Homology, Homotopy and Applications, vol. 14(2), 2012, pp.91–99

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 $f\colon X \to Y$ is a function, then we will occasionally use the notation $f\colon X \to Y : x \mapsto f(x)$ 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 $m, n \in \mathbb{N}$, δ_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 $d\colon A \to A$ 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 $\operatorname{Der} A$. 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 $f\colon (A, d_1) \to (B, d_2)$ is a ring homomorphism $f\colon A \to B$ 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.

Received May 4, 2012; published on November 8, 2012.
2000 Mathematics Subject Classification: 12H05, 12H20.
Key words and phrases: automorphism, comorphism, derivation, Hurwitz series.
Article available at `http://intlpress.com/HHA/v14/n2/a6` and `doi:10.4310/HHA.2012.v14.n2.a6`

Lemma 1.1. *Suppose that (A, d) is a differential ring and $f\colon A \to B$ and $g\colon B \to A$ are ring homomorphisms such that $f \circ g = \mathrm{id}_B$. 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 $h\colon \mathbb{N} \to A\colon n \mapsto h(n)$. 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

$$\partial_A\colon HA \to HA\colon (h_0, h_1, h_2, \ldots) \mapsto (h_1, h_2, h_3, \ldots),$$

that is, ∂_A is the left shift operator. Observe that if d is a derivation on A, then

$$Hd\colon HA \to HA\colon (h_0, h_1, h_2, \ldots) \mapsto (d(h_0), d(h_1), d(h_2), \ldots)$$

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

$$\lambda_A\colon A \to HA\colon a \mapsto (a, 0, 0, \ldots)$$

and

$$\varepsilon_A\colon HA \to A\colon (h_0, h_1, h_2, \ldots) \mapsto h_0.$$

Furthermore, if d is a derivation on A then

$$\widetilde{d}\colon A \to HA\colon a \mapsto (a, d(a), d^2(a), \ldots)$$

is also a ring homomorphism, called the *Hurwitz homomorphism* of d. Note that $\widetilde{0}_A = \lambda_A$. If $f\colon A \to B$ is a ring homomorphism, then $Hf\colon HA \to HB$ 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 ε, λ and ∂ instead of ε_A, λ_A and ∂_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

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

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

$$\text{for any } h \in HA, (h \cdot x^{[k]})(n) = \begin{cases} 0, & \text{if } n < k; \\ \binom{n}{k} h(n-k), & \text{otherwise.} \end{cases} \tag{1}$$

We define the *order* of $0 \neq h \in HA$, denoted by $\operatorname{ord}(h)$, to be the minimum $i \in \mathbb{N}$ such that $h(i) \neq 0$ and when $h = 0$, $\operatorname{ord}(h) := \infty$. Using this order, one can define a metric δ on HA by $\delta(g,h) = (\frac{1}{2})^{\operatorname{ord}(g-h)}$; 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 *comorphism* α on a ring A is a ring homomorphism $\alpha\colon A \to HA$ such that the diagrams

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[dr, "\mathrm{id}_A"'] & HA \arrow[d, "\varepsilon_A"] \\ & A \end{tikzcd} \qquad \text{and} \qquad \begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\alpha"'] & HA \arrow[d, "\widetilde{\partial}"] \\ HA \arrow[r, "H\alpha"] & HHA \end{tikzcd}$$

commute. Examples of comorphisms on A include λ_A and $\widetilde{d}$, where d is a derivation on A. The set of all comorphisms on A will be denoted by Comor A.

It is well-known that if A is a differential ring with derivation d and $\mathbb{Q} \subseteq A$, then there is a differential ring homomorphism

$$T\colon (A, d) \to (A[[t]], d/dt)\colon a \mapsto \sum_{n=0}^{\infty} \frac{d^{(n)}(a)}{n!} t^n$$

called the *Taylor homomorphism* of d. From the ring homomorphism

$$A[[t]] \to A\colon \sum_{n=0}^{\infty} a_n t^n \mapsto a_0,$$

by Proposition 2.1 of [**1**] we get a natural differential ring homomorphism

$$\psi_A\colon (A[[t]], d/dt) \to (HA, \partial_A)\colon \sum_{n=0}^{\infty} a_n t^n \mapsto (n! a_n). \tag{2}$$

When $\mathbb{Q} \subset A$, the Taylor homomorphism T and the Hurwitz homomorphism $\widetilde{d}$ are related by ψ_A via the commutative diagram

$$\begin{tikzcd} & A[[t]] \arrow[dr, "\psi_A"] & \\ A \arrow[ur, "T"] \arrow[rr, "\widetilde{d}"] & & HA \end{tikzcd}$$

and, moreover, ψ_A is an isomorphism. However, the Taylor homomorphism T is defined only in case $\mathbb{Q} \subseteq A$, while the Hurwitz homomorphism $\widetilde{d}$ is defined for any differential ring A of any characteristic.

