LOCALLY NILPOTENT DERIVATIONS ON POLYNOMIAL RINGS IN TWO VARIABLES OVER A FIELD OF CHARACTERISTIC ZERO

By
Nyobe Likeng Samuel Aristide, B.Sc., M.S.
March 2017

A Thesis
submitted to the School of Graduate Studies and Research
in partial fulfillment of the requirements
for the degree of
Master of Science in Mathematics[1]

[1]The M.Sc. Program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

The main goal of this thesis is to present the theory of Locally Nilpotent Derivations and to show how it can be used to investigate the structure of the polynomial ring in two variables $k[X, Y]$ over a field k of characteristic zero. The thesis gives a complete proof of Rentschler's Theorem, which describes all locally nilpotent derivations of $k[X, Y]$. Then we present Rentschler's proof of Jung's Theorem, which partially describes the group of automorphisms of $k[X, Y]$. Finally, we present the proof of the Structure Theorem for the group of automorphisms of $k[X, Y]$.

Key Words: Locally nilpotent derivation, Rentschler's Theorem, Tame automorphisms, Wild automorphisms.

Acknowledgements

I would like to thank my supervisor Professor Daniel Daigle, who has always been there for me when I was facing some difficulties in my courses and who patiently allowed me to understand the theory developed in this thesis. He also helped with editing of my English in this thesis; and all over who believed in me when I was facing some hard moment at the beginning of my program.

Dedication

I dedicate this work to my parents.

Contents

Introduction

Throughout this thesis the word *ring* means a commutative ring with a unity.

A derivation of a ring B is a map $D : B \longrightarrow B$ satisfying $D(a+b) = D(a) + D(b)$ and $D(ab) = D(a)b + aD(b)$ for all $a, b \in B$.

A derivation D of a ring B is said to be *locally nilpotent* if:

$$\text{for each } b \in B, \text{ there exists } n \in \mathbb{N} \text{ such that } D^n(b) = 0.$$

Let k be a field. Given the ring $B = k[X, Y]$, the polynomial ring in two variables over k, two problems may be stated:

(1) Describe the structure of the group of automorphisms of the k-algebra $k[X, Y]$.

(2) Assuming that k has characteristic zero, describe all locally nilpotent derivations of $k[X, Y]$.

Problem (1) has been solved by Jung in 1942 and by van der Kulk in 1953. Problem (2) was solved by Rentschler in 1968. The objective of this thesis is to present these solutions, using the book of Freudenburg [6] as our main reference.

Let k be a field and $n \geq 1$, and let $k[X_1, \ldots, X_n]$ be the polynomial ring in n variables. The automorphism group of the k-algebra $k[X_1, \ldots, X_n]$ is denoted $\mathrm{GA}_n(k)$, and is called the *general affine group in dimension n.* Let $\mathrm{Af}_n(k)$ be the set of $\phi \in \mathrm{GA}_n(k)$ given by

$$\phi(X_j) = a_{1j}X_1 + \cdots + a_{nj}X_n + b_j \qquad \text{for } 1 \leq j \leq n,$$

where $b_1, \ldots, b_n \in k$ and $(a_{ij}) \in \mathrm{GL}_n(k)$ and $\mathrm{BA}_n(k)$ be the set of $\phi \in \mathrm{GA}_n(k)$ given by

$$\phi(X_i) = a_i X_i + f_i \qquad \text{for } 1 \leq i \leq n,$$

where $a_1, \ldots, a_n \in k^\times$, $f_1 \in k$, and $f_i \in k[X_1, \ldots, X_{i-1}]$ for all i such that $1 < i \leq n$. Then $\mathrm{Af}_n(k)$ and $\mathrm{BA}_n(k)$ are subgroups of $\mathrm{GA}_n(k)$. The elements of $\mathrm{Af}_n(k)$ are called the *affine automorphisms* and those of $\mathrm{BA}_n(k)$ the *triangular automorphisms*; $\mathrm{Af}_n(k)$ and $\mathrm{BA}_n(k)$ are sometimes called the *affine subgroup* and the *triangular subgroup* of $\mathrm{GA}_n(k)$. The subgroup of $\mathrm{GA}_n(k)$ generated by $\mathrm{Af}_n(k) \cup \mathrm{BA}_n(k)$ is called the *tame subgroup* of $\mathrm{GA}_n(k)$, and the elements of that subgroup are called the *tame automorphisms* of $k[X_1, \ldots, X_n]$. An automorphism that is not tame is said to be *wild*. It is natural to ask:

Is it the case that all automorphisms of $k[X_1, \ldots, X_n]$ are tame?

In 1942 Jung showed in his paper [9] that $\mathrm{GA}_2(k) = \langle \mathrm{Af}_2(k) \cup \mathrm{BA}_2(k) \rangle$ in the particular case where k is of characteristic zero; in other words, he showed that all automorphisms of $k[X, Y]$ are tame. In 1953 van der Kulk showed in [10] that this result is also true when k is of positive characteristic. The same article of van der Kulk also contains a Structure Theorem for $\mathrm{GA}_2(k)$ (Theorem 3.4.4 of this thesis), which asserts that each element of this group has a unique factorization of a certain kind. This result of van der Kulk completely describes the structure of the group $\mathrm{GA}_2(k)$.

It is interesting to note that the results of Jung and van der Kulk cannot be extended in higher dimension. As we will see in the last chapter, there exist wild automorphisms of $k[X, Y, Z]$ and it is an open problem to describe the structure of $\mathrm{GA}_3(k)$.

The following theorem, proved by Rentschler in [18] in 1968, gives a complete solution to the Problem (2) stated above:

> **Rentschler's Theorem.** *Let $B = k[X, Y]$ where k is a field of characteristic zero, and let $D : B \to B$ be a locally nilpotent derivation. Then there exist a tame automorphism α of B and a polynomial $f(X) \in k[X]$ such that $\alpha \circ D \circ \alpha^{-1} = f(X)\frac{\partial}{\partial Y}$.*

Rentschler also showed that his Theorem implies Jung's Theorem as a corollary, and this will be our approach for proving Jung's Theorem in this thesis.

Let us discuss locally nilpotent derivations in general, to give some perspective on Problem (2). We write $\mathrm{LND}(B)$ for the set of locally nilpotent derivations of a ring B.

It was known before Rentschler's article that locally nilpotent derivations are closely related to group actions on algebraic varieties. More precisely, if $X \subseteq \mathbb{C}^n$ is an affine algebraic variety and $A(X)$ is its affine coordinate ring (i.e., $A(X) = \mathbb{C}[X_1, \ldots, X_n]/I(X)$ where $I(X) \subset \mathbb{C}[X_1, \ldots, X_n]$ is the ideal of X), then studying the locally nilpotent derivations of the ring $A(X)$ is equivalent to studying the actions of the algebraic group $\mathbb{G}_a = (\mathbb{C}, +)$ on the algebraic variety X. In particular, studying the locally nilpotent derivations of $\mathbb{C}[X, Y]$ is equivalent to studying the actions of $\mathbb{G}_a$ on the algebraic variety $\mathbb{C}^2$. This is actually the reason why Rentschler proved the above Theorem: his article [18] gives a complete description of all actions of $\mathbb{G}_a$ on $\mathbb{C}^2$, and he obtained that result as a consequence of his description of the locally nilpotent derivations of $\mathbb{C}[X, Y]$.

Given an algebra B over a field k of characteristic zero, locally nilpotent derivations may be used for investigating the automorphisms of B. Indeed, it can be shown that for each $D \in \mathrm{LND}(B)$ the map

$$\begin{array}{rcl} \exp(D) : B & \to & B \\ b & \mapsto & \sum_{n=0}^{\infty} \frac{1}{n!} D^n(b) \end{array}$$

is an automorphism of B as a k-algebra. In the case where $B = k[X_1, \ldots, X_n]$, it is conjectured that $\mathrm{GA}_n(k) = \left\langle \mathrm{Af}_n(k) \cup \{\exp(D) \mid D \in \mathrm{LND}(B)\} \right\rangle$, and it is believed that in order to understand $\mathrm{GA}_n(k)$ it will be necessary to first understand $\mathrm{LND}(B)$.

Locally nilpotent derivations are also very useful for defining invariants of rings. For instance, if B is a ring then $\mathrm{ML}(B) = \bigcap_{D \in \mathrm{LND}(B)} \ker(D)$ is a subring of B which is called the *Makar-Limanov invariant* of B. The ring invariants defined in terms of locally nilpotent derivations are currently the subject of much research activity.

These are some of the reasons why locally nilpotent derivations are now regarded as an important tool for investigating the structure of commutative rings. The aim of the thesis is to present the basic theory of locally nilpotent derivations, and to show how that theory can be used to investigate the ring $k[X, Y]$.

This thesis is organised as follows:

Chapter 1 gathers some preliminaries on several topics: basic algebra, polynomial rings and systems of variables, transcendence degree, degree functions and graded rings.

Chapter 2 is about Locally Nilpotent Derivations. We first give some basic facts from this theory, and prove the Slice Theorem. At the end of this chapter we present the technique of homogenization of derivations, which has a particular importance for the proof of Rentschler's Theorem.

Chapter 3 focuses on the polynomial ring $k[X, Y]$, and in particular on the above problems (1) and (2). We give a complete proof of Rentschler's Theorem, and deduce Jung's Theorem as a corollary. Our proof of Jung's Theorem is based on the one given in [6], which is essentially the one given by Rentschler. As we already mentioned, van der Kulk showed that Jung's Theorem is valid over an arbitrary field. However our proof is only valid in characteristic zero.

We also give a complete proof of the Structure Theorem for $\mathrm{GA}_2(k)$ (our proof is for the case $\operatorname{char} k = 0$). This, however, turned out to be more complicated than expected. We were planning to follow the proof given in [6], but there is a step in that argument that we could not understand. Namely, on page 90 of [6], one considers an arbitrary $\kappa \in \mathrm{GA}_2(k)$ and a factorization $\kappa = ch_1 \cdots h_n$ satisfying certain requirements, and one has to show that such a factorization of κ is unique. On line -7 of that page, it is claimed that it is enough to prove the special case "$\kappa = $ identity" of that statement; no justification is given for that claim, and we don't see why it is true. The case "$\kappa = $ identity" is correctly proved in [6], but as far as we can see, this does not prove the Theorem. Resolving this issue added several pages to the proof, so finally our proof of the Structure Theorem is quite different from that given in [6].

Chapter 4 gives some remarks on the locally nilpotent derivations and the automorphisms of the polynomial ring in three variables. More precisely we observe that Rentschler's Theorem is not true in dimension 3 and that some elements of $\mathrm{GA}_3(k)$ are wild.

References. Our main references are Freudenburg's book [6], Daigle's lecture notes

[3], and the articles of Jung [9], van der Kulk [10] and Rentschler [18].

Since this thesis is of an expository nature, all results contained in it are known, and in principle each result should come with a reference. We do that whenever possible, but there remains a certain number of results for which we are unable to find suitable references. Typically, these are simple results known to the experts, but whose proofs are not published or hard to locate. An example of that is the sequence of results (1.2.7, 1.2.9, 1.2.19, 1.2.20 and 1.2.22) on polynomial rings.

Chapter 1

Preliminaries

In this chapter, we recall some basic notions which will be used later in this thesis; most of these results can be found in any textbook of commutative algebra.

1.1 Basic definitions

In this thesis, the word *ring* has the following meaning:

Definition 1.1.1. A *ring* is a set B with two binary operations (addition and multiplication) satisfying:

1. $(B, +)$ is an abelian group.

2. Multiplication is commutative, associative and distributive over addition:

$$xy = yx, \text{ for all } x, y \in B$$

$$(xy)z = x(yz), \quad \text{for all } x, y, z \in B$$

$$x(y + z) = xy + xz, \quad \text{for all } x, y, z \in B.$$

3. Multiplication has an identity element, denoted 1 or 1_B:

$$x1 = x = 1x, \text{ for all } x \in B.$$

Definition 1.1.2. A *unit* of a ring B is an element $x \in B$ satisfying $xy = 1$ for some $y \in B$. The symbol $B^\times$ denotes the set of all units of B.

