AUTOMORPHISMS OF HURWITZ SERIES

WILLIAM F. KEIGHER AND VARADHARAJ R. SRINIVASAN

(communicated by Charles A. Weibel)

Abstract

In this article we will define the notions of Hurwitz automorphism and comorphism of the ring of Hurwitz series. A Hurwitz automorphism is the analog of a Seidenberg automorphism of a power series ring when the characteristic of the underlying ring is not necessarily zero. We will show that the sets of all Hurwitz automorphisms, comorphisms, and derivations of the underlying ring are naturally isomorphic to one another.

1. Introduction

Let $A$ be a commutative ring with identity and let $HA$ be the ring of Hurwitz series over $A$. In this article, we introduce and study the notions of comorphism and Hurwitz automorphism of $HA$. We show that the set of all derivations on $A$ is naturally isomorphic to both the set of Hurwitz automorphisms of $HA$ (see Theorem 3.6) and the set of comorphisms on $A$ (see Theorem 2.1).

Throughout, all rings are associative, commutative and unitary, and $A$ and $B$ will typically denote rings. If $f: X \to Y$ is a function, then we will occasionally use the notation $f: X \to Y: x \mapsto f(x)$ to describe the action of $f$ on elements $x \in X$. The natural numbers $\{0, 1, 2, \ldots\}$ will be denoted by $\mathbb{N}$, and similarly $\mathbb{Q}$ and $\mathbb{C}$ will denote the rational numbers and complex numbers, respectively. For any $m, n \in \mathbb{N}$, $\delta_n^m$ will denote the Kronecker delta, i.e., $\delta_n^m = 1$ if $m = n$ and $\delta_n^m = 0$ if $m \neq n$.

Definitions and Conventions

If $A$ is a ring, then a derivation on $A$ is an additive mapping $d: A \to A$ such that, for all $a, b \in A$, $d(ab) = d(a)b + ad(b)$. Examples include the familiar $d/dt$ on the ring $\mathbb{C}[t]$ of polynomials in $t$ with coefficients in $\mathbb{C}$, and for any ring $A$, the trivial derivation $0_A$ defined by $0_A(a) = 0$ for any $a \in A$. The set of all derivations of $A$ will be denoted by $\text{Der} A$. A differential ring consists of a pair $(A, d)$, where $A$ is a ring and $d$ is a derivation on $A$. If $(A, d_1)$ and $(B, d_2)$ are differential rings, then a differential ring homomorphism $f: (A, d_1) \to (B, d_2)$ is a ring homomorphism $f: A \to B$ such that $d_2 \circ f = f \circ d_1$.

The following result is probably well-known, but we record it here, as it will be useful later. The proof is immediate.
Suppose that \( f \) and \( g \) are ring homomorphisms such that \( f \circ g = \text{id}_B \). Then \( f \circ d \circ g \) is a derivation on \( B \).

**Ring of Hurwitz series**

From [1] we recall that for any ring \( A \), the ring of Hurwitz series over \( A \), denoted by \( HA \), consists of sequences \( h = (h_0, h_1, h_2, \ldots) \), where \( h_n \in A \) for each \( n \in \mathbb{N} \). It is often convenient to view a Hurwitz series as a function \( h : \mathbb{N} \to A : n \mapsto h(n) \). Let \( g, h \in HA \). Addition in \( HA \) is defined termwise, i.e.,

\[(g + h)(n) = g(n) + h(n),\]

and the Hurwitz product of \( g \) and \( h \) is given by

\[(g \cdot h)(n) = \sum_{k=0}^{n} \binom{n}{k} g(k)h(n - k)\]

for all \( n \in \mathbb{N} \), where \( \binom{n}{k} \) denotes the binomial coefficient.

