Hiroshima Math. J., **52** (2022), 17–42
doi:10.32917/h2021011

$\mathbf{G}_a$-actions on the affine line over a non-reduced ring

Motoki Kuroda and Shigeru Kuroda

(Received February 26, 2021)
(Revised November 11, 2021)

Abstract. In this paper, we study $\mathbf{G}_a$-actions on the affine spaces over a commutative ring of characteristic p^e, where p is a prime number and $e \geq 2$. We say that a $\mathbf{G}_a$-action is *red-nontrivial* (resp. *red-trivial*) if it is nontrivial (resp. trivial) modulo p. We give a structure theorem for red-nontrivial $\mathbf{G}_a$-actions on the affine lines under some mild assumptions. Interestingly, the invariant ring for such an action is either the ring of constants or non-finitely generated. We show that every red-trivial $\mathbf{G}_a$-action on the affine space over a certain class of commutative rings is uniquely determined by two derivations, whose invariant ring is finitely generated if the base ring is noetherian. By combining these results, we completely determine the $\mathbf{G}_a$-actions on the affine lines over a certain class of commutative rings of positive characteristic, including $\mathbf{Z}/m\mathbf{Z}$ for any $m \geq 2$.

1. Introduction

Throughout this paper, a ring means a commutative ring with nonzero identity. For a ring R, an R-algebra means a commutative ring containing R as a subring. Let A be an R-algebra, T and U indeterminates over A, and $\sigma : A \to A[T]$ a homomorphism of R-algebras. We define R-linear maps $\delta_i^\sigma : A \to A$ for $i \geq 0$ by $\sigma(a) = \sum_{i \geq 0} \delta_i^\sigma(a) T^i$ for each $a \in A$. Recall that σ defines an action of the additive group $\mathbf{G}_a = \operatorname{Spec} R[T]$ on $\operatorname{Spec} A$ if and only if the following conditions hold.

(A1) $\delta_0^\sigma = \mathrm{id}_A$.

(A2) $\sum_{i \geq 0} \sigma(\delta_i^\sigma(a)) U^i = \sum_{i \geq 0} \delta_i^\sigma(a)(T + U)^i$ for each $a \in A$.

When this is the case, we call σ a $\mathbf{G}_a$-*action* on A (over R). We say that σ is *trivial* if the invariant ring $A^\sigma := \bigcap_{i \geq 1} \ker \delta_i^\sigma = \{a \in A \mid \sigma(a) = a\}$ is equal to A, that is, σ is the inclusion map $A \hookrightarrow A[T]$. We denote the trivial $\mathbf{G}_a$-action by $\imath$. For any $\mathbf{G}_a$-action σ on A and $b \in A^\sigma \backslash A^*$, a $\mathbf{G}_a$-action on A/bA is naturally induced from σ.

The Second author is supported by JSPS KAKENHI Grant Number 18K03219.

2020 *Mathematics Subject Classification*. Primary 14R20; Secondary 13A50.

Key words and phrases. additive group action, positive characteristic, invariant ring, non-finite generation.

One of the important problems in Affine Algebraic Geometry is to determine all the $\mathbf{G}_a$-actions on the polynomial ring $R[\boldsymbol{x}] = R[x_1, \dots, x_n]$ in n variables over R. When $n = 1$, we write $R[\boldsymbol{x}] = R[x]$. In the case R is an integral domain, it is well known that a homomorphism $\sigma : R[x] \to R[x][T]$ of R-algebras is a $\mathbf{G}_a$-action if and only if $\sigma(x) \in x + RT$ when $\operatorname{char} R = 0$, and $\sigma(x) \in x + \sum_{i \geq 0} RT^{p^i}$ when $p := \operatorname{char} R > 0$ (cf. Lemma 5).

Assume that $R = K$ is a field, and let σ be a $\mathbf{G}_a$-action on $K[\boldsymbol{x}]$. When $n = 2$, there exist $y_1, y_2 \in K[\boldsymbol{x}]$ such that $K[\boldsymbol{x}] = K[y_1, y_2]$ and $y_1 \in K[\boldsymbol{x}]^\sigma$ by Rentschler [11] if $p = 0$, and by Miyanishi [9] if $p > 0$ (see also [5], [6]). If this is the case, σ is a $\mathbf{G}_a$-action on $K[y_1][y_2]$ over $K[y_1]$. Hence, we are reduced to the one variable case. For $n \geq 3$, Freudenburg [3] constructed $\mathbf{G}_a$-actions σ on $K[\boldsymbol{x}]$ for which there do not exist $y_1, \dots, y_n \in K[\boldsymbol{x}]$ such that $K[\boldsymbol{x}] = K[y_1, \dots, y_n]$ and $y_1 \in K[\boldsymbol{x}]^\sigma$. This type of $\mathbf{G}_a$-action is difficult to understand. It is an open problem to determine all the $\mathbf{G}_a$-actions on $K[\boldsymbol{x}]$ for $n \geq 3$.

We mention that $K[x_1, x_2, x_3]^\sigma \simeq R[x_1, x_2]$ if $p = 0$ by Miyanishi [8]. On the other hand, the K-algebra $K[\boldsymbol{x}]^\sigma$ is not always finitely generated if $p = 0$ and $n \geq 5$ by Daigle-Freudenburg [2]. The problem of finite generation of $K[\boldsymbol{x}]^\sigma$ is a special case of *Hilbert's fourteenth problem*, and is of great interest.

When R is not an integral domain, $\mathbf{G}_a$-actions on $R[\boldsymbol{x}]$ are not studied well, even in the low-dimensional cases. If R is reduced, then we can explicitely describe all the $\mathbf{G}_a$-actions on $R[x]$ (see Section 9). However, the situation is far different when R is non-reduced. The difficulty comes from a lack of effective tools, such as the slice theorem. As far as we know, even for $R = \mathbf{Z}/m\mathbf{Z}$ with $m \geq 2$ not square-free, the $\mathbf{G}_a$-actions on $R[x]$ are not completely determined previously.

Now, assume that $m := \operatorname{char} R > 0$, and write $m = p_1^{e_1} \cdots p_t^{e_t}$, where $p_1, \dots, p_t$ are distinct prime numbers and $e_1, \dots, e_t \geq 1$. Then, the ring $A = A/mA$ is isomorphic to $\bigoplus_{i=1}^t (A/p_i^{e_i} A)$ by the Chinese Remainder Theorem. Moreover, every $\mathbf{G}_a$-action σ on A over R induces a $\mathbf{G}_a$-action on $A/p_i^{e_i} A$ over R_i for $i = 1, \dots, t$, where R_i is the image of R in $A/p_i^{e_i} A$. Conversely, for any given $\mathbf{G}_a$-actions σ_i on $A/p_i^{e_i} A$ over R_i for $i = 1, \dots, t$, the map

$$A \simeq \bigoplus_{i=1}^t (A/p_i^{e_i} A) \ni (a_i)_{i=1}^t \mapsto (\sigma_i(a_i))_{i=1}^t \in \bigoplus_{i=1}^t (A/p_i^{e_i} A)[T] \simeq A[T]$$

is a $\mathbf{G}_a$-action on A over R. Therefore, it suffices to consider the case $t = 1$.

Throughout this paper, let p be a prime number and $e \geq 2$ unless otherwise specified. We study a $\mathbf{G}_a$-action σ on A when $\operatorname{char} R = p^e$. We say that σ is *red-trivial* (resp. *red-nontrivial*) if the $\mathbf{G}_a$-action on A/pA induced from σ

is trivial (resp. nontrivial). Equivalently, σ is red-trivial (resp. red-nontrivial) if $\sigma(a) - a \in pA[T]$ for each $a \in A$ (resp. $\sigma(a) - a \notin pA[T]$ for some $a \in A$).

We have the following results for red-nontrivial $\mathbf{G}_a$-actions on $A = R[x]$.

Theorem 1. *Let R be a ring with* $\operatorname{char} R = p^e$ *such that pR is a prime ideal of R and $(p^2R : pR) = pR$. Then, for every red-nontrivial $\mathbf{G}_a$-action σ on $R[x]$, the following assertions hold.*

(i) *There exists $a \in R \backslash pR$ such that $\sigma(x) \in x + aT + pTR[x][T]$.*

(ii) *There exists $y \in R_a[x]$ such that $R_a[x] = R_a[y]$ and $\sigma(y) = y + T$, where R_a is the localization of R by the multiplicatively closed set $\{a^i \mid i \geq 0\}$.*

(iii) *If a is not a zero-divisor of R, then we have $R[x]^\sigma = R$.*

(iv) *If $R[x]^\sigma \neq R$, then the R-algebra $R[x]^\sigma$ is not finitely generated.*

Here are some remarks. We have $(p^2R : pR) = pR$ if and only if $pr \notin p^2R$ for any $r \in R \backslash pR$. Since p is a nilpotent element of R, and pR is a prime ideal of R, we see that pR is the nilradical of R. Since a in (i) is not nilpotent, we have $R_a \neq \{0\}$. If a is not a zero-divisor of R, then $R_a[x]$ contains $R[x]$. Since the invariant ring for the $\mathbf{G}_a$-action on $R_a[x] = R_a[y]$ over R_a defined by $y \mapsto y + T$ is equal to R_a, (iii) follows from (ii) (see also Lemma 3). (iv) is a consequence of a more general result (Theorem 3).

The following is a corollary to Theorem 1.

Corollary 1. *Let R be a ring such that* $\operatorname{char} R = p^e$ *and pR is a maximal ideal of R. Then, for every red-nontrivial $\mathbf{G}_a$-action σ on $R[x]$, the following assertions hold.*

(i) *There exists $y \in R[x]$ such that $R[x] = R[y]$ and $\sigma(y) = y + T$.*

(ii) *We have $R[x]^\sigma = R$.*

In fact, if $\operatorname{char} R = p^e$ and pR is a maximal ideal of R, then R is a zero-dimensional noetherian local ring satisfying $(p^2R : pR) = pR$ (Lemma 7).

For example, Corollary 1 says that, up to a change of variables, every red-nontrivial $\mathbf{G}_a$-action on $(\mathbf{Z}/p^e\mathbf{Z})[x]$ is equal to the $\mathbf{G}_a$-action defined by $x \mapsto x + T$.

To discuss red-trivial $\mathbf{G}_a$-actions, it is convenient to extend the notion of $\mathbf{G}_a$-actions as follows. Note that we can also consider the conditions (A1) and (A2) for a homomorphism $\sigma : A \to A[[T]]$ of R-algebras, where $A[[T]]$ is the formal power series ring in T over A. We call σ an *analytic* $\mathbf{G}_a$*-action* on A (over R) if (A1) and (A2) hold, or equivalently $(\delta_i^\sigma)_{i=0}^\infty$ is a so-called *iterative higher R-derivation* of A (cf. [10, §27]). To avoid confusion, we will sometimes call a $\mathbf{G}_a$-action $\sigma : A \to A[T]$ an *algebraic* $\mathbf{G}_a$*-action* on A. We regard an algebraic $\mathbf{G}_a$-action as an analytic $\mathbf{G}_a$-action satisfying $\sigma(A) \subset A[T]$.

When $\operatorname{char} R = p^e$, we say that an analytic $\mathbf{G}_a$-action σ on A is *red-trivial* if $\sigma(a) - a \in pA[[T]]$ for each $a \in A$. We mainly study such σ in the case $A = R[\boldsymbol{x}]$ with $R = S/p^eS$, where S is a subring of a $\mathbf{Q}$-algebra with $p \notin S^*$. We note that a ring S is a subring of a $\mathbf{Q}$-algebra if and only if $\operatorname{char} S = 0$ and no element of $\mathbf{Z}\setminus\{0\} \subset S$ is a zero-divisor of S. In this case, we have $\operatorname{char} R = p^e$. Actually, $p^{e'} \notin p^eS$ for any $1 \le e' < e$, since p is not a zero-divisor nor a unit of S. We construct a bijection between the set of red-trivial, analytic $\mathbf{G}_a$-actions σ on $R[\boldsymbol{x}]$, and the set of pairs (δ, Δ) of R-derivations $\delta : R[\boldsymbol{x}] \to R[\boldsymbol{x}]$ and $\Delta : R[\boldsymbol{x}] \to R[\boldsymbol{x}][[T]]$ with certain conditions. Under this correspondence, we have $R[\boldsymbol{x}]^\sigma = \ker \delta \cap \ker \Delta$ (Corollary 3 (i)). We also determine the set of pairs (δ, Δ) for which the corresponding analytic $\mathbf{G}_a$-actions on $R[\boldsymbol{x}]$ are algebraic in the following cases (cf. Corollaries 2 and 3 (ii), and Theorem 6 (iii)).

(a) $p \ge 3$. (b) $n = 1$, $p = 2$ and $\sqrt{2S} = 2S$.

Remark 1. Let $\tilde{R} = S/(p_1^{e_1} \cdots p_t^{e_t}S)$, where $p_1, \dots, p_t$ are distinct prime numbers, S is a subring of a $\mathbf{Q}$-algebra such that $p_1S, \dots, p_tS$ are maximal ideals of S, and $e_1, \dots, e_t \ge 1$. Then, we have $\operatorname{char} \tilde{R} = p_1^{e_1} \cdots p_t^{e_t}$, and $R_i := \tilde{R}/p_i^{e_i}\tilde{R} \simeq S/p_i^{e_i}S$ for each i. Moreover, p_iR_i is a maximal ideal of R_i, $\sqrt{p_iS} = p_iS$ and $p_i \notin S^*$. Hence, if $e_i \ge 2$, then we can use Corollary 1 and the results for red-trivial $\mathbf{G}_a$-actions mentioned above for $R = R_i$. If $e_i = 1$, then R_i is a field, and the $\mathbf{G}_a$-actions of $R_i[x]$ are already determined. Therefore, we can determine all the $\mathbf{G}_a$-actions on $\tilde{R}[x]$.

For example, for $R = \mathbf{Z}/m\mathbf{Z}$ with $m \ge 2$, we can determine all the $\mathbf{G}_a$-actions σ on $R[x]$. In this case, $R[x]^\sigma$ is always finitely generated by the following theorem.