A ring which has only one element is called a *zero ring*. It is well known that a ring B is a zero ring if and only if $1_B = 0_B$.

Definition 1.1.3.
1. An *integral domain* (or simply a *domain*) is a nonzero ring B such that, for all $x, y \in B$, the condition $xy = 0$ implies $x = 0$ or $y = 0$.
2. A *field* is a nonzero ring F such that each element of $F \setminus \{0\}$ is a unit.

Definition 1.1.4. A *subring* of a ring B is a subgroup of $(B, +)$ which is closed under the multiplication of B and which contains 1_B, the identity of B.

Definition 1.1.5. Let A and B be rings. A *ring homomorphism* from A to B is a set map $\varphi : A \longrightarrow B$ satisfying $\varphi(1_A) = 1_B$ and:

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \quad \text{and} \quad \varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2) \quad \text{for all} \quad a_1, a_2 \in A.$$

For any ring B there exists exactly one ring homomorphism from $\mathbb{Z}$ to B. This unique homomorphism $\eta : \mathbb{Z} \longrightarrow B$ is defined by:

$$\text{For each } n \in \mathbb{Z}, \quad \eta(n) = n1_B = \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{n} & \text{if } n > 0 \\ -(\underbrace{1 + 1 + \cdots + 1}_{|n|}) & \text{if } n < 0 \\ 0 & \text{if } n = 0. \end{cases}$$

Note that $\ker \eta$ is an ideal of $\mathbb{Z}$. So there exists a unique nonnegative integer $p \geq 0$ such that $\ker \eta = (p)$.

Definition 1.1.6. The nonnegative integer p defined above is called the *characteristic* of B.

It is easy to see that if B is a domain, its characteristic is either zero or a prime number.

Definition 1.1.7. Let B be a domain.

1. An element p of B is said to be *irreducible* if $p \notin B^\times \cup \{0\}$ and if the condition $p = xy$ (with $x, y \in B$) implies that $\{x, y\} \cap B^\times \neq \emptyset$.

2. An element p of B is said to be *prime* if $p \notin B^\times \cup \{0\}$ and if the condition $p|xy$ (with $x, y \in B$) implies that $p|x$ or $p|y$.

3. Two elements a and b are said to be *associates* in B, if $a = ub$ for some $u \in B^\times$.

The following result is Proposition 10 of the Section 8.3 of [4].

Proposition 1.1.8. *In a domain B, every prime element is irreducible.*

Proof. Let p be prime such that $p = xy$ in B. Then p divides x or y (since p is prime). Assume without loss of generality that p divides x, then $x = \mu p$ for some $\mu \in B$. This implies that $x = \mu p = \mu xy$; so $x(1 - y\mu) = 0$. Since B is a domain and $x \neq 0$, we thus have $y\mu = 1$, that is $y \in B^\times$. Thus p is irreducible. □

Remark 1.1.9. The converse is not necessarily true.

Definition 1.1.10. A *unique factorization domain* (UFD) is a domain B such that each element of $B \setminus (B^\times \cup \{0\})$ is a product of prime elements.

Example 1.1.11. 1. The ring $\mathbb{Z}$ of integers is a UFD.

2. A field is trivially a UFD.

3. If A is a UFD, then the polynomial ring $A[X_1, \cdots, X_n]$ is a UFD.

The following well known result is Proposition 12 of Section 8.3 of [4] but the approach here is quite different.

Proposition 1.1.12. *If B is a UFD, then an element of B is irreducible if and only if it is prime.*

Proof. We have already shown in Proposition 1.1.8 that every prime element is irreducible in a domain. Now assume that p is an irreducible element in B, then $p \in B \setminus (B^\times \cup \{0\})$ and since B is a UFD p can be written as $p = q_1 q_2 \cdots q_r$; where all the q_i for $i = 1, \cdots, r$ are prime. But p is irreducible, this forces $r = 1$. Hence $p = q_1$ and then p is prime. □

Definition 1.1.13. Let A be a ring. An *A-module* is a a pair (M, μ), where M is an abelian group (written additively) and μ is a mapping of $A \times M$ into M such that, if we write ax for $\mu(a, x)$ $(a \in A,\ x \in M)$, the following axioms are satisfied:

1. $a(x + y) = ax + ay$,
2. $(a + b)x = ax + bx$,
3. $(ab)x = a(bx)$,
4. $1x = x$ $\qquad (a, b \in A;\quad x, y \in M)$.

A *submodule* of an A-module M is a subgroup N of M satisfying $ax \in N$ for all $a \in A$, $x \in N$.

We shall assume that the reader is familiar with the basic concepts of the theory of modules.

Definition 1.1.14. Let A be a ring. An *A-algebra* is a pair (B, f), where B is a ring and $f : A \longrightarrow B$ is a ring homomorphism.

Example 1.1.15.

1. Suppose A is a subring of a ring B. Then the inclusion map $i : A \longrightarrow B$ is a ring homomorphism, so (B, i) is an A-algebra. One says B is an A-algebra without mentioning i.
2. Let A be a ring. The zero ring is an A-algebra.
3. Let A be a ring and $n \in \mathbb{Z}_+$. Then the polynomial ring $A[X_1, \cdots, X_n]$ is an A-algebra with the inclusion homomorphism $i : A \longrightarrow A[X_1, \cdots, X_n]$.

Remark 1.1.16.

1. If k is a field and (B, f) is a k-algebra such that $B \neq 0$, then f is injective. So k can be canonically identified with its image in B. Thus a nonzero k-algebra (where k is a field) is effectively a ring containing k as a subring.
2. For any ring A, there exists a unique ring homomorphism $\mathbb{Z} \longrightarrow A$. Thus every ring is automatically a $\mathbb{Z}$-algebra. Moreover, if A is of characteristic 0, then A is a ring containing $\mathbb{Z}$ as a subring.

3. Let (B, f) be an A-algebra. Given $a \in A$ and $b \in B$, we can define a product $ab = f(a)b$. This product confers to B a structure of A-module.

Definition 1.1.17. Let (B, f) and (C, g) be two A-algebras. An *A-algebra homomorphism* (or simply an *A-homomorphism*) $h : B \longrightarrow C$ is a ring homomorphism which satisfies $h \circ f = g$. If this is the case, then $h : B \longrightarrow C$ is a homomorphism of A-modules.

Remark 1.1.18. Let A be a ring.

1. Let C be a subring of two rings B and D. Then it is easy to check that a ring homomorphism $\varphi : B \longrightarrow D$ is a C-algebra homomorphism if and only if it satisfies $\varphi(c) = c$ for all $c \in C$.

2. If B is an A-algebra, then the identity map $B \longrightarrow B$ is an A-homomorphism.

3. A composition of A-homomorphisms is an A-homomorphism.

4. If $\varphi : B \longrightarrow C$ is a bijective A-homomorphism, then $\varphi^{-1} : C \longrightarrow B$ is an A-homomorphism. In that case we say that φ is an isomorphism of A-algebras, or simply an A-isomorphism.

Definition 1.1.19. Let A be a ring and (B, f) an A-algebra. A *subalgebra* R of B is a subring R of B satisfying $f(A) \subseteq R$.

Remark 1.1.20. Let A be a ring.

1. If R is a subalgebra of an A-algebra B, then R is also an A-algebra and the inclusion $R \longrightarrow B$ is an A-homomorphism.

2. If B is an A-algebra then an arbitrary intersection of subalgebras of B is a subalgebra of B.

3. Given (B, f) and (C, g) two A-algebras and an A-homomorphism $h : B \longrightarrow C$, we have $h(B)$ is a subalgebra of C.

Definition 1.1.21. Let A be a ring, (B, f) an A-algebra and S a subset of B. The *subalgebra of B generated by S* is defined to be the intersection of all subalgebras R of B satisfying $S \subseteq R$. It is denoted by $A[S]$.

Remark 1.1.22. Let A be a ring, (B, f) an A-algebra and S a subset of B.

1. The subalgebra $A[S]$ of (B, f) is the intersection of all the subrings R of B satisfying $f(A) \cup S \subseteq R$. In the case where A is a subring of B, $A[S]$ is the smallest subring of B containing $A \cup S$.

2. The subalgebra $A[S]$ of (B, f) is the smallest subalgebra of B that contains S.

3. If S is a finite set, say $S = \{f_1, \cdots, f_n\}$, we write $A[f_1, \cdots, f_n]$ instead of $A[\{f_1, \cdots, f_n\}]$.

4. If $S = \emptyset$, then $A[\emptyset] = f(A)$.

1.2 Basic properties of polynomial rings

In this section we recall some basic results about polynomial rings which will be very useful later in this thesis.

Definition 1.2.1. Given a ring A and $n \in \mathbb{Z}_+$, we write $A[X_1, \cdots, X_n]$ for the polynomial ring in n variables over A. We assume that the reader is familiar with this ring. Note the following:

1. Each element P of $A[X_1, \cdots, X_n]$ is a formal expression

$$P = \sum_{(j_1, \cdots, j_n) \in \mathbb{N}^n} a_{j_1, \cdots, j_n} X_1^{j_1} \cdots X_n^{j_n}, \quad \text{where } a_{j_1, \cdots, j_n} \in A \text{ for all } (j_1, \cdots, j_n) \in \mathbb{N}^n$$

   and $a_{j_1, \cdots, j_n} = 0$ for all $(j_1, \cdots, j_n)$ except possibly finitely many of them. Note that a polynomial is a formal sum, not a function.

2. The element $a_{j_1, \cdots, j_n} X_1^{j_1} \cdots X_n^{j_n}$ of this formal sum is called a *monomial term* of P.

3. If $a_{j_1,\cdots,j_n} \neq 0$, then the exponent j_i of X_i is called the *degree in* X_i of the monomial $a_{j_1,\cdots,j_n}X_1^{j_1}\cdots X_n^{j_n}$. The sum $j = j_1 + j_2 + \cdots + j_n$ is called the *degree* of this monomial. A polynomial is called *homogeneous* if all its monomials with nonzero coefficients $a_{j_1,\cdots,j_n}$ have the same degree.

4. *The degree* of a nonzero polynomial is the largest degree of any of its nonzero monomial terms. The degree of the zero polynomial is $-\infty$.

5. If P is a polynomial in n variables, the sum of all the monomials in P of degree m is called the *homogeneous component* of P of degree m ($m \in \mathbb{N}$).

Remark 1.2.2.

- If $P \neq 0$ is of degree n, then P may be written as the sum $P_0 + P_1 + \cdots + P_n$ where P_m is the homogeneous component of P of degree m, for $0 \leq m \leq n$ (where some P_m may be zero).

- Note that $A[X_1, \cdots, X_n]$ can be defined inductively by

$$A[X_1, \cdots, X_n] = A[X_1, \cdots, X_{n-1}][X_n].$$

  This means that we can consider polynomials in n variables with coefficients in A, simply as polynomials in one variable (say X_n), but now with coefficients that are themselves polynomials in $n-1$ variables.

- The degree of a polynomial (as defined in part (4) of Definition 1.2.1) is an element of $\mathbb{N} \cup \{-\infty\}$.

- When A is a domain we have $A[X_1, \cdots .X_n]^\times = A^\times$.

Definition 1.2.3. Let A be a ring and B an A-algebra.

a. Given $P = \sum_{i_1,\cdots,i_n} a_{i_1,\cdots,i_n}X_1^{i_1}\cdots X_n^{i_n} \in A[X_1, \cdots, X_n]$ and $(b_1, \cdots, b_n) \in B^n$, we define $P(b_1, \cdots, b_n) \in B$ by:

$$P(b_1, \cdots, b_n) = \sum_{i_1,\cdots,i_n} a_{i_1,\cdots,i_n}b_1^{i_1}\cdots b_n^{i_n}.$$

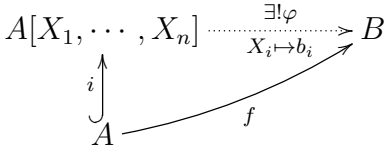
b. Given $b = (b_1, \cdots, b_n) \in B^n$, we define the map

$$\begin{aligned} \mathrm{ev}_b : A[X_1, \cdots, X_n] &\longrightarrow B \\ P(X_1, \cdots, X_n) &\longmapsto P(b_1, \cdots, b_n), \end{aligned}$$

which we call *"evaluation at b"*.