The ring \( HA \) is a differential ring with derivation

\[ \partial_A : HA \to HA : (h_0, h_1, h_2, \ldots) \mapsto (h_1, h_2, h_3, \ldots), \]

which is often convenient to view a Hurwitz series as a function \( h : \mathbb{N} \to A : n \mapsto h(n) \). Let \( g, h \in HA \). Addition in \( HA \) is defined termwise, i.e.,

\[(g + h)(n) = g(n) + h(n),\]

and the Hurwitz product of \( g \) and \( h \) is given by

\[(g \cdot h)(n) = \sum_{k=0}^{n} \binom{n}{k} g(k)h(n - k)\]

for all \( n \in \mathbb{N} \), where \( \binom{n}{k} \) denotes the binomial coefficient.

The ring \( HA \) is a differential ring with derivation

\[ \partial_A : HA \to HA : (h_0, h_1, h_2, \ldots) \mapsto (h_1, h_2, h_3, \ldots), \]

that is, \( \partial_A \) is the left shift operator. Observe that if \( d \) is a derivation on \( A \), then

\[ Hd : HA \to HA : (h_0, h_1, h_2, \ldots) \mapsto (d(h_0), d(h_1), d(h_2), \ldots) \]

is a derivation on \( HA \), and \( Hd \circ \partial = \partial \circ Hd \). For any ring \( A \), there are natural ring homomorphisms

\[ \lambda_A : A \to HA : a \mapsto (a, 0, 0, \ldots) \]

and

\[ \varepsilon_A : HA \to A : (h_0, h_1, h_2, \ldots) \mapsto h_0. \]

Furthermore, if \( d \) is a derivation on \( A \) then

\[ \bar{d} : A \to HA : a \mapsto (a, d(a), d^2(a), \ldots) \]

is also a ring homomorphism, called the Hurwitz homomorphism of \( d \). Note that \( 0_A = \lambda_A \). If \( f : A \to B \) is a ring homomorphism, then \( Hf : HA \to HB \) is defined as follows: for \( h = (h_0, h_1, h_2, \ldots) \), \( Hf(h) = (f(h_0), f(h_1), f(h_2), \ldots) \).

For convenience and when there is no ambiguity, we will often use \( \varepsilon, \lambda \) and \( \partial \) instead of \( \varepsilon_A, \lambda_A \) and \( \partial_A \) respectively.

**Divided powers**

From [2] we recall that for any ring \( A \), the divided powers \( x^{[i]} \) in \( HA \), for \( i \in \mathbb{N} \), are defined by

\[ x^{[i]}(n) := \delta_A^n, \]

so that \( x^{[0]} = 1_{HA} \), \( x^{[1]} = (0, 1, 0, \ldots) \), \( x^{[2]} = (0, 0, 1, 0, \ldots) \), etc. The following results are easy to check:

\[ x^{[m]} \cdot x^{[n]} = \binom{m + n}{n} x^{[m+n]}, \quad \forall m, n \in \mathbb{N} \]
and
\[
\text{for any } h \in HA, (h \cdot x^{[k]})(n) = \begin{cases} 0, & \text{if } n < k; \\ \binom{n}{k} h(n-k), & \text{otherwise.} \end{cases}
\]

We define the \textit{order} of \( 0 \neq h \in HA \), denoted by \( \text{ord}(h) \), to be the minimum \( i \in \mathbb{N} \) such that \( h(i) \neq 0 \) and when \( h = 0 \), \( \text{ord}(h) := \infty \). Using this order, one can define a metric on \( HA \) by\[
(\gamma;\varepsilon) = \left( \frac{1}{2} \right)^{\text{ord}(\gamma \varepsilon)}; \text{ see [2].}
\]
Using this topology on \( HA \) and the divided powers \( x^{[i]} \), it is easy to see that for any \( h \in HA \), \( h = \sum_{n=0}^{\infty} h(n)x^{[n]} \).