Theorem 2. *Let $\tilde{R} = S/(p_1^{e_1} \cdots p_t^{e_t}S)$, where $p_1, \dots, p_t$ are distinct prime numbers, S is a subring of a $\mathbf{Q}$-algebra such that $p_1S, \dots, p_tS$ are prime ideals of S, and $e_1, \dots, e_t \ge 1$. Then, the $\tilde{R}$-algebra $\tilde{R}[x]^\sigma$ is finitely generated for any $\mathbf{G}_a$-action σ on $\tilde{R}[x]$.*

In the situation of Theorem 2, we can describe generators of $\tilde{R}[x]^\sigma$ explicitely. We prove this theorem in Section 8.

This paper is organized as follows. In Section 2, we study finite generation of the invariant ring for a homomorphism $R[x] \to R[x][T]$ of R-algebras with certain conditions, and prove Theorem 1 (iv) as a special case. We also give some examples in which the invariant rings are not finitely generated. The rest of Theorem 1, and Corollary 1 are proved in Section 3. In Section 4, we overview the main results for red-trivial $\mathbf{G}_a$-actions. We discuss the details in Sections 5 through 8. In Section 9, we describe the $\mathbf{G}_a$-actions on $R[x]$ when R is a reduced ring.

2. Non-finitely generated invariant rings

The goal of this section is to prove the following theorem, which includes Theorem 1 (iv) as a special case. For a ring R, we denote by $\mathrm{nil}(R)$ the nilradical of R. For a homomorphism $\sigma : R[x] \to R[x][T]$ of R-algebras, we define the invariant ring as $R[x]^{\sigma} := \{f \in R[x] \mid \sigma(f) = f\}$.

Theorem 3. *Let R be a ring such that $\mathrm{nil}(R)$ is a prime ideal of R, and let $\sigma : R[x] \to R[x][T]$ be a homomorphism of R-algebras such that $\sigma(x) - x$ belongs to $TR[x][T]$, but does not belong to $\mathrm{nil}(R[x][T])$. Then, we have either (1) $R[x]^{\sigma} = R$, or (2) the R-algebra $R[x]^{\sigma}$ is not finitely generated.*

Under the assumption of Theorem 1, the prime ideal pR is equal to $\mathrm{nil}(R)$ as remarked. Hence, we have $pR[x][T] = \mathrm{nil}(R[x][T])$, to which $\sigma(x) - x$ does not belong by red-nontriviality. By (A1), $\sigma(x) - x$ belongs to $TR[x][T]$. Thus, the assumption of Theorem 3 is satisfied. Therefore, Theorem 1 (iv) follows from Theorem 3.

Theorem 3 is proved by combining the following three lemmas. These lemmas hold for any ring S.

Lemma 1. *Let A be a finitely generated S-subalgebra of $S + \mathrm{nil}(S[x])$. Then, $\{\deg f \mid f \in A \setminus \{0\}\}$ is bounded above.*

Proof. Let $f_1, \dots, f_t \in A \setminus \{0\}$ be such that $A = S[f_1, \dots, f_t]$. Since $A \subset S + \mathrm{nil}(S[x])$ by assumption, we may take $f_1, \dots, f_t$ from $\mathrm{nil}(S[x])$. Take $e \geq 1$ so that $f_1^e = \cdots = f_t^e = 0$. Then, $\deg f$ is less than $et \max\{\deg f_i \mid i = 1, \dots, t\}$ for all $f \in S[f_1, \dots, f_t] = A$. □

Lemma 2. *Let $\mathfrak{p} \in \operatorname{Spec} S$, and let $\sigma : S[x] \to S[x][T]$ be a homomorphism of S-algebras such that $\sigma(x) - x$ belongs to $TS[x][T]$, but does not belong to $\mathfrak{p}S[x][T]$. Then, we have $S[x]^{\sigma} \subset S + \mathfrak{p}S[x]$.*

Proof. Suppose that there exists $f(x) \in S[x]^{\sigma}$ not belonging to $S + \mathfrak{p}S[x]$. Then, the image of $f(x)$ in $(S/\mathfrak{p})[x]$ is a polynomial of positive degree. Since $S/\mathfrak{p}$ is an integral domain, and $F := \sigma(x) - x$ lies in $TS[x][T] \setminus \mathfrak{p}S[x][T]$, we see that the image of $\sigma(f(x)) = f(x + F)$ in $(S/\mathfrak{p})[x][T]$ is of positive degree in T, and thus is not equal to the image of $f(x)$. This contradicts that $f(x + F) = \sigma(f(x)) = f(x)$ in $S[x][T]$. □

Lemma 3. *Let $\sigma : S[x] \to S[x][T]$ be a homomorphism of S-algebras with $F := \sigma(x) - x \in TS[x][T] \setminus \{0\}$. If $S[x]^{\sigma} \neq S$, then there exists $a \in S \setminus \{0\}$ such that $aF = 0$.*

Proof. It suffices to show that F is a zero-divisor of $S[x][T]$ (cf. [1, Chapter 1, Exercise 3]). Take any $f(x) \in S[x]^{\sigma} \setminus S$, and write $f(x + T) =$

$f(x) + \sum_{i=1}^{d} f_i T^i$, where $d := \deg f(x)$ and $f_i \in S[x]$. Then, f_d is nonzero, since f_d is the leading coefficient of $f(x)$. Hence, $I := \{i \mid f_i \neq 0\}$ is not empty. Let $l := \min I$. Then, we have $f(x) = \sigma(f(x)) = f(x+F) = f(x) + \sum_{i=l}^{d} f_i F^i$. It follows that $g(x,T)F^l = \sum_{i=l}^{d} f_i F^i = 0$, where $g(x,T) := \sum_{i=0}^{d-l} f_{i+l} F^i$. Since $F \in TS[x][T]$ by assumption, we see that $g(x,0) = f_l \neq 0$. Thus, we get $g(x,T) \neq 0$. Therefore, F is a zero-divisor of $S[x][T]$. □

We remark that, in Lemma 3, ax^l belongs to $S[x]^{\sigma}$ for each $l \geq 1$, since $a(x+F)^l = ax^l$. Hence, $\{\deg f \mid f \in S[x]^{\sigma} \setminus \{0\}\}$ is not bounded above.

Proof (of Theorem 3). Assume that (1) does not hold. Then, by the remark above, $\{\deg f \mid f \in R[x]^{\sigma} \setminus \{0\}\}$ is not bounded above. Noting $\operatorname{nil}(R)R[x] = \operatorname{nil}(R[x])$ and $\operatorname{nil}(R)R[x][T] = \operatorname{nil}(R[x][T])$, we have $R[x]^{\sigma} \subset R + \operatorname{nil}(R[x])$ by Lemma 2. Therefore, we get (2) by Lemma 1. □

Finally, we give some examples of $\mathbf{G}_a$-actions whose invariant rings are not finitely generated. In the following examples, a and b denote variables.

The first one is an example of Theorem 1.

Example 1. Set $R := \mathbf{Z}[a,b]/(p^e, p^2ab, p^3b)$, where p is a prime number, and $e \geq 3$. First, we check that R satisfies the assumptions of Theorem 1. It is easy to see that $\operatorname{char} R = p^e$, and pR is a prime ideal of R. To show $(p^2R : pR) = pR$, it suffices to check that $pr \in p^2R$ implies $r \in pR$ for $r \in R$. Take $f \in \mathbf{Z}[a,b]$ such that $\bar{f} = r$. Since $pr \in p^2R$, there exists $g \in \mathbf{Z}[a,b]$ such that $pf - p^2g \in (p^e, p^2ab, p^3b)$. This implies $f \in p\mathbf{Z}[a,b]$, and so $r = \bar{f} \in pR$.

Now, we define a $\mathbf{G}_a$-action σ on $R[x]$ by $\sigma(x) = x + aT$. Then, σ is red-nontrivial, and $\sigma(p^2bx) = p^2b(x+aT) = p^2bx$. Hence, we have $R[x]^{\sigma} \neq R$. Therefore, the R-algebra $R[x]^{\sigma}$ is not finitely generated by Theorem 1 (iv).

Next, we give an example of Theorem 3 in the case $\operatorname{char} R = 0$.

Example 2. Set $R := \mathbf{Z}[a,b]/(a^2, ab)$. Then, we have $\operatorname{char} R = 0$, and $\operatorname{nil}(R) = aR \in \operatorname{Spec} R$. We define a $\mathbf{G}_a$-action σ on $R[x]$ by $\sigma(x) = x + bT$. Since $\sigma(ax) = a(x+b) = ax$, we have $R[x]^{\sigma} \neq R$. Therefore, $R[x]^{\sigma}$ is not finitely generated by Theorem 3.

In the following example, $\sigma(x) - x$ belongs to $\operatorname{nil}(R[x][T])$.

Example 3. Let S be a subring of a $\mathbf{Q}$-algebra. Then, $R := S[a]/(a^e)$ is also a subring of a $\mathbf{Q}$-algebra, where $e \geq 2$. We define a $\mathbf{G}_a$-action σ on $R[x]$ by $\sigma(x) = x + a^{e-1}T$. Then, we claim that $R[x]^{\sigma} = R + aR[x]$. In fact, for $f(x) \in R[x]$, we have $f(x + a^{e-1}T) = f(x) + a^{e-1}T\, df/dx$, in which $a^{e-1}\, df/dx = 0$ if and only if $f(x) \in R + aR[x]$. By Lemma 1, the R-algebra $R + aR[x]$ is not finitely generated.

In Example 3, if we replace S with a ring with $m := \operatorname{char} S > 0$, then $R[x]^\sigma$ contains $R[x^m]$, since $dx^m/dx = 0$. Hence, $R[x]$ is integral over $R[x]^\sigma$. If R is noetherian, this implies that the R-algebra $R[x]^\sigma$ is finitely generated (cf. [1, Proposition 7.8]).

3. Red-nontrivial $\mathbf{G}_a$-actions on the affine lines

In this section, we prove (i) and (ii) of Theorem 1, and Corollary 1.

Lemma 4. *Let K be a field. Then, for any $f(T) \in K[T]\setminus K$, we have*

$$K[f(T), U] \cap K[T, f(U)] = K[f(T), f(U)].$$

Proof. Set $d := \deg f(T)$ and $B := K[f(T), f(U)]$. Since K is a field, we may assume that $f(T)$ is monic. Then, $A[T] = \bigoplus_{i=0}^{d-1} A[f(T)]T^i$ holds for any ring A. Hence, we have $K[T, f(U)] = \bigoplus_{i=0}^{d-1} BT^i$, $K[f(T), U] = \bigoplus_{j=0}^{d-1} BU^j$ and

$$K[T, U] = \bigoplus_{i=0}^{d} K[f(T), U]T^i = \bigoplus_{i=0}^{d}\bigoplus_{j=0}^{d} BT^iU^j.$$

This implies that $K[f(T), U] \cap K[T, f(U)] = B$. □

Let R be any ring, and σ a $\mathbf{G}_a$-action on $R[x]$. Then, $F(x, T) := \sigma(x) - x$ belongs to $TR[x][T]$ by (A1). By (A2), we have $\sigma(x) + F(\sigma(x), U) = x + F(x, T + U)$, which is equivalent to

$$F(x + F(x, T), U) = F(x, T + U) - F(x, T). \tag{3.1}$$

The following lemma is well known.

Lemma 5. *If R is an integral domain, then we have $F(x, T) \in R[T]$, and so $F(x, T + U) = F(x, T) + F(x, U)$ by* (3.1). *This implies $F(x, T) \in RT$ when* $\operatorname{char} R = 0$, *and $F(x, T) \in \sum_{i \geq 0} RT^{p^i}$ when $p :=$* $\operatorname{char} R > 0$.

Proof. It suffices to verify $F(x, T) \in R[T]$ (see Lemma 8 for the last statement). Set $\delta := \deg_T F(x, T)$. Then, as a polynomial in T and U, the right-hand side of (3.1) is of total degree δ. Suppose that $F(x, T) \notin R[T]$. Let $l \geq 1$ be such that the coefficient of T^l in $F(x, T)$ is of x-degree $m \geq 1$. Then, since R is an integral domain, the monomial $x^tT^{\delta m}U^l$ appears in the left-hand side of (3.1) for some $t \geq 0$, which is absurd. □

Now, let R be as in Theorem 1, and assume that σ is red-nontrivial. Write $F(x, T) = \sum_{i,j} \alpha_{i,j}x^iT^j$, where $\alpha_{i,j} \in R$. Let I_0, I_1, and I_2 be the sets of (i, j) such that $\alpha_{i,j} \notin pR$, $\alpha_{i,j} \in pR\setminus p^2R$, and $\alpha_{i,j} \in p^2R$, respectively.

For $l = 0, 1, 2$, take $f_l(x, T) \in TR[x][T]$ so that $\sum_{(i,j)\in I_l} \alpha_{i,j} x^i T^j = p^l f_l(x, T)$. Then, we have $F(x, T) = \sum_{l=0}^{2} p^l f_l(x, T)$. For $l = 0, 1$, the coefficient of each monomial appearing in $f_l(x, T)$ does not belong to $pR \backslash \{0\}$. Moreover, we have $f_0(x, T) \neq 0$ by red-nontriviality.

Since R/pR is an integral domain of characteristic p, the image of $F(x, T)$ in $(R/pR)[x][T]$ belongs to $\sum_{i\geq 0}(R/pR)T^{p^i}$ by Lemma 5. Since $\alpha_{i,j} \notin pR$ for each $(i, j) \in I_0$, it follows that $f_0(x, T)$ belongs to $\sum_{i\geq 0} RT^{p^i}$. So, we write

$$f(T) := f_0(x, T) = \sum_{i=0}^{d} a_i T^{p^i}, \tag{3.2}$$

where $d \geq 0$, and $a_0, \dots, a_d \in (R \backslash pR) \cup \{0\}$ with $a_d \neq 0$.

Proof (of Theorem 1 (i)). Our goal is to show that $d = 0$. By (3.1), we have

$$\begin{aligned} &F(x, T + U) - F(x, T) - F(x, U) \\ &\quad = F(x + F(x, T), U) - F(x, U) \\ &\quad \equiv pf_1(x + f(T), U) - pf_1(x, U) \qquad (\mathrm{mod}\ p^2R[x][T, U]), \end{aligned} \tag{3.3}$$

since $f_0(x, T)$ is independent of x. Set $q_l := (T + U)^l - T^l - U^l$ for each $l \geq 1$. Then, q_l belongs to $pR[T, U]$ whenever l is a power of p. Hence, we have

$$f(T + U) - f(T) - f(U) = \sum_{i=0}^{d} a_i q_{p^i} = pg(T, U) \tag{3.4}$$

for some symmetric polynomial $g(T, U) \in R[T, U]$.