The following is the **universal property of the polynomial algebra**. It implies, among other things, that ev_b is a homomorphism of A-algebras. The proof of the universal property can be found in standard algebra textbooks.

Theorem 1.2.4. *Let A be a ring, $n \geq 1$ and $A[X_1, \cdots, X_n]$ the polynomial ring in n variables over A. Then for any choice of an A-algebra (B, f) and of an n-tuple $b = (b_1, \cdots, b_n) \in B^n$, there exists a unique A-homomorphism $\varphi : A[X_1, \cdots, X_n] \longrightarrow B$ satisfying $\varphi(X_i) = b_i$ for all $i = 1, \cdots, n$.*



Moreover, the following hold:

a. $\varphi = \mathrm{ev}_b$

b. $\mathrm{Im}\,\varphi = A[b_1, \cdots, b_n] = \{ P(b_1, \cdots, b_n) \mid P \in A[X_1, \cdots, X_n] \}$.

Definition 1.2.5. Let A be a subring of a ring B. An element $b \in B$ is said to be *algebraic* over A if there exists a nonzero polynomial $P \in A[T]$ such that $P(b) = 0$. Otherwise b is *transcendental* over A. If P can be chosen to be monic over A then b is said to be *integral* over A.
We say that B is algebraic over A if each element of B is algebraic over A.
We say that A is *algebraically closed* in B if each element of $B \setminus A$ is transcendental over A.
We say that A is *integrally closed* in B if no element of $B \setminus A$ is integral over A.

Definition 1.2.6. Let B be an algebra over a ring A. An element $f = (f_1, \cdots, f_n) \in B^n$ is said to be *algebraically dependent* over A if there exists $P \in A[X_1, \cdots, X_n] \setminus \{0\}$ such that $P(f_1, \cdots, f_n) = 0$. Otherwise $f = (f_1, \cdots, f_n)$ is said to be *algebraically independent* over A.

Notation. Let B be an algebra over a ring A and let $n \in \mathbb{N}$. We write

$$B = A^{[n]}$$

as an abbreviation for the sentence:

$$B \text{ is } A\text{-isomorphic to the polynomial algebra } A[X_1, \ldots, X_n].$$

Note that the conditions $B_1 = A^{[n]}$ and $B_2 = A^{[n]}$ do NOT imply that $B_1 = B_2$.

Corollary 1.2.7. *Let B be an algebra over a ring A. If $f = (f_1, \cdots, f_n) \in B^n$ is algebraically independent over A then $A[f_1, \cdots, f_n] = A^{[n]}$.*

Proof. The universal property 1.2.4 implies that $\mathrm{ev}_f : A[X_1, \cdots, X_n] \longrightarrow A[f_1, \cdots, f_n]$ is a surjective A-homomorphism. If $P \in \ker(\mathrm{ev}_f)$ then $P(f_1, \ldots, f_n) = \mathrm{ev}_f(P) = 0$, so $P = 0$ since f is algebraically independent over A. Therefore $\ker(\mathrm{ev}_f) = 0$ and so ev_f is an A-isomorphism. □

The converse of Corollary 1.2.7 is true, but is more difficult to prove. We will prove it in Proposition 1.2.22.

Example 1.2.8.

1. Let $B = \mathbb{C}[X, Y, Z]$; the element X^2Y^3+1 of B is transcendental over $\mathbb{C}$, so Corollary 1.2.7 implies that $\mathbb{C}[X^2Y^3 + 1] = \mathbb{C}^{[1]}$.

2. Let $B = \mathbb{C}[X, Y, Z]$ and $(X^2, Y^3, Z^2) \in B^3$. Since (X^2, Y^3, Z^2) is algebraically independent over $\mathbb{C}$, Corollary 1.2.7 implies that $\mathbb{C}[X^2, Y^3, Z^2] = \mathbb{C}^{[3]}$.

Proposition 1.2.9. *For an algebra B over a ring A, the following conditions are equivalent:*

a. $B = A^{[n]}$

b. There exist $f_1, \cdots, f_n \in B$ such that $(f_1, \cdots, f_n)$ is algebraically independent over A and $A[f_1, \cdots, f_n] = B$.

Proof. $b) \Rightarrow a)$ is Corollary 1.2.7.
$a) \Rightarrow b)$ The condition $B = A^{[n]}$ implies that there exists an A-isomorphism $\phi : A[X_1, \cdots, X_n] \longrightarrow B$. Set $f_1 = \phi(X_1), \cdots, f_n = \phi(X_n)$. Since ϕ is an A-homomorphism that sends X_i to f_i for all $i = 1, \ldots, n$, we must have $\mathrm{Im}(\phi) = A[f_1, \cdots, f_n]$ by part (b) of Theorem 1.2.4. As ϕ is surjective, $B = \mathrm{Im}(\phi) = A[f_1, \cdots, f_n]$.

Note that $\phi = \mathrm{ev}_f$ by part (a) of Theorem 1.2.4. If $P \in A[X_1, \cdots, X_n]$ is such that $P(f_1, \cdots, f_n) = 0$ then $\phi(P) = \mathrm{ev}_f(P) = P(f_1, \cdots, f_n) = 0$, so $P = 0$ since ϕ is injective. Thus $(f_1, \cdots, f_n)$ is algebraically independent over A. □

Definition 1.2.10. A ring B is *Noetherian* if it satisfies the following equivalent conditions:

(i) Every infinite ascending sequence $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of ideals of B stabilizes; that is there exists a nonnegative integer n such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

(ii) Every non empty collection of ideals of B has a maximal element.

(iii) Every ideal of B is finitely generated.

Example 1.2.11. Every field is a Noetherian ring.

The following basic results on Noetherian rings (1.2.12–1.2.15) can be found in Chapter 7 of [1].

Theorem 1.2.12 (Hilbert's Basis Theorem)**.** *If A is a Noetherian ring then so is the polynomial ring $A[X]$.*

Corollary 1.2.13. *If A is a Noetherian ring, then so is the polynomial ring in n variables $A[X_1, \cdots, X_n]$, for every $n \geq 1$.*

Lemma 1.2.14. *If A is a Noetherian ring and $A \to B$ is a surjective ring homomorphism then B is a Noetherian ring.*

Lemma 1.2.15. *Any finitely generated algebra over a Noetherian ring is itself a Noetherian ring.*

The following result is Exercise 10, Section 2, Chapter 1 of [11].

Lemma 1.2.16. *Let B be a Noetherian ring and $\varphi : B \longrightarrow B$ a ring homomorphism. If φ is surjective then φ is bijective.*

Definition 1.2.17. Let A be a ring, $n \in \mathbb{Z}_+$ and $B = A[X_1, \cdots, X_n]$ a polynomial ring in n variables over A. A *system of variables in B* is an n-tuple $(f_1, \cdots, f_n) \in B^n$ satisfying $B = A[f_1, \cdots, f_n]$.

Example 1.2.18. Let $B = \mathbb{C}[X, Y, Z]$.

1. (X, Y, Z) is a system of variables in B.
2. Since $\mathbb{C}[X, Y, Z + X^2Y] = B$, $(X, Y, Z + X^2Y)$ is a system of variables in B.
3. We have $\mathbb{C}[X, Y, Z, XY + Z^2] = B$ but $(X, Y, Z, XY + Z^2)$ is not a system of variables in B (because such a system must be a triple by definition).

Proposition 1.2.19. *Let A be a ring and $B = A[X_1, \cdots, X_n]$. Let $(f_1, \cdots, f_n) \in B^n$ be a system of variables in B. Then:*

i. $(f_1, \cdots, f_n)$ is algebraically independent over A.

ii. There exists an A-automorphism $\Phi : B \longrightarrow B$ such that $\Phi(X_i) = f_i$ for all $i = 1, \ldots, n$.

Proof. We have $A[f_1, \cdots, f_n] = B$ since $f = (f_1, \cdots, f_n)$ is a system of variables in B. Consider the A-homomorphism $\mathrm{ev}_f : A[X_1, \cdots, X_n] \longrightarrow A[X_1, \cdots, X_n]$. Then $\mathrm{Im}(\mathrm{ev}_f) = A[f_1, \cdots, f_n] = B$, so ev_f is surjective.

To prove the Proposition, it's enough to prove that condition (i) is true. Indeed, if $(f_1, \ldots, f_n)$ is algebraically independent over A then $\ker(\mathrm{ev}_f) = 0$, so ev_f is an A-automorphism, so $\Phi = \mathrm{ev}_f$ satisfies condition (ii).

So let us prove that $f = (f_1, \ldots, f_n)$ is algebraically independent over A. We first prove this in the case where A is Noetherian. Then $A[X_1, \cdots, X_n]$ is Noetherian by Corollary 1.2.13 and $\mathrm{ev}_f : A[X_1, \cdots, X_n] \to A[X_1, \cdots, X_n]$ is surjective, so Lemma 1.2.16 implies that ev_f is an A-automorphism. Therefore $\ker(\mathrm{ev}_f) = \{0\}$ and so f is algebraically independent over A.

We now drop the assumption that A is Noetherian. By contradiction, assume that $(f_1, \ldots, f_n)$ is algebraically dependent over A. Then there exists $Q \in A[T_1, \ldots, T_n] \setminus \{0\}$ such that $Q(f_1, \ldots, f_n) = 0$ (where $A[T_1, \ldots, T_n]$ is a polynomial ring in n variables over A). Since $A[f_1, \ldots, f_n] = B$, there also exist $P_1, \ldots, P_n \in A[T_1, \ldots, T_n]$ such that $X_i = P_i(f_1, \ldots, f_n)$ for $i = 1, \ldots, n$. Choose a finite subset S of A such that all coefficients of $Q, P_1, \ldots, P_n, f_1, \ldots, f_n$ belong to S.

Consider the minimal subring R of A. Since R is isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}/m\mathbb{Z}$ for some $m > 0$, R is a Noetherian ring. Since S is finite, the subring $A_0 = R[S]$ of A is a finitely generated algebra over R, so A_0 is Noetherian by Lemma 1.2.15. Note that $f_1, \ldots, f_n \in A_0[X_1, \ldots, X_n]$ and $Q, P_1, \ldots, P_n \in A_0[T_1, \ldots, T_n]$. For each $i = 1, \ldots, n$ we have

$$X_i = P_i(f_1, \ldots, f_n) \in A_0[f_1, \ldots, f_n].$$

It follows that $A_0[f_1, \ldots, f_n] = A_0[X_1, \ldots, X_n]$, so $(f_1, \ldots, f_n)$ is a system of variables of $A_0[X_1, \ldots, X_n]$. Since A_0 is Noetherian, the first part of the proof implies that $(f_1, \ldots, f_n)$ is algebraically independent over A_0. But $Q \in A_0[T_1, \ldots, T_n] \setminus \{0\}$ satisfies $Q(f_1, \ldots, f_n) = 0$, so we have a contradiction. □

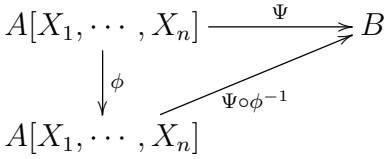
Corollary 1.2.20. *Let A be a ring and let $(f_1, \cdots, f_n)$ be a system of variables of $A[X_1, \cdots, X_n]$. Then for each A-algebra B and each $(b_1, \cdots, b_n) \in B^n$, there exists a unique A-homomorphism $\Phi : A[X_1, \cdots, X_n] \to B$ such that $\Phi(f_i) = b_i$ for all $i = 1, \ldots, n$.*

Proof. Write $f = (f_1, \ldots, f_n)$. By Theorem 1.2.4, there exist unique A-homomorphisms

$$\Psi : A[X_1, \cdots, X_n] \longrightarrow B \quad \text{and} \quad \phi : A[X_1, \cdots, X_n] \longrightarrow A[X_1, \cdots, X_n]$$

such that $\Psi(X_i) = b_i$ and $\phi(X_i) = f_i$ for $i = 1, \cdots, n$. By the same result we have $\phi = \mathrm{ev}_f$ and $\mathrm{Im}(\phi) = A[f_1, \ldots, f_n]$, so ϕ is surjective (note that $A[X_1, \cdots, X_n] = A[f_1, \cdots, f_n]$ since f is a system of variables of $A[X_1, \cdots, X_n]$). By Proposition 1.2.19, f is algebraically independent over A, and this implies that $\ker(\phi) = \ker(\mathrm{ev}_f) = 0$, so ϕ is an A-automorphism of $A[X_1, \ldots, X_n]$. Thus we obtain the following commutative

diagram.