**Comor \( A \) and Haut \( A \)**

A \textit{comorphism} \( \alpha \) on a ring \( A \) is a ring homomorphism \( \alpha : A \to HA \) such that the diagrams
\[
\begin{array}{ccc}
A & \xrightarrow{\alpha} & HA \\
\downarrow{\text{id}_A} & & \downarrow{\varepsilon_A} \\
A & \to & HA
\end{array}
\quad \text{and} \quad
\begin{array}{ccc}
A & \xrightarrow{\alpha} & HA \\
\downarrow{\alpha} & & \downarrow{\tilde{\delta}} \\
HA & \xrightarrow{H\alpha} & HHA
\end{array}
\]

commute. Examples of comorphisms on \( A \) include \( \lambda_A \) and \( \tilde{d} \), where \( d \) is a derivation on \( A \). The set of all comorphisms on \( A \) will be denoted by \( \text{Comor} A \).

It is well-known that if \( A \) is a differential ring with derivation \( d \) and \( Q \subseteq A \), then there is a differential ring homomorphism
\[
T : (A, d) \to (A[[t]], d/dt) : a \mapsto \sum_{n=0}^{\infty} \frac{d^{(n)}(a)}{n!} t^n
\]
called the \textit{Taylor homomorphism} of \( d \). From the ring homomorphism
\[
A[[t]] \to A : \sum_{n=0}^{\infty} a_n t^n \mapsto a_0,
\]
by Proposition 2.1 of [1] we get a natural differential ring homomorphism
\[
\psi_A : (A[[t]], d/dt) \to (HA, \partial_A) : \sum_{n=0}^{\infty} a_n t^n \mapsto (n! a_n).
\]
(2)

When \( Q \subset A \), the Taylor homomorphism \( T \) and the Hurwitz homomorphism \( \tilde{d} \) are related by \( \psi_A \) via the commutative diagram
\[
\begin{array}{ccc}
A[[t]] & \xrightarrow{T} & A \\
\downarrow{\psi_A} & & \downarrow{\tilde{d}} \\
A & \xrightarrow{\tilde{d}} & HA
\end{array}
\]

and, moreover, \( \psi_A \) is an isomorphism. However, the Taylor homomorphism \( T \) is defined only in case \( Q \subseteq A \), while the Hurwitz homomorphism \( \tilde{d} \) is defined for any differential ring \( A \) of any characteristic.
A ring endomorphism $\sigma$ of $HA$ is called a Hurwitz endomorphism if, for all $n \in \mathbb{N}$, $\sigma$ satisfies the following conditions:

\begin{align}
(\varepsilon \circ \partial \circ \sigma \circ \lambda)^n &= \varepsilon \circ \partial^n \circ \sigma \circ \lambda, \\
\sigma(x^n) &= x^n, \\
\text{ord}(h) &\leq \text{ord}(\sigma(h)) \tag{5}.
\end{align}

We note that the condition (3) is equivalent to $\sigma \circ \lambda \in \text{Comor}_A$ and that the condition (5) guarantees the continuity of $\sigma$ with respect to the metric $\delta$. Furthermore, if $\sigma$ is bijective then we call $\sigma$ a Hurwitz automorphism of $HA$. The set of all Hurwitz automorphisms of $HA$ will be denoted by $\text{Haut}_A$.

The next two sections of this article are dedicated to proving the equivalence between $\text{Der}_A$ and $\text{Comor}_A$.

2. Equivalence of $\text{Der}_A$ and $\text{Comor}_A$

The following theorem shows that $\text{Der}_A$ and $\text{Comor}_A$ are equivalent as sets. From the definition of a comorphism and from Lemma 1.1, we see that $\varepsilon \circ \partial \circ e \circ \partial$ is a derivation on $A$ for any $e \in \text{Comor}_A$.

**Theorem 2.1.** Consider the mappings $\Omega: \text{Der}_A \rightarrow \text{Comor}_A$ defined by $\Omega(d) = e \circ d$, and $\Delta: \text{Comor}_A \rightarrow \text{Der}_A$ defined by $\Delta(e) = (\varepsilon \circ \partial \circ e)(0).$ Then $\Delta \circ \Omega = \text{id}_{\text{Der}_A}$ and $\Omega \circ \Delta = \text{id}_{\text{Comor}_A}$, so that $\text{Der}_A \cong \text{Comor}_A$ as sets.