Now, suppose that $d \geq 1$. If we regard q_{p^d} as an element of $\mathbf{Z}[T, U]$, then the coefficient $\binom{p^d}{p^{d-1}}$ of the monomial $M := T^{p^{d-1}} U^{p^d - p^{d-1}}$ in q_{p^d} has the form pu for some $u \in \mathbf{Z} \backslash p\mathbf{Z}$. Since the coefficient of M in (3.4) is pua_d, we may take $g(T, U)$ so that the coefficient of M in $g(T, U)$ is ua_d. We note that ua_d lies in $R \backslash pR$, since $u \in (\mathbf{Z}/p^e\mathbf{Z})^* \subset R^*$ and $a_d \in R \backslash pR$. To obtain a contradiction, we first investigate the structure of $g(T, U)$.

By (3.4), the left-hand side of (3.3) is congruent to $p(g(T, U) + f_1(x, T + U) - f_1(x, T) - f_1(x, U))$ modulo $p^2R[x][T, U]$. Since $(p^2R : pR) = pR$ by assumption, it follows that

$$\begin{aligned} &g(T, U) + f_1(x, T + U) - f_1(x, T) - f_1(x, U) \\ &\quad \equiv f_1(x + f(T), U) - f_1(x, U) \qquad (\mathrm{mod}\ pR[x][T, U]). \end{aligned} \tag{3.5}$$

In the rest of the proof, $f(T)$, $g(T,U)$, $f_1(x,T)$ and q_l denote their images in $(R/pR)[x][T,U]$. Write

$$f_1(x,T) = \sum_{i\geq 0} h_i(T)x^i, \qquad \text{where } h_i(T) \in T(R/pR)[T],$$

and set

$$h(T,U) := h_0(T+U) - h_0(T) - h_0(U) = f_1(0,T+U) - f_1(0,T) - f_1(0,U).$$

Then, from (3.5) with $x = 0$, we get

$$P := g(T,U) + h(T,U) = f_1(f(T),U) - f_1(0,U) = \sum_{i\geq 1} h_i(U)f(T)^i. \tag{3.6}$$

Let K be the field of fractions of R/pR. Then, P belongs to $K[f(T),U]$. Since $P = g(T,U) + h(T,U)$ is a symmetric polynomial, P also belongs to $K[T,f(U)]$. Thus, P belongs to $K[f(T),f(U)]$ by Lemma 4.

Set $P_i := f(T+U)^i - f(T)^i - f(U)^i$ for each $i \geq 1$. Since $\operatorname{char} K = p$, we have $f(T+U) = f(T) + f(U)$ by (3.2) (cf. Section 4.1). Hence, P_i belongs to $K[f(T),f(U)]$. Since $f(T)^i \in a_d^i T^{ip^d} + \sum_{j=i}^{ip^d-1} KT^j$ by (3.2), we also have $P_i \in a_d^i q_{ip^d} + \sum_{j=i}^{ip^d-1} Kq_j$.

Now, choose $P' \in \sum_{i\geq 1} KP_i$ so that the total degree μ of

$$P - P' = g(T,U) + h(T,U) - P' \tag{3.7}$$

is minimal. Note that P' lies in $\sum_{i\geq 1} Kq_i$ and $K[f(T),f(U)]$. We show that $\mu \leq p^d$ by contradiction. Suppose that $\mu > p^d$. Then, since $\deg g(T,U) \leq \deg f(T) = p^d$ by (3.4), the highest homogeneous part H of $P - P'$ is equal to that of $h(T,U) - P'$. We claim that $h(T,U) - P' \in \sum_{i\geq 1} Kq_i$ and $P - P' \in K[f(T),f(U)]$, since $h(T,U) \in \sum_{i\geq 1} Kq_i$ by construction, and $P \in K[f(T), f(U)]$ as mentioned. Because q_i is either zero or a homogeneous polynomial of degree i for each i, it follows that $H = sq_\mu$ for some $s \in K^*$. Since $f(T)$ and $f(U)$ are of degree p^d, we can write $\mu = \deg(P - P') = \mu' p^d$, where $\mu' \geq 2$. Then, $sa_d^{-\mu'} P_{\mu'}$ belongs to $sq_\mu + \sum_{j<\mu} Kq_j = H + \sum_{j<\mu} Kq_j$. Hence, we get $\deg(P - P' - sa_d^{-\mu'} P_{\mu'}) < \mu$. This contradicts the minimality of μ, proving $\mu \leq p^d$. Therefore, noting $P - P' \in K[f(T),f(U)]$, we can write $P - P' = \alpha f(T) + \beta f(U) + \gamma$, where $\alpha, \beta, \gamma \in K$. Then, (3.7) gives that

$$g(T,U) = \alpha f(T) + \beta f(U) + \gamma + P' - h(T,U). \tag{3.8}$$

As mentioned before, the monomial M appears in $g(T,U)$ with coefficient $ua_d \in K^*$. Clearly, M does not appear in $\alpha f(T) + \beta f(U) + \gamma$. Since q_{p^d} is zero in $K[T,U]$, and no monomial of degree p^d appears in p_l for $l \neq p^d$, we see that M does not appear in $P' - h(T, U) \in \sum_{l \geq 1} Kq_l$. Therefore, M does not appear in the right-hand side of (3.8). This is a contradiction. □

Our next goal is to prove Theorem 1 (ii). Let S be any ring. Recall that $y = \sum_{i \geq 0} b_i x^i \in S[x]$ satisfies $S[y] = S[x]$ if and only if $b_1 \in S^*$ and $b_i \in \mathrm{nil}(S)$ for all $i \geq 2$ (cf. Remark after Lemma 5 of [12]). Hence, if q is an element of $\mathrm{nil}(S)$, then $S[y] = S[x]$ holds for each $y \in S^* x + qS[x]$.

Lemma 6. *Let σ be a $\mathbf{G}_a$-action on $S[x]$ such that $\sigma(x) \in x + T + qS[x][T]$ for some $q \in \mathrm{nil}(S)$. Then, there exists $y \in x + qS[x]$ such that $\sigma(y) = y + T$.*

Proof. Suppose that the assertion is false. Then, we can find the greatest $l \in \mathbf{Z}$ for which there exists $y \in x + qS[x]$ such that $\sigma(y) \in y + T + q^l S[x][T]$, since $q \in \mathrm{nil}(S)$. Since $\sigma(x) \in x + T + qS[x][T]$ by assumption, we have $l \geq 1$. Take $y \in x + qS[x]$ and $g \in S[x][T]$ such that $\sigma(y) = y + T + q^l g$. We write $g = g(y, T)$, since $S[y] = S[x]$ as remarked. Then, (A2) yields

$$\sigma(y) + U + q^l g(\sigma(y), U) = y + (T + U) + q^l g(y, T + U). \tag{3.9}$$

Since $l \geq 1$, we have $q^l g(\sigma(y), U) \equiv q^l g(y + T, U)$ modulo $\mathfrak{a} := q^{l+1} S[x][T, U]$. Hence, (3.9) gives that

$$q^l g(y, T) + q^l g(y + T, U) \equiv q^l g(y, T + U) \qquad (\mathrm{mod}\ \mathfrak{a}).$$

Set $g_1(y) := g(0, y)$. Then, this congruence, with $U \mapsto T$, $T \mapsto y$ and $y \mapsto 0$, gives that

$$q^l g_1(y) + q^l g(y, T) \equiv q^l g_1(y + T) \qquad (\mathrm{mod}\ \mathfrak{a}). \tag{3.10}$$

Now, set $z := y - q^l g_1(y) \in x + qS[x]$. Then, we have

$$\begin{aligned} \sigma(z) = \sigma(y) - q^l g_1(\sigma(y)) &\equiv (y + T + q^l g(y, T)) - q^l g_1(y + T) \\ &\equiv y + T - q^l g_1(y) = z + T \qquad (\mathrm{mod}\ \mathfrak{a}) \end{aligned}$$

by (3.10). Hence, $\sigma(z) - z - T$ belongs to $\mathfrak{a} \cap S[x][T] = q^{l+1} S[x][T]$. This contradicts the maximality of l. □

Proof (of Theorem 1 (ii)). Let $a \in R \backslash pR$ be as in Theorem 1 (i), and set $z := a^{-1} x \in R_a[x]$. Then, $\sigma(z)$ belongs to $z + T + pR_a[x][T]$. Since $p \in \mathrm{nil}(R)$, we know by Lemma 6 that $\sigma(y) = y + T$ for some $y \in z + pR_a[z] \subset (R_a)^* x + pR_a[x]$. This y satisfies $R_a[y] = R_a[x]$ as remarked above. □

Finally, we derive Corollary 1 from Theorem 1.

Lemma 7. *If R is a ring such that* $\mathrm{char}\, R = p^e$ *with $e \geq 2$, and pR is a maximal ideal of R, then R is a zero-dimensional noetherian local ring, and $(p^2 R : pR) = pR$.*

Proof. Note that $pR \subset \operatorname{nil}(R)$. Since pR is a maximal ideal of R by assumption, and every prime ideal of R contains $\operatorname{nil}(R)$, we see that pR is the unique prime ideal of R. Hence, R is a zero-dimensional local ring. The set of ideals of R is $\{p^d R \mid 0 \leq d < e\}$, since each $r \in R \backslash \{0\}$ has the form $r = p^d s$ for some $0 \leq d < e$ and $s \in R \backslash pR = R^*$. Hence, R is noetherian. If $(p^2 R : pR) \neq pR$, then $pr = p^2 s$ holds for some $r \in R \backslash pR = R^*$ and $s \in R$. Since $r - ps \in R^*$ and $p(r - ps) = pr - p^2 s = 0$, we get $p = 0$. This contradicts $e \geq 2$. □

Proof (of Corollary 1). By Lemma 7, R satisfies the assumption of Theorem 1. Moreover, since R is a local ring with maximal ideal pR, we have $R_a = R$ for every $a \in R \backslash pR = R^*$. Therefore, the assertion follows from (ii) and (iii) of Theorem 1. □

4. Theory of red-trivial $\mathbf{G}_a$-actions

Sections 4 through 8 are devoted to the study of red-trivial $\mathbf{G}_a$-actions. In this section, we overview our main results.

Let R be any ring, and A any R-algebra. For an A-module M, an R-linear map $D : A \to M$ is called an *R-derivation* if $D(ab) = bD(a) + aD(b)$ holds for each $a, b \in A$. The A-module consisting of all R-derivations $A \to M$ is denoted by $\operatorname{Der}_R(A, M)$. For each A-submodule M' of M, we regard $\operatorname{Der}_R(A, M')$ as an A-submodule of $\operatorname{Der}_R(A, M)$ in a natural way. We write $\operatorname{Der}_R A := \operatorname{Der}_R(A, A)$, where the scalar multiplication of $M = A$ is the ring multiplication, and call $D \in \operatorname{Der}_R A$ an *R-derivation of A*. We remark that δ_1^σ is an R-derivation of A for any analytic $\mathbf{G}_a$-action σ on A, since $(ab + \delta_1^\sigma(ab)T + \cdots) = (a + \delta_1^\sigma(a)T + \cdots)(b + \delta_1^\sigma(b)T + \cdots)$ for each $a, b \in A$.

Now, assume that $\operatorname{char} R = p^e$. Let $\mathrm{RT}_R(A)$ (resp. $\mathrm{RT}'_R(A)$) be the set of red-trivial, algebraic (resp. analytic) $\mathbf{G}_a$-actions on A over R. We define an equivalence relation on $\mathrm{RT}_R(A)$ (resp. $\mathrm{RT}'_R(A)$) by $\sigma \sim \tau$ if $\delta_1^\sigma = \delta_1^\tau$ for $\sigma, \tau \in \mathrm{RT}_R(A)$ (resp. $\sigma, \tau \in \mathrm{RT}'_R(A)$), and denote by $[\sigma]$ (resp. $[\sigma]'$) the equivalence class of $\sigma \in \mathrm{RT}_R(A)$ (resp. $\sigma \in \mathrm{RT}'_R(A)$). Note that

$$\mathrm{RT}_R(A)_1 := \{\delta_1^\sigma \mid \sigma \in \mathrm{RT}_R(A)\} \qquad \text{and} \qquad \mathrm{RT}'_R(A)_1 := \{\delta_1^\sigma \mid \sigma \in \mathrm{RT}'_R(A)\}$$

are subsets of $\operatorname{Der}_R(A, pA)$, which are regarded as the quotient spaces of $\mathrm{RT}_R(A)$ and $\mathrm{RT}'_R(A)$, respectively. Our first task is to describe $[\sigma]$ and $[\tau]'$ for $\sigma \in \mathrm{RT}_R(A)$ and $\tau \in \mathrm{RT}'_R(A)$. By definition, we have $[\sigma] = [\sigma]' \cap \mathrm{RT}_R(A)$ for each $\sigma \in \mathrm{RT}_R(A)$.

4.1. Additive polynomials and power series. Let $f(T) = \sum_{i \geq 0} a_i T^i \in A[[T]]$, where $a_i \in A$. We say that $f(T)$ is *additive* if $f(T + U) = f(T) + f(U)$, or equivalently $a_i(T+U)^i = a_iT^i + a_iU^i$ for all $i \geq 0$. Clearly, aT is additive for any $a \in A$. If $\operatorname{char} A = p$, then aT^{p^k} is also additive for any $a \in A$ and $k \geq 0$. In fact, the following lemma holds for any ring A (cf. [7, Lemma 2.3]).

Lemma 8. *For an integer $l \geq 2$ and $a \in A \backslash \{0\}$, we have $a(T+U)^l = a(T^l + U^l)$ if and only if there exist $d \geq 1$ and a prime number q such that $l = q^d$ and $\{m \in \mathbf{Z} \mid ma = 0\} = q\mathbf{Z}$.*

Note that, for a prime number q and $a \in A \backslash \{0\}$, we have $\{m \in \mathbf{Z} \mid ma = 0\} = q\mathbf{Z}$ if and only if $qa = 0$, since $\{m \in \mathbf{Z} \mid ma = 0\}$ is a proper ideal of $\mathbf{Z}$.