Set $\Phi = \Psi \circ \phi^{-1}$, then clearly $\Phi(f_i) = b_i$ for all $i = 1, \cdots, n$.

If $\Phi' : A[X_1, \cdots, X_n] \to B$ is any A-homomorphism satisfying $\Phi'(f_i) = b_i$ for all i, then $\Phi' \circ \phi$ sends X_i to b_i for all i, so $\Phi' \circ \phi = \Psi$ by uniqueness of Ψ. Then $\Phi' = \Psi \circ \phi^{-1} = \Phi$, proving uniqueness. □

Example 1.2.21. The triple $(X, Y, Z + X^2Y)$ is a system of variables in $\mathbb{Z}[X, Y, Z]$, $\mathbb{R}$ is a $\mathbb{Z}$-algebra and $(\sqrt{2}, \frac{1}{7}, \sqrt{3}) \in \mathbb{R}^3$. So Corollary 1.2.20 implies that there exists a unique $\mathbb{Z}$-homomorphism $\Phi : \mathbb{Z}[X, Y, Z] \longrightarrow \mathbb{R}$ such that $\Phi(X) = \sqrt{2}$, $\Phi(Y) = \frac{1}{7}$ and $\Phi(Z + X^2Y) = \sqrt{3}$.

Proposition 1.2.22. *Let B be an algebra over a ring A, let $(f_1, \cdots, f_n) \in B^n$ and consider the subalgebra $A[f_1, \cdots, f_n]$ of B. The following are equivalent:*

1. $A[f_1, \cdots, f_n] = A^{[n]}$
2. $(f_1, \cdots, f_n)$ *is algebraically independent over A.*

Proof. 2) ⇒ 1) is Corollary 1.2.7.

1) ⇒ 2). Since $A[f_1, \cdots, f_n] = A^{[n]}$, there exists an A-isomorphism

$$\Phi : A[f_1, \cdots, f_n] \longrightarrow A[X_1, \cdots, X_n].$$

Set $g_i = \Phi(f_i),\ i = 1, \cdots, n$. We have $g_i \in A[X_1, \cdots, X_n]$ for all i, so $A[g_1, \cdots, g_n] \subseteq A[X_1, \cdots, X_n]$; let us prove that equality holds. Let $Q \in A[X_1, \cdots, X_n]$. Since Φ is surjective there exists $\xi \in A[f_1, \cdots, f_n]$ such that $\Phi(\xi) = Q$. We have $\xi = P(f_1, \cdots, f_n)$ for some $P \in A[X_1, \cdots, X_n]$, so

$$Q = \Phi(\xi) = \Phi(P(f_1, \cdots, f_n)) = P(g_1, \cdots, g_n) \in A[g_1, \cdots, g_n].$$

So $A[g_1, \cdots, g_n] = A[X_1, \cdots, X_n]$, hence $g = (g_1, \cdots, g_n)$ is a system of variables. By Proposition 1.2.19, $(g_1, \cdots, g_n)$ is algebraically independent over A.

If $H \in A[X_1, \cdots, X_n]$ is such that $H(f_1, \cdots, f_n) = 0$, then

$$H(g_1, \ldots, g_n) = H(\Phi(f_1), \ldots, \Phi(f_n)) = \Phi(H(f_1, \cdots, f_n)) = 0,$$

so $H = 0$ because $(g_1, \cdots, g_n)$ is algebraically independent over A. This shows that $(f_1, \cdots, f_n)$ is algebraically independent over A, so (1) $\Rightarrow$ (2). □

We generalize the notion of a system of variables (compare with Definition 1.2.17):

Definition 1.2.23. Let A be a ring and $B = A^{[n]}$. By a *system of variables* in B, we mean an n-tuple $(f_1, \ldots, f_n) \in B^n$ satisfying $B = A[f_1, \ldots, f_n]$.

Remark 1.2.24. Let A be a ring and $B = A^{[n]}$.

1. *There exists a system of variables in B.* Indeed, there exists an A-isomorphism $\phi : A[X_1, \ldots, X_n] \to B$; then $(\phi(X_1), \ldots, \phi(X_n))$ is a system of variables in B.
2. *If $(f_1, \ldots, f_n)$ is a system of variables in B, then $(f_1, \ldots, f_n)$ is algebraically independent over A.* Indeed, this follows from Proposition 1.2.22.

1.3 Degree functions and factorially closed subrings

Definition 1.3.1. Let B be a ring. A $\mathbb{Z}$-*valued degree function* on B is a set map

$$\deg : B \longrightarrow \mathbb{Z} \cup \{-\infty\}$$

satisfying the following conditions for all $f, g \in B$:

1. $\deg(f) = -\infty$ if and only if $f = 0$;
2. $\deg(fg) = \deg(f) + \deg(g)$;
3. $\deg(f + g) \leq \max\{\deg f, \deg g\}$.

An $\mathbb{N}$-*valued degree function* on B is a set map $\deg : B \longrightarrow \mathbb{N} \cup \{-\infty\}$ that satisfies the above conditions $1 - 3$ for all $f, g \in B$.

By a *degree function*, we mean either a $\mathbb{Z}$-valued or an $\mathbb{N}$-valued degree function.

Example 1.3.2. Let $B = A[X_1, \cdots, X_n]$ be the polynomial ring in n variables over a ring A. Given $f \in B$, let $\deg(f)$ denote the usual degree of f as a polynomial in $X_1, \cdots, X_n$ (as defined in Definition 1.2.1), and recall that $\deg(0) = -\infty$ by convention. This defines a set map $\deg : B \longrightarrow \mathbb{N} \cup \{-\infty\}, \quad f \longmapsto \deg(f)$. It is well known that if A is an *integral domain* then this map $\deg : B \longrightarrow \mathbb{N} \cup \{-\infty\}$ is a degree function in the sense of Definition 1.3.1. If A is not an integral domain then we have $\deg(fg) \leq \deg(f) + \deg(g)$ for all $f, g \in B$, but equality does not necessarily hold, so the map deg is not necessarily a degree function.

The following lemma is Exercise 4.2 of [3].

Lemma 1.3.3. *If B is a nonzero ring that admits a degree function, then B is an integral domain.*

Proof. Let $\deg : B \longrightarrow M \cup \{-\infty\}$ be a degree function (where M is either $\mathbb{Z}$ or $\mathbb{N}$). Let $f, g \in B \setminus \{0\}$. Then $\deg(f), \deg(g) \in M$ and $\deg(fg) = \deg(f) + \deg(g) \in M$, so $\deg(fg) \neq -\infty$, so $fg \neq 0$. □

Example 1.3.4. Let $B = A[X, Y] = A^{[2]}$ be a polynomial ring in two variables over a domain A. Consider the two systems of variables $f_1 = (X, Y)$, $f_2 = (X + Y^2, Y)$ in B and the element $P = X + Y^2$ of B. If we denote by $\deg_{f_1}$ and $\deg_{f_2}$ the degree functions associated to the systems of variables f_1 and f_2 respectively, then we have $\deg_{f_1}(P) = 2$ and $\deg_{f_2}(P) = 1$.

The following result is Exercise 4.5 of [3].

Lemma 1.3.5. *Let $\varphi : B \longrightarrow B'$ be an injective ring homomorphism. If $d : B' \longrightarrow \mathbb{N} \cup \{-\infty\}$ is a degree function, then $d \circ \varphi : B \longrightarrow \mathbb{N} \cup \{-\infty\}$ is also a degree function.*

Proof. Straightforward. □

Lemma 1.3.6. *Let A be a domain and $B = A^{[n]}$. Then each system of variables $f = (f_1, \ldots, f_n)$ in B determines an $\mathbb{N}$-valued degree function*

$$\deg_f : B \to \mathbb{N} \cup \{-\infty\}$$

that has the following property:

(∗) *for each* $b \in B$, $\deg_f(b)$ *is equal to the degree of the unique polynomial* $P(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ *that satisfies* $b = P(f_1, \ldots, f_n)$.

Proof. Let $f = (f_1, \ldots, f_n)$ be a system of variables in B (i.e., $B = A[f_1, \ldots, f_n]$). Let $A[X_1, \ldots, X_n]$ be the polynomial ring in n variables and consider the A-homomorphism $\mathrm{ev}_f : A[X_1, \ldots, X_n] \to B$. Since $B = A[f_1, \ldots, f_n]$, ev_f is surjective. Since $(f_1, \ldots, f_n)$ is algebraically independent over A, ev_f is injective. So we may consider the A-isomorphism $\phi = (\mathrm{ev}_f)^{-1} : B \to A[X_1, \ldots, X_n]$. Let $d : A[X_1, \ldots, X_n] \to \mathbb{N} \cup \{-\infty\}$ be the standard degree function on $A[X_1, \ldots, X_n]$ (i.e., $d(g) =$ degree of g as a polynomial in $X_1, \ldots, X_n$) and define

$$\deg_f = d \circ \phi : B \to \mathbb{N} \cup \{-\infty\}.$$

By Lemma 1.3.5, $\deg_f$ is a degree function on B. For each $b \in B$, $\phi(b)$ is equal to the unique polynomial $P(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ that satisfies $b = P(f_1, \ldots, f_n)$. So $\deg_f$ satisfies condition (∗). □

Definition 1.3.7. Let $A \subseteq B$ be domains. We say that A is *factorially closed* in B if:

$$\forall x, y \in B \setminus \{0\}, \quad xy \in A \Longrightarrow x, y \in A.$$

Example 1.3.8. Let $B[X]$ be the polynomial ring in one variable over an integral domain B. Then B is factorially closed in $B[X]$.

The next result gives an important property of $\mathbb{N}$-*valued degree functions*. Note that $\mathbb{Z}$-*valued degree functions* do not have the analogous property.

The following is Lemma 5.2 of [3].

Lemma 1.3.9. *Let* B *be a domain with a degree function* $\deg : B \longrightarrow \mathbb{N} \cup \{-\infty\}$. *Then the set* $\{x \in B \mid \deg x \leq 0\}$ *is a factorially closed subring of* B.

Proof. Clearly this set is a subring of B and for $x, y \in B \setminus \{0\}$ such that $\deg(xy) \leq 0$, we have $\deg(x) \leq 0$ and $\deg(y) \leq 0$, since $\deg(xy) = \deg(x) + \deg(y)$ and the degree function has values in $\mathbb{N} \cup \{-\infty\}$. □

Lemma 1.3.10. *If A and B are two domains such that $B = A^{[n]}$, then A is factorially closed in B.*

Proof. Let $X = (X_1, \cdots, X_n)$ be a system of variables in B. By Lemma 1.3.6, X determine a degree function $\deg : B \longrightarrow \mathbb{N} \cup \{-\infty\}$ (in the sense of Definition 1.2.1) such that $\{P \in B \mid \deg(P) \leq 0\} = A$. By Lemma 1.3.9 we have that A is factorially closed in B. □

Example 1.3.11. Let $B = k[X, Y] = k^{[2]}$ where k is a field and $A = k[X^2]$ be a subring of B. Then we have $B \neq A^{[1]}$. In fact assume that $B = A^{[1]}$, then A must be factorially closed in B. But $X \in B \setminus \{0\}$ and $X \notin A$ while $XX = X^2 \in A$, so A is not factorially closed in B. Hence $B \neq A^{[1]}$.

The following proposition can be found in [3] as Exercise 5.7.

