^\delta$ for all $x, y \in I$. Two such $R$-valued derivations of two-sided dense two-sided
ideals of \( R \) are identified if they coincide on a two-sided dense two-sided ideal of \( R \). Let \( D(R) \) denote the set of all such \( R \)-valued derivations on two-sided dense two-sided ideals of \( R \). By Fact 1, all \( R \)-valued derivations of two-sided dense two-sided ideals of \( R \) can be uniquely extended to derivations of \( U \) and can be characterized as follows: A derivation \( \delta \) of \( U \) is an \( R \)-valued derivation of a two-sided dense two-sided ideal of \( R \) if and only if there exists a two-sided dense two-sided ideal \( I \) of \( R \) such that \( I^\delta \subseteq R \). Obviously, \( D(R) \) forms a right \( C \)-vector space and includes both \( \text{Der}(R) \cdot C \) and \( \text{Der}_i(Q_o) \) as \( C \)-subspaces; in notation: \( D(R) \supseteq \text{Der}(R) \cdot C + \text{Der}_i(Q_o) \).

In Kharchenko's work [7] and the later generalization [2, 10], derivations are assumed to be in \( D(R) \) and regular derivation words are defined with respect to an ordered basis \( (M, <) \) of the \( C \)-space \( D(R) \) modulo the \( C \)-subspace \( \text{Der}_i(Q_o) \).

We collect some simple properties we need in the following:

**Fact 6.** If \( R \) is both right and left faithful, then the following hold:

1. \( D(R) \subseteq \text{Der}(U_0) \).
2. \( D(R) \subseteq \text{Der}(Q_o) \subseteq \text{Der}(Q) \).
3. \( \text{Aut}(R) \subseteq \text{Aut}(U_0) \).
4. \( G(R) \subseteq G(Q_o) \subseteq G(Q) \).

If \( R \) is semiprime, then the following hold:

5. \( \text{Der}(Q) \cap \text{Der}_i(U) = \text{Der}_i(Q) \).
6. \( D(R) \cap \text{Der}_i(U) = D(R) \cap \text{Der}_i(Q) = D(R) \cap \text{Der}(Q_o) \).
7. \( \text{Aut}(Q) \cap \text{Aut}_i(U) = \text{Aut}_i(Q) \).
8. \( G(R) \cap \text{Aut}_i(U) = G(R) \cap \text{Aut}_i(Q) = G(R) \cap \text{Aut}_i(Q_o) \).

**Proof.** Let \( \delta \in D(R) \) be an \( R \)-valued derivation map defined on a two-sided dense two-sided ideal \( I_0 \) of \( R \). For \( a \in U_0 \), let \( I_1 \) be a two-sided dense two-sided ideal of \( R \) such that \( I_1a \subseteq R \). Set \( I = I_0 \cap I_1 \) and \( J = I^2 \).

Note that \( J \) is also a two-sided dense two-sided ideal of \( R \). We have \( J^\delta = (I^2)^\delta = I^\delta \pm I^\delta \subseteq I \) and \( (Ja)^\delta \subseteq (I(ia))^\delta \subseteq (JR)^\delta \subseteq I^\delta \subseteq R \). Hence \( Ja^\delta \subseteq (Ja)^\delta + J^\delta a \subseteq R + Ia \subseteq R \). So \( a^\delta \in U_0 \) and (1) is proved.

Analogously, if \( a \) falls in the right Martindale quotient ring of \( R \), then so does \( a^\delta \). But \( Q_o \) is the intersection of the left and the right Martindale quotient rings of \( R \). So if \( a \in Q_o \), then \( a^\delta \in Q_o \). Hence the first inclusion of (2) is proved.

To show the second inclusion of (2), note that \( Q \) is also the two-sided Utumi quotient ring of \( Q_o \). Let \( \delta \in \text{Der}(Q_o) \). For any \( a \in Q \), since \( a \in U \), by Fact 1, \( a^\delta \) falls in the left Utumi quotient ring \( U \) of \( Q_o \) and symmetrically, \( a^\delta \) also falls in the right Utumi quotient ring of \( Q_o \). But \( Q \) is also the two-
sided Utumi quotient ring of $Q_0$ and hence is the intersection of the left and the right Utumi quotient rings of $Q_0$. So for any $a \in Q$, $a^\delta$ falls in the two-sided Utumi quotient ring $Q$ of $Q_0$. That is, $Q^\delta \subseteq Q$. Hence $\delta \in \text{Der}(Q)$, as desired. Thus (2) is proved.

To prove (3), let $\sigma \in \text{Aut}(R)$. For $a \in U_0$, pick a two-sided dense two-sided ideal $I$ of $R$ such that $Ia \subseteq R$. Then $I^\sigma a^\sigma = (Ia)^\sigma \subseteq R^\sigma = R$. But $I^\sigma$ is also a two-sided dense two-sided ideal of $R$. So $a^\sigma \in U_0$ as desired.

Since $Q$ is also the two-sided Utumi quotient ring of $Q_0$, the second inclusion of (4) follows from Facts 2 and 3. To see the first inclusion, let $a \in Q_0$ and let $I$ be a two-sided dense two-sided ideal of $R$ such that $aI \cup Ia \subseteq R$. For $g \in G$, $a^gI^g \cap I^g a^g \subseteq R^g = R$. Since $I^g$ is also a two-sided dense two-sided ideal of $R$, $a^g \in U_0$, as desired.

To prove (5), let $a \in U$ be such that ad$(a) \in \text{Der}(Q)$. Since $U$ is also the left Utumi quotient ring of $Q$, there exists a dense left ideal $\lambda$ of $Q$ such that $\lambda a \subseteq Q$. Then $a\lambda \subseteq (a\lambda - \lambda a) + \lambda a \subseteq \lambda^{ad(a)} + \lambda a \subseteq Q$. Let $I = \lambda Q$ be the two-sided ideal of $Q$ generated by $\lambda$. By the semiprimeness of $Q$, the two-sided ideal $I$, including the dense left ideal $\lambda$, is two-sided dense. Hence $a$ falls in the two-sided Utumi quotient ring of $Q$, which is equal to $Q$ itself.

To prove (6), since $D(R) \cap \text{Der}^l(U) \supseteq D(R) \cap \text{Der}^l(Q) \supseteq D(R) \cap \text{Der}^l(Q_0)$, it suffices to show $D(R) \cap \text{Der}^l(U) = D(R) \cap \text{Der}^l(Q_0)$: Let $a \in U$ be such that ad$(a) \in D(R)$. Let $I$ be a two-sided dense two-sided ideal of $R$ such that $I^{ad(a)} \subseteq R$. Let $\lambda = \{x \in I : xa \subseteq R\}$ and $\rho = \{x \in I : ax \subseteq R\}$. Suppose that $x \notin \lambda$. Then $xa \notin R$ and $ax - xa = xa^{ad(a)} \subseteq I^{ad(a)} \subseteq R$. So $ax = (ax - xa) + xa = xa^{ad(a)} + xa \subseteq R$ and hence $x \in \rho$. So $\lambda \subseteq \rho$. Similarly, $\rho \subseteq \lambda$ and hence $\lambda = \rho$. Thus $\lambda$ is a two-sided ideal of $R$. By the defining axiom 2 for $U$, $Ra^{-1}$ is left dense. The two-sided ideal $\lambda$, being equal to $I \cap Ra^{-1}$, is also left dense and, by the semiprimeness of $R$, must be two-sided dense. We have found a two-sided dense two-sided ideal $\lambda(=\rho)$ such that $\lambda a \subseteq R$ and $a\lambda \subseteq R$. So $a \in Q_0$ and hence ad$(a) \in \text{Der}^l(Q_0)$, as desired.