We denote by $A[[T]]^{(p)}$ (resp. $A[[T]]_+^{(p)}$) the set of $f \in A[[T]]$ of the form $f = \sum_{i \geq 0} b_i T^{p^i}$ (resp. $f = \sum_{i \geq 1} b_i T^{p^i}$) for some $b_i \in A$. We set $A[T]^{(p)} := A[[T]]^{(p)} \cap A[T]$ and $A[T]_+^{(p)} := A[[T]]_+^{(p)} \cap A[T]$. Elements of $A[T]^{(p)}$ are often called *p-polynomials*.

Let M be an A-module, and $m \in M$. Then, for each $D \in \operatorname{Der}_R A$, the map $Dm : A \ni a \mapsto D(a)m \in M$ is an R-derivation. If $\mathcal{D}$ is an A-submodule of $\operatorname{Der}_R A$, then $\mathcal{D}m := \{Dm \mid D \in \mathcal{D}\}$ is an A-submodule of $\operatorname{Der}_R(A, M)$. In this notation, for each $a \in A$, the A-module $\operatorname{Der}_R(A, aA[[T]]^{(p)})$ is the direct product of $\operatorname{Der}_R(A, aA)T^{p^i}$ for $i \geq 0$. If the R-algebra A is finitely generated, then $\operatorname{Der}_R(A, aA[T]^{(p)})$ is the direct sum of $\operatorname{Der}_R(A, aA)T^{p^i}$ for $i \geq 0$.

4.2. Equivalence classes. Let R be any ring with $\operatorname{char} R = p^e$, and A any R-algebra. Let $\mathcal{M}$ be the set of $\varDelta \in \operatorname{Der}_R(A, A[[T]])$ such that $p\varDelta = 0$. We define

$$\mathscr{D}' := \operatorname{Der}_R(A, pA[[T]]^{(p)}) \cap \mathcal{M}, \qquad \mathscr{D}'_+ := \operatorname{Der}_R(A, pA[[T]]_+^{(p)}) \cap \mathcal{M},$$

$$\mathscr{D} := \operatorname{Der}_R(A, pA[T]^{(p)}) \cap \mathcal{M}, \qquad \mathscr{D}_+ := \operatorname{Der}_R(A, pA[T]_+^{(p)}) \cap \mathcal{M}.$$

Remark 2. (i) For each $\varDelta \in \mathscr{D}'$ and $a \in A$, we have $p\varDelta(a) = 0$ and $\varDelta(a) \in A[[T]]^{(p)}$. Hence, $\varDelta(a)$ is additive by Lemma 8.

(ii) Since $\operatorname{char} R = p^e$ and $e \geq 2$, we see that $\mathscr{D}' \supset \operatorname{Der}_R(A, p^{e-1}A[[T]]^{(p)})$. If $e = 2$, then we have $\mathscr{D}' = \operatorname{Der}_R(A, pA[[T]]^{(p)})$. Similar statements hold for $\mathscr{D}'_+$, $\mathscr{D}$ and $\mathscr{D}_+$.

Let $\operatorname{Hom}_R(A, A[[T]])$ be the R-module consisting of all R-linear maps $A \to A[[T]]$. Then, $\mathrm{RT}'_R(A)$ and $\operatorname{Der}_R(A, A[[T]])$ are contained in $\operatorname{Hom}_R(A, A[[T]])$. For each $\mathcal{S}, \mathcal{S}' \subset \operatorname{Hom}_R(A, A[[T]])$ and $\psi \in \operatorname{Hom}_R(A, A[[T]])$, we define

$$\mathcal{S} + \mathcal{S}' := \{\phi + \phi' \mid \phi \in \mathcal{S},\ \phi' \in \mathcal{S}'\} \qquad \text{and} \qquad \psi + \mathcal{S} := \{\psi + \phi \mid \phi \in \mathcal{S}\}.$$

We prove the following theorem in Section 5.

Theorem 4. *Let R be any ring with* $\operatorname{char} R = p^e$*, and A any R-algebra with* $\operatorname{Ann}_A(p) = \operatorname{Ann}_R(p)A$*. Then, the following assertions hold.*

(i) *We have* $\mathrm{RT}'_R(A) + \mathscr{D}' \subset \mathrm{RT}'_R(A)$ *and* $\mathrm{RT}_R(A) + \mathscr{D} \subset \mathrm{RT}_R(A)$.

(ii) *We have* $[\sigma]' = \sigma + \mathscr{D}'_+$ *for each* $\sigma \in \mathrm{RT}'_R(A)$.

(iii) *We have* $[\sigma] = \sigma + \mathscr{D}_+$ *for each* $\sigma \in \mathrm{RT}_R(A)$.

The following corollary is a consequence of Theorem 4, where $\imath$ is the trivial $\mathbf{G}_a$-action on A.

Corollary 2. *Let R and A be as in Theorem* 4. *If $e = 2$, then we have* $\mathrm{RT}'_R(A)_1 = \mathrm{RT}_R(A)_1 = \mathrm{Der}_R(A, pA)$, $\mathrm{RT}'_R(A) = \imath + \mathscr{D}'$ *and* $\mathrm{RT}_R(A) = \imath + \mathscr{D}$.

Proof. By Theorem 4 (i), we have $\imath + \mathscr{D}' \subset \mathrm{RT}'_R(A)$ and $\imath + \mathscr{D} \subset \mathrm{RT}_R(A)$. Moreover, since $e = 2$, we know by Remark 2 (ii) that

$$\mathscr{D}' = \mathrm{Der}_R(A, pA)T + \mathscr{D}'_+ \qquad \text{and} \qquad \mathscr{D} = \mathrm{Der}_R(A, pA)T + \mathscr{D}_+.$$

Hence, we get $\mathrm{RT}'_R(A)_1 = \mathrm{RT}_R(A)_1 = \mathrm{Der}_R(A, pA)$. Thus, $\imath + \mathscr{D}'$ and $\imath + \mathscr{D}$ contain systems of representatives for the equivalence relations on $\mathrm{RT}'_R(A)$ and $\mathrm{RT}_R(A)$, respectively. Thanks to (ii) and (iii) of Theorem 4, this implies that $\mathrm{RT}'_R(A) = \imath + \mathscr{D}'$ and $\mathrm{RT}_R(A) = \imath + \mathscr{D}$. □

In the following, we consider the case where A is the polynomial ring $R[\boldsymbol{x}] = R[x_1, \dots, x_n]$.

Remark 3. (i) $\operatorname{Ann}_{R[\boldsymbol{x}]}(s) = \operatorname{Ann}_R(s)R[\boldsymbol{x}]$ holds for each $s \in R$, since $f \in R[\boldsymbol{x}]$ satisfies $sf = 0$ if and only if all the coefficients of f belongs to $\operatorname{Ann}_R(s)$. Therefore, the conclusion of Theorem 4 holds for $A = R[\boldsymbol{x}]$.

(ii) For each $a \in R[\boldsymbol{x}]$, we have $a\,\mathrm{Der}_R\, R[\boldsymbol{x}] \subset \mathrm{Der}_R(R[\boldsymbol{x}], aR[\boldsymbol{x}])$. If δ is in $\mathrm{Der}_R(R[\boldsymbol{x}], aR[\boldsymbol{x}])$, then $\delta = \sum_{i=1}^n \delta(x_i)\partial/\partial x_i = a\sum_{i=1}^n f_i\partial/\partial x_i \in a\,\mathrm{Der}_R\, R[\boldsymbol{x}]$, where we write $\delta(x_i) = af_i$ with $f_i \in R[\boldsymbol{x}]$. Hence, we get $\mathrm{Der}_R(R[\boldsymbol{x}], aR[\boldsymbol{x}]) = a\,\mathrm{Der}_R\, R[\boldsymbol{x}]$.

(iii) We have

$$\mathrm{RT}_R(R[\boldsymbol{x}])_1 \subset \mathrm{RT}'_R(R[\boldsymbol{x}])_1 \subset \mathrm{Der}_R(R[\boldsymbol{x}], pR[\boldsymbol{x}]) = p\,\mathrm{Der}_R\, R[\boldsymbol{x}].$$

4.3. Lifts and restrictions. Let S be a ring in which p is not a zero-divisor nor a unit. Then, S is of characteristic zero, and $R := S/p^eS$ is of characteristic p^e. For each $f \in S[\boldsymbol{x}]$, we denote by $\bar{f}$ the image of f in $R[\boldsymbol{x}]$.

Lemma 9. *Let $R = S/p^eS$ be as above, and let $1 \le v < u \le e$. Then, $p^va \in p^uR$ implies $a \in p^{u-v}R$ for $a \in R$. Hence, we have $(p^uR : p^vR) = p^{u-v}R$.*

Proof. Take $\alpha \in S$ with $\bar{\alpha} = a$. If $p^va \in p^uR$, then $p^v\alpha - p^u\beta \in p^eS$ for some $\beta \in S$. Since $1 \le v < u \le e$, and p is not a zero-divisor of S, it follows that $\alpha \in p^{u-v}\beta + p^{e-v}S \subset p^{u-v}S$. Therefore, we have $a \in p^{u-v}R$. □

Using Lemma 9 for $u = e$ and $v = 1$, we get $\mathrm{Ann}_R(p) = p^{e-1}R$. This implies that $\mathrm{Ann}_{R[\boldsymbol{x}][[T]]}(p) = p^{e-1}R[\boldsymbol{x}][[T]]$. Since $\Delta \in \mathrm{Der}_R(R[\boldsymbol{x}], R[\boldsymbol{x}][[T]])$ satisfies $p\Delta = 0$ if and only if $\Delta(R[\boldsymbol{x}]) \subset \mathrm{Ann}_{R[\boldsymbol{x}][[T]]}(p)$, we know that $\mathcal{M} = \mathrm{Der}_R(R[\boldsymbol{x}], p^{e-1}R[\boldsymbol{x}][[T]])$. Then, the following proposition is readily verified.

Proposition 1. *Let $R = S/p^eS$ be as above and $A = R[\boldsymbol{x}]$. Then, we have*

$$\mathscr{D}' = \mathrm{Der}_R(R[\boldsymbol{x}], p^{e-1}R[\boldsymbol{x}][[T]]^{(p)}), \qquad \mathscr{D}'_+ = \mathrm{Der}_R(R[\boldsymbol{x}], p^{e-1}R[\boldsymbol{x}][[T]]_+^{(p)}),$$

$$\mathscr{D} = \mathrm{Der}_R(R[\boldsymbol{x}], p^{e-1}R[\boldsymbol{x}][T]^{(p)}), \qquad \mathscr{D}_+ = \mathrm{Der}_R(R[\boldsymbol{x}], p^{e-1}R[\boldsymbol{x}][T]_+^{(p)}).$$

For each $\delta \in \mathrm{Der}_R\, R[\boldsymbol{x}]$, there exist $g_1, \dots, g_n \in S[\boldsymbol{x}]$ such that $\overline{g_i} = \delta(x_i)$ for $i = 1, \dots, n$. Then, $D := \sum_{i=1}^n g_i \partial/\partial x_i \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ satisfies $\overline{D(f)} = \delta(\bar{f})$ for each $f \in S[\boldsymbol{x}]$. We call D a *lift* of δ. Lifts of δ are not uniquely determined by δ. However, if δ lies in $p\,\mathrm{Der}_R\, R[\boldsymbol{x}]$, then any lift of δ lies in $p\,\mathrm{Der}_S\, S[\boldsymbol{x}]$, since $\bar{f} \in pR[\boldsymbol{x}]$ implies $f \in pS[\boldsymbol{x}]$ for any $f \in S[\boldsymbol{x}]$.

In the rest of Section 4, we consider the case $R = S/p^eS$, where

$$S \text{ is a subring of a } \mathbf{Q}\text{-algebra with } p \notin S^*. \tag{4.1}$$

In this case, no element of $\mathbf{Z} \setminus \{0\}$ is a zero-divisor of S. Let $S_{\mathcal{U}_0}$ and $S_{\mathcal{U}_1}$ be the localizations of S by the multiplicatively closed sets $\mathcal{U}_0 := \mathbf{Z} \setminus \{0\}$ and $\mathcal{U}_1 := \mathbf{Z} \setminus p\mathbf{Z}$, respectively. Then, we have $S \subset S_{\mathcal{U}_1} \subset S_{\mathcal{U}_0}$ and $\mathbf{Q} \subset S_{\mathcal{U}_0}$. Let τ be an analytic $\mathbf{G}_a$-action on $S_{\mathcal{U}_0}[\boldsymbol{x}]$ over $S_{\mathcal{U}_0}$. We say that τ *restricts to* $S_{\mathcal{U}_1}[\boldsymbol{x}]$ if $\tau(S_{\mathcal{U}_1}[\boldsymbol{x}]) \subset S_{\mathcal{U}_1}[\boldsymbol{x}][[T]]$, or equivalently $\delta_l^\tau(x_i) \in S_{\mathcal{U}_1}[\boldsymbol{x}]$ for each $l \geq 1$ and $i = 1, \dots, n$. When this is the case, τ induces an analytic $\mathbf{G}_a$-action σ on $(S_{\mathcal{U}_1}/p^eS_{\mathcal{U}_1})[\boldsymbol{x}] \simeq R[\boldsymbol{x}]$.

Remark 4. For σ and τ as above, the following statements hold.

(i) σ is red-trivial if $\delta_l^\tau(x_i) \in pS_{\mathcal{U}_1}[\boldsymbol{x}]$ for all $l \geq 1$ and $i = 1, \dots, n$.

(ii) σ is an algebraic $\mathbf{G}_a$-action if there exists $N > 0$ as follows: For any $l \geq N$ and $i = 1, \dots, n$, we have $\delta_l^\tau(x_i) \in p^eS_{\mathcal{U}_1}[\boldsymbol{x}]$.