**Proof.** It is easy to see that $\varepsilon(\partial(\bar{d}(a))) = d(a)$ for any $a \in A$. Thus $\Delta(\Omega(d)) = d$.

For $e \in \text{Comor}_A$ and $a \in A$, we have

$$\Omega(\Delta(e))(a) = (\varepsilon, \varepsilon \circ \partial \circ e(a), (\varepsilon \circ \partial \circ e)^2(a), \ldots).$$

From the definition of Comor $A$, we have $\bar{\partial} \circ e(a) = H \circ e(a)$, which in turn gives us the relation, for any $n \in \mathbb{N}$,

$$\partial^n \circ e = e \circ \partial^n \circ e.$$ 

A straightforward computation, using the above equation, will give us the relation $\varepsilon \circ \partial^n \circ e = (\varepsilon \circ \partial \circ e)^n$. Note that $\varepsilon \circ \partial^n \circ e(a) = e(a)(n)$. Thus it follows that $e(a) = \Omega(\varepsilon \circ \partial \circ e)(a)$, and thus $\Omega(\Delta(e)) = e$. 

3. Equivalence of $\text{Der}_A$ and $\text{Haut}_A$

In this section, we will show that there is a natural isomorphism between the sets $\text{Der}_A$ and $\text{Haut}_A$.

**Lemma 3.1.** Let $\sigma \in \text{Haut}_A$, $a \in A$, $k \in \mathbb{N}$, $h \in HA$ and define $d_{\sigma}$ by $d_{\sigma} := \varepsilon \circ \partial \circ \sigma \circ \lambda$. Then

1. $\sigma(\lambda(a)) = \sigma(ax^0) = (a, d_{\sigma}(a), d_{\sigma}^2(a), \ldots)$,
2. \( d_\sigma \) is a derivation on \( A \) and \( \sigma(\lambda(a)) = \tilde{d}_\sigma(a) \). That is, the diagram

\[
\begin{array}{ccc}
A & \xleftarrow{\lambda} & HA \\
\tilde{d}_\sigma & \searrow & \\
& HA & \downarrow \sigma
\end{array}
\]

commutes, and

3. \( \sigma(ax[k])(n) = \begin{cases} 0, & \text{if } n < k; \\ \binom{n}{k}d^n_{\sigma} - k(a), & \text{if } n \geq k. \end{cases} \)

Proof. Item 1. follows immediately from equation (3). From item 1. it follows that \( \varepsilon \circ \sigma \circ \lambda = \text{id}_A \). Thus from Lemma 1.1 we obtain that \( d_\sigma \) is a derivation on \( A \). Since \( \sigma \) is a homomorphism, we have \( \sigma(ax[k]) = \sigma(ax[0]) \cdot \sigma(x[k]) \), and since \( \sigma(x[k]) = x[k] \), we have

\[
\sigma(ax[k]) = \sigma(ax[0]) \cdot x[k].
\]

Now from item 1. of this lemma and from equation (1), item 3. follows. \( \Box \)

**Theorem 3.2.** Let \( \sigma \in \text{Haut} A \) and \( h \in HA \). Then for each \( n \in \mathbb{N} \),

\[
\sigma(h)(n) = \sum_{k=0}^{n} \binom{n}{k}d^n_{\sigma} - k(h(k)),
\]

where \( d_\sigma \) is the derivation given by \( d_\sigma := \varepsilon \circ \partial \circ \sigma \circ \lambda \).