To prove (7), let $a \in U$ be invertible such that $aQa^{-1} \subseteq Q$. Since $U$ is also the left Utumi quotient ring of $Q$, there exists a dense left ideal $\lambda$ of $Q$ such that $\lambda a^{-1} \subseteq Q$. By (0) of Fact 0, $\lambda a^{-1}$ is a dense left ideal of $Q$. Now $a(\lambda a^{-1}Q) \subseteq (a\lambda a^{-1})Q \subseteq Q$. But the two-sided ideal $\lambda a^{-1}Q$ of $Q$, including the dense left ideal $\lambda a^{-1}$, must be two-sided dense, by the semiprimeness of $Q$. So $a$ falls in its two-sided Utumi quotient ring of $Q$, which is equal to $Q$ itself.

Property (8) is proved similarly: Let $a \in U$ be invertible such that $aRa^{-1} \subseteq R$. There exists a dense left ideal $\lambda$ of $R$ such that $\lambda a^{-1} \subseteq R$. By (0) of Fact 0, the left ideal $\lambda a^{-1}$ of $R$ is left dense. So $a(\lambda a^{-1}R) \subseteq (a\lambda a^{-1})R \subseteq R$. But the two-sided ideal $\lambda a^{-1}R$ of $R$ of $R$, including the dense left ideal $\lambda a^{-1}$, must be two-sided dense itself, by the semiprimeness of $R$. So $a \in Q_0$, as desired.
From the fact $D(R) \cap \text{Der}_1(Q_0) = D(R) \cap \text{Der}_1(Q)$, any independent subset $M$ of the $C$-space $D(R)$ modulo the $C$-subspace $D(R) \cap \text{Der}(Q_0)$ must also be an independent subset of $\text{Der}(Q)$ modulo $\text{Der}_1(Q)$. Hence the notion of regular derivation words in Kharchenko's original work [7] (and also in [2, 10]) is merely a special instance of our more general context here.

I. PROOF OF MAIN THEOREM

From here to the end of the paper, we always assume the following:

1. $R$ is a prime ring;
2. $Q$ is $R$'s two-sided Utumi quotient ring;
3. $U$ is $R$'s left Utumi quotient ring;
4. $C$ is $R$'s extended centroid.

Linear Generalized Polynomial Identities with a Single Antiautomorphism

Let $\nu \in \text{Ant}(R)$. A DP$(M)$ $\phi$ of the form

$$\phi = \sum_{i=1}^{n} a_i x b_i + \sum_{j=1}^{m} c_j x^r d_j,$$

where $a_i, b_i, c_j, d_j \in U$, is called a linear generalized polynomial with the single antiautomorphism $\nu$, or simply, with a single antiautomorphism, if the antiautomorphism $\nu$ is understood. Accordingly, the DI$(M)$ given by $\phi = 0$ is called a linear generalized polynomial identity with the single antiautomorphism $\nu$, or simply, with a single antiautomorphism. For a subset $\mathcal{S}$ of $\text{Ant}(R)$, if $\nu \in \mathcal{S}$, then $\phi$ is called a linear generalized polynomial with a single antiautomorphism in $\mathcal{S}$. The identity map of $R$ can be an antiautomorphism of $R$ when and only when $R$ is commutative. Assume that the antiautomorphism $\nu$ of $\phi$ is not the identity of $G(R)$. Then $\phi$ as given in the above expression is trivial if and only if $\sum_i a_i \otimes_C b_i = \sum_j c_j \otimes_C d_j = 0$. Following the abbreviations introduced in Section 0, a linear generalized polynomial (or identity) with a single antiautomorphism (in $\mathcal{S}$) is abbreviated as a linear GP (or GPI respectively) with a single antiautomorphism (in $\mathcal{S}$).

We begin with the following lemma, whose proof is based on a computation in Theorem 1 of [11] (or Theorem 3 of [10]).

**Lemma 1.** Let $R$ be a prime ring. If $R$ satisfies a nontrivial linear generalized polynomial identity with a single antiautomorphism, then $R$ satisfies a nontrivial ordinary GPI.
Proof. Assume that $R$ satisfies a nontrivial linear generalized polynomial identity with a single antiautomorphism

$$\varphi(x) = \sum_{i=1}^{n} a_i x b_i + \sum_{j=1}^{m} c_j x^r d_j = 0,$$

where $\nu$ is a non-identity antiautomorphism of $R$. Without loss of generality, we may assume that $a_1, \ldots, a_n$ are linearly independent over $C$. If $n > 1$, then, by Lemma 1 of [7], there exists $\beta \in B$ such that $\beta \in \bigcap_{k=2}^{n} a_k^\perp$ and such that $\beta \notin a_1^\perp$. Consider $\varphi(x) \cdot \beta$. Obviously, $\varphi(x) \cdot \beta$ vanishes on $R$. Also, $\varphi(x) \cdot \beta$ contains only one nonzero term involving $x$, namely the term $(a_1 \cdot \beta) x b_1$, and hence is a nontrivial GPI of $R$ with a single antiautomorphism. Replacing $\varphi(x)$ by $\varphi(x) \cdot \beta$, we may assume from the start that the nontrivial GPI of $R$ with a single antiautomorphism is of the simpler form

$$\varphi(x) = axb + \sum_{j=1}^{m} c_j x^r d_j = 0.$$ 

Without loss of generality, we may assume that $c_1, \ldots, c_m$ are linearly independent over $C$. Pick a dense left ideal $\lambda$ of $R$ such that $\lambda a \subseteq R$. For $r \in \lambda$, $\varphi(ra) = a(ra) b + \sum_{j=1}^{m} c_j (ra)^r d_j = (ara) x b + \sum_{j=1}^{m} c_j x^r (ra)^r d_j.$

(Note that we cannot write $(ra)^r = a^r r^r$ in general, since the antiautomorphism $\nu$ may not be defined on $a \in U$!) Multiplying $\varphi(x)$ from the left-hand side by $ar$, we have

$$ar\varphi(x) = arxab + \sum_{j=1}^{m} (arc_j) x^r d_j.$$ 

Hence

$$\varphi(ra) - ar\varphi(x) = \sum_{j=1}^{m} c_j x^r (ra)^r d_j - \sum_{j=1}^{m} (arc_j) x^r d_j.$$ 

Set

$$\psi(x) = \varphi(ra^{(r-1)}) - ar\varphi(x^{(r-1)})
= \sum_{j=1}^{m} c_j x(ra)^r d_j - \sum_{j=1}^{m} (arc_j) xd_j.$$
Then obviously, \( \psi(x) = 0 \) is a linear ordinary GPI of \( R \). By Lemma 2 of [11], the left coefficients \( c_1, \ldots, c_m, arc_1, \ldots, arc_m \) of the indeterminate \( x \) in \( \psi \) are linearly dependent over \( C \). We can finish our proof by quoting the main theorem in [12]. However, we give here a direct argument, which also furnishes an alternative proof of the main theorem in [12]. Let \( C_{4m-1}(x_1, \ldots, x_{2m}, y_1, \ldots, y_{2m-1}) \) be the Capelli polynomial defined on page 12 [13]. By [13, Theorem 7.6.16, p. 285],
\[
C_{4m-1}(c_1, \ldots, c_m, arc_1, \ldots, arc_m, y_1, \ldots, y_{2m-1}) = 0
\]
holds for any \( y_1, \ldots, y_{2m-1} \in R \) and any arbitrary \( r \in \lambda \). Hence the GPI
\[
C_{4m-1}(c_1, \ldots, c_m, axc_1, \ldots, axc_m, y_1, \ldots, y_{2m-1}) = 0
\]
holds on the dense left ideal \( \lambda \) of \( R \) and hence must also hold on the whole ring \( R \) by the result of [11]. We verify that the ordinary GP
\[
C_{4m-1}(c_1, \ldots, c_m, axc_1, \ldots, axc_m, y_1, \ldots, y_{2m-1})
\]
is nontrivial as follows: Expand the linearly \( C \)-independent set \( \{c_1, \ldots, c_m\} \) into a basis \( \mathcal{B} = \{c_1, \ldots, c_m, c_{m+1}, c_{m+2}, \ldots\} \) of \( U \) over \( C \). Write \( a \) as a \( C \)-linear combination of elements of \( \mathcal{B} \): \( a = \sum_i \alpha_i c_i \), where \( \alpha_i \in C \) and \( c_i \in \mathcal{B} \). Substitute this expression of \( a \) into \( C_{4m-1}(c_1, \ldots, c_m, axc_1, \ldots, axc_m, y_1, \ldots, y_{2m-1}) \) and, using the multilinearity of the Capelli polynomial, write \( C_{4m-1}(c_1, \ldots, c_m, axc_1, \ldots, axc_m, y_1, \ldots, y_{2m-1}) \) as a \( C \)-linear combination of \( \mathcal{B} \)-monomials as explained in [1]. Since \( a \neq 0 \), some \( \alpha_x \neq 0 \). Let us say \( \alpha_x \neq 0 \). It is easy to see that the coefficient of the \( \mathcal{B} \)-monomial
\[
c_1 y_1 c_2 y_2 \cdots c_m y_m (c_s x c_1) y_{m+1} (c_s x c_2) y_{m+2} \cdots y_{2m-1} (c_s x c_m)
\]
in the above expansion is \( \alpha_x^m \), which is nonzero by our choice of \( \alpha_x \). Hence
\[
C_{4m-1}(c_1, \ldots, c_m, axc_1, \ldots, axc_m, y_1, \ldots, y_{2m-1})
\]
is a nontrivial GP and gives rise to our desired nontrivial ordinary GPI of \( R \).