4.4. Exponential actions.

In the case $\mathbf{Q} \subset R$, the following fact is well known (cf. [10, §27]): For each $\delta \in \mathrm{Der}_R\, A$, an analytic $\mathbf{G}_a$-action $\exp T\delta$ on A is defined by

$$\exp T\delta : A \ni a \mapsto \sum_{l \geq 0} \frac{\delta^l(a)}{l!} T^l \in A[[T]].$$

Conversely, every analytic $\mathbf{G}_a$-action σ on A is equal to $\exp T\delta_1^\sigma$. Thus, σ is uniquely determined by δ_1^σ, and $A^\sigma = \ker \delta_1^\sigma$. We note that, for $\delta \in \mathrm{Der}_R\, R[\boldsymbol{x}]$, the $\mathbf{G}_a$-action $\exp T\delta$ is algebraic if and only if δ is *locally nilpotent*, i.e., for each $a \in A$, there exists $l \geq 0$ such that $\delta^l(a) = 0$.

Now, let $R = S/p^eS$ be as in (4.1). Since $S_{\mathcal{U}_0}$ contains $\mathbf{Q}$, each $D \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ induces the analytic $\mathbf{G}_a$-action $\exp TD$ on $S_{\mathcal{U}_0}[\boldsymbol{x}]$, where we extend D to an $S_{\mathcal{U}_0}$-derivation of $S_{\mathcal{U}_0}[\boldsymbol{x}]$ in a natural way.

We prove the following theorem in Section 6.

Theorem 5. *Let $R = S/p^eS$, where S is a subring of a $\mathbf{Q}$-algebra with $p \notin S^*$. Then, the following assertions hold for each $\delta \in p\,\mathrm{Der}_R\, R[\boldsymbol{x}]$.*

(i) *For any lift $D \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ of δ, the analytic $\mathbf{G}_a$-action $\exp TD$ on $S_{\mathcal{U}_0}[\boldsymbol{x}]$ restricts to $S_{\mathcal{U}_1}[\boldsymbol{x}]$, and induces a red-trivial, analytic $\mathbf{G}_a$-action ε on $R[\boldsymbol{x}]$ such that $\delta_1^{\varepsilon} = \delta$.*

(ii) *ε is uniquely determined by δ, and independent of the choice of the lift D of δ.*

(iii) *We have $\ker\delta = R[\boldsymbol{x}]^{\varepsilon}$.*

(iv) *If one of the following holds, then ε is an algebraic $\mathbf{G}_a$-action on $R[\boldsymbol{x}]$:*

(a) $p \geq 3$.

(b) *At least one of the lifts of δ is locally nilpotent.*

(c) *$p = 2$, and there exists $r \in \sqrt{2S}$ such that $\delta \in 2\bar{r}\,\mathrm{Der}_R\, R[\boldsymbol{x}]$.*

(d) *$p = 2$ and $\delta \in 2\mathcal{D}_R$.*

Here, for a ring T, we define $T[\boldsymbol{x}^2] := T[x_1^2, \dots, x_n^2]$ and

$$\mathcal{D}_T := \{D \in \mathrm{Der}_T\, T[\boldsymbol{x}] \mid D(x_i) \in T[\boldsymbol{x}^2] + 2T[\boldsymbol{x}] \text{ for } i = 1, \dots, n\}.$$

We note that $\phi(T[\boldsymbol{x}^2] + 2T[\boldsymbol{x}]) = T[\boldsymbol{x}^2] + 2T[\boldsymbol{x}]$ holds for any automorphism ϕ of the T-algebra $T[\boldsymbol{x}]$. Hence, the definition of $\mathcal{D}_T$ is independent of the system $x_1, \dots, x_n$ of variables of $T[\boldsymbol{x}]$.

We call the $\mathbf{G}_a$-action ε defined in Theorem 5 the *exponential action* of δ, and write $\overline{\exp}\, T\delta := \varepsilon$. By Theorem 5 (i), we have $\mathrm{RT}'_R(R[\boldsymbol{x}])_1 = p\,\mathrm{Der}_R\, R[\boldsymbol{x}]$, and $\{\overline{\exp}\, T\delta \mid \delta \in p\,\mathrm{Der}_R\, R[\boldsymbol{x}]\}$ is a system of representatives for the equivalence relation on $\mathrm{RT}'_R(R[\boldsymbol{x}])$. Thus, we know by Theorem 4 (ii) that

$$\Phi : p\,\mathrm{Der}_R\, R[\boldsymbol{x}] \times \mathscr{D}'_+ \ni (\delta, \Delta) \mapsto \overline{\exp}\, T\delta + \Delta \in \mathrm{RT}'_R(R[\boldsymbol{x}]) \qquad (4.2)$$

is bijective. For each $(\delta, \Delta) \in p\,\mathrm{Der}_R\, R[\boldsymbol{x}] \times \mathscr{D}'_+$, we have $\Phi((\delta, \Delta)) \sim \overline{\exp}\, T\delta$, so we get $\delta_1^{\Phi((\delta,\Delta))} = \delta_1^{\overline{\exp}\, T\delta} = \delta$ by Theorem 5 (i).

We also have the following consequence of Theorems 4 and 5.

Corollary 3. *Let $R = S/p^eS$ be as in* (4.1).

(i) *Set $\sigma := \Phi((\delta, \Delta))$ for $(\delta, \Delta) \in p\,\mathrm{Der}_R\, R[\boldsymbol{x}] \times \mathscr{D}'_+$. Then, we have*

$$R[\boldsymbol{x}]^{\sigma} = R[\boldsymbol{x}]^{\overline{\exp}\, T\delta} \cap \ker \Delta = \ker\delta \cap \ker\Delta. \qquad (4.3)$$

If R is noetherian, then the R-algebra $R[\boldsymbol{x}]^{\sigma}$ is finitely generated.

(ii) *If $p \geq 3$, then we have $\Phi(p\,\mathrm{Der}_R\, R[\boldsymbol{x}] \times \mathscr{D}_+) = \mathrm{RT}_R(R[\boldsymbol{x}])$.*

(iii) *If $p = 2$, then we have $\Phi(2\mathcal{D}_R \times \mathscr{D}_+) \subset \mathrm{RT}_R(R[\boldsymbol{x}])$.*

Proof. (i) First, we prove (4.3). Set $\varepsilon := \overline{\exp}\, T\delta$. Since $\sigma = \varepsilon + \varDelta$, we see that $f \in R[\boldsymbol{x}]^{\varepsilon} \cap \ker \varDelta$ implies $\sigma(f) = \varepsilon(f) + \varDelta(f) = f$, and so $f \in R[\boldsymbol{x}]^{\sigma}$. For the reverse inclusion, note that $\delta_1^{\sigma} = \delta$, and $\ker \delta = R[\boldsymbol{x}]^{\varepsilon}$ by Theorem 5 (iii). Hence, we have $R[\boldsymbol{x}]^{\sigma} = \bigcap_{i \geq 1} \ker \delta_i^{\sigma} \subset \ker \delta_1^{\sigma} = R[\boldsymbol{x}]^{\varepsilon}$. Thus, $f \in R[\boldsymbol{x}]^{\sigma}$ implies $\sigma(f) = f = \varepsilon(f)$, and so $\varDelta(f) = \sigma(f) - \varepsilon(f) = 0$. Therefore, $R[\boldsymbol{x}]^{\sigma}$ is contained in $R[\boldsymbol{x}]^{\varepsilon} \cap \ker \varDelta$, proving the first equality. Since $R[\boldsymbol{x}]^{\varepsilon} = \ker \delta$, the second equality is clear.

Since $\operatorname{char} R = p^e$, and δ and $\varDelta$ are derivations, f^{p^e} belongs to $\ker \delta \cap \ker \varDelta = R[\boldsymbol{x}]^{\sigma}$ for each $f \in R[\boldsymbol{x}]$. Hence, $R[\boldsymbol{x}]$ is integral over $R[\boldsymbol{x}]^{\sigma}$. This implies the second statement (cf. [1, Proposition 7.8]).

(ii) If $p \geq 3$, then we have $\{\overline{\exp}\, T\delta \mid \delta \in p \operatorname{Der}_R R[\boldsymbol{x}]\} \subset \mathrm{RT}_R(R[\boldsymbol{x}])$ by (a) of Theorem 5 (iv). Hence, by Theorem 5 (i), we see that $\mathrm{RT}_R(R[\boldsymbol{x}])_1 = p \operatorname{Der}_R R[\boldsymbol{x}]$, and $\{\overline{\exp}\, T\delta \mid \delta \in p \operatorname{Der}_R R[\boldsymbol{x}]\}$ is a system of representatives for the equivalence relation on $\mathrm{RT}_R(R[\boldsymbol{x}])$. Therefore, the assertion follows from Theorem 4 (iii).

(iii) Take any $\delta \in 2\mathcal{D}_R$. By (d) of Theorem 5 (iv), $\overline{\exp}\, T\delta$ belongs to $\mathrm{RT}_R(R[\boldsymbol{x}])$. Hence, we have $\Phi(\{\delta\} \times \mathscr{D}_+) = \overline{\exp}\, T\delta + \mathscr{D}_+ = [\overline{\exp}\, T\delta] \subset \mathrm{RT}_R(R[\boldsymbol{x}])$ by Theorem 4 (iii). □

We have determined the structure of $\mathrm{RT}_R(R[\boldsymbol{x}])$ when $e = 2$ or $p \geq 3$ (Corollaries 2 and 3 (ii)). When $p = 2$, we have

$$2\mathcal{D}_R \subset \mathrm{RT}_R(R[\boldsymbol{x}])_1 \subset 2 \operatorname{Der}_R R[\boldsymbol{x}].$$

We prove the following theorem in Section 7.

Theorem 6. *Let $R = S/p^eS$ be as in* (4.1). *If $p = 2$ and $e \geq 3$, then the following assertions hold.*

(i) *We have $\mathrm{RT}_R(R[\boldsymbol{x}])_1 \neq 2\mathrm{Der}_R R[\boldsymbol{x}]$.*

(ii) *If $n \geq 2$ or $\sqrt{2S} \neq 2S$, then we have $2\mathcal{D}_R \neq \mathrm{RT}_R(R[\boldsymbol{x}])_1$.*

(iii) *If $n = 1$ and $\sqrt{2S} = 2S$, then we have $2\mathcal{D}_R = \mathrm{RT}_R(R[\boldsymbol{x}])_1$, and so $\Phi(2\mathcal{D}_R \times \mathscr{D}_+) = \mathrm{RT}_R(R[\boldsymbol{x}])$.*

5. Structure of red-trivial $\mathbf{G}_a$-actions

The goal of this section is to prove Theorem 4.

Proof (of Theorem 4 (i)). First, we prove $\mathrm{RT}'_R(A) + \mathscr{D}' \subset \mathrm{RT}'_R(A)$. Take any $\sigma \in \mathrm{RT}'_R(A)$ and $\varDelta \in \mathscr{D}'$, and set $\tau := \sigma + \varDelta$. Then, $\tau : A \to A[[T]]$ is R-linear, and satisfies $\tau(1) = \sigma(1) + \varDelta(1) = \sigma(1) = 1$. By the choice of $\varDelta$ and σ, we have $p\varDelta(a) = 0$ and $\varDelta(a), \sigma(a) - a \in pA[[T]]$ for each $a \in A$. Hence, for each $a, b \in A$, we get

$$\begin{aligned}\tau(a)\tau(b) &= (\sigma(a)+\Delta(a))(\sigma(b)+\Delta(b))\\ &= \sigma(a)\sigma(b)+(a+(\sigma(a)-a))\Delta(b)+(b+(\sigma(b)-b))\Delta(a)\\ &= \sigma(a)\sigma(b)+a\Delta(b)+b\Delta(a)=\sigma(ab)+\Delta(ab)=\tau(ab).\end{aligned}$$

Therefore, τ is a homomorphism of R-algebras.

Fix any $a \in A$. Since $\sigma(a)-a \in pTA[[T]]$ and $\Delta(a) \in pA[[T]]^{(p)} \subset pTA[[T]]$, we have $\tau(a)-a \in pTA[[T]]$. This proves (A1) and the red-triviality for τ. To check (A2), write $f(T) := \Delta(a) = \sum_{i\geq 1} b_i T^i$, where $b_i \in pA$. Then, we have $\tau(a) = a + \sum_{i\geq 1}\delta_i^\sigma(a)T^i + \sum_{i\geq 1} b_i T^i$. We would like to show that

$$\tau(a)+\sum_{i\geq 1}\tau(\delta_i^\sigma(a))U^i+\sum_{l\geq 1}\tau(b_i)U^i = a+\sum_{i\geq 1}\delta_i^\sigma(a)(T+U)^i+f(T+U). \quad (5.1)$$

From $p\Delta = 0$, we see that the following statements hold.

(i) $\tau(pb) = p\tau(b) = p(\sigma(b)+\Delta(b)) = p\sigma(b) = \sigma(pb)$ for any $b \in A$.

(ii) For each $i \geq 1$, we have $b_i \in \mathrm{Ann}_A(p)$. Since $\mathrm{Ann}_A(p) = \mathrm{Ann}_R(p)A$ by assumption, we can write $b_i = \sum_k r_{i,k}b_{i,k}$, where $r_{i,k} \in \mathrm{Ann}_R(p)$ and $b_{i,k} \in A$.

Since σ is red-trivial by assumption, $\delta_l^\sigma(A) \subset pA$ holds for each $l \geq 1$. Hence, we get $\delta_l^\sigma(b_i) = \sum_k \sum_{l\geq 1} r_{i,k}\delta_l^\sigma(b_{i,k}) = 0$. Therefore, we have

(iii) $\sigma(b_i) = b_i + \sum_{l\geq 1}\delta_l^\sigma(b_i)T^l = b_i$ for each $i \geq 1$.

Now, since $\delta_i^\sigma(a), b_i \in pA$, we know by (i) and (iii) that $\tau(\delta_i^\sigma(a)) = \sigma(\delta_i^\sigma(a))$ and $\tau(b_i) = \sigma(b_i) = b_i$ for each i. Hence, the left-hand side of (5.1) is equal to

$$\begin{aligned}\tau(a)+\sum_{i\geq 1}\sigma(\delta_i^\sigma(a))U^i+\sum_{i\geq 1}b_iU^i &= (\sigma(a)+f(T))+\sum_{i\geq 1}\sigma(\delta_i^\sigma(a))U^i+f(U)\\ &= a+\sum_{i\geq 1}\delta_i^\sigma(a)(T+U)^i+f(T)+f(U),\end{aligned}$$

where the last equality is due to (A2) for σ. Since $f(T)$ is additive by Remark 2 (i), this is equal to the right-hand side of (5.1).