Proof. Let \( h \in HA \) and write \( h = \sum_{k=0}^{\infty} h(k)x[k] \). Then

\[
\sigma(h)(n) = \sigma\left( \sum_{k=0}^{n} h(k)a[k] \right)(n) + \sigma\left( \sum_{k=n+1}^{\infty} h(k)x[k] \right)(n)
\]

\[
= \sum_{k=0}^{n} \sigma(h(k)x[k])(n) + \sigma\left( \sum_{k=n+1}^{\infty} h(k)x[k] \right)(n).
\]

Now since the ord \( (\sum_{k=n+1}^{\infty} h(k)x[k]) \geq n + 1 \), from condition (5), we obtain that \( \sigma\left( \sum_{k=n+1}^{\infty} h(k)x[k] \right)(t) = 0 \) for all \( t \leq n \). Now from Lemma 3.1 item 3., it follows that \( \sigma(h)(n) = \sum_{k=0}^{n} \binom{n}{k}d^n_{\sigma} - k(h(k)) \).

For any \( d \in \text{Der} A \), \( h \in HA \), and \( n \in \mathbb{N} \), define

\[
\sigma_d(h)(n) = \sum_{k=0}^{n} \binom{n}{k}d^n_{\sigma} - k(h(k)).
\]

(7)

In the next few results, we will show that \( \sigma_d \) is a Hurwitz automorphism.

**Theorem 3.3.** For any \( d \in \text{Der} A \), \( \sigma_d \) is a Hurwitz endomorphism of \( HA \).
Proof. From the fact that \(d^n\) is additive, it is easy to see that \(\sigma_d\) is also additive. Let 
\(h = (h_0, h_1, \ldots), g = (g_0, g_1, \ldots) \in HA\) and from equation (7), we have

\[
(\sigma_d(h) \cdot \sigma_d(g))(n) = \sum_{k=0}^{n} \binom{n}{k} \sigma_d(h)(k)\sigma_d(g)(n-k)
\]

\[
= \sum_{k=0}^{n} \binom{n}{k} \left( \sum_{j=0}^{k} \binom{k}{j} d^{k-j}(h_j) \right) \left( \sum_{i=0}^{n-k} \binom{n-k}{i} d^{n-k-i}(g_i) \right)
\]

\[
= \sum_{k=0}^{n} \sum_{j=0}^{k} \sum_{i=0}^{n-k} \binom{n}{k} \binom{k}{j} \binom{n-k}{i} d^{k-j}(h_j)d^{n-k-i}(g_i). \tag{8}
\]

On the other hand, since \((h \cdot g)(p) = \sum_{q=0}^{p} \binom{p}{q} h_q g_{p-q}\), we have

\[
\sigma(h \cdot g)(n) = \sum_{p=0}^{n} \binom{n}{p} d^n p \sum_{q=0}^{p} \binom{p}{q} h_q g_{p-q}
\]

\[
= \sum_{p=0}^{n} \sum_{r=0}^{n-p} \binom{n}{p} \binom{p}{r} d^{n-p-r}(h_q)d^r (g_{p-q}). \tag{9}
\]

We will now show that equations (8) and (9) are identical. Note that both the equations (8) and (9) have the same number of terms. Consider the equations \(n - p - r = k - j, r = n - k - i, q = j\) and \(p - q = i\). Solving for \(p, q\) and \(r\), we obtain \(q = j, p = i + j, r = n - k - i\). Substituting for \(p, q\) and \(r\) in \(\binom{n}{p} \binom{p}{r}\), we obtain

\[
\binom{n}{i+j} \binom{i+j}{j} \binom{n-i-j}{n-k-i} = \frac{n!}{i!j!(k-j)!(n-k-i)!}.
\]

On the other hand,

\[
\binom{n}{k} \binom{k}{j} \binom{n-k}{i} = \frac{n!}{i!j!(k-j)!(n-k-i)!}.
\]

Thus \(\sigma_d\) is a ring endomorphism. From the definition of \(\sigma_d\), it is clear that \(\sigma_d(x^k) = x^k\) and \(\sigma_d(ax^n)(n) = d^n(a)\), and thus \(\sigma_d(ax^n) = (a, d(a), d^2(a), \ldots)\). Since \(\lambda(a) = ax^0\), it is now easy to check that \(\varepsilon \circ \delta \circ \sigma_d \circ \lambda = d\) and that \(\varepsilon \circ \partial^n \circ \sigma_d \circ \lambda = d^n\) for any \(n\). Hence \(\sigma_d\) is a Hurwitz endomorphism.

\[\square\]

**Lemma 3.4.** If \(d_1, d_2 \in \text{Der } A\) with \(d_1 \circ d_2 = d_2 \circ d_1\), then \(\sigma_{d_1} \circ \sigma_{d_2} = \sigma_{d_1+d_2} = \sigma_{d_2} \circ \sigma_{d_1}\).