**Linear Differential Identities with (Anti)automorphisms**

Let \((M, <)\) be an ordered independent subset of \( \text{Der}(Q) \) modulo \( \text{Der}_1(Q) \) and let \( \mathcal{R} \) be an independent subset of \( G(R) \) modulo \( G_1(R) \). A reduced \( \text{DP}(M) \varphi \) is said to be **linear** in the indeterminate \( x \) if \( \varphi \) assumes the form
\[
\varphi = \sum_{i,j} a_{ij} x^{\Delta_i} g_i b_{ij},
\]
where \( \Delta_i \in \Omega(M, <), g_i \in \mathcal{R} \) and \( a_{ij}, b_{ij} \) are reduced \( \text{DP}(M) \)s not involving the indeterminate \( x \). In the above expression of the \( \text{DP}(M) \varphi \), if all \( a_{ij}, b_{ij} \)
are merely elements of $U$, then the $DP(M)$ $\phi$ is said to be linear. In other words, a reduced $DP(M)$ is said to be linear if it involves only one indeterminate and is linear in this indeterminate. A reduced $DP(M)$ is said to be multilinear if it is linear in each indeterminate which it involves. A multilinear reduced $DP(M)$ in the indeterminates $x_1, \ldots, x_n$ is a sum of terms of the form

$$a_0 x_{i_1}^{\Delta_1} a_1 \cdots a_{n-1} x_{i_n}^{\Delta_n} a_n,$$

where $a_0, a_j \in U$, $\Delta_j \in \Omega(M, \prec)$, $g_j \in \mathcal{R}$ for $j = 1, \ldots, n$ and where $x_{i_1}, \ldots, x_{i_n}$ is a permutation of $x_1, \ldots, x_n$. A reduced $DI(M) \phi = 0$ is said to be linear in $x$ (multilinear, linear respectively), if the corresponding reduced $DP(M) \phi$ is linear in $x$ (multilinear, linear respectively).

The following lemma is crucial in our proof and is essentially our version of Lemmas 2 and 3 of [7] and Theorem 1 of [10] (or Lemma 3 of [2]).

**Lemma 2.** Let $R$ be a prime ring and let $Q$ be its two-sided Utumi quotient ring. Let $(M, \prec)$ be an ordered independent subset of $Der(Q)$ modulo $Der_1(Q)$ and let $\mathcal{R}$ be an independent subset of $G(R)$ modulo $G_1(R)$. Set

$$\mathcal{S} = \{ \sigma^{-1} v : \sigma \in \mathcal{R} \cap Aut(R) \text{ and } v \in \mathcal{R} \cap Ant(R) \}.$$

If the prime ring $R$ satisfies a nontrivial reduced linear $DI(M)$ with respect to $(M, \prec)$ and $\mathcal{R}$, then $R$ satisfies a nontrivial linear GPI with a single antiautomorphism in the set $\mathcal{S}$.

As applications, we show that Lemma 2 above indeed generalizes Lemmas 2 and 3 of [7] and Theorem 1 of [10]: First, let $\mathcal{R} = \{ 1 \}$, where $1$ is the identity automorphism of $Q$. We compute the set $\mathcal{S}$ as defined in Lemma 2 above: If $R$ is commutative, then the identity map $1$ is also an antiautomorphism of $Q$ and hence $\mathcal{S} = \{ 1 \}$. If $R$ is noncommutative, then $\mathcal{S} = \emptyset$ (the empty set). That is,

$$\mathcal{S} = \begin{cases} 1 & \text{if } R \text{ is commutative;} \\ \emptyset & \text{if } R \text{ is noncommutative.} \end{cases}$$

In either case, linear GPIs with a single antiautomorphism in $\mathcal{S}$ are merely ordinary linear GPIs and must be trivial by Lemma 2 of [11]. Hence Lemma 2 above gives Lemma 2 of [7] as a special instance. Next, let $\mathcal{R} \subseteq Aut(R)$, that is, let $\mathcal{R}$ consist entirely of automorphisms of $R$. If $R$ is noncommutative, then $\mathcal{S} = \emptyset$ (the empty set), since $\mathcal{R} \cap Ant(R) = \emptyset$. If the ring $R$ is commutative, then any element of $\mathcal{R}$ is also an antiautomorphism of $R$ and hence $\mathcal{S} = \{ \sigma^{-1} v : \sigma, v \in \mathcal{R} \}$. That is,

$$\mathcal{S} = \begin{cases} \{ \sigma^{-1} v : \sigma, v \in \mathcal{R} \} \subseteq Aut(R), & \text{if } R \text{ is commutative;} \\ \emptyset, & \text{if } R \text{ is noncommutative.} \end{cases}$$
By Lemma 1 of [11] again for the noncommutative \( R \) or by the well-known Dedekind lemma for the commutative \( R \), the prime ring \( R \) does not satisfy any nontrivial linear GPI with a single antiautomorphism in \( \mathcal{S} \). Hence Lemma 2 above gives Lemma 3 of [7] as a special instance. Finally, assume that \( R \) is endowed with an involution \( * \). Let \( \mathcal{A} = \{ *, 1 \} \). Then \( \mathcal{S} = \mathcal{A} \) or \( \mathcal{S} = \{ * \} \) according to whether \( R \) is commutative or not. Hence Lemma 2 above also gives Theorem 1 of [10] or Lemma 3 of [2] as a special instance.

The following consequence of Lemma 2 is our versions of Theorem 2 of [7], Theorem 4 of [10], and Lemma 4 of [2]:

**Lemma 3.** Let \( R \) be a prime ring and let \( Q \) be its two-sided Utumi quotient ring. Let \( (M, <) \) be an ordered independent subset of \( \text{Der}(Q) \) modulo \( \text{Der}_1(Q) \) and let \( \mathcal{A} \) be an independent subset of \( \text{G}(R) \) modulo \( \text{G}_1(R) \). Set

\[
\mathcal{S} = \{ \sigma^{-1} \nu: \sigma \in \mathcal{A} \cap \text{Aut}(R) \text{ and } \nu \in \mathcal{A} \cap \text{Ant}(R) \}.
\]

Assume that \( \phi(x_i^{A_k g_k}) = 0 \) is a reduced multilinear \( \text{DI}(M) \) of the prime ring \( R \), where \( A_k \in \Omega(M, <) \), \( g_k \in \mathcal{A} \) and \( \phi(z_{ijk}) \) is an ordinary GP in distinct indeterminates \( z_{ijk} \). If \( R \) does not satisfy any nontrivial linear GPI with a single antiautomorphism in \( \mathcal{S} \), then \( \phi(z_{ijk}) = 0 \) is a GPI of the prime ring \( R \).