Since $\mathrm{RT}_R(A)+\mathscr{D} \subset \mathrm{RT}'_R(A)+\mathscr{D}' \subset \mathrm{RT}'_R(A)$ as shown above, and $\tau(A) \subset A[T]$ for each $\tau \in \mathrm{RT}_R(A)+\mathscr{D}$, we see that $\mathrm{RT}_R(A)+\mathscr{D} \subset \mathrm{RT}_R(A)$. □

The following lemma holds for any ring R, and any R-algebra A.

Lemma 10. *Let σ and τ be analytic $\mathbf{G}_a$-actions on A, and $N \geq 1$ an integer such that $\delta_i^\sigma = \delta_i^\tau$ for all $0 \leq i < N$. Then, the following assertions hold.*

(i) *$\delta := \delta_N^\sigma - \delta_N^\tau$ belongs to $\mathrm{Der}_R A$.*

(ii) *$\delta(a)(T+U)^N = \delta(a)T^N + \delta(a)U^N$ holds for each $a \in A$.*

(iii) *If $\delta \neq 0$ and $N \geq 2$, then there exist a prime number q and $d \geq 1$ such that $N = q^d$ and $q\delta = 0$.*

Proof. (i) Clearly, δ is R-linear. For each $a, b \in A$, we have

$$\sum_{i \geq 0} \delta_i^\sigma(ab)T^i = \sigma(ab) = \sigma(a)\sigma(b) = \left(\sum_{i \geq 0} \delta_i^\sigma(a)T^i\right)\left(\sum_{j \geq 0} \delta_j^\sigma(b)T^j\right).$$

From this equality, we obtain $\delta_N^\sigma(ab) = \sum_{i=0}^N \delta_i^\sigma(a)\delta_{N-i}^\sigma(b)$ by comparing the coefficients of T^N. Similarly, we have $\delta_N^\tau(ab) = \sum_{i=0}^N \delta_i^\tau(a)\delta_{N-i}^\tau(b)$. Since $\delta_i^\sigma(a)\delta_{N-i}^\sigma(b) = \delta_i^\tau(a)\delta_{N-i}^\tau(b)$ for $1 \leq i < N$ by assumption, and $\delta_0^\sigma = \delta_0^\tau = \mathrm{id}_A$ by (A1), it follows that

$$\delta(ab) = \delta_N^\sigma(ab) - \delta_N^\tau(ab) = \sum_{i=0,N} (\delta_i^\sigma(a)\delta_{N-i}^\sigma(b) - \delta_i^\tau(a)\delta_{N-i}^\tau(b)) = a\delta(b) + \delta(a)b.$$

(ii) Set $\mathfrak{a} := TA[[T, U]] + UA[[T, U]]$. Since no polynomial of degree N belongs to the ideal $\mathfrak{a}^{N+1}$, it suffices to verify $\delta(a)(T + U)^N \equiv \delta(a)(T^N + U^N)$ $(\mathrm{mod}\ \mathfrak{a}^{N+1})$ for each $a \in A$. In the rest of the proof, we assume that all congruences are modulo $\mathfrak{a}^{N+1}$. By (A2) for σ, we have

$$\sigma(a) + \sum_{i=1}^N \sigma(\delta_i^\sigma(a))U^i \equiv a + \sum_{i=1}^N \delta_i^\sigma(a)(T + U)^i. \tag{5.2}$$

Since $\delta_i^\sigma(a) = \delta_i^\tau(a)$ for $1 \leq i < N$ and $\delta_N^\sigma(a) = \delta_N^\tau(a) + \delta(a)$, the right-hand side of (5.2) is equal to $a + \sum_{i=1}^N \delta_i^\tau(a)(T + U)^i + \delta(a)(T + U)^N$, and the left-hand side of (5.2) is equal to

$$\sigma(a) + \sum_{i=1}^N \sigma(\delta_i^\tau(a))U^i + \sigma(\delta(a))U^N. \tag{5.3}$$

For each $b \in A$, we have $\sigma(b) \equiv \tau(b) + \delta(b)T^N$ and $\sigma(b)U^i \equiv \tau(b)U^i$ for $i \geq 1$, and $\sigma(b)U^N \equiv bU^N$ by (A1) for σ. Hence, we see that

$$\begin{aligned}(5.3) &\equiv \tau(a) + \delta(a)T^N + \sum_{i=1}^N \tau(\delta_i^\tau(a))T^i + \delta(a)U^N \\ &\equiv a + \sum_{i=1}^N \delta_i^\tau(a)(T + U)^i + \delta(a)(T^N + U^N),\end{aligned}$$

where the second congruence is due to (A2) for τ. Therefore, we conclude that $\delta(a)(T + U)^N \equiv \delta(a)(T^N + U^N)$.

(iii) Take any $b \in \delta(A)\setminus\{0\}$. Then, we have $b(T + U)^N = b(T^N + U^N)$ by (ii). Hence, by Lemma 8, there exist $d \geq 1$ and a prime number q such that $N = q^d$ and $qb = 0$. Since N is a fixed integer, we see that q is independent of the choice of b. Therefore, we have $q\delta(A) = \{0\}$, proving $q\delta = 0$. □

In the situation of Lemma 10 (iii), assume that $\operatorname{char} R = p^e$. Then, q must be equal to p, for otherwise $q \in (\mathbf{Z}/p^e\mathbf{Z})^* \subset R^*$, and so $q\delta \neq 0$, a contradiction. Assume further that σ and τ are red-trivial. Then, we have $\delta(A) \subset pA$. Hence, $\delta T^N : A \ni a \mapsto \delta(a)T^N \in A[[T]]$ belongs to $\mathscr{D}_+$.

Lemma 11. *Assume that* $\operatorname{char} R = p^e$ *and* $\operatorname{Ann}_A(p) = \operatorname{Ann}_R(p)A$. *If* $\sigma, \tau \in \mathrm{RT}'_R(A)$ *satisfy* $\delta_1^\sigma = \delta_1^\tau$, *then* $(\delta_i^\tau - \delta_i^\sigma)T^i \in \mathscr{D}_+$ *holds for all* $i \geq 2$. *Hence,* $\tau = \sigma + (\tau - \sigma)$ *belongs to* $\sigma + \mathscr{D}'_+$.

Proof. Suppose that the lemma is false. Let N be the minimal integer with $(\delta_N^\tau - \delta_N^\sigma)T^N \notin \mathscr{D}_+$. Then, we have $N \geq 2$, and $(\delta_i^\tau - \delta_i^\sigma)T^i$ belongs to $\mathscr{D}_+$ for $2 \leq i < N$. Hence, by Theorem 4 (i), we know that

$$\sigma' := \sigma + \sum_{i=2}^{N-1} (\delta_i^\tau - \delta_i^\sigma)T^i \in \mathrm{RT}'_R(A).$$

By construction, we have $\delta_i^{\sigma'} = \delta_i^\tau$ for $1 \leq i < N$ and $\delta_N^{\sigma'} = \delta_N^\sigma \neq \delta_N^\tau$. Therefore, by the remark before this lemma, we obtain that $(\delta_N^\tau - \delta_N^\sigma)T^N = (\delta_N^\tau - \delta_N^{\sigma'})T^N \in \mathscr{D}_+$, a contradiction. □

Now, we are ready to give a

Proof (of (ii) and (iii) of Theorem 4). (ii) Take any $\sigma \in \mathrm{RT}'_R(A)$. Then, we have $[\sigma]' \subset \sigma + \mathscr{D}'_+$ by Lemma 11. For the reverse inclusion, take any $\Delta \in \mathscr{D}'_+$ and set $\tau := \sigma + \Delta$. Then, τ belongs to $\mathrm{RT}'_R(A)$ by Theorem 4 (i). Since $\Delta(A) \subset A[[T]]_+^{(p)} \subset T^2A[[T]]$, we get $\delta_1^\tau = \delta_1^\sigma$. Therefore, τ belongs to $[\sigma]'$.

(iii) Take any $\sigma \in \mathrm{RT}_R(A)$, and $\tau \in [\sigma]$. Then, since $\delta_1^\tau = \delta_1^\sigma$, we know by Lemma 11 that $\Delta := \tau - \sigma \in \mathscr{D}'_+$. Since σ and τ are algebraic $\mathbf{G}_a$-actions, we have $\Delta(a) = \tau(a) - \sigma(a) \in A[T]$ for each $a \in A$. Hence, we get $\Delta \in \mathscr{D}_+$, and so $\tau = \sigma + \Delta \in \sigma + \mathscr{D}_+$. By (i) and (ii) of Theorem 4, we have $\sigma + \mathscr{D}_+ \subset [\sigma]' \cap \mathrm{RT}_R(A) = [\sigma]$. □

6. Legendre's formula

Let v_p be the *p-adic valuation* of $\mathbf{Q}$. Namely, we define $v_p(0) = \infty$, and $v_p(\alpha) = r$ for each $\alpha \in \mathbf{Q}^*$, where $r \in \mathbf{Z}$ is such that $\alpha = p^r\alpha'/\alpha''$ for some $\alpha', \alpha'' \in \mathbf{Z}\backslash p\mathbf{Z}$. For each $\alpha \in \mathbf{R}$, we define $\lfloor \alpha \rfloor := \max\{r \in \mathbf{Z} \mid r \leq \alpha\}$. The following formula is well known.

Theorem 7 (Legendre's formula). *For each integer* $l \geq 1$, *we have* $v_p(l!) = \sum_{i=1}^{\infty} \lfloor l/p^i \rfloor$.

Let $l = \sum_{j=0}^{k} l_j p^j$ be the p-adic expansion of l, where $0 \le l_j < p$. Then, since $\lfloor l/p^i \rfloor = \sum_{j=i}^{k} l_j p^{j-i}$, we know by Theorem 7 that

$$v_p(l!) = \sum_{i=1}^{\infty} \left\lfloor \frac{l}{p^i} \right\rfloor = \sum_{j=1}^{k} \sum_{i=0}^{j-1} l_j p^i = \sum_{j=1}^{k} \frac{l_j(p^j - 1)}{p-1} = \frac{l - \sum_{i=1}^{k} l_i}{p-1}, \tag{6.4}$$

and so $v_p(p^l/l!) = l - v_p(l!) > l(p-2)/(p-1) \ge 0$. Here are some consequences:

(1°) We can write $p^l/l! = pa_l$, where $a_l \in \mathbf{Z}_{\mathcal{U}_1}$.

(2°) Assume that $p \ge 3$. Then, for every $e \ge 1$, there exists $N \ge 1$ such that $\{p^l/l! \mid l \ge N\} \subset p^e \mathbf{Z}_{\mathcal{U}_1}$.

(3°) By (6.4), we have $v_2(2^l/l!) = 1$ if and only if $l = 2^k$ for some $k \ge 0$.

Proof (of Theorem 5). (i) Let $D \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ be a lift of δ. Since δ is in $p\,\mathrm{Der}_R\, R[\boldsymbol{x}]$, we can write $D = pD_0$, where $D_0 \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ (cf. Section 4.3). By (1°), it follows that

$$\frac{D^l(x_i)}{l!} = \frac{p^l}{l!} D_0^l(x_i) = pa_l D_0^l(x_i) \in pS_{\mathcal{U}_1}[\boldsymbol{x}] \qquad \text{for } i = 1, \dots, n.$$

Therefore, $\exp TD$ restricts to $S_{\mathcal{U}_1}[\boldsymbol{x}]$, and induces a red-trivial, analytic $\mathbf{G}_a$-action ε on $R[\boldsymbol{x}]$. By construction, we have $\delta_1^{\varepsilon} = \delta$.

(ii) Take another lift $D' \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ of δ, and set $D'' := D' - D$. Since D'' induces the zero derivation of $R[\boldsymbol{x}]$, we have $D''(S[\boldsymbol{x}]) \subset p^e S[\boldsymbol{x}]$. By Remark 3 (ii), we can write $D'' = p^e D_0''$, where $D_0'' \in \mathrm{Der}_S\, S[\boldsymbol{x}]$. Then, we have $D' = D + D'' = p(D_0 + p^{e-1} D_0'')$, and

$$\frac{(D')^l(x_i)}{l!} = pa_l (D_0 + p^{e-1} D_0'')^l(x_i) \in pa_l D_0^l(x_i) + p^e S_{\mathcal{U}_1}[\boldsymbol{x}]$$

for all $l \ge 1$ and $i = 1, \dots, n$. This shows that $\exp TD$ and $\exp TD'$ induce the same analytic $\mathbf{G}_a$-action on $R[\boldsymbol{x}]$.

(iii) Clearly, $R[\boldsymbol{x}]^{\varepsilon} = \bigcap_{l \ge 1} \ker \delta_l^{\varepsilon}$ is contained in $\ker \delta_1^{\varepsilon} = \ker \delta$. To show $\ker \delta \subset R[\boldsymbol{x}]^{\varepsilon}$, take any $f \in \ker \delta$, and $g \in S[\boldsymbol{x}]$ with $\bar{g} = f$. Since $\overline{D(g)} = 0$, we can write $D(g) = p^e h$, where $h \in S[\boldsymbol{x}]$. Then, for each $l \ge 1$, we have

$$\frac{D^l(g)}{l!} = \frac{p^e D^{l-1}(h)}{l!} = p^e \frac{p^{l-1} D_0^{l-1}(h)}{l!} = p^e a_l D_0^{l-1}(h) \in p^e S_{\mathcal{U}_1}[\boldsymbol{x}],$$

since $p^l/l! = pa_l$. This implies that $\delta_l^{\varepsilon}(f) = 0$. Therefore, f belongs to $R[\boldsymbol{x}]^{\varepsilon}$.