Proposition 1.3.12. *Given A and B two domains such that $A \subseteq B$, we have:*

$$A \text{ is factorially closed in } B \Longrightarrow A \text{ is algebraically closed in } B$$
$$\Longrightarrow A \text{ is integrally closed in } B.$$

Proof. Assume that A is factorially closed in B and consider $b \in B$ algebraic over A. Let $f \in A[T] \setminus \{0\}$ of minimal degree such that $f(b) = 0$. If $b = 0$ then $b \in A$. Now assume that $b \neq 0$ and $f(T) = \sum_{i=0}^{n} a_i T^i \in A[T]$, $a_n \neq 0$ $(n \geq 1)$.

$$\begin{aligned} f(b) = 0 &\Longrightarrow a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n = 0 \\ &\Longrightarrow a_1 b + a_2 b^2 + \cdots + a_n b^n = -a_0 \\ &\Longrightarrow b g(b) \in A, \end{aligned}$$

where $g(T) = a_1 + a_2 T + \cdots + a_n T^{n-1} \in A[T]$ is nonzero because $a_n \neq 0$. Since $\deg(g) < \deg(f)$, we have $g(b) \neq 0$ and hence $b \in A$ (because A is factorially closed in B and $bg(b) \in A$). Hence A is algebraically closed in B.
Assume now that A is algebraically closed in B, and let C be the set of integral elements of B over A. We show that $A = C$. For all $a \in A$, we have $f(X) = X - a \in A[X] \setminus \{0\}$, and $f(a) = 0$, so $A \subseteq C$. Moreover, if $c \in C$ then $f(c) = 0$ for some nonzero monic $f \in A[T]$ so c is algebraic over A and hence $c \in A$, showing that $C \subseteq A$. Thus $A = C$ and so A is integrally closed in B. □

Lemma 1.3.13. *Let A be a domain and $f \in B = A[X_1, \cdots, X_n] = A^{[n]}$. If $\deg(f) = d \geq 1$ then f is transcendental over A.*

Proof. By Lemma 1.3.10, A is factorially closed in B. So A is algebraically closed in B by Proposition 1.3.12. Since $f \in B \setminus A$, f is transcendental over A. □

Definition 1.3.14. A field L is said to be *algebraically closed* if every nonconstant polynomial in $L[X]$ splits in $L[X]$.

Proposition 1.3.15. *Let $B = k^{[n]}$, where k is an algebraically closed field. Given $f \in B \setminus k$ and $A = k[f]$ a subring of B, the following are equivalent:*

(i) A is factorially closed in B.

(ii) For all $\lambda \in k$, $f - \lambda$ is irreducible in B.

Proof. $(i) \Longrightarrow (ii)$ Note that f is transcendental over k and hence $A = k[f] = k^{[1]}$ by Corollary 1.2.7. So f is a system of variables in A and, by Lemma 1.3.6, we may consider the degree function $\deg_f : A \longrightarrow \mathbb{N} \cup \{-\infty\}$ associated to f (that is, if $\omega \in A$ then $\deg_f(\omega)$ is the degree of ω as a polynomial in f). Assume that $f - \lambda = gh$ where $g, h \in B \setminus \{0\}$. Since $f - \lambda \in A$, then we must have $g, h \in A$ since A is factorially closed in B; but $f - \lambda = gh \Longrightarrow \deg_f(f - \lambda) = \deg_f(g) + \deg_f(h)$ that is $1 = \deg_f(g) + \deg_f(h)$, so $\deg_f(g) = 0$ or $\deg_f(h) = 0$ and thus $g \in k^\times$ or $h \in k^\times$. Therefore $f - \lambda$ is irreducible in B.
$(ii) \Longrightarrow (i)$ Let $g, h \in B \setminus \{0\}$ such that $gh \in A = k[f]$. Then there is $P(t) \in k[t]$ such that $gh = P(f)$.

If $\deg_t(P) < 1$, then we have $P(t) \in k^\times$ and so $gh = P(f) \in k^\times$. Thus $g, h \in k^\times$ since by Lemma 1.3.10, k is factorially closed in B; therefore $g, h \in A$.

Now if $m = \deg_t(P) \geq 1$, then $P(t) = \lambda \Pi_{i=1}^m (t - \lambda_i)$ where $\lambda \in k^\times$ and $\lambda_i \in k$, $i \in \{1, \cdots, m\}$, since k is a algebraically closed field. Thus $gh = P(f) = \lambda \Pi_{i=1}^m (f - \lambda_i)$; since $f - \lambda_i$ is irreducible in B for all i, g and h are subproducts of $\lambda \Pi_{i=1}^m (f - \lambda_i)$ and hence $g, h \in A$. □

Example 1.3.16. 1. Let $B = k[X, Y] = k^{[2]}$ where k is an algebraically closed field. We have $f = XY + 1 \in B \setminus k$ but $f - 1$ is not irreducible in B. Thus $k[f]$ is not factorially closed in B.

2. $B = \mathbb{C}[X, Y] = \mathbb{C}^{[2]}$ and $f = X^2 + Y^2 \in B \setminus \{0\}$. We have $\mathbb{C}[f]$ is not factorially closed since f is not irreducible in B.

3. Let $B = k[X, Y] = k^{[2]}$ where k is an algebraically closed field; we have $k[X^2 + Y^3]$ is factorially closed in B since for all $\lambda \in k$, $X^2 - Y^3 - \lambda$ is irreducible in B.

The following lemma can be found in [3] as Exercise 5.4.

Lemma 1.3.17. *Let A be factorially closed subring in a domain B. The following hold:*

1. *$A^\times = B^\times$.*

2. *An element of A is irreducible in A if and only if it is irreducible in B.*

3. *If an element of A is prime in B then it is prime in A.*

4. *If B is a UFD then so is A.*

Proof. 1. Since A is a subring of B we have $A^\times \subseteq B^\times$. Now let $x \in B^\times$, we have $x \neq 0$ and there is $y \in B \setminus \{0\}$ such that $xy = 1_B$. Morever $1_B \in A$ since A is a subring of B. Thus we have $x, y \in A$, and so $x \in A^\times$. Hence $B^\times \subseteq A^\times$ and thus $A^\times = B^\times$.

2. $\Longrightarrow$) Let $p \in A$ be an irreducible element in A. We have $p \notin B^\times \cup \{0\}$ (by part (1)). Moreover assume that $p = ab$ in B, then $a, b \in A$ (since A is factorially closed in B and $p \in A$), thus $a \in A^\times = B^\times$ or $b \in A^\times = B^\times$ (since p is irreducible in A). Therefore p is irreducible in B.
$\Longleftarrow$) Now assume that $p \in A$ is irreducible in B, we have $p \notin A^\times \cup \{0\}$ (by 1). Let $a, b \in A$ such that $p = ab$ we have $a \in B^\times = A^\times$ or $b \in B^\times = A^\times$ (since p is irreducible in B). Hence p is irreducible in A.

3. Let $p \in A$ such that p is prime in B. Then $p \in A \setminus (A^\times \cup \{0\})$ (by part (1)). Given $a, b \in A$ such that $p|ab$ in A, we have $p|a$ or $p|b$ in B (since p is prime in B). We may assume that $p|a$ in B. Then there exists $x \in B$ such that $px = a$.

Since A is factorially closed in B it follows that $x \in A$, so $p|a$ in A. This shows that p is prime in A.

4. Let $a \in A \setminus (A^\times \cup \{0\})$. Then $a \in B \setminus (B^\times \cup \{0\})$, so we have $a = p_1 p_2 \cdots p_m$ where p_i, $i = 1, \cdots, m$ are prime elements in B. But all p_i are in A (since A is factorially closed) and so they must be prime in A (by part (3)). Therefore A is a UFD.

□

1.4 $\mathbb{Z}$-graded rings

Definition 1.4.1. A $\mathbb{Z}$-*graded ring* is a ring B together with a direct sum decomposition $B = \oplus_{n\in\mathbb{Z}} B_n$, where all the B_n are subgroups of $(B, +)$ satisfying $B_n B_m \subseteq B_{m+n}$ for all $n, m \in \mathbb{Z}$. The decomposition $B = \oplus_{n\in\mathbb{Z}} B_n$ is called a $\mathbb{Z}$-*grading* of B.

Remark 1.4.2. Let $B = \oplus_{n\in\mathbb{Z}} B_n$ be a $\mathbb{Z}$-graded ring.

1. An element of B is *homogeneous* if it belongs to $\cup_{n\in\mathbb{Z}} B_n$.

2. If $f \in B$ is homogeneous and $f \neq 0$, then there is a unique $d \in \mathbb{Z}$ such that $f \in B_d$. In this situation we say that f is *homogeneous of degree* d.

3. The element 0 is homogeneous of degree $-\infty$.

4. An element f of B is of the form $f = \sum_{n\in\mathbb{Z}} f_n$, where $f_n \in B_n$ for all $n \in \mathbb{Z}$, and $f_n = 0$ for all n except possibly finitely many of them. So f is a finite sum of homogeneous elements and this decomposition is unique.

Example 1.4.3. Take $B = k[X]$ where k is a field.

We define

$$B_n = \begin{cases} \text{span}_k\{X^n\} = \{aX^n \mid a \in k\} & \text{if } n \geq 0 \\ 0 & \text{if } n < 0. \end{cases}$$

Clearly $B = \oplus_{n\in\mathbb{Z}} B_n$, so $k[X]$ is a $\mathbb{Z}$-graded ring.

Example 1.4.4. Let k be a field and consider the polynomial ring $B = k[X_1, \cdots, X_n]$. Let $\omega = (\omega_1, \cdots, \omega_n) \in \mathbb{Z}^n$, and for each $d \in \mathbb{Z}$ define

$$B_d = \text{span}_k \{ X_1^{e_1} X_2^{e_2} \cdots X_n^{e_n} \mid (e_1, \cdots, e_n) \in \mathbb{N}^n \text{ and } e_1\omega_1 + \cdots + e_n\omega_n = d \}.$$

In fact B is a k-vector space and each B_d is a subspace of B. Clearly $B = k[X_1, \cdots, X_n] = \oplus_{d\in\mathbb{Z}} B_d$ and $B_{d_1} B_{d_2} \subseteq B_{d_1+d_2}$ for all $d_1, d_2 \in \mathbb{Z}$. So the n-tuple ω determines a $\mathbb{Z}$-grading of B. In this grading, if an element f is homogeneous of degree d, then we write $\deg_\omega(f) = d$.

The $\mathbb{Z}$-grading defined above is such that $\deg_\omega(X_i) = \omega_i,\ i = 1, \cdots, n$ and is called an *ω-grading* of $k[X_1, \cdots, X_n]$. When $\omega = (1, \cdots, 1)$, the grading is called the *standard $\mathbb{Z}$-grading* of B. A polynomial that is homogeneous with respect to the standard $\mathbb{Z}$-grading is called a *standard homogeneous polynomial*.

Example 1.4.5. Let $B = k[X, Y]$ where k is a field, and let $\omega = (2, -3)$. Then we have the ω-grading $B = \oplus_{n\in\mathbb{Z}} B_n$, where $B_n = \text{span}_k \{ X^i Y^j \mid 2i - 3j = n \}$. The elements X^2Y and $X^2Y + X^5Y^3$ are homogeneous of degree 1; the element XY is homogeneous of degree -1.