**Proof.** Assume that \( R \) does not satisfy any nontrivial linear GPI with a single antiautomorphism in \( \mathcal{S} \). By Lemma 2, any linear \( \text{DI}(M) \) of \( R \) which is reduced with respect to \((M, <)\) and \( \mathcal{A} \) must be trivial. Let us assign arbitrarily certain fixed values from the prime ring \( R \) to all of the indeterminates \( x_2, x_3, \ldots \), other than \( x_1 \) in the multilinear \( \text{DP}(M) \) \( \phi(x_i^{A_k g_k}) \). The resulting expression \( \phi^{(1)}(x_1^{A_k g_k}) = 0 \), being a linear \( \text{DI}(M) \) of the prime ring \( R \) and being reduced with respect to \((M, <)\) and \( \mathcal{S} \), must be trivial. Thus the identity \( \phi^{(1)}(z_{ijk}) = 0 \), obtained from \( \phi^{(1)}(x_i^{A_k g_k}) = 0 \) by substituting the new indeterminates \( z_{ijk} \) for \( x_i^{A_k g_k} \), is also trivial and hence holds trivially on the ring \( R \). Since the values assigned to the indeterminates \( x_2, x_3, \ldots \), are completely arbitrary, the identity \( \phi(z_{ijk}, x_i^{A_k g_k})_{i \geq 2} = 0 \), obtained from \( \phi(x_i^{A_k g_k}) = 0 \) by substituting \( z_{ijk} \) for \( x_i^{A_k g_k} \), also holds on \( R \). Continuing in this manner, we can finally replace all \( x_i^{A_k g_k} \) in \( \phi(x_i^{A_k g_k}) = 0 \) by the new distinct indeterminates \( z_{ijk} \) and thus obtain the ordinary GPI \( \phi(z_{ijk}) = 0 \) of the prime ring \( R \), as desired.

**Proof of Main Theorem**

Let \( \phi(x) \) be a \( \text{DP}(M) \) involving the indeterminate \( x \) (and perhaps also some others). Let \( y \) be an indeterminate not occurring in \( \phi \). The \( \text{DP}(M) \) \( \phi(x + y) - \phi(x) - \phi(y) \) is called the the \( \text{DP}(M) \) obtained by linearization with respect to the indeterminate \( x \). As for ordinary GPs without deriva-
tions and (anti)automorphisms, if a nontrivial reduced $DP(M)$ is not linear in the indeterminate $x$, then the $DP(M)$ obtained by linearization with respect to this indeterminate $x$ is also nontrivial. By repeating the linearization process, we can always obtain a nontrivial multilinear $DP(M)$ from a given nontrivial $DP(M)$. Hence, if a ring satisfies a nontrivial $DI(M)$, then this ring also satisfies a nontrivial multilinear $DI(M)$.

Assuming Lemma 2 in the above, we are now ready to give

**Proof of Main Theorem.** Let us fix an ordered basis $(M, <)$ of $Der(Q)$ modulo $Der_i(Q)$ and a basis $R$ of $G(R)$ modulo $G_i(R)$. As explained above, we may assume that the ring $R$ satisfies a nontrivial, reduced, multilinear $DI(M)$ $\psi(x^{g_1}x^k) = 0$, where $A_1, x \in \Omega(M, <)$, $g_k \in R$ and where $\psi(z_{yj})$ is a nontrivial ordinary GP in distinct indeterminates $z_{yj}$. Assume on the contrary that the ring $R$ does not satisfy any nontrivial ordinary GPIs. By Lemma 1, the ring $R$ does not satisfy any nontrivial linear GPI with a single antiautomorphism either. By Lemma 3, the ring $R$ satisfies the ordinary GPI $\psi(z_{yj}) - 0$. This is a contradiction.

II. PROOF OF LEMMA 2

Before proceeding to the proof of Lemma 2, we need additional notions about linear $DP(M)$s. First, let $N$ be the set of all nonnegative integers $\{0, 1, 2, \ldots\}$. For each nonnegative integer $n \geq 0$, let $\bar{n} = \{i \in N : 0 \leq i < n\}$. Hence, $\emptyset$ is simply the empty set $\emptyset$ and, if $n > 0$, $\bar{n} = \{0, 1, \ldots, n - 1\}$. Let $\langle A, + \rangle$ be an abelian group with the addition operation $+$. Assume that for each $i \in \bar{n}$, $a_i \in A$. Then for each $n > 0$, we define

$$\sum_{i \in \bar{n}} a_i = a_0 + \cdots + a_{n-1}.$$ 

We also postulate that

$$\sum_{i \in \emptyset} a_i = \text{the addition identity } 0 \text{ of the abelian group } \langle A, + \rangle.$$ 

Let $(M, <)$ be an ordered independent subset of $Der(Q)$ modulo $Der_i(Q)$ and let $R$ be an independent subset of $G(R)$ modulo $G_i(R)$. A linear reduced $DP(M)$ $\varphi$ (with respect to $(M, <)$ and $R$) in the indeterminate $x$ can be written in the form

$$\varphi(x) = \sum_{g \in R, A \in \Omega(M, <)} \sum_{j \in n(g, A)} a_{g, d}^{(j)} x^{g_1 b_{g, d}^{(j)}}, \quad (2)$$

where each $n(g, A) \in N$ depends on $g \in R, A \in \Omega(M, <)$ and vanishes for all
but finitely many \( g \in \mathcal{R} \) \( \Delta \in \Omega(M, \prec) \). The \( \text{DP}(M) \varphi(x) \) given in (2) is nontrivial if and only if

\[
\sum_{j \in n(g, \Delta)} a^{(j)}_{g, \Delta} \otimes c b^{(j)}_{g, \Delta} \neq 0
\]

for some \( g \in \mathcal{R} \) and \( \Delta \in \Omega(M, \prec) \). For given \( \Delta \in \Omega(M, \prec) \) and \( g \in \mathcal{R} \), \( \Delta g \) is said to occur nontrivially in the \( \text{DP}(M) \varphi \) if and only if \( \sum_{j \in n(g, \Delta)} a^{(j)}_{g, \Delta} \otimes c b^{(j)}_{g, \Delta} \neq 0 \). An element \( g \in \mathcal{R} \) is said to occur nontrivially in the linear \( \text{DP}(M) \varphi(x) \) if and only if \( \Delta g \) occurs nontrivially in \( \varphi \) for some \( \Delta \in \Omega(M, \prec) \). The support of the linear \( \text{DP}(M) \varphi \) (with respect to \( (M, \prec) \) and \( \mathcal{R} \)) is defined to be the set

\[
\{ g \in \mathcal{R} : g \text{ occurs nontrivially in } \varphi(x) \}.
\]

For \( g \) in the support of \( \varphi \), the set

\[
\{ \Delta \in \Omega(M, \prec) : \Delta g \text{ occurs nontrivially in } \varphi(x) \}
\]

is a nonempty finite set and hence possesses a unique \( \prec \)-greatest element. Thus, for each \( g \) in the support of \( \varphi \), we define \( \Delta_{\varphi, g} \) to be the \( \prec \)-greatest regular derivation word of the nonempty finite set \( \{ \Delta \in \Omega(M, \prec) : \Delta g \text{ occurs nontrivially in } \varphi(x) \} \). For \( \Delta g \) occurring nontrivially in \( \varphi \), where \( \Delta \in \Omega(M, \prec) \) and \( g \in \mathcal{R} \), by picking an expression of \( \varphi \) such that \( n(g, \Delta) \) is minimal possible, we may assume that in the expression (2) of the linear \( \text{DP}(M) \varphi \), the set \( \{ a^{(j)}_{g, \Delta} : j \in n(g, \Delta) \} \) of left coefficients of \( x^{\Delta g} \) and the set \( \{ b^{(j)}_{g, \Delta} : j \in n(g, \Delta) \} \) of right coefficients of \( x^{\Delta g} \) are both \( \mathbb{C} \)-linearly independent.