(iv) It suffices to find a lift $D \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ of δ and $N \ge 1$ such that, for all $l \ge N$ and $i = 1, \dots, n$, we have $D^l(x_i)/l! \in p^e S_{\mathcal{U}_1}[\boldsymbol{x}]$. The case (b) is clear. Since every lift D of δ has the form $D = pD_0$ for some $D_0 \in \mathrm{Der}_S\, S[\boldsymbol{x}]$, the case (a) follows from (2°). In the case (c), we can find $D_1 \in \mathrm{Der}_S\, S[\boldsymbol{x}]$ for which $D = 2rD_1$ is a lift of δ. Since r is in $\sqrt{2S}$, there exists $N \geq 1$ such that $r^N \in 2^eS$. Then, $D^l(x_i)/l! = 2a_lr^ND_1^l(x_i) \in 2^eS_{U_1}[\boldsymbol{x}]$ holds for all $l \geq N$ and $i = 1,\dots,n$. In the case (d), we can find $D_2 \in \mathcal{D}_S$ for which $2D_2$ is a lift of δ. By Lemma 12 (ii) below, there exists $N > 0$ such that $D_2^l(x_i) \in 2^{e-1}S[\boldsymbol{x}]$ for all $l \geq N$ and $i = 1,\dots,n$. Then, $D^l(x_i)/l! = (2^l/l!)D_2^l(x_i) = 2a_lD_2^l(x_i) \in 2^eS_{U_1}[\boldsymbol{x}]$ holds for all $l \geq N$ and $i = 1,\dots,n$. □

The following lemma holds for any ring S.

Lemma 12. *We set* $B := S[\boldsymbol{x}^2] + 2S[\boldsymbol{x}]$.

(i) *If* $f \in B$, *then* $\partial^{2l}f/\partial x_i^{2l} \in 2^lB$ *holds for each* $l \geq 1$ *and* $i = 1,\dots,n$.

(ii) *Let* $D \in \mathcal{D}_S$ *and* $e \geq 1$. *Then,* $D^l(x_i)$ *belongs to* $2^eS[\boldsymbol{x}]$ *for each* $l > 2e(e-1)n$ *and* $i = 1,\dots,n$.

Proof. (i) It suffices to prove the case $l = 1$ and $f \in S[\boldsymbol{x}^2] \cup 2S[\boldsymbol{x}]$. It is easy to see that $\partial^2f/\partial x_i^2$ belongs to $2S[\boldsymbol{x}^2]$ if $f \in S[\boldsymbol{x}^2]$, and to $4S[\boldsymbol{x}]$ if $f \in 2S[\boldsymbol{x}]$. In either case, $\partial^2f/\partial x_i^2$ belongs to $2B$.

(ii) Write $D = \sum_{i=1}^n f_i\partial/\partial x_i$, where $f_i \in B$. Set $|\boldsymbol{k}| := k_1 + \cdots + k_n$ and

$$\partial^{\boldsymbol{k}} := \frac{\partial^{|\boldsymbol{k}|}}{\partial x_1^{k_1}\cdots\partial x_n^{k_n}} \qquad \text{for each } \boldsymbol{k} = (k_1,\dots,k_n) \in (\mathbf{Z}_{\geq 0})^n.$$

Now, fix $l > 2e(e-1)n$ and $1 \leq i_0 \leq n$. Then, we have

$$D^l(x_{i_0}) = \sum_{i_1=1}^n f_{i_1}\frac{\partial}{\partial x_{i_1}}\sum_{i_2=1}^n f_{i_2}\frac{\partial}{\partial x_{i_2}}\cdots\sum_{i_{l-1}=1}^n f_{i_{l-1}}\frac{\partial f_{i_0}}{\partial x_{i_{l-1}}},$$

which is a sum of polynomials of the form $g := f_{n_1}(\partial^{\boldsymbol{k}_2}f_{n_2})(\partial^{\boldsymbol{k}_3}f_{n_3})\cdots(\partial^{\boldsymbol{k}_l}f_{n_l})$. Here, $n_1,\dots,n_l \in \{1,\dots,n\}$, and $\boldsymbol{k}_2,\dots,\boldsymbol{k}_l \in (\mathbf{Z}_{\geq 0})^n$ satisfy

$$|\boldsymbol{k}_2| + \cdots + |\boldsymbol{k}_l| = l - 1 \geq 2e(e-1)n. \tag{6.5}$$

We show that $g \in 2^eS[\boldsymbol{x}]$. This is true if $\#\{i \mid \boldsymbol{k}_i \neq 0\} \geq e$, since $\partial f/\partial x_i \in 2S[\boldsymbol{x}]$ holds for any $f \in B$ and i. So, assume that $\#\{i \mid \boldsymbol{k}_i \neq 0\} < e$. Then, by (6.5), there exist i and j for which the j-th component of $\boldsymbol{k}_i$ is at least $2e$. By (i), this implies that $\partial^{\boldsymbol{k}_i}f_{n_i} \in 2^eS[\boldsymbol{x}]$, proving $g \in 2^eS[\boldsymbol{x}]$. □

7. The case where $p = 2$

The goal of this section is to prove Theorem 6. Let S be a subring of a $\mathbf{Q}$-algebra with $2 \notin S^*$, and let $R = S/2^eS$ with $e \geq 2$. We consider the four types of $\delta \in 2\mathrm{Der}_R\, R[\boldsymbol{x}]$ defined as follows.

(A) $\delta := 2x_1\partial/\partial x_1$.

(B) $\delta := 2x_1\partial/\partial x_2$.

(C) $\delta := 2\bar{r}x_1\partial/\partial x_1$, where $r \in \sqrt{2S}\backslash 2S$.
(D) $\delta := 2f\partial/\partial x_1$, where $f \in R[x_1]\backslash(R[x_1^2] + 2R[x_1])$.

We note that (B) and (C) require that $n \geq 2$ and $\sqrt{2S} \neq 2S$, respectively. For δ in (B) and (C), $\overline{\exp}\, T\delta$ belongs to $\mathrm{RT}_R(R[\boldsymbol{x}])$ by (b) and (c) of Theorem 5 (iv). Hence, δ in (B) and (C) lies in $\mathrm{RT}_R(R[\boldsymbol{x}])_1$.

Proof (of Theorem 6 (ii)). It suffices to check that δ in (B) and (C) are not in $2\mathcal{D}_R$, i.e., $2x_1, 2\bar{r}x_1 \notin 2(R[\boldsymbol{x}^2] + 2R[\boldsymbol{x}])$. Since $1, \bar{r} \notin 2R$, we show that $2ax_1 \notin 2(R[\boldsymbol{x}^2] + 2R[\boldsymbol{x}])$ for any $a \in R\backslash 2R$. If $2ax_1 \in 2(R[\boldsymbol{x}^2] + 2R[\boldsymbol{x}])$, then we have $2a \in 4R$. Since $(4R : 2R) = 2R$ by Lemma 9, it follows that $a \in 2R$, a contradiction. □

To prove (i) and (iii) of Theorem 6, it suffices to verify that δ does not belong to $\mathrm{RT}_R(R[\boldsymbol{x}])_1$ in the case (A), and in the case (D) when $\sqrt{2S} = 2S$, since any element of $2\,\mathrm{Der}_R\, R[x]\backslash 2\mathcal{D}_R$ is written as δ in (D) if $n = 1$. These statements follow from the two lemmas below.

Lemma 13. *Assume that* $e \geq 3$. *For* $\delta \in 2\,\mathrm{Der}_R\, R[\boldsymbol{x}]$, *we set* $\varepsilon := \overline{\exp}\, T\delta$. *If* $\delta_{2^k}^{\varepsilon}(x_1) \notin 4R[\boldsymbol{x}]$ *holds for each* $k \geq 1$, *then* δ *does not belong to* $\mathrm{RT}_R(R[\boldsymbol{x}])_1$.

Proof. Suppose that there exists $\sigma \in \mathrm{RT}_R(R[\boldsymbol{x}])$ with $\delta_1^{\sigma} = \delta$. Then, we have $\varepsilon \in [\sigma]' = \sigma + \mathscr{D}'_+$ by Theorems 4 (ii). Hence, $\varepsilon - \sigma$ belongs to $\mathscr{D}'_+$. Thus, by Proposition 1, $\delta_{2^k}^{\varepsilon} - \delta_{2^k}^{\sigma} \in \mathrm{Der}_R(R[\boldsymbol{x}], 2^{e-1}R[\boldsymbol{x}]) = 2^{e-1}\,\mathrm{Der}_R\, R[\boldsymbol{x}]$ holds for each $k \geq 1$. Since $e \geq 3$ by assumption, it follows that $\delta_{2^k}^{\varepsilon}(x_1) - \delta_{2^k}^{\sigma}(x_1) \in 4R[\boldsymbol{x}]$ for all $k \geq 1$. On the other hand, $\delta_{2^l}^{\sigma}(x_1) = 0$ holds for $l \gg 0$, because σ is an algebraic $\mathbf{G}_a$-action. Then, we get $\delta_{2^l}^{\varepsilon}(x_1) = \delta_{2^l}^{\varepsilon}(x_1) - \delta_{2^l}^{\sigma}(x_1) \in 4R[\boldsymbol{x}]$, a contradiction. □

Lemma 14. *Assume that* $e \geq 2$. *If* δ *is as in* (A), *or if* $\sqrt{2S} = 2S$ *and* δ *is as in* (D), *then* $\varepsilon := \overline{\exp}\, T\delta$ *satisfies* $\delta_{2^k}^{\varepsilon}(x_1) \notin 4R[\boldsymbol{x}]$ *for all* $k \geq 1$.

Proof. (A) Note that $D := 2x_1\partial/\partial x_1 \in 2\,\mathrm{Der}_S\, S[\boldsymbol{x}]$ is a lift of δ, and $D^l(x_1) = 2^l x_1$ for each $l \geq 0$. Suppose that $\delta_{2^k}^{\varepsilon}(x_1) \in 4R[\boldsymbol{x}]$ for some $k \geq 1$, and set $l := 2^k$. Then, there exists $s \in S_{\mathcal{U}_1}$ such that $2^l/l! - 4s \in 2^e S_{\mathcal{U}_1}$. By (3°) in Section 6, we can write $2^l/l! = 2a$, where $a \in \mathbf{Z}_{\mathcal{U}_1}\backslash 2\mathbf{Z}_{\mathcal{U}_1}$. Then, we have $a - 2s \in 2^{e-1}S_{\mathcal{U}_1}$, and so $a \in 2S_{\mathcal{U}_1}$, since S is a subring of a $\mathbf{Q}$-algebra and $e \geq 2$. Therefore, a belongs to $2S_{\mathcal{U}_1} \cap \mathbf{Z}_{\mathcal{U}_1} = 2\mathbf{Z}_{\mathcal{U}_1}$, a contradiction.

(D) Take $g \in S[x_1]\backslash(S[x_1^2] + 2S[x_1])$ with $\bar{g} = f$, and set $D := g\partial/\partial x_1$. Then, $2D$ is a lift of δ. Since $g \notin S[x_1^2] + 2S[x_1]$, there appears in g a monomial cx_1^j with $c \in S\backslash 2S$ and an odd number $j > 0$. Since $2S = \sqrt{2S}$ is equal to the intersection of all $\mathfrak{p} \in \mathrm{Spec}\, S$ with $2 \in \mathfrak{p}$, we can find $\mathfrak{p} \in \mathrm{Spec}\, S$ such that $2 \in \mathfrak{p}$ and $c \notin \mathfrak{p}$. Then, we have $g \notin \mathfrak{p}S[\boldsymbol{x}]$.

We show that $D^l(x_1) \notin \mathfrak{p}S[\boldsymbol{x}]$ for each $l \geq 1$. Write $h^{(l)} := \partial^l h/\partial x_1^l$ for each $h \in S[\boldsymbol{x}]$ and $l \geq 0$. Then, we have $D^l(x_1) = g \cdot (D^{l-1}(x_1))^{(1)}$. Since $g \notin$

$\mathfrak{p}S[\boldsymbol{x}]$, and $\mathfrak{p}S[\boldsymbol{x}]$ is a prime ideal of $S[\boldsymbol{x}]$, it suffices to show that $(D^l(x_1))^{(1)} \notin \mathfrak{p}S[\boldsymbol{x}]$ for each $l \geq 0$. We prove this by induction on l. The assertion is clear if $l = 0$. Assume that $l \geq 1$. Then, we have

$$(D^l(x_1))^{(1)} = (g \cdot (D^{l-1}(x_1))^{(1)})^{(1)} = g \cdot (D^{l-1}(x_1))^{(2)} + g^{(1)} \cdot (D^{l-1}(x_1))^{(1)}. \quad (7.1)$$

Since $(x_1^i)^{(2)} = i(i-1)x_1^{i-2} \in 2S[\boldsymbol{x}] \subset \mathfrak{p}S[\boldsymbol{x}]$ for each $i \in \mathbf{Z}_{\geq 0}$, we see that $(D^{l-1}(x_1))^{(2)}$ belongs to $\mathfrak{p}S[\boldsymbol{x}]$. By induction assumption, $(D^{l-1}(x_1))^{(1)}$ does not belong to $\mathfrak{p}S[\boldsymbol{x}]$. So, we show that $g^{(1)} \notin \mathfrak{p}S[\boldsymbol{x}]$. The monomial jcx_1^{j-1} appears in $g^{(1)}$. Since $c \notin \mathfrak{p}$, $2 \in \mathfrak{p}$, and j is an odd number, we have $jc \notin \mathfrak{p}$, and so $g^{(1)} \notin \mathfrak{p}S[\boldsymbol{x}]$. Therefore, (7.1) does not belong to $\mathfrak{p}S[\boldsymbol{x}]$.