Proof. Let \(h = (h_0, h_1, \ldots) \in HA\). Then

\[
\sigma_{d_2}(\sigma_{d_1}(h))(n) = \sum_{k=0}^{n} \binom{n}{k} d_2^{n-k} \left( \sum_{i=0}^{k} \binom{k}{i} d_1^{k-i}(h_i) \right)
\]

\[
= \sum_{k=0}^{n} \sum_{i=0}^{k} \binom{n}{k} \binom{k}{i} d_2^{n-k} d_1^{k-i}(h_i).
\]
Similarly,
\[
\sigma_{d_1+d_2}(h)(n) = \sum_{j=0}^{n} \binom{n}{j} (d_1 + d_2)^{n-j}(h_j)
\]
\[
= \sum_{j=0}^{n} \binom{n}{j} \left( \sum_{l=0}^{n-j} \binom{n-j}{l} d_1^{n-j-l}(d_2^l(h_j)) \right)
\]
\[
= \sum_{j=0}^{n} \sum_{l=0}^{n-j} \binom{n}{j} \binom{n-j}{l} d_1^{n-j-l}(d_2^l(h_j)).
\]

Note that when \( j = i \) and \( l = n - k \), we have \( d_1^{n-j-l}(d_2^l(h_j)) = d_2^{n-k}(d_1^{k-i}(h_i)) \). Now substituting \( j = i \) and \( l = n - k \) in \( \binom{n}{i} \), we obtain \( \binom{n}{n-i} \). On the other hand, \( \binom{n}{i} = \binom{n}{n-i} \). Thus \( \sigma_{d_1+d_2} = \sigma_d \circ \sigma_{d_1} \). Similarly, it follows that \( \sigma_{d_1+d_2} = \sigma_{d_2} \circ \sigma_{d_1} \).

**Theorem 3.5.** For any \( d \in \text{Der } A \), \( \sigma_d \) is a Hurwitz automorphism of \( HA \) and \( \sigma_d^{-1} = \sigma_{-d} \).

**Proof.** We only need to show that \( \sigma_d \) has an inverse for each \( d \). It is easy to check that the automorphism corresponding to the trivial derivation, \( 0_A \), is the identity map \( \text{id}_{HA} \). Since \( d \) and \( -d \) are commuting derivations, it follows from Lemma 3.4 that \( \text{id}_{HA} = \sigma_0_{A} = \sigma_{d+(-d)} = \sigma_d \circ \sigma_{-d} \). Thus \( \sigma_d \) is a Hurwitz automorphism with inverse \( \sigma_{-d} \).

**Theorem 3.6.** Let \( \Phi: \text{Der } A \to \text{Haut } A \) and \( \Psi: \text{Haut } A \to \text{Der } A \) be defined by \( \Phi(d) = \sigma_d \) and \( \Psi(\sigma) = d_\sigma \), where \( d_\sigma := \varepsilon \circ d \circ \sigma \circ \lambda \). Then \( \Phi \circ \Psi = \text{id}_{\text{Haut } A} \) and \( \Psi \circ \Phi = \text{id}_{\text{Der } A} \). Thus \( \text{Der } A \) and \( \text{Haut } A \) are isomorphic sets.