Again, let \( (M, \prec) \) be an ordered independent subset of \( \text{Der}(Q) \) modulo \( \text{Der}_r(Q) \) and let \( \mathcal{R} \) be an independent subset of \( G(R) \) modulo \( G_r(R) \). Let \( \mathcal{L}(M, \mathcal{R}) \) denote the set of all linear \( \text{DP}(M) \)s in the variable \( x \) which are reduced with respect to \( (M, \prec) \) and \( \mathcal{R} \). We define a partial order \( < \) on \( \mathcal{L}(M, \mathcal{R}) \) as follows: Let \( \varphi_1, \varphi_2 \in \mathcal{L}(M, \mathcal{R}) \). We define \( \varphi_1 < \varphi_2 \) if either of the following conditions holds:

1. The support of \( \varphi_1 \) is a proper subset of the support of \( \varphi_2 \).
2. The support of \( \varphi_1 \) is equal to the support of \( \varphi_2 \) and \( \Delta_{\varphi_1, g} \leq \Delta_{\varphi_2, g} \) for all \( g \) in the support of \( \varphi_1 \) and \( \Delta_{\varphi_1, g} < \Delta_{\varphi_2, g} \) for at least one \( g \) in the support of \( \varphi_1 \).

Here, the important thing to observe is that if \( M \) is finite, then the partial order \( < \) defined on \( \mathcal{L}(M, \mathcal{R}) \) is well-founded. That is, there does not exist an infinite sequence \( \varphi_i \in \mathcal{L}(M, \mathcal{R}) \) (\( i = 0, 1, 2, \ldots \)) such that \( \varphi_{i+1} < \varphi_i \), for \( i = 0, 1, 2, \ldots \). Let \( \bar{M} \) and \( \bar{\mathcal{R}} \) be finite subsets of \( M \) and \( \mathcal{R} \), respectively. Then the partial order \( < \) on \( \mathcal{L}(\bar{M}, \bar{\mathcal{R}}) \) is well-founded. Note that the partial
order $<$ on $\mathcal{L}(\bar{M}, \bar{R})$ is the restriction of the partial order $<$ on $\mathcal{L}(M, R)$. Note also that, for a given $\varphi \in \mathcal{L}(M, R)$, there exist finite subsets $\bar{M}, \bar{R}$ of $M, R$, respectively, such that $\varphi \in \mathcal{L}(\bar{M}, \bar{R})$.

As before, let $(M, <)$ be an ordered independent subset of $\text{Der}(Q)$ modulo $\text{Der}_i(Q)$ and let $\bar{R}$ be an independent subset of $G(R)$ modulo $G_i(R)$. Assume $h \in G(R)$. We define $h\bar{R} = \{hg : g \in \bar{R}\}$ and $M^h = hMh^{-1} = \{h\delta h^{-1} : \delta \in M\} = \{\delta^h : \delta \in M\}$, where $\delta^h = h\delta h^{-1}$. We also define the linear order $<^h$ on $M^h$ as follows: For $\delta_1, \delta_2 \in M$, $\delta_1^h <^h \delta_2^h$ if and only if $\delta_1 < \delta_2$. Obviously, $h\bar{R}$ is also an independent subset of $G(R)$ modulo $G_i(R)$ and $(M^h, <^h)$ is also an ordered independent subset of $\text{Der}(Q)$ modulo $\text{Der}_i(Q)$. If $\bar{R}$ (or $(M, <)$ respectively) is a basis of $G(R)$ modulo $G_i(R)$ (or an ordered basis of $\text{Der}(Q)$ modulo $\text{Der}_i(Q)$ respectively), then so is $h\bar{R}$ (or $(M^h, <^h)$ respectively).

As explained in Section 0, the linear order $<^h$ on $M^h$ can be extended to $\Omega(M^h, <^h)$. For a derivation word $\Delta = \delta_1 \delta_2 \cdots \delta_m$, where $\delta_i \in M$ ($i = 1, \ldots, m$), we set $\Delta^h = \delta_1^h \delta_2^h \cdots \delta_m^h$. The following two facts are obvious:

1. $\Delta \in \Omega(M, <)$ if and only if $\Delta^h \in \Omega(M^h, <^h)$;
2. For $\Delta_1, \Delta_2 \in \Omega(M, <)$, $\Delta_1 < \Delta_2$ if and only if $\Delta_1^h <^h \Delta_2^h$.

Suppose that $\varphi(x) \in \mathcal{L}(M, R)$ is given by the expression (2). For $h \in G(R)$, we have

$$
\varphi(x^h) = \sum_{g \in \bar{R}} \sum_{A \in \Omega(M, <)} a^{(j)}_{g, A} (x^h)^a b^{(j)}_{g, A} \quad (2')
$$

The expression $(2')$ above gives the reduced expression of the DP$(M)$ $\varphi(x^h)$ with respect to $(M^h, <^h)$ and $h\bar{R}$. The following facts are obvious:

1. $\varphi(x) \in \mathcal{L}(M, R)$ if and only if $\varphi(x^h) \in \mathcal{L}(M^h, h\bar{R})$.
2. For $\varphi(x) \in \mathcal{L}(M, R)$, the regular derivation word $\Delta_{\varphi(x), h\bar{R}}$ with respect to $(M^h, <^h)$ and $h\bar{R}$ is equal to

$$
(\Delta_{\varphi(x), h\bar{R}}) \text{ with respect to } (M, <) \text{ and } R^h.
$$

3. The support of $\varphi(x^h)$ with respect to $(M^h, <^h)$ and $h\bar{R}$ is equal to the set

$$
\{hg : g \text{ is in the support of } \varphi \text{ with respect to } (M, <) \text{ and } \bar{R}\}.
$$

4. For $\varphi_1(x), \varphi_2(x) \in \mathcal{L}(M, R)$, $\varphi_1(x) < \varphi_2(x)$ with respect to $(M, <)$ and $\bar{R}$ if and only if $\varphi_1(x^h) <^h \varphi_2(x^h)$ with respect to $(M^h, <^h)$ and $h\bar{R}$.
(5) For a subset \( L_0 \) of \( L(M, \mathcal{R}) \), \( \varphi(x) \) is a \(<\)-minimal element of \( L_0 \) if and only if \( \varphi(x^h) \) is a \(<^h\)-minimal element of the subset \( \{\psi(x^n) : \psi(x) \in L_0\} \) of \( L(M^n, h\mathcal{R}) \).

Now we are ready to give:

**Proof of Lemma 2.** Let \((M, <)\) be an ordered independent subset of \( \text{Der}(Q) \) modulo \( \text{Der}_i(Q) \) and let \( \mathcal{R} \) be an independent subset of \( G(R) \) modulo \( G_i(R) \). Assume that \( R \) satisfies a nontrivial reduced linear DI(M) \( \varphi = 0 \) with \( \varphi \in L(M, \mathcal{R}) \). We must produce a nontrivial linear GPI with a single antiautomorphism in the set

\[
\mathcal{Y} = \{\sigma^{-1}v : \sigma \in \mathcal{R} \cap \text{Aut}(R) \text{ and } v \in \mathcal{R} \cap \text{Ant}(R)\}.
\]

As explained above, there exist finite subsets \( M \) and \( \mathcal{R} \) of \( M \) and \( \mathcal{R} \), respectively, such that \( \varphi \in L(M, \mathcal{R}) \). By replacing \( M \) and \( \mathcal{R} \) by \( \bar{M} \) and \( \bar{\mathcal{R}} \), respectively, we may assume from the start that \( M \) and \( \mathcal{R} \) are finite sets. Hence, the partial order \(<\) defined on \( L(M, \mathcal{R}) \) is a well-founded relation. Replacing \( \varphi \) by a \(<\)-minimal one, we may assume from the beginning that \( \varphi \in L(M, \mathcal{R}) \) is a \(<\)-minimal element in the set

\[
\{\psi \in L(M, \mathcal{R}) : \psi = 0 \text{ is a nontrivial linear reduced DI(M) of the \text{given prime ring } } R\}.
\]

The \(<\)-minimality of the DP(M) \( \varphi \) is characterized by the following three properties:

1. \( \varphi \in L(M, \mathcal{R}) \),
2. \( \varphi = 0 \) is a nontrivial linear reduced DI(M) of the ring \( R \), and
3. for any \( \psi \in L(M, \mathcal{R}) \), if \( \psi < \varphi \), then \( \psi = 0 \) is not a nontrivial linear reduced DI(M) of \( R \).