A ring endomorphism σ of HA is called a *Hurwitz endomorphism* if, for all $n \in \mathbb{N}$, σ satisfies the following conditions:

$$(\varepsilon \circ \partial \circ \sigma \circ \lambda)^n = \varepsilon \circ \partial^n \circ \sigma \circ \lambda, \tag{3}$$

$$\sigma(x^{[n]}) = x^{[n]}, \tag{4}$$

$$\operatorname{ord}(h) \leqslant \operatorname{ord}(\sigma(h)). \tag{5}$$

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

The next two sections of this article are dedicated to proving the equivalence between $\operatorname{Der} A$, $\operatorname{Comor} A$ and $\operatorname{Haut} A$.

2. Equivalence of $\operatorname{Der} A$ and $\operatorname{Comor} A$

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

Theorem 2.1. *Consider the mappings* $\Omega\colon \operatorname{Der} A \to \operatorname{Comor} A$ *defined by* $\Omega(d) = \widetilde{d}$ *and* $\Delta\colon \operatorname{Comor} A \to \operatorname{Der} A$ *defined by* $\Delta(\alpha) = \varepsilon \circ \partial \circ \alpha$. *Then* $\Delta \circ \Omega = \mathrm{id}_{\operatorname{Der} A}$ *and* $\Omega \circ \Delta = \mathrm{id}_{\operatorname{Comor} A}$, *so that* $\operatorname{Der} A \cong \operatorname{Comor} A$ *as sets.*

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

For $\alpha \in \operatorname{Comor} A$ and $a \in A$, we have

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

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

$$\partial^n \circ \alpha = \alpha \circ \varepsilon \circ \partial^n \circ \alpha. \tag{6}$$

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

3. Equivalence of $\operatorname{Der} A$ and $\operatorname{Haut} A$

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

Lemma 3.1. *Let* $\sigma \in \operatorname{Haut} A$, $a \in A$, $k \in \mathbb{N}$, $h \in HA$ *and define* d_σ *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_σ is a derivation on A and $\sigma(\lambda(a)) = \widetilde{d}_\sigma(a)$. That is, the diagram

$$\begin{tikzcd} A \arrow[dr, "\lambda"] \arrow[dd, "\widetilde{d}_\sigma"'] & \\ & HA \arrow[dl, "\sigma"] \\ HA & \end{tikzcd}$$

commutes, and

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

Proof. Item 1. follows immediately from equation (3). From item 1. it follows that $\varepsilon \circ \sigma \circ \lambda = \mathrm{id}_A$. Thus from Lemma 1.1 we obtain that d_σ is a derivation on A. Since σ 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. $\square$

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

$$\sigma(h)(n) = \sum_{k=0}^{n} \binom{n}{k} d_\sigma^{n-k}(h(k)),$$

where d_σ 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

$$\begin{aligned} \sigma(h)(n) &= \sigma\left(\sum_{k=0}^{n} h(k)a^{[k]}\right)(n) + \sigma\left(\sum_{k=n+1}^{\infty} h(k)x^{[k]}\right)(n) \\ &= \sum_{k=0}^{n} \sigma(h(k)x^{[k]})(n) + \sigma\left(\sum_{k=n+1}^{\infty} h(k)x^{[k]}\right)(n). \end{aligned}$$

Now since the ord $\big(\sum_{k=n+1}^{\infty}(h(k))x^{[k]}\big) \geqslant n+1$, from condition (5), we obtain that $\sigma\big(\sum_{k=n+1}^{\infty}(h(k))x^{[k]}\big)(t) = 0$ for all $t \leqslant n$. Now from Lemma 3.1 item 3., it follows that $\sigma(h)(n) = \sum_{k=0}^{n} \binom{n}{k} d_\sigma^{n-k}(h(k))$. $\square$

For any $d \in \operatorname{Der} A$, $h \in HA$, and $n \in \mathbb{N}$, define

$$\sigma_d(h)(n) = \sum_{k=0}^{n} \binom{n}{k} d^{n-k}(h(k)). \tag{7}$$

In the next few results, we will show that σ_d is a Hurwitz automorphism.