**Proof.** For any \( \sigma \in \text{Haut } A \), \( \Phi(\Psi(\sigma)) = \Phi(d_\sigma) = \sigma_{d_\sigma} \). Note that for \( h = (h_0, h_1, \ldots) \), \( \sigma_{d_\sigma}(h)(n) = \sum_{k=0}^{n} \binom{n}{k} d_2^{n-k}(h_k) \). But from the definition of \( \sigma \), we know that \( \sigma(h)(n) = \sum_{k=0}^{n} \binom{n}{k} d_1^{n-k}(h_k) \). Thus \( \Phi(\Psi(\sigma)) = \sigma \).

For \( d \in \text{Der } A \), \( \Psi(\Phi(d)) = \Psi(\sigma_d) = d_{\sigma_d} \) and for any \( a \in A \), we know that \( \sigma_d(\lambda(a)) = (a, d(a), d^2(a), \ldots) \) and thus \( d_{\sigma_d}(a) = \varepsilon \circ d \circ \sigma_d \circ \lambda(a) = d(a) \). Thus \( \Psi(\Phi(d)) = d \).

Since \( \Psi \) is the inverse of \( \Phi \), it follows that \( \Phi \) and \( \Psi \) are isomorphisms (of sets).

4. Commuting derivations and Hurwitz automorphisms

We first recall that a ring \( A \) is said to have no 2-torsion if for any \( a \in A \), if \( 2a = 0 \), then \( a = 0 \). It is clear that such a ring \( A \) is not of characteristic 2, and that if \( 2 \) is invertible in \( A \), then \( A \) has no 2-torsion.

In this section we will show that if \( \Delta \subset \text{Der } A \) is a subgroup of \( \text{Der } A \) consisting of commuting derivations, then \( \Phi(\Delta) \subset \text{Haut } A \) is an abelian group (with respect to \( \circ \)). We will also show that if \( G \subset \text{Haut } A \) is an abelian group and if \( A \) has no 2-torsion, then \( \Delta = \{ d_\sigma \mid \sigma \in G \} \) is a subgroup of \( \text{Der } A \) consisting of commuting derivations.
Theorem 4.1. Let $\Delta \subset \text{Der} A$ be a subgroup of $\text{Der} A$ consisting of commuting derivations. Then $\Phi(\Delta) \subset \text{Haut} A$ is an abelian group (with respect to $\circ$). Moreover,

$$\Phi|_{\Delta}: (\Delta, +) \to (\Phi(\Delta), \circ)$$

is a group isomorphism.

**Proof.** Let $\sigma_1, \sigma_2 \in \Phi(\Delta)$. For notational convenience, let $d_i := d_{\sigma_i}$ for $i = 1, 2$. Then from Theorem 3.6, we know that $d_1, d_2 \in \Delta$ and that $\sigma_{d_i} = \sigma_i$ for $i = 1, 2$. Now applying Lemma 3.4, we obtain that

$$\Phi(d_1 + d_2) = \Phi(d_1) \circ \Phi(d_2).$$

Now since $d_1 + d_2 \in \Delta$, we have $\sigma_1 \circ \sigma_2 \in \Phi(\Delta)$.

Let $\sigma \in \Phi(\Delta)$. From Theorem 3.6, we know that $d_\sigma \in \Delta$ and $\sigma = \sigma_{d_\sigma}$. But from Theorem 3.5 we know that $\sigma_{-d_\sigma}$ is the inverse of $\sigma$. Since $-d_\sigma \in \Delta$, we have $\sigma_{-d_\sigma} \in \Phi(\Delta)$. Hence $\Phi(\Delta)$ forms a group. Now from Lemma 3.4, it follows that $\Phi(\Delta)$ is an abelian group. Also note that for any $d \in \text{Der} A$, $\Phi(0_A) = \sigma_{0_A} = \sigma_{d + -d} = \sigma_d \circ \sigma_{-d} = \text{id}_{HA}$. Thus $\Phi|_{\Delta}$ is a group isomorphism. \qed

Theorem 4.2. Let $A$ be a ring having no 2-torsion and let $G \subset \text{Haut} A$ be an abelian group. Then $\Psi(G) = \{d_\sigma \mid \sigma \in G\}$ is a subgroup of $\text{Der} A$ consisting of commuting derivations. Moreover, $\Psi|_{G}: (G, \circ) \to (\Psi(G), +)$ is a group isomorphism.