**Claim 1.** The support of the DP(M) \( \varphi \) with respect to \((M, <)\) and \( \mathcal{R} \) has at most one automorphism.

**Reason.** Suppose that \( \varphi \) is given by the expression (2) above. Assume on the contrary that \( \sigma_1, \sigma_2, \ldots, \sigma_n \in \mathcal{R}, \) where \( n > 1 \), are distinct automorphisms in the support of \( \varphi \). For simplicity of notation, let us write \( A_i = A_{\varphi, \sigma_i} \) for \( i = 1, \ldots, n \),

\[
j(i) = n(\sigma_i, A_i)
\]

and

\[
a(g, A, j) = a_{g, A}^{(j)} \quad \text{for } g \in \mathcal{R}, A \in \Omega(M, <) \text{ and } j \in \bar{n}(g, A).
\]

\[
b(g, A, j) = b_{g, A}^{(j)}
\]
Without loss of generality, we may assume that, for each \( i = 1, \ldots, n \), the set of left coefficients \( \{ a_{(\sigma_i, \delta, j)} : j \in j(i) \} \) of \( x^{A_i} \) in the DP(M) \( \phi \) is \( C \)-linearly independent. Since \( \sigma_i \in \mathcal{R} \cap \text{Aut}(R) \) \( (i = 1, \ldots, n) \) are independent in \( G(R) \) modulo \( G_i(R) \) and hence must also be independent in the set (or the group) \( \text{Aut}(R) \) modulo \( \text{Aut}_i(R) \), \( a_{(\sigma_i, \delta, j)} \) is right independent of relative to the sequence of automorphisms
\[
\sigma_1, \ldots, \sigma_1, \sigma_2, \ldots, \sigma_2, \ldots, \sigma_n, \ldots, \sigma_n.
\]
(See [6] for the definition.) By Proposition 1 of [6], there exists \( \beta \in B \) such that \( a_{(\sigma_i, \delta, 0)} \cdot \beta \neq 0 \) and such that \( a_{(\sigma_i, \delta, j)} \cdot \beta^{\sigma_i} = 0 \) for all \( i \neq 1 \) and \( j \in j(i) \) or for \( i = 1 \) and \( 0 \neq j \in j(1) \). By the formula (1) of Section 0,
\[
\varphi(x) \cdot \beta = (a_{(\sigma_i, \delta, 0)} \cdot \beta^{\sigma_i}) x^{A_i} h_{(\sigma_i, \delta, 0)} + \cdots,
\]
where the dots denote a sum of terms \( c x^{A_i} d \) with \( \delta < \delta_i \) for \( i = 1, \ldots, n \). Hence \( \varphi(x) \cdot \beta < \varphi(x) \). Since \( a_{(\sigma_i, \delta, 0)} \cdot \beta^{\sigma_i} \neq 0 \), the DP(M) \( \varphi(x) \cdot \beta \) is a nontrivial element in \( \mathcal{L}(M, \mathcal{R}) \). But \( \varphi(x) \cdot \beta = 0 \) is obviously also a DI(M) of the ring \( R \). This contradicts the \( <^\ast \)-minimality of the DP(M) \( \varphi \).

**Claim 2.** The support of the DP(M) \( \varphi \) with respect to \((M, <)\) and \( \mathcal{R} \) has at most one antiautomorphism.

**Reason.** Pick arbitrarily an antiautomorphism \( \nu \in \text{Ant}(R) \). Consider the reduced DP(M) \( \varphi(x^\nu) \) given by the expression (2) above. Set \( M^\nu = \{ \delta^\nu : \delta \in M \} \), and \( \nu\mathcal{R} = \{ \nu g : g \in \mathcal{R} \} \). By the explanation given at the beginning of this section, \( \varphi(x^\nu) \) satisfies the following corresponding \( <^\nu \)-minimality properties:

1. \( \varphi(x^\nu) \in \mathcal{L}(M^\nu, \nu\mathcal{R}) \),
2. \( \varphi(x^\nu) = 0 \) is a nontrivial linear reduced DI(M) of the given prime ring \( R \),
3. for any \( \psi \in \mathcal{L}(M^\nu, \nu\mathcal{R}) \), if \( \psi <^\nu \varphi(x^\nu) \), then \( \psi - 0 \) is not a nontrivial DI(M) of the ring \( R \).

Arguing as in Claim 1, we can show similarly that the support of the DP(M) \( \varphi(x^\nu) \), which is reduced with respect to \((M^\nu, <^\nu)\) and \( \nu\mathcal{R} \), contains at most one antiautomorphism. But this is equivalent to the fact that the support of \( \varphi(x) \), with respect to \((M, <)\) and \( \mathcal{R} \), contains at most one antiautomorphism.
Let \( \sigma \in \mathcal{R} \cap \text{Aut}(R) \) and \( \nu \in \mathcal{R} \cap \text{Ant}(R) \) be respectively the only possible automorphism and the only possible antiautomorphism in the support of the DP(M) \( \varphi(x) \) (with respect to \((M, <)\) and \(\mathcal{R}\)). Then \( \varphi(x) \) can be written in the form

\[
\varphi(x) = \sum_{i,j} a_{i,j}^{(i)} x^{A_{i,j}} b_{i,j}^{(i)} + \sum_{k,l} c_{k,l}^{(l)} x^{F_{k,l}} d_{k,l}^{(l)},
\]

where \( A_{i,j}, F_{k,l} \in \Omega(M, <) \). Consider the DP(M) \( \varphi(x^{\sigma^{-1}}) \). By means of the basic identity (11),

\[
(\varphi(x^{\sigma^{-1}})) = 2 \sum_{i,j} a_{i,j}^{(i)} (x^{\sigma^{-1}})^{A_{i,j}} b_{i,j}^{(i)} + \sum_{k,l} c_{k,l}^{(l)} (x^{\sigma^{-1}})^{F_{k,l}} d_{k,l}^{(l)}
\]

\[
= \sum_{i,j} a_{i,j}^{(i)} x^{A_{i,j} \sigma^{-1}} b_{i,j}^{(i)} + \sum_{k,l} c_{k,l}^{(l)} x^{F_{k,l} \sigma^{-1} \nu} d_{k,l}^{(l)},
\]

where \( A_{i,j} \sigma^{-1}, F_{k,l} \sigma^{-1} \in \Omega(M^{\sigma^{-1}}, <(\sigma^{-1})) \) and \( \sigma^{-1} \nu \in \sigma^{-1} \mathcal{R} \). Note that \( (\sigma^{-1} \mathcal{R}) \cap \text{Ant}(R) = \sigma^{-1}(\mathcal{R} \cap \text{Ant}(R)) \subseteq \mathcal{S} \), where \( \mathcal{S} \) as defined in the statement of Lemma 2, is the set

\[\{ \tau^{-1} \mu : \tau \in \mathcal{R} \cap \text{Aut}(R) \text{ and } \mu \in \mathcal{R} \cap \text{Ant}(R) \} \]

We also compute

\[\{ \tau^{-1} \mu : \tau \in \sigma^{-1} \mathcal{R} \cap \text{Aut}(R) \text{ and } \mu \in \sigma^{-1} \mathcal{R} \cap \text{Ant}(R) \} \]

\[= \{ (\sigma^{-1} \tau)^{-1} (\sigma^{-1} \mu) : \tau \in \mathcal{R} \cap \text{Aut}(R) \text{ and } \mu \in \mathcal{R} \cap \text{Ant}(R) \} \]

\[\subseteq \{ \tau^{-1} \mu : \tau \in \mathcal{R} \cap \text{Aut}(R) \text{ and } \mu \in \mathcal{R} \cap \text{Ant}(R) \} = \mathcal{S} \]