Now, suppose that $\delta_{2^k}^{\varepsilon}(x_1)$ belongs to $4R[\boldsymbol{x}]$ for some $k \geq 1$, and set $l := 2^k$. Then, there exists $h \in S_{\mathcal{U}_1}[\boldsymbol{x}]$ such that $(2^l/l!)D^l(x_1) - 4h \in 2^e S_{\mathcal{U}_1}[\boldsymbol{x}]$. By (3°) in Section 6, we can write $2^l/l! = 2b$, where $b \in \mathbf{Z}_{\mathcal{U}_1} \backslash 2\mathbf{Z}_{\mathcal{U}_1}$. Since $b \in (\mathbf{Z}_{\mathcal{U}_1})^* \subset (S_{\mathcal{U}_1})^*$, 2 is not a zero-divisor of $S_{\mathcal{U}_1}$, and $e \geq 2$, it follows that $D^l(x_1) \in 2S_{\mathcal{U}_1}[\boldsymbol{x}] \subset \mathfrak{p}S_{\mathcal{U}_1}[\boldsymbol{x}]$. We claim that $\mathfrak{p}S_{\mathcal{U}_1}[\boldsymbol{x}] \cap S[\boldsymbol{x}] = \mathfrak{p}S[\boldsymbol{x}]$. Indeed, since $\mathfrak{p} \cap \mathbf{Z} = 2\mathbf{Z}$ and $\mathcal{U}_1 = \mathbf{Z} \backslash 2\mathbf{Z}$, we have $\mathfrak{p} \cap \mathcal{U}_1 = \emptyset$. Hence, $\mathfrak{p}S_{\mathcal{U}_1}$ is a prime ideal of $S_{\mathcal{U}_1}$ with $\mathfrak{p}S_{\mathcal{U}_1} \cap S = \mathfrak{p}$. Since $D^l(x_1)$ lies in $S[\boldsymbol{x}]$ by construction, we know that $D^l(x_1)$ belongs to $\mathfrak{p}S[\boldsymbol{x}]$. This is a contradiction. □

This completes the proof of Theorem 6.

Remark 5. Assume that $e = 2$, and let δ be as in (A). Then, $\overline{\exp}\, T\delta$ is not an algebraic $\mathbf{G}_a$-action by Lemma 14. However, δ belongs to $\mathrm{RT}_R(R[\boldsymbol{x}])_1$, since $\mathrm{RT}_R(R[\boldsymbol{x}])_1 = \mathrm{Der}_R(R[\boldsymbol{x}], 2R[\boldsymbol{x}]) = 2\,\mathrm{Der}_R\, R[\boldsymbol{x}]$ by Corollary 2.

8. Generators of invariant rings

Throughout this section, assume that $n = 1$ and $R = S/p^eS$, where

$$S \text{ is a subring of a } \mathbf{Q}\text{-algebra such that } pS \in \operatorname{Spec} S. \quad (8.1)$$

We describe generators of the R-algebra $R[x]^{\sigma}$ for $\sigma \in \mathrm{RT}'_R(R[x]) \backslash \{\imath\}$.

Remark 6. For each $a, b \in S$ with $a \notin pS$ and $b \notin p^eS$, we have $ab \notin p^eS$ by (8.1). Hence, no element of $R \backslash pR$ is a zero-divisor of R. Similarly, no element of $R[x][[T]] \backslash pR[x][[T]]$ is a zero-divisor of $R[x][[T]]$, since $S[x][[T]]$ is a subring of a $\mathbf{Q}$-algebra and $pS[x][[T]] \in \operatorname{Spec} S[x][[T]]$.

By (4.2) and Corollary 3 (i), there exist $\delta \in p\,\mathrm{Der}_R\, R[x]$ and $\Delta \in \mathscr{D}'_+$ such that $\sigma = \overline{\exp}\, T\delta + \Delta$ and $R[x]^{\sigma} = \ker \delta \cap \ker \Delta$. Write $\delta = f_1 d/dx$ and $\Delta = f_2 d/dx$, where $f_1 \in pR[x]$ and $f_2 \in pR[x][[T]]_+^{(p)}$. For each $f \in R[x][[T]]$, we define

$$\mathrm{ord}_p(f) := \max\{l \in \{0, \dots, e\} \mid f \in p^l R[x][[T]]\}.$$

Then, we have $d_i := \operatorname{ord}_p(f_i) \geq 1$ for $i = 1, 2$, and $u := e - \min\{d_1, d_2\} < e$. Set

$$u_l := u - v_p(l) \qquad \text{and} \qquad T_l := p^{u_l} x^l \qquad \text{for } l = 1, \dots, p^u.$$

Remark 7. (i) Since $\sigma \neq \iota$, we have $(f_1, f_2) \neq (0, 0)$. Hence, d_1 or d_2 is less than e. Therefore, u is positive.

(ii) We have $u_l \geq 1$ for $i = 1, \dots, p^u - 1$, and $u_{p^u} = 0$.

The following theorem generalizes the main result of the Master's Thesis of Yuto Imamura [4].

Theorem 8. *Let $R = S/p^e S$ be as in* (8.1), *and $\sigma \in \mathrm{RT}'_R(R[x]) \setminus \{\iota\}$. Then, in the notation above, we have $R[x]^\sigma = R[T_1, \dots, T_{p^u}]$.*

Proof. For $i \in \{1, 2\}$, write $f_i = p^{d_i} g_i$, where $g_i \in R[x][[T]] \setminus pR[x][[T]]$. Then, g_i is not a zero-divisor of $R[x][[T]]$ by Remark 6. Hence, we have $f_i\, dh/dx = 0$ if and only if $p^{d_i}\, dh/dx = 0$ for $h \in R[x]$.

For $l = 1, \dots, p^u$, we have $v_p(p^{d_i} p^{u_l} l) = d_i + u_l + v_p(l) = d_i + u \geq e$. Hence, $p^{d_i}\, dT_l/dx = p^{d_i} p^{u_l} l x^{l-1} = 0$ holds in $R[x]$. Thus, δ and Δ kill $T_1, \dots, T_{p^u}$. Therefore, $R[T_1, \dots, T_{p^u}]$ is contained in $\ker \delta \cap \ker \Delta = R[x]^\sigma$.

For the reverse inclusion, take any $h = \sum_{l \geq 0} c_l x^l \in R[x]^\sigma$, where $c_l \in R$. We show that $c_l x^l \in R[T_1, \dots, T_{p^u}]$ for each l. Since $\delta(h) = \Delta(h) = 0$, we have

$$0 = p^{d_i} \frac{dh}{dx} = \sum_{l \geq 0} c_l p^{d_i} l x^{l-1} \qquad \text{for } i = 1, 2.$$

Hence, $c_l p^{d_i} l = 0$ holds for each $l \geq 1$ and $i = 1, 2$. Fix $l \geq 1$, and let $q, r \in \mathbf{Z}$ be the quotient and the remainder of l divided by p^u, respectively. Write $c_l = p^s c$ and $r = p^{v_p(r)} r'$, where $s := \operatorname{ord}_p(c_l)$, $c \in R \setminus pR$ and $r' \in \mathbf{Z} \setminus p\mathbf{Z}$. Choose $i \in \{1, 2\}$ so that $d_i = \min\{d_1, d_2\}$. Then, since $d_i + u = e$, we have $p^{d_i} l = p^{d_i}(p^u q + r) \equiv p^{d_i} r \pmod{p^e}$. Hence, $c p^{s + d_i + v_p(r)} r' = c_l p^{d_i} r = c_l p^{d_i} l = 0$ holds in R. Since c is not a zero-divisor of $R[x]$ by Remark 6, $r' \in (\mathbf{Z}/p^e\mathbf{Z})^* \subset R^*$, and $\operatorname{char} R = p^e$, this implies that $s + d_i + v_p(r) \geq e$. Thus, we get $s \geq e - d_i - v_p(r) = u - v_p(r) = u_r$. Therefore, we have $c_l x^l = c p^{s - u_r} p^{u_r} x^r (x^{p^u})^q = c p^{s - u_r} T_r T_{p^u}^q$, which belongs to $R[T_1, \dots, T_{p^u}]$. □

Proof (of Theorem 2). Note that $\operatorname{char} \tilde{R} = p_1^{e_1} \cdots p_t^{e_t}$, and $R_i := \tilde{R}/p_i^{e_i} \tilde{R} \simeq S/p_i^{e_i} S$ for each i. By the Chinese Remainder Theorem, it suffices to show that, for $i = 1, \dots, t$ and any $\mathbf{G}_a$-action σ on $R_i[x]$ over R_i, the R_i-algebra $R_i[x]^\sigma$ is finitely generated. If $e_i = 1$, then R_i is an integral domain. In this case, we have $R_i[x]^\sigma = R_i$ unless σ is trivial (cf. Lemma 3). So, assume that $e_i \geq 2$. If σ is red-trivial, then we can apply Theorem 8. We show that $R_i[x]^\sigma = R_i$ if σ is red-nontrivial. Note that $p_i R_i \in \operatorname{Spec} R_i$, and $(p_i^2 R_i : p_i R_i) =$

p_iR_i by Lemma 9. Hence, the assumption of Theorem 1 is fulfilled. Since no element of $R_i \backslash p_iR_i$ is a zero-divisor of R_i by Remark 6, we have $R_i[x]^\sigma = R_i$ by Theorem 1 (iii). □

9. $\mathbf{G}_a$-actions on the reduced affine lines

In closing this paper, we shortly mention the case where R is reduced. Let $\mathscr{P}$ be the set of prime numbers. We define $\mathscr{A}$ to be the set of $f \in R[T]$ of the form

$$f = aT + \sum_{l \geq 1} \sum_{p \in \mathscr{P}} a_{l,p} T^{p^l},$$

where $a \in R$, and $a_{l,p} \in R$ is such that $pa_{l,p} = 0$ for each $l \geq 1$ and $p \in \mathscr{P}$.

Theorem 9. *Let R be a reduced ring, and $\sigma : R[x] \to R[x][T]$ a homomorphism of R-algebras. Then, σ is a $\mathbf{G}_a$-action on $R[x]$ if and only if $\sigma(x) - x$ belongs to $\mathscr{A}$.*

Proof. By Lemma 8, every element of $\mathscr{A}$ is additive. Noting this, we can check the "if" part easily. To show the "only if" part, assume that σ is a $\mathbf{G}_a$-action. Then, by (A1), we can write

$$f := \sigma(x) - x = \sum_{i \geq 0} \sum_{j \geq 1} a_{i,j} x^i T^j, \qquad \text{where } a_{i,j} \in R.$$

Take any $\mathfrak{p} \in \operatorname{Spec} R$. Then, σ induces a $\mathbf{G}_a$-action on $(R/\mathfrak{p})[x]$ over the integral domain $R/\mathfrak{p}$. Hence, modulo $\mathfrak{p}R[x][T]$, we have $f \equiv a_{0,1}T$ if $\operatorname{char}(R/\mathfrak{p}) = 0$, and $f \equiv \sum_{l \geq 0} a_{0,p^l} T^{p^l}$ if $\operatorname{char}(R/\mathfrak{p}) = p > 0$ (cf. Lemma 5). In either case, $a_{i,j}$ belongs to $\mathfrak{p}$ if $i \geq 1$ or j is not a power of a prime number. Since this holds for all $\mathfrak{p} \in \operatorname{Spec} R$, and R is reduced by assumption, it follows that $a_{i,j} = 0$ if $i \geq 1$ or j is not a power of a prime number. Hence, we have $f = a_{0,1}T + \sum_{l \geq 1} \sum_{p \in \mathscr{P}} a_{0,p^l} T^{p^l}$, which belongs to $R[T]$. Then, (A2) implies that f is additive. Thus, we know by Lemma 8 that $pa_{0,p^l} = 0$ holds for each $l \geq 1$ and $p \in \mathscr{P}$. Therefore, f belongs to $\mathscr{A}$. □

Remark 8. (i) If $\mathbf{Q} \subset R$, then we have $\mathscr{A} = \{aT \mid a \in R\}$, since $pa \neq 0$ for any $p \in \mathscr{P}$ and $a \in R \backslash \{0\}$.

(ii) If $\operatorname{char} R = p \in \mathscr{P}$, then we have $\mathscr{A} = R[T]^{(p)}$, since $pa = 0$ for any $a \in R$, and $qa \neq 0$ for any $q \in \mathscr{P} \backslash \{p\}$ and $a \in R \backslash \{0\}$.

Example 4. Let $R_1 := \mathbf{Z}[a,b]/(2a,3b)$ and $R_2 := \mathbf{Z}[a,b]/(2a,3b,6)$, where a and b are variables. Then, we have $\operatorname{char} R_1 = 0$ and $\operatorname{char} R_2 = 6$. For $i = 1,2$, we can define a $\mathbf{G}_a$-action on $R_i[x]$ by $\sigma(x) = x + aT^2 + bT^3$.

References

[1] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, MA, 1969.

[2] D. Daigle and G. Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension 5, J. Algebra **221** (1999), 528–535.

[3] G. Freudenburg, Actions of $\mathbf{G}_a$ on $\mathbf{A}^3$ defined by homogeneous derivations, J. Pure Appl. Algebra **126** (1998), 169–181.

[4] Y. Imamura, On the invariant ring of a certain exponential map on the polynomial ring over a non-reduced commutative ring, Master's Thesis, Tokyo Metropolitan University, January, 2018.

[5] H. Kojima, Locally finite iterative higher derivations on $k[x, y]$, Colloq. Math. **137** (2014), no. 2, 215–220.

[6] S. Kuroda, The automorphism theorem and additive group actions on the affine plane, Nihonkai Math. J. **28** (2017), no. 1, 65–68.

[7] S. Kuroda, A generalization of Nakai's theorem on locally finite iterative higher derivations, Osaka J. Math. **54** (2017), 335–341.

[8] M. Miyanishi, Normal affine subalgebras of a polynomial ring, Algebraic and Topological Theories—to the memory of Dr. Takehiko Miyata (Tokyo), Kinokuniya, 1985, pp. 37–51.

[9] M. Miyanishi, G_a-action of the affine plane, Nagoya Math. J. **41** (1971), 97–100.

[10] H. Matsumura, Commutative ring theory, translated from the Japanese by M. Reid, second edition, Cambridge Studies in Advanced Mathematics, 8, Cambridge University Press, Cambridge, 1989.

[11] R. Rentschler, Opérations du groupe additif sur le plan affine, C. R. Acad. Sci. Paris Sér. A-B **267** (1968), 384–387.

[12] A. Sathaye, On linear planes, Proc. Amer. Math. Soc. **56** (1976), 1–7.

Motoki Kuroda
Department of Mathematical Sciences
Tokyo Metropolitan University
1-1 *Minami-Osawa, Hachioji*
Tokyo 192-0397, *Japan*
E-mail: kuroda-motoki@ed.tmu.ac.jp

Shigeru Kuroda
Department of Mathematical Sciences
Tokyo Metropolitan University
1-1 *Minami-Osawa, Hachioji*
Tokyo 192-0397, *Japan*
E-mail: kuroda@tmu.ac.jp