Theorem 3.3. *For any $d \in \operatorname{Der} A$, σ_d is a Hurwitz endomorphism of HA.*

Proof. From the fact that d^n is additive, it is easy to see that σ_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

$$\begin{aligned}(\sigma_d(h) \cdot \sigma_d(g))(n) &= \sum_{k=0}^{n} \binom{n}{k} \sigma_d(h)(k)\sigma_d(g)(n-k) \\ &= \sum_{k=0}^{n} \binom{n}{k} \left(\sum_{j=0}^{k} \binom{k}{j} d^{k-j}(h_j) \right) \left(\sum_{i=0}^{n-k} \binom{n-k}{i} d^{n-k-i}(g_i) \right) \\ &= \sum_{k=0}^{n} \sum_{j=0}^{k} \sum_{i=0}^{n-k} \binom{n}{k} \binom{k}{j} \binom{n-k}{i} d^{k-j}(h_j) d^{n-k-i}(g_i). \qquad (8)\end{aligned}$$

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

$$\begin{aligned}\sigma(h \cdot g)(n) &= \sum_{p=0}^{n} \binom{n}{p} d^{n-p} \left(\sum_{q=0}^{p} \binom{p}{q} h_q g_{p-q} \right) \\ &= \sum_{p=0}^{n} \sum_{q=0}^{p} \sum_{r=0}^{n-p} \binom{n}{p} \binom{p}{q} \binom{n-p}{r} d^{n-p-r}(h_q) d^r(g_{p-q}). \qquad (9)\end{aligned}$$

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 $\binom{n}{p}\binom{p}{q}\binom{n-p}{r}$, 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 σ_d is a ring endomorphism. From the definition of σ_d, it is clear that $\sigma_d(x^{[k]}) = x^{[k]}$ and $\sigma_d(ax^{[0]})(n) = d^n(a)$, and thus $\sigma_d(ax^{[0]}) = (a, d(a), d^2(a), \ldots)$. Since $\lambda(a) = ax^{[0]}$, it is now easy to check that $\varepsilon \circ \partial \circ \sigma_d \circ \lambda = d$ and that $\varepsilon \circ \partial^n \circ \sigma_d \circ \lambda = d^n$ for any n. Hence σ_d is a Hurwitz endomorphism. ☐

Lemma 3.4. *If $d_1, d_2 \in \operatorname{Der} A$ 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

$$\begin{aligned}\sigma_{d_2}(\sigma_{d_1}(h))(n) &= \sum_{k=0}^{n} \binom{n}{k} d_2^{n-k} \left(\sum_{i=0}^{k} \binom{k}{i} d_1^{k-i}(h_i) \right) \\ &= \sum_{k=0}^{n} \sum_{i=0}^{k} \binom{n}{k} \binom{k}{i} d_2^{n-k}(d_1^{k-i}(h_i)).\end{aligned}$$

Similarly,

$$\begin{aligned}\sigma_{d_1+d_2}(h)(n) &= \sum_{j=0}^{n}\binom{n}{j}(d_1+d_2)^{n-j}(h_j)\\ &= \sum_{j=0}^{n}\binom{n}{j}\left(\sum_{l=0}^{n-j}\binom{n-j}{l}d_1^{n-j-l}(d_2^{l}(h_j))\right)\\ &= \sum_{j=0}^{n}\sum_{l=0}^{n-j}\binom{n}{j}\binom{n-j}{l}d_1^{n-j-l}(d_2^{l}(h_j)).\end{aligned}$$

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 $\binom{n}{j}\binom{n-j}{l}$, we obtain $\frac{n!}{i!(k-i)!(n-k)!}$. On the other hand, $\binom{n}{k}\binom{k}{i} = \frac{n!}{i!(k-i)!(n-k)!}$. Thus $\sigma_{d_1+d_2} = \sigma_{d_2}\circ\sigma_{d_1}$. Similarly, it follows that $\sigma_{d_1+d_2} = \sigma_{d_1}\circ\sigma_{d_2}$. □