Hence, without affecting our formulation of Lemma 2, we may, from the beginning, replace \((M, <)\) and \(\mathcal{R}\) by \((M^{\sigma^{-1}}, <(\sigma^{-1}))\) and \(\sigma^{-1} \mathcal{R}\), respectively, and consider the DI(M) \( \varphi(x^{\sigma^{-1}}) = 0 \) instead of \( \varphi(x) = 0 \). Then the identity 1 of \( G(R) \) is in the set \( \mathcal{R} \) and hence \( \mathcal{R} \cap \text{Ant}(R) \subseteq \mathcal{S} \). Also under this reduction, the DP(M) \( \varphi \) assumes the simple form

\[
\varphi(x) = \sum_{i=1}^{m} \sum_{j=1}^{m} a_{i,j}^{(i)} x^{A_{i,j}} b_{i,j}^{(i)} + \sum_{k=1}^{m} \sum_{l=1}^{m} c_{k,l}^{(l)} x^{F_{k,l}} d_{k,l}^{(l)},
\]

where \( A_{i,j}, F_{k,l} \in \Omega(M, <) \), 1 (the identity of \( G(R) \)) \( \in \mathcal{R} \cap \text{Aut}(R) \), and \( \nu \in \mathcal{R} \cap \text{Ant}(R) \subseteq \mathcal{S} \).

**Claim 3.** Let 1 be the identity of the automorphism group \( \text{Aut}(R) \). Then the regular derivation word \( A_{\varphi,1} \) is the empty word.

**Reason.** We may assume that \( A_{\varphi,1} = A_1 \). This is equivalent to saying that \( A_i \geq A_1 \) for all \( A_i \) occurring in the expression (3) of \( \varphi \). We divide the argument into two cases:
Case 1. \( n_1 = 1 \): Then in the DP(M) \( \varphi(x) \), the only term involving \( x^{d_1} \) is \( a_1^{(1)} x^{d_1} b_1^{(1)} \). Assume on the contrary that \( \Delta_1 = \delta_1 \delta_2 \cdots \delta_m (m \geq 1) \), where

\[
\begin{align*}
(1) & \quad \delta_1 = \delta_2 = \cdots = \delta_s \neq \delta_{s+1} \\
(2) & \quad 0 < s < p \text{ if the characteristic of the given prime ring } R \text{ is the prime number } p \geq 2.
\end{align*}
\]

Set \( \bar{A}_1 = \delta_2 \cdots \delta_m \). Let \( \mu_1, \ldots, \mu_n \) be all derivations in \( M \) other than \( \delta_1 \), such that the derivation words \( \mu_1 \bar{A}_1, \ldots, \mu_n \bar{A}_1 \) occur as some \( \Delta_i \) in the DP(M) \( \varphi \). Let us say \( \Delta_{r(\gamma)} = \mu_\gamma \bar{A}_1 \) for \( \gamma = 1, \ldots, n \). We also assume that the derivation word \( \bar{A}_1 \) itself occurs in the DP(M) \( \varphi \) as \( \Delta_{r_0} \). In view of the formula (1') of Section 0, for \( \beta \in B \), the sum of terms of \( \varphi(x) \cdot \beta \) containing \( x^{d_1} \) has the form

\[
\sum_{\gamma=1}^{n} \sum_{j=1}^{n_{r(\gamma)}} (a_{r(\gamma)}^{(j)} : \beta) x^{d_1} b_{r(\gamma)}^{(j)} + \sum_{j} (a_{r_0}^{(j)} : \beta) x^{d_1} b_{r_0}^{(j)}.
\]

Also, the only term containing \( x^{d_1} \) in the DP(M) \( \varphi(x) \cdot \beta \) is \( (a_1^{(1)} : \beta) x^{d_1} b_1^{(1)} \). Hence, if \( a_1^{(1)} : \beta = 0 \), then \( \varphi(x) \cdot \beta < \varphi(x) \). But \( \varphi(x) \cdot \beta = 0 \) is obviously a DI(M) of the ring \( R \). Since \( \varphi(x) \cdot \beta \in \mathcal{L}(M, R) \), \( \varphi(x) \cdot \beta \) must be trivial by the \(<\)-minimality of the DP(M) \( \varphi \). So, for those \( \beta \in B \) such that \( a_1^{(1)} : \beta = 0 \), we have

\[
\sum_{\gamma=1}^{n} \sum_{j=1}^{n_{r(\gamma)}} (a_{r(\gamma)}^{(j)} : \beta) \otimes_C b_{r(\gamma)}^{(j)} + \sum_{j} (a_{r_0}^{(j)} : \beta) \otimes_C b_{r_0}^{(j)} = 0.
\]

(4)

Note that \( 0 < s \) and \( s < p \) if the characteristic of \( R \) is a prime \( p \). So \( s \), as an element of \( C \), is always invertible in \( Q \). Hence \( a_1^{(1)} : \beta^d_1 \) can be expressed as a \( C \)-linear combination of \( a_{r(\gamma)}^{(j)} : \beta^{\mu_{\gamma}} (\gamma = 1, \ldots, n, j = 1, \ldots, n_{r(\gamma)}) \) and \( a_{r_0}^{(j)} : \beta (j = 1, \ldots, n_{r_0}) \). Using the linearity of \( ( ) \cdot \beta^{\mu_{\gamma}}, ( ) \cdot \beta \), and introducing new notation \( h, d_\gamma (\gamma = 1, \ldots, n) \), we have

\[
a_1^{(1)} : \beta^d_1 + \sum_{\gamma=1}^{n} d_\gamma : \beta^{\mu_{\gamma}} + h \cdot \beta = 0,
\]

for those \( \beta \in B \) such that \( a_1^{(1)} : \beta = 0 \). Since the right coefficients of (4) do not depend on \( \beta \), the elements \( d_\gamma \) and \( h \) do not depend on \( \beta \) either. This shows that the mapping

\[
\xi: a_1^{(1)} : \beta \mapsto a_1^{(1)} : \beta^d_1 + \sum_{\gamma} d_\gamma : \beta^{\mu_{\gamma}} + h \cdot \beta,
\]

where \( \beta \) ranges over \( B \), is well-defined.

The map \( \xi \) is defined on the \( R \)-bimodule \( \{ a_1^{(1)} : \beta : \beta \in B \} \) of \( U \). Let \( \lambda \) be a dense left ideal of \( R \) such that \( \lambda a_1^{(1)} \subseteq R \). Obviously, the set \( \lambda a_1^{(1)} R \) forms
a nonzero two-sided ideal of \( R \) and is a subset of \( \{ a^{(1)}_1 \beta : \beta \in B \} \). Thus the \( R \)-bimodule \( \{ a^{(1)}_1 \beta : \beta \in B \} \) of \( U \) is two-sided dense. Furthermore, for \( v \in R \) and \( \beta \in B \), we compute

\[
\xi(v(a^{(1)}_1 \beta)) = \xi((a^{(1)}_1 \beta) \cdot (1 \otimes v)) = \xi(a^{(1)}_1 \beta (1 \otimes v))
\]

\[
= a^{(1)}_1 \beta (1 \otimes v)^{\delta_1} + \sum_{\gamma} d_{\gamma} \beta (1 \otimes v)^{\mu_{\gamma}} + h \beta (1 \otimes v)
\]

\[
= a^{(1)}_1 \beta (1 \otimes v) + \sum_{\gamma} d_{\gamma} \beta (1 \otimes v)^{\mu_{\gamma}} + h \beta (1 \otimes v)
\]

\[
= (a^{(1)}_1 \beta^{\delta_1}) (1 \otimes v) + \sum_{\gamma} (d_{\gamma} \beta^{\mu_{\gamma}}) (1 \otimes v) + (h \beta) (1 \otimes v)
\]

\[
= (a^{(1)}_1 \beta^{\delta_1} + \sum_{\gamma} d_{\gamma} \beta^{\mu_{\gamma}} + h \beta) (1 \otimes v) = v \xi(a^{(1)}_1 \beta).
\]