Lemma 1.4.6. *Let $B = \oplus_{n\in\mathbb{Z}} B_n$ be a $\mathbb{Z}$-graded ring. The following hold:*

(*i*) $1_B \in B_0$

(*ii*) *The subgroup B_0 is a subring of B.*

Proof. We have $1_B \in B$, then $1_B = \sum_{n\in\mathbb{Z}} f_n$, where $f_n \in B_n$. Thus for every $g_m \in B_m$ ($m \in \mathbb{Z}$), we have $g_m = g_m.1_B = \sum_{n\in\mathbb{Z}} f_n g_m$ and $f_n g_m \in B_{n+m}$. Consequently $f_n g_m = 0$ for all $n \neq 0$. It follows that if $n \neq 0$ then $f_n g = 0$ for all $g \in B$. In particular for $g = 1_B$, we have $f_n = 0$ for any $n \neq 0$. Hence $1_B = f_0 \in B_0$. Moreover, B_0 is a subgroup of $(B, +)$, $1_B \in B_0$ and $B_0 B_0 \subseteq B_0$, so B_0 is a subring and then (*ii*) is shown. □

Definition 1.4.7. Let $B = \oplus_{d\in\mathbb{Z}} B_d$ be a $\mathbb{Z}$-graded ring.

a) Let $f = \sum_{d\in\mathbb{Z}} f_d$ be an element of B (where $f_d \in B_d$ for all $d \in \mathbb{Z}$). The set $\text{supp}(f) = \{ d \in \mathbb{Z} \mid f_d \neq 0 \}$ is finite and is called *the support* of f.

b) We define the set map

$$\begin{aligned} \deg : B &\longrightarrow \mathbb{Z} \cup \{-\infty\} \\ f &\longmapsto \begin{cases} \max(\mathrm{supp}(f)) \ if \ f \neq 0 \\ -\infty \qquad\qquad if \ f = 0. \end{cases} \end{aligned}$$

Remark 1.4.8. Let B be a $\mathbb{Z}$-graded ring.

a) The map $\deg : B \longrightarrow \mathbb{Z} \cup \{-\infty\}$ defined in Definition 1.4.7 satisfies:

(i) $\deg(f) = -\infty \iff f = 0$

(ii) $\deg(fg) \leq \deg(f) + \deg(g) \ \ \forall \ f, g \in B$

(iii) $\deg(f+g) \leq \max\{\deg f, \deg g\} \ \forall \ f, g \in B$

(iv) If $\deg(f) \neq \deg(g)$, then $\deg(f+g) = \max\{\deg(f), \deg(g)\}$.

b) Assume that B is a domain. Then equality holds in a-ii) and consequently the map $\deg : B \longrightarrow \mathbb{Z} \cup \{-\infty\}$ is a degree function in the sense of Definition 1.3.1. We call it the *degree function determined by the grading.*

Proposition 1.4.9. *Let B be a $\mathbb{Z}$-graded domain and let $f, g \in B \setminus \{0\}$. If fg is homogeneous, then f and g are homogeneous.*

Proof. For $f \in B \setminus \{0\}$, set $m(f) = \min(\mathrm{supp}(f))$ and define the map:

$$\begin{aligned} L : B \setminus \{0\} &\longrightarrow \mathbb{N} \\ f &\longmapsto \deg(f) - m(f). \end{aligned}$$

Since B is domain, we have $m(fg) = m(f) + m(g)$ and consequently $L(fg) = L(f) + L(g)$. Now observe that an element $f \in B \setminus \{0\}$ is homogeneous if and only if $L(f) = 0$. Thus since fg is homogeneous, we have:

$$\begin{aligned} L(fg) = 0 &\Longrightarrow L(f) + L(g) = 0 \\ &\Longrightarrow L(f) = L(g) = 0. \end{aligned}$$

Therefore f and g are homogeneous. □

1.5 Rings of fractions and transcendence degree

Definition 1.5.1. Let A be a ring. A subset S of A is said to be *multiplicatively closed* if $1_A \in S$ and S is closed under multiplication.

Example 1.5.2.

- Given $\alpha \in A$, the subset $S = \{\alpha^n\}_{n\geq 0}$ of A is multiplicatively closed.
- If $\mathfrak{p}$ is a prime ideal of a ring A, the subset $S = A \setminus \mathfrak{p}$ of A is multiplicatively closed.

If S is a multiplicatively closed subset of a ring A then we can form the ring $S^{-1}A$, called the *ring of fractions* of A with respect to S. If M is an A-module then we can form the $S^{-1}A$-module $S^{-1}M$, called a *module of fractions*. We assume that the reader is familiar with the basic properties of $S^{-1}A$ and $S^{-1}M$.

Notation. Let A be a ring and S a multiplicatively closed subset of A.

- If $\alpha \in A$ and $S = \{\alpha^n\}_{n\geq 0}$, then we write A_α for $S^{-1}A$.
- If $\mathfrak{p}$ is a prime ideal of A and $S = A \setminus \mathfrak{p}$, we write $A_\mathfrak{p}$ for $S^{-1}A$.

Remark 1.5.3. Given a ring A and a multiplicatively closed subset S of A, the following hold:

(a) $S^{-1}A$ is the zero ring if and only if $0 \in S$.

(b) Let A, B be two rings such that $A \subseteq B$, and let S a multiplicatively closed subset of A. Then we have $S^{-1}A \subseteq S^{-1}B$. Moreover, if $M \subseteq N$ are A-modules then $S^{-1}M \subseteq S^{-1}N$.

The following proposition is the first Remark of the Chapter 3 of [1].

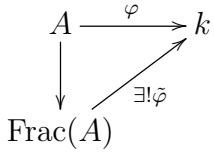
Proposition 1.5.4. *If A is a domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is a field.*

Proof. Clearly by Remark 1.5.3, $S^{-1}A \neq 0$. Furthermore for all $a/s \in S^{-1}A \setminus \{0\}$ we have $a \neq 0$ so $s/a \in S^{-1}A$. Thus $(a/s)(s/a) = 1/1 = 1_{S^{-1}A}$ and $S^{-1}A$ is a field. □

Definition 1.5.5. Let A be a domain. The field $S^{-1}A$ defined in the previous proposition is called the *field of fractions* of A. It is denoted by $\operatorname{Frac} A$.

Remark 1.5.6. If A is a domain of characteristic zero, then $\mathbb{Q} \subseteq \operatorname{Frac} A$.

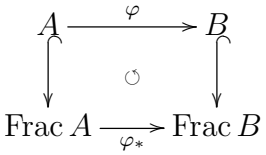
Theorem 1.5.7. *Let A be a domain and k a field. If $\varphi : A \longrightarrow k$ is a ring monomorphism, then there is a unique homomorphism $\tilde{\varphi} : \operatorname{Frac}(A) \longrightarrow k$ such that $\tilde{\varphi}(t) = \varphi(t)$ for all $t \in A \subseteq \operatorname{Frac}(A)$.*



Proof. This is Theorem 1.17 of [2]. □

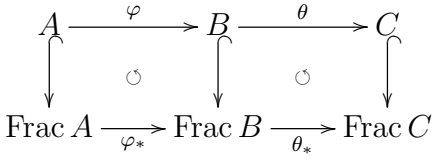
Remark 1.5.8. Let A be a domain and k a field containing A. Then we have $\operatorname{Frac}(A) \subseteq k$. The field $\operatorname{Frac}(A)$ is the smallest subfield of k containing A.

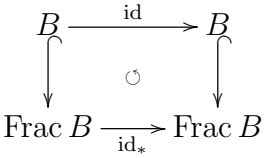
Lemma 1.5.9. *Let A, B and C be domains, and let $\varphi : A \longrightarrow B$ be a ring monomorphism. There exists a unique ring homomorphism $\varphi_* : \operatorname{Frac} A \longrightarrow \operatorname{Frac} B$ which satisfies $\varphi_*(t) = \varphi(t)$ whenever $t \in A \subseteq \operatorname{Frac} A$. That is the following diagram commutes:*



Moreover this construction has the following properties:

- *If $\varphi : A \longrightarrow B$ and $\theta : B \longrightarrow C$ are monomorphisms between integral domains, then $(\theta \circ \varphi)_* = \theta_* \circ \varphi_*$.*
- *For any integral domain B, the identity homomorphism $\mathrm{id} : B \longrightarrow B$ induces the identity homomorphism $\mathrm{id}_* : \operatorname{Frac} B \longrightarrow \operatorname{Frac} B$.*





Proof. This follows from Theorem 1.17 of [2]. □

Notation. If k is a field, $k^{(n)} = \mathrm{Frac}(k^{[n]}) =$ field of fractions of $k^{[n]}$.

Definition 1.5.10. Let A be a ring. A sequence $(M_i, f_i)_i$ where M_i is an A-module and f_i an A-linear map, defined as:

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

is said to be *exact at* M_i if $\mathrm{Im}(f_i) = \ker(f_{i+1})$. Such a sequence is said to be *exact* if it is exact at each M_i.
In particular the sequence:

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact if and only if it is exact at M', M and M'', if and only if f is injective, g is surjective and $\mathrm{Im}(f) = \ker(g)$. The last sequence, when it is exact, is called a *short exact sequence.*

The following result is Proposition 3.3 of Chapter 3 of [1].

Proposition 1.5.11. *Let A be a ring, $f : M' \longrightarrow M$ and $g : M \longrightarrow M''$ two A-module homomorphisms. Given S a multiplicatively closed subset of A, we have:*

(a) *The map $S^{-1}f : S^{-1}M' \longrightarrow S^{-1}M,\ m/s \longmapsto f(m)/s$ is a well defined $S^{-1}A$-module homomorphism. Moreover, $S^{-1}(g \circ f) = (S^{-1}g) \circ (S^{-1}f)$.*

(b) *The operation S^{-1} is exact: If $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact at M, then $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ is exact at $S^{-1}M$.*

Proof. *a*) is straightforward.
Now by assumption in *b*) we have $g \circ f = 0$, hence $S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0$; thus $\mathrm{Im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Let $m/s \in \ker(S^{-1}g)$, we have $g(m)/s = 0$ in $S^{-1}M$; hence there exists $t \in S$ such that $tg(m) = 0$ in M''. But $tg(m) = g(tm)$, since g is an A-module homomorphism. Thus $tm \in \ker(g) = \mathrm{Im}(f)$, therefore there exists $m' \in M'$ such that $tm = f(m')$.
Hence in $S^{-1}M$, we have $m/s = f(m')/st = (S^{-1}f)(m'/st) \in \mathrm{Im}(S^{-1}f)$.
Thus $\ker(S^{-1}g) \subseteq \mathrm{Im}(S^{-1}f)$. Therefore *b*) is shown. □

Definition 1.5.12. Let L, K be two fields such that $K \subseteq L$. Then we say that K is a *subfield* of L or L is an *extension (field)* of K.

1. A subset $\{s_1, \cdots, s_n\}$ of L (where $n \geq 1$ and $s_1, \cdots, s_n$ are distinct) is *algebraically independent over* K if there is no $P \in K[X_1, \cdots, X_n] \setminus \{0\}$ such that $P(s_1, \cdots, s_n) = 0$. An arbitrary subset S of L is called algebraically independent if every finite subset of S is algebraically independent. A subset S of L is *algebraically dependent* over K if it is not algebraically independent.

2. A field L is said to be an *algebraic closure* of a subfield K when it is algebraically closed and algebraic over K.

3. If S is a subset of L, we define $K(S)$ to be the intersection of all subfields of L that contain $K \cup S$. Then $K(S)$ is a field such that $K \subseteq K(S) \subseteq L$. The field $K(S)$ is the smallest subfield of L containing K and the subset S.
   If $S = \{s_1, \cdots, s_n\} \subseteq L$, then it can be shown that $K(s_1, \cdots, s_n)$ is the set of elements of the form $\dfrac{f(s_1, \cdots, s_n)}{g(s_1, \cdots, s_n)}$ where $f(X_1, \cdots, X_n), g(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]$ and $g(s_1, \cdots, s_n) \neq 0$.

Remark 1.5.13. Let $K \subseteq L$ be a field extension.

(a) The empty set is algebraically independent over K.

(b) If $b \in L$, then $\{b\}$ is algebraically independent over K if and only if b is transcendental over K.

Theorem 1.5.14. *Let $F \subseteq K \subseteq L$ be field extensions. If K is algebraic over F and L is algebraic over K, then L is algebraic over F.*

Proof. This is Theorem 20 in chapter 13 of [4]. □

Notation. Let $K \subseteq L$ be a field extension. We denote by $\overline{K}$ the set of all elements of L which are algebraic over K.

Proposition 1.5.15. *Let $K \subseteq L$ be a field extension. The subset $\overline{K}$ of L is a subfield of L containing K and the extension $K \subseteq \overline{K}$ is algebraic.*

Proof. This is corollary 19 in chapter 13 of [4]. □

Definition 1.5.16. Let $K \subseteq L$ be a field extension. A *transcendence basis* of $K \subseteq L$ is a subset $S \subseteq L$ satisfying:

- S is algebraically independent over K;
- L is algebraic over $K(S)$.

Lemma 1.5.17. *Let $K \subseteq L$ be a field extension.*

- *A transcendence basis of $K \subseteq L$ is a maximal subset (with respect to inclusion) of L which is algebraically independent over K.*
- *If S is a subset of L such that L is algebraic over $K(S)$ and S is minimal among subsets of L with this property, then S is a transcendence basis of L over K.*

Proof. These are Proposition 9.12 and Lemma 9.9 of [13]. □

Theorem 1.5.18. *Let $K \subseteq L$ be a field extension.*

1. *There exists at least one transcendence basis of $K \subseteq L$.*
2. *Any two transcendence bases of $K \subseteq L$ have the same cardinality.*

Proof. These are shown in Theorem 19.14 and 19.15 of [14]. □

Definition 1.5.19. The *transcendence degree* of $K \subseteq L$ is the cardinality of a transcendence basis of $K \subseteq L$; it is denoted by $\mathrm{trdeg}_K(L)$.

Proposition 1.5.20. *Let $K \subseteq L \subseteq M$ be field extensions. Then we have*

$$\mathrm{trdeg}_K(M) = \mathrm{trdeg}_K(L) + \mathrm{trdeg}_L(M).$$

Proof. This is Proposition 19.18 of [14]. □

Corollary 1.5.21. *Let $K \subseteq L \subseteq M$ be field extensions. Then we have*

$$\mathrm{trdeg}_K(M) < \infty \text{ if and only if } \mathrm{trdeg}_K(L) < \infty \text{ and } \mathrm{trdeg}_L(M) < \infty.$$

Proof. This follows from Proposition 19.18 of [14]. □

Example 1.5.22. (a) A field extension $K \subseteq L$ is algebraic if and only if $\mathrm{trdeg}_K(L) = 0$ (the empty set is a transcendence basis).

(b) Let $K[X_1, \cdots, X_n]$ be a polynomial ring over a field K, and consider $L = K(X_1, \cdots, X_n)$ the field of fractions of $K[X_1, \cdots, X_n]$. The subset $\{X_1, \cdots, X_n\} \subset L$ is a transcendence basis of the field extension $K \subseteq L$, hence $\mathrm{trdeg}_K K(X_1, \cdots, X_n) = n$. Furthermore, $K(X_1, \cdots, X_n) = \mathrm{Frac}(K[X_1, \cdots, X_n]) = \mathrm{Frac}(K^{[n]}) = K^{(n)}$, hence $\mathrm{trdeg}_K K^{(n)} = n$.

Lemma 1.5.23. *Consider the polynomial ring $B = A[X_1, \cdots, X_n]$ where A is a domain. Then* $\mathrm{Frac}\, B = (\mathrm{Frac}\, A)(X_1, \cdots, X_n)$.

Proof.

We have $B = A[X_1, \cdots, X_n] \subseteq (\mathrm{Frac}\, A)[X_1, \cdots, X_n]$
$\subseteq \mathrm{Frac}((\mathrm{Frac}\, A)[X_1, \cdots, X_n]) = (\mathrm{Frac}\, A)(X_1, \cdots, X_n)$.

Since $(\mathrm{Frac}\, A)(X_1, \cdots, X_n)$ is a field that contains B, we have

$$B \subseteq \mathrm{Frac}\, B \subseteq (\mathrm{Frac}\, A)(X_1, \cdots, X_n).$$

Since $A \subseteq B$ we have $\mathrm{Frac}\, A \subseteq \mathrm{Frac}\, B$. Furthermore, since $\mathrm{Frac}\, A \subseteq \mathrm{Frac}\, B$ and $X_1, \cdots, X_n \in \mathrm{Frac}\, B$, we have $(\mathrm{Frac}\, A)(X_1, \cdots, X_n) \subseteq \mathrm{Frac}\, B$.
So $\mathrm{Frac}\, B = (\mathrm{Frac}\, A)(X_1, \cdots, X_n)$. □

Notation. Given A, B two domains such that $A \subseteq B$, we define $\mathrm{trdeg}_A(B)$ to be equal to the transcendence degree of $\mathrm{Frac}\, B$ over $\mathrm{Frac}\, A$.

The following proposition can be found in [3] as Exercise 6.3.

Proposition 1.5.24. *1. Let $A \subseteq B$ be domains. Then we have* $\mathrm{trdeg}_A(B) = 0$ *if and only if B is algebraic over A.*

2. Given a domain A and $B = A^{[n]}$, we have $\mathrm{trdeg}_A(B) = n$.

3. Given three domains A, B and C such that $A \subseteq B \subseteq C$, we have $\mathrm{trdeg}_A(C) < \infty$ *if and only if both* $\mathrm{trdeg}_A(B) < \infty$ *and* $\mathrm{trdeg}_B(C) < \infty$. *Moreover if* $\mathrm{trdeg}_A(C) < \infty$, *then*

$$\mathrm{trdeg}_A(C) = \mathrm{trdeg}_A(B) + \mathrm{trdeg}_B(C).$$

Proof. 1. $\Rightarrow$) Assume that $\operatorname{trdeg}_A B = 0$, that is $\operatorname{trdeg}_{\operatorname{Frac} A} \operatorname{Frac} B = 0$. Then $\operatorname{Frac} B$ is algebraic over $\operatorname{Frac} A$. Now since $B \subseteq \operatorname{Frac} B$, then for all $b \in B$, there exists $f \in (\operatorname{Frac} A)[X] \setminus \{0\}$ such that $f(b) = 0$. Set $g(X) = sf(X)$, where $s = s_0 s_1 \cdots s_n$, $n = \deg(f)$ and the $s_i \in A \setminus \{0\}$ are the denominators of the coefficients of f. Thus $g(X) \in A[X] \setminus \{0\}$, and $g(b) = 0$; therefore B is algebraic over A.

$\Leftarrow$) Let $b/s \in \operatorname{Frac} B$ and consider the field extension $\operatorname{Frac} A \subseteq \operatorname{Frac} B$. Since B is algebraic over A, we have b, s are algebraic over A and thus over $\operatorname{Frac} A$. So $b, s \in \overline{\operatorname{Frac} A}$ and since $\overline{\operatorname{Frac} A}$ is a field by Proposition 1.5.15 we obtain that $b/s \in \overline{\operatorname{Frac} A}$. Thus b/s is algebraic over $\operatorname{Frac} A$, then $\operatorname{Frac} B$ is algebraic over $\operatorname{Frac} A$. Therefore $\operatorname{trdeg}_{\operatorname{Frac} A} \operatorname{Frac} B = 0$; that is $\operatorname{trdeg}_A B = 0$.

2. Let us write $B = A[X_1, \cdots, X_n]$. By Lemma 1.5.23, $\operatorname{Frac} B = (\operatorname{Frac} A)(X_1, \cdots, X_n)$. So by Example 1.5.22-b), we get $\operatorname{trdeg}_{\operatorname{Frac} A}(\operatorname{Frac} B) = n$ and hence $\operatorname{trdeg}_A(B) = n$.

3. Since $A \subseteq B \subseteq C$, we have $\operatorname{Frac} A \subseteq \operatorname{Frac} B \subseteq \operatorname{Frac} C$ by Remark 1.5.3-b); and the result follows from Proposition 1.5.20.

□

Lemma 1.5.25. *Let A, B and C be three domains such that $A \subseteq B \subseteq C$. If B is algebraic over A and C is algebraic over B, then C is algebraic over A.*

Proof. It is a consequence of Proposition 1.5.24. □

The next corollary is Exercise 6.4 of [3].

Corollary 1.5.26. *Let $A \subseteq B$ be domains, such that A is algebraically closed in B and $\operatorname{trdeg}_A(B) < \infty$. If A' is a ring such that $A \subseteq A' \subseteq B$ and $\operatorname{trdeg}_A(B) = \operatorname{trdeg}_{A'}(B)$, then $A = A'$.*

Proof. By Proposition 1.5.24-3), we get $\operatorname{trdeg}_A A' = 0$ and so A' is algebraic over A. Hence $A' = A$ since A is algebraically closed in B. □

The following two corollaries will be very useful later on in the text.

Corollary 1.5.27. *Given domains $A \subseteq B$, define $\overline{A} = \{b \in B \mid b \text{ is algebraic over } A\}$. Then $\overline{A}$ is a subring of B that contains A and $\overline{A}$ is algebraic over A.*

Proof. By Proposition 1.5.15 the set $\overline{\operatorname{Frac} A} = \{x \in \operatorname{Frac} B \mid x \text{ is algebraic over } \operatorname{Frac} A\}$ is a subfield of $\operatorname{Frac} B$ that contains $\operatorname{Frac} A$. We have the inclusions $A \subseteq \operatorname{Frac} A \subseteq \overline{\operatorname{Frac} A} \subseteq \operatorname{Frac} B \supseteq B$. Since B and $\overline{\operatorname{Frac} A}$ are subrings of $\operatorname{Frac} B$, it follows that $B \cap \overline{\operatorname{Frac} A}$ is a subring of $\operatorname{Frac} B$. It is easy to see that $\overline{A} = B \cap \overline{\operatorname{Frac} A}$, so $\overline{A}$ is a subring of $\operatorname{Frac} B$; since $\overline{A} \subseteq B$, it is in fact a subring of B. By definition, every element of $\overline{A}$ is algebraic over A, so $\overline{A}$ is algebraic over A. □

Corollary 1.5.28. *Let $A \subseteq B$ be domains and suppose that $b_1, \cdots, b_n \in B$ are such that $B = A[b_1, \cdots, b_n]$. If each b_i is algebraic over A, then B is algebraic over A.*

Proof. Define $\overline{A} = \{b \in B \mid b \text{ is algebraic over } A\}$, then Corollary 1.5.27 implies that $\overline{A}$ is a subring of B, $A \subseteq \overline{A} \subseteq B$ and $\overline{A}$ is algebraic over A. Since $A \subseteq \overline{A}$ and $b_1, \cdots, b_n \in \overline{A}$, we have $A[b_1, \cdots, b_n] \subseteq \overline{A}$, so $B = \overline{A}$ and hence B is algebraic over A. □

Chapter 2

Locally Nilpotent Derivations

In this chapter we introduce the theory of locally nilpotent derivations and we present some results which we will use in the next chapter.

2.1 Derivations

Definition 2.1.1. Let B be a ring. A *derivation* of a ring B is a map $D : B \longrightarrow B$ satisfying: For all $f, g \in B$

$$D(f+g) = D(f) + D(g)$$

$$D(fg) = D(f)g + fD(g).$$

Notation. The set of all derivations of a ring B is denoted by $\operatorname{Der} B$.

Example 2.1.2. Let B be a ring.

1. The zero map $B \longrightarrow B,\ x \longmapsto 0$, is a derivation, called the the *zero derivation.*

2. Let $B[t]$ be the polynomial ring in one variable over B. The map $D : B[t] \longrightarrow B[t]$ defined by:

$$D\left(\sum_{i=0}^{n} a_i t^i\right) = \sum_{i=1}^{n} i a_i t^{i-1}, \quad \textit{where } \sum_{i=0}^{n} a_i t^i \in B[t],$$

is a derivation. It is denoted by $\dfrac{d}{dt} : B[t] \longrightarrow B[t]$.

The next proposition is Exercise 1.7 of [3].

Proposition 2.1.3. *Let B be a ring, $D \in \operatorname{Der} B$ and $f_1, \cdots, f_n \in B$ where n is a positive integer. The following hold:*

1. *For all $f \in B$, the map $fD : B \longrightarrow B, x \longmapsto fD(x)$ is a derivation.*
2. *$D(f_1 + \cdots + f_n) = D(f_1) + \cdots + D(f_n)$*
3. *For all $f, g, h \in B$, $D(fgh) = ghD(f) + fhD(g) + fgD(h)$. More generally,*

$$D(f_1 \cdots f_n) = f_2 \cdots f_n D(f_1) + f_1 f_3 \cdots f_n D(f_2) + \cdots + f_1 \cdots f_{n-2} f_n D(f_{n-1}) + f_1 \cdots f_{n-1} D(f_n).$$

4. *For $f \in B$ and $k > 0$, $\quad D(f^k) = kf^{k-1}D(f)$.*

Proof. Straightforward. □

Corollary 2.1.4. *The set $\operatorname{Der} B$ of all derivations of a ring B is a B-module.*

Proof. It is easy to show that $(\operatorname{Der} B, +)$ is an abelian group. Moreover, by Proposition 2.1.3 we can define the map $B \times \operatorname{Der} B \longrightarrow \operatorname{Der} B, (f, D) \longmapsto fD$ which satisfies the axioms of Definition 1.1.13. Hence $\operatorname{Der} B$ is a B-module. □

Definition 2.1.5. Given, $D \in \operatorname{Der} B$, the set $\ker D = \{b \in B \mid D(b) = 0\}$ is called the *kernel of D*. It can also be called the *ring of constants* of D and be denoted B^D.

The proposition below can be found in [3] as Exercise 1.5.

Proposition 2.1.6. *Let B be a ring and $D \in \operatorname{Der} B$. Then $\ker D$ is a subring of B.*

Proof. We have $D(1) = D(1^2) = 2D(1) \Longrightarrow D(1) = 0$. Moreover $D(1-1) = D(1) + D(-1)$, but $D(0) = D(0+0) = 2D(0) \Longrightarrow D(0) = 0$; hence $D(-1) = -D(1) = 0$. Thus $1 \in \ker D$ and $-1 \in \ker D$. Now given $x, y \in \ker D$ it is easy to see that $x + y \in \ker D$ and $xy \in \ker D$. Therefore $\ker D$ is a subring of B. □

Example 2.1.7. Let k be a field. Consider the polynomial ring $k[t]$ and the derivation $D = \dfrac{d}{dt}$. When k is of positive characteristic p we have $\ker D = k[t^p]$, otherwise $\ker D = k$.

Remark 2.1.8. The only derivation $D : \mathbb{Z} \longrightarrow \mathbb{Z}$ is the zero derivation; this is because $\ker D$ is a subring of $\mathbb{Z}$ and the only subring of $\mathbb{Z}$ is $\mathbb{Z}$.

Definition 2.1.9. Let A, B be two rings such that $A \subseteq B$. An *A-derivation* of B is a derivation $D : B \longrightarrow B$ satisfying $D(a) = 0$ for all $a \in A$.
The set of all A-derivations of a ring B is denoted by $\mathrm{Der}_A(B)$. It is clear that $\mathrm{Der}_A(B)$ is a B-submodule of $\mathrm{Der}(B)$.

The lemma below is Exercise 3.1 of [3].

Lemma 2.1.10. *Let B be a $\mathbb{Q}$-algebra. Then we have* $\mathrm{Der}(B) = \mathrm{Der}_{\mathbb{Q}}(B)$.

Proof. If $B = 0$ the result is trivial. Assume that $B \neq 0$ and hence that $\mathbb{Q} \subseteq B$. Let $D \in \mathrm{Der}(B)$. Since $\ker D$ is a subring of B we have $\mathbb{Z} \subseteq \ker D$. If $n \in \mathbb{Z}$ and $n > 0$ then

$$0 = D(1) = D(\underbrace{\frac{1}{n} + \cdots + \frac{1}{n}}_{n \text{ times}}) = nD\left(\frac{1}{n}\right) \Longrightarrow D\left(\frac{1}{n}\right) = 0.$$

Since $\mathbb{Z} \subseteq \ker D$ and $\frac{1}{n} \in \ker D$ for all $n > 0$, we have $\mathbb{Q} \subseteq \ker D$. □

The next result is Exercise 1.10 of [3].

Proposition 2.1.11. *Let A be a ring and $B = A[t] = A^{[1]}$. If $D_1, D_2 \in \mathrm{Der}_A(B)$ satisfy $D_1(t) = D_2(t)$, then $D_1 = D_2$.*

Proof. Since $\mathrm{Der}_A(B)$ is a B-submodule of $\mathrm{Der}\, B$ and $D_1, D_2 \in \mathrm{Der}_A(B)$, we have $D_1 - D_2 \in \mathrm{Der}_A(B)$ and so $\ker(D_1 - D_2)$ is a subring of B. Moreover $A \subseteq \ker(D_1 - D_2)$ and $t \in \ker(D_1 - D_2)$. Hence $A[t] \subseteq \ker(D_1 - D_2)$, which implies that $D_1 - D_2 = 0$. □

Example 2.1.12. Let A be a ring and $B = A[X_1, \cdots, X_n] = A^{[n]}$. For all $j \in \{1, \cdots, n\}$, define $\frac{\partial}{\partial X_j} : B \longrightarrow B$ by

$$\frac{\partial}{\partial X_j}\left(\sum_{i_1, \cdots, i_n} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}\right) = \sum_{i_1, \cdots, i_n} i_j a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_{j-1}^{i_{j-1}} X_j^{i_j - 1} X_{j+1}^{i_{j+1}} \cdots X_n^{i_n},$$

where $\sum_{i_1,\cdots,i_n} a_{i_1\cdots i_n} X_1^{i_1}\cdots X_n^{i_n} \in B$.
Then $\frac{\partial}{\partial X_j} \in \mathrm{Der}_A(B)$. This derivation is called the *partial derivative with respect to* X_j. Also by definition of $\frac{\partial}{\partial X_j}$ we have:

$$\frac{\partial}{\partial X_j}(X_i) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j. \end{cases}$$

The following is Lemma 1.12 of [3].

Lemma 2.1.13. *Let A be a ring and $B = A[X_1, \cdots, X_n]$.*

1. *Given any $f_1, \cdots, f_n \in B$ there exists a unique $D \in \mathrm{Der}_A(B)$ satisfying $D(X_i) = f_i$ for all $i = 1, \cdots, n$.*

2. *The set $\mathrm{Der}_A(B)$ is a free B-module with basis $\{\frac{\partial}{\partial X_1}, \cdots, \frac{\partial}{\partial X_n}\}$.*

Proof. 1. Since $\mathrm{Der}_A(B)$ is a B-submodule of $\mathrm{Der}(B)$ and $\{\frac{\partial}{\partial X_1}, \cdots, \frac{\partial}{\partial X_n}\}$ are elements of $\mathrm{Der}_A(B)$ it follows that $\sum_{i=1}^n f_i \frac{\partial}{\partial X_i} \in \mathrm{Der}_A(B)$. Set $D = \sum_{i=1}^n f_i \frac{\partial}{\partial X_i}$, then clearly $D(X_i) = f_i$ for all $i \in \{1, \cdots, n\}$. Let $D' \in \mathrm{Der}_A(B)$ be such that $D'(X_i) = f_i$ for all i. Set $D_0 = D - D'$, then $D_0 \in \mathrm{Der}_A(B)$, hence $\ker D_0$ is a subring of B, $X_i \in \ker D_0$ for all $i \in \{1, \cdots, n\}$ and $A \subseteq \ker(D_0)$. So $B \subseteq \ker(D_0)$, hence $D_0 = 0$, that is $D = D'$.

2. Note that $\{\frac{\partial}{\partial X_1}, \cdots, \frac{\partial}{\partial X_n}\}$ is a finite subset of $\mathrm{Der}_A(B)$. Let $D \in \mathrm{Der}_A(B)$ and set $a_i = D(X_i) \in B$; by part (1), $D = \sum_{i=1}^n a_i \frac{\partial}{\partial X_i}$. Hence $\{\frac{\partial}{\partial X_1}, \cdots, \frac{\partial}{\partial X_n}\}$ is a generating set for the module $\mathrm{Der}_A(B)$.
Suppose that $a_1, \cdots, a_n \in B$ are such that $\sum_{i=1}^n a_i \frac{\partial}{\partial X_i} = 0$. Evaluating at each X_j, $j = 1, \cdots, n$, we get $a_j = 0$ for all j. So $\{\frac{\partial}{\partial X_1}, \cdots, \frac{\partial}{\partial X_n}\}$ is linearly independent over B and hence is a basis of $\mathrm{Der}_A(B)$. So $\mathrm{Der}_A(B)$ is free.

□

Remark 2.1.14. • Given rings $A \subseteq B$, the B-module $\mathrm{Der}_A(B)$ is not necessarily free. The previous result tell us that it is free when B is a polynomial ring over A.

- When $B = A^{[n]}$ where A is a ring, each system of variables $\gamma = (U_1, \cdots, U_n)$ of B determines a system of A-derivation $\frac{\partial}{\partial U_1}, \cdots, \frac{\partial}{\partial U_n}$. The derivation $\frac{\partial}{\partial U_j}$ is the unique element of $\mathrm{Der}_A(B)$ satisfying $\frac{\partial U_i}{\partial U_j} = \delta_{ij}$. For instance let $B = A^{[2]}$ and consider the two systems of variables $\gamma = (X, Y)$ and $\gamma' = (X, X^2 - Y) = (X, V)$. Relatively to the first system of variables, we have $\frac{\partial Y}{\partial X} = 0$ and relatively to the second we have $\frac{\partial Y}{\partial X} = \frac{\partial (X^2 - V)}{\partial X} = 2X$. So $\partial_X^{\gamma} \neq \partial_X^{\gamma'}$, and therefore distinct systems of variables may induce distinct bases (in Lemma 2.1.13 (2)).

The following useful result is Exercise 1.14 of [3].

Lemma 2.1.15. *Let B be a ring and $D \in \mathrm{Der}\, B$.*

1. *Consider a polynomial $f(T) = \sum_{i=0}^{n} a_i T^i \in B[T]$ $(a_i \in B)$ and $b \in B$. Then*

$$D(f(b)) = f^{(D)}(b) + f'(b)D(b)$$

where $f^{(D)}(T) = \sum_{i=0}^{n} D(a_i)T^i \in B[T]$ and $f'(T) = \sum_{i=1}^{n} i a_i T^{i-1}$.

2. *Consider a polynomial $f(T_1, \cdots, T_n) \in B[T_1, \cdots, T_n]$ and $b_1, \cdots, b_n \in B$. Then*

$$D(f(b_1, \cdots, b_n)) = f^{(D)}(b_1, \cdots, b_n) + \sum_{i=1}^{n} f_{T_i}(b_1, \cdots, b_n) D(b_i),$$

where $f_{T_i} = \dfrac{\partial f}{\partial T_i} \in B[T_1, \cdots, T_n]$.

Proof. 1. We have

$$\begin{aligned} D(f(b)) &= D(\sum_{i=0}^{n} a_i b^i) \\ &= D(a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n) \\ &= D(a_0) + D(a_1)b + \cdots + D(a_n)b^n + a_1 D(b) + a_2 D(b^2) + \cdots + a_n D(b^n) \\ &= \sum_{i=0}^{n} D(a_i) b^i + a_1 D(b) + 2a_2 b D(b) + \cdots + n a_n b^{n-1} D(b) \\ &= f^{(D)}(b) + f'(b) D(b). \end{aligned}$$

2. Let us first consider a monomial $g(T_1, \cdots, T_n) = aT_1^{i_1} \cdots T_n^{i_n} \in B[T_1, \cdots, T_n]$ (where $a \in B$ and $i_1, \cdots, i_n \in \mathbb{N}$). Then

$$\begin{aligned} D(g(b_1, \cdots, b_n)) &= D(ab_1^{i_1} \cdots b_n^{i_n}) \\ &= D(a)b_1^{i_1} \cdots b_n^{i_n} + \sum_i^n ab_1^{i_1} \cdots b_{j-1}^{i_j-1} D(b_j^{i_j}) b_{j+1}^{i_j+1} \cdots b_n^{i_n} \\ &= D(a)b_1^{i_1} \cdots b_n^{i_n} + \sum_i^n i_j a b_1^{i_1} \cdots b_{j-1}^{i_j-1} b_j^{i_j-1} b_{j+1}^{i_j+1} \cdots b_n^{i_n} D(b_j) \\ &= g^{(D)}(b_1, \cdots, b_n) + \sum_{j=1}^n g_{T_j}(b_1, \cdots, b_n) D(b_j). \end{aligned}$$

Since a general polynomial $f(T_1, \cdots, T_n) \in B[T_1, \cdots, T_n]$ is a finite sum of monomials such as $g(T_1, \cdots, T_n)$, it follows that $D(f(b_1, \cdots, b_n)) = f^{(D)}(b_1, \cdots, b_n) + \sum_{i=1}^n f_{T_i}(b_1, \cdots, b_n) D(b_i)$.

□

Corollary 2.1.16. *Let $A \subseteq B$ be rings, let $D \in \mathrm{Der}_A(B)$ and let $s \in B$ be such that $D(s) = 1$. Then for any $