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

Proof. We only need to show that σ_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 id_{HA}. Since d and $-d$ are commuting derivations, it follows from Lemma 3.4 that $\mathrm{id}_{HA} = \sigma_{0_A} = \sigma_{d+(-d)} = \sigma_d\circ\sigma_{-d}$. Thus σ_d is a Hurwitz automorphism with inverse σ_{-d}. □

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

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

For $d \in \operatorname{Der} A$, $\Psi(\Phi(d)) = \Psi(\sigma_d) = d_{\sigma_d}$ and for any $a \in A$, we know that $\sigma_d(\lambda(a)) = (a, d(a), d^2(a), \ldots)$ and thus $d_{\sigma_d}(a) = \varepsilon\circ\partial\circ\sigma_d\circ\lambda(a) = d(a)$. Thus $\Psi(\Phi(d)) = d$. Since Ψ is the inverse of Φ, it follows that Φ and Ψ 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 $\Delta \subset \operatorname{Der} A$ is a subgroup of $\operatorname{Der} A$ consisting of commuting derivations, then $\Phi(\Delta) \subset \operatorname{Haut} A$ is an abelian group (with respect to $\circ$). We will also show that if $G \subset \operatorname{Haut} A$ is an abelian group and if A has no 2-torsion, then $\Delta = \{d_\sigma \mid \sigma \in G\}$ is a subgroup of $\operatorname{Der} A$ consisting of commuting derivations.

Theorem 4.1. *Let $\Delta \subset \operatorname{Der} A$ be a subgroup of $\operatorname{Der} A$ consisting of commuting derivations. Then $\Phi(\Delta) \subset \operatorname{Haut} A$ is an abelian group (with respect to $\circ$). Moreover,*

$$\Phi|_\Delta \colon (\Delta, +) \to (\Phi(\Delta), \circ)$$

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

$$\Phi(d_1 + d_2) = \sigma_{d_1+d_2} = \sigma_{d_1} \circ \sigma_{d_2} = \sigma_1 \circ \sigma_2 = \Phi(d_1) \circ \Phi(d_2).$$

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 σ_{-d_σ} is the inverse of σ. 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 $d \in \operatorname{Der} A$, $\Phi(0_A) = \sigma_{0_A} = \sigma_{d+-d} = \sigma_d \circ \sigma_{-d} = \mathrm{id}_{HA}$. Thus $\Phi|_\Delta$ is a group isomorphism. □

Theorem 4.2. *Let A be a ring having no 2-torsion and let $G \subset \operatorname{Haut} A$ be an abelian group. Then $\Psi(G) = \{d_\sigma \mid \sigma \in G\}$ is a subgroup of $\operatorname{Der} A$ consisting of commuting derivations. Moreover, $\Psi|_G \colon (G, \circ) \to (\Psi(G), +)$ 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 σ_1 and σ_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

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

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 σ_{-d} is the inverse of σ_d. Then $\sigma_{-d} \in G$, and thus $-d = \Psi(\sigma_{-d}) \in \Psi(G)$. Hence $\Psi(G)$ is a subgroup of $\operatorname{Der} A$ consisting of commuting derivations. Since Φ and Ψ are inverses, it follows that $\Psi|_G$ is a group isomorphism. □

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), $\psi_A \colon A[[T]] \to HA$ 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

$$\begin{tikzcd} A[[T]] \arrow[r, "\psi_A"] \arrow[d, "E"'] & HA \arrow[d, "\sigma_d"] \\ A[[T]] \arrow[r, "\psi_A"] & HA \end{tikzcd}$$

commutes. Thus a Hurwitz automorphism is a generalization of a Seidenberg automorphism to include the case when $\mathbb{Q} \nsubseteq A$, 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

[**1**] W.F. Keigher, On the ring of Hurwitz series, *Comm. Algebra* **25** (1997), no. 6, 1845–1859.

[**2**] W.F. Keigher and F.L. Pritchard, Hurwitz series as formal functions, *J. Pure Appl. Algebra* **146** (2000), no. 3, 291–304.

[**3**] A. Seidenberg, Derivations and integral closure, *Pacific J. Math.* **16** (1966), no. 1, 167–173.

[**4**] W. Waterhouse, Notes toward higher differential algebra, *J. Pure Appl. Algebra* **7** (1976), no. 2, 121–132.

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