Hence, by (2) of Fact 0, there exists \( t \in U \) such that for \( \beta \in B \),

\[
(a^{(1)}_1 \beta) t = \xi(a^{(1)}_1 \beta) = a^{(1)}_1 \beta^{\delta_1} + \sum_{\gamma} d_{\gamma} \beta^{\mu_{\gamma}} + h \beta.
\]

For \( x \in R \) and \( \beta \in B \), we compute

\[
(a^{(1)}_1 \beta)(xt) = ((a^{(1)}_1 \beta)x) t = ((a^{(1)}_1 \beta) (x \otimes 1)) t = (a^{(1)}_1 \beta (x \otimes 1)) t
\]

\[
= a^{(1)}_1 \beta (x \otimes 1)^{\delta_1} + \sum_{\gamma} d_{\gamma} \beta (x \otimes 1)^{\mu_{\gamma}} + h \beta (x \otimes 1)
\]

\[
= a^{(1)}_1 \beta (x \otimes 1) + \beta (x \otimes 1)^{\delta_1}
\]

\[
\quad + \sum_{\gamma} d_{\gamma} \beta (x \otimes 1)^{\mu_{\gamma}} + h \beta (x \otimes 1)
\]

\[
= a^{(1)}_1 \beta (x \otimes 1) + \beta (x^{\delta_1} \otimes 1)
\]

\[
\quad + \sum_{\gamma} d_{\gamma} \beta (x^{\mu_{\gamma}} \otimes 1) + h \beta (x \otimes 1)
\]

\[
= (a^{(1)}_1 \beta^{\delta_1}) x + (a^{(1)}_1 \beta) x^{\delta_1}
\]

\[
\quad + \sum_{\gamma} (d_{\gamma} \beta^{\mu_{\gamma}}) x + \sum_{\gamma} (d_{\gamma} \beta) x^{\mu_{\gamma}} + (h \beta) x
\]

(5)

and

\[
(a^{(1)}_1 \beta)(tx) = ((a^{(1)}_1 \beta) t) x = (\xi(a^{(1)}_1 \beta)) x
\]

\[
= (a^{(1)}_1 \beta^{\delta_1}) x + \sum_{\gamma} (d_{\gamma} \beta^{\mu_{\gamma}}) x + (h \beta) x
\]

(6)
Subtracting (6) from (5), we obtain

\[(a_1^{(1)} \cdot \beta)[x, t] = (a_1^{(1)} \cdot \beta)(xt - tx)\]

\[= (a_1^{(1)} \cdot \beta) x^\delta_1 + \sum_{\gamma} (d_{\gamma} \cdot \beta) x^{\mu_{\gamma}}. \tag{7}\]

Write \(a_1^{(1)} = a_1\). Expand \(a_1\) into a basis \(\{a_1, a_2, \ldots\}\) of the subspace \(a_1^{(1)} \cdot C + \sum d_{\gamma} \cdot C\). Express \(d_{\gamma}\) in terms of this basis,

\[d_{\gamma} = \alpha_{\gamma} a_1 + \cdots ,\]

where \(\alpha_{\gamma} \in C\). Let \(\beta \in \bigcap_{i \geq 2} a_2^{\perp}\). Then \(d_{\gamma} \cdot \beta = \alpha_{\gamma} (a_1 \cdot \beta)\). By (7), we have

\[(a_1^{(1)} \cdot \beta) \left( [x, t] - x^\delta_1 - \sum_{\gamma} \alpha_{\gamma} x^{\mu_{\gamma}} \right) = 0.\]

Since the set \(\{a_1^{(1)} \cdot \beta: \beta \in \bigcap_{i \geq 2} a_2^{\perp}\}\) is a nonzero \(R\)-bimodule of \(U\) and must be two-sided dense, we have

\[[x, t] = x^\delta_1 + \sum_{\gamma} \alpha_{\gamma} x^{\mu_{\gamma}}.\]

The right-hand side of the above identity says that the inner derivation \(\text{ad}(t)\) defined by \(t \in U\) is an element of \(\text{Der}(Q)\). By (5) of Fact 6, \(\text{ad}(t) \in \text{Der}(Q) \cap \text{Der}_c(U) = \text{Der}_c(Q)\). But this contradicts the \(C\)-independence of \(M\) modulo \(\text{Der}_c(Q)\). Hence \(d_{\gamma}\) is empty, as desired.

Case 2. \(n_1 > 1\): Without loss of generality, we may assume that \(a_1^{(1)}, a_2^{(1)}, \ldots, a_{n_1}^{(1)}\) are \(C\)-linearly independent. By Lemma 1 of [7], there exists \(\beta \in B\) such that \(\beta \in \bigcap_{i \geq 2} (a_i^{(1)})^\perp\) and \(\beta \notin (a_1^{(1)})^\perp\). Consider \(\varphi(x) \cdot \beta\). By means of the formula (1') of Section 0, in the \(\text{DP}(M)\) \(\varphi(x) \cdot \beta\), the only nonzero term which involves \(x^d_1\) is \((a_1^{(1)} \cdot \beta) x^d_1 b_1^{(1)}\). So the \(\text{DP}(M)\) \(\varphi(x) \cdot \beta\) must be nontrivial. Obviously, \(\varphi(x) \cdot \beta \in \mathcal{L}(M, \mathcal{R})\) and \(\varphi(x) \cdot \beta = 0\) gives a nontrivial linear \(\text{DI}(M)\) of \(R\). It is also obvious that \(\varphi(x) \cdot \beta\) is a \(<\)-minimal element of the set

\[\{\psi \in \mathcal{L}(M, \mathcal{R}): \psi = 0\ \text{is a nontrivial reduced linear} \ \text{DI}(M) \ \text{of} \ \text{R}\}.\]

Applying the same argument as that given in Case 1 to the \(\text{DP}(M)\) \(\varphi(x) \cdot \beta\), we obtain that \(A_1\) is empty as before.

**Claim 4.** The regular derivation word \(A_{\varphi, x}\) is empty.

**Reason.** Let us assume that \(\Gamma_1 = A_{\varphi, x}\). That is, \(\Gamma_1 \supseteq \Gamma_k\) for all \(\Gamma_k\) occurring in the expression (3) of the \(\text{DP}(M)\) \(\varphi\). Consider \(\varphi(x^{-1})\). By means of the basic identity 11, we have
\[ \varphi(x^{v+1}) = \sum_{i,j} a_{i,j}^{(v+1)} x^{v+1} a_{i,j}^{(v+1)} b_{i,j}^{(v+1)} + \sum_{k} c_{k}^{(v+1)} x^{v} d_{k}^{(v+1)} \]

where \( a_{i,j}^{(v+1)} \) and \( b_{i,j}^{(v+1)} \) are elements of the set \( \Omega(M^{(v+1)}, <^{(v+1)}) \). As explained at the beginning of this section, \( \varphi(x^{v+1}) \) is also a \( <^{(v+1)} \)-minimal element of the set

\[ \{ \psi \in \mathcal{L}(M^{(v+1)}, v^{-1}R) : \psi = 0 \text{ is a nontrivial reduced linear DI}(M) \text{ of } R \} \]

Applying the same argument as that in Claim 3 to \( \varphi(x^{v+1}) \), we obtain analogously that the derivation word \( \Gamma_{1}^{(v+1)} \) is empty and hence \( \Gamma_{1} \) is also empty, as desired.

In view of Claims 3 and 4, the DP(M) \( \varphi(x) \) assumes the desired form

\[ \varphi(x) = \sum_{i} a_{i} x b_{i} + \sum_{k} c_{k} x^{v} d_{k}, \]

where \( v \in \mathcal{S} \). Hence \( \varphi(x) = 0 \) gives the desired nontrivial reduced linear GPI with a single antiautomorphism in the set \( \mathcal{S} \).

REFERENCES