**Proof.** Let $\sigma_1, \sigma_2 \in G$ and let $a \in A$. For notational convenience, let $d_i := d_{\sigma_i}$ for $i = 1, 2$. Since $\sigma_1$ and $\sigma_2$ commute, we have $\sigma_1(\sigma_2(\lambda(a))(n)) = \sigma_2(\sigma_1(\lambda(a)))(n)$ for all $n$. That is,

$$\sum_{k=0}^{n} \binom{n}{k} d_1^{n-k}(d_2^k(a)) = \sum_{k=0}^{n} \binom{n}{k} d_2^{n-k}(d_1^k(a))$$

for all $n$. In particular, when $n = 2$, the above equation reduces to

$$d_1^2(a) + 2d_1(d_2(a)) + d_2(a) = d_2^2(a) + 2d_2(d_1(a)) + d_1^2(a).$$

Thus we have $2d_2(d_1(a)) = 2d_1(d_2(a))$, and since $A$ has no 2-torsion, we obtain that $d_2(d_1(a)) = d_1(d_2(a))$ for all $a \in A$. Hence $d_1$ and $d_2$ commute. From Lemma 3.4 it follows that $\sigma_{d_1 + d_2} = \sigma_{d_1} \circ \sigma_{d_2}$, and now from Theorem 3.6, we obtain that $d_1 + d_2 \in \Psi(G)$. Let $d \in \Psi(G)$; then $\sigma_d \in G$ and from Theorem 3.5 we know that $\sigma_{-d}$ is the inverse of $\sigma_d$. Then $\sigma_{-d} \in G$, and thus $-d = \Psi(\sigma_{-d}) \in \Psi(G)$. Hence $\Psi(G)$ is a subgroup of $\text{Der} A$ consisting of commuting derivations. Since $\Phi$ and $\Psi$ are inverses, it follows that $\Psi|_{G}$ is a group isomorphism. \qed

Remark 4.3. We recall from [4] that for a ring $A$ with $\mathbb{Q} \subseteq A$, a Seidenberg automorphism over $A$ is an automorphism $E$ of $A[[T]]$ leaving $T$ fixed and reducing to the identity modulo $T$. Such an $E$ restricted to $A$ gives a derivation on $A$, and conversely every derivation on $A$ extends uniquely to a Seidenberg automorphism over $A$. Further, if $\mathbb{Q} \subseteq A$ then as noted in equation (2), $\psi_A: A[[T]] \to HA$ is an isomorphism and that if $E$ is a Seidenberg automorphism over $A$ and $d$ is the derivation on $A$ from
E, then the diagram

\[
\begin{array}{ccc}
A[[T]] & \xrightarrow{\psi_A} & HA \\
E & \downarrow{\psi_A} & \downarrow{\sigma_A} \\
A[[T]] & \xrightarrow{\psi_A} & HA
\end{array}
\]

commutes. Thus a Hurwitz automorphism is a generalization of a Seidenberg automorphism to include the case when \( \mathbb{Q} \not\subseteq A \), such as when the characteristic of \( A \) is positive.

**Acknowledgements**

The authors thank Colas Bardavid, Alexey Ovchinnikov and Camilo Sanabria for their helpful remarks. The authors also thank the participants of the Kolchin Seminar in Differential Algebra for their constant support and encouragement throughout this project.

**References**


William F. Keigher  keigher@rutgers.edu

Department of Mathematics and Computer Science, Rutgers University, 101 Warren Street, Newark, NJ 07102

Varadharaj R. Srinivasan  v.ravisrinivasan@gmail.com

Department of Mathematical Sciences, Indian Institute of Science Education and Research, Mohali, Knowledge City, Sector 81, SAS Nagar, Punjab 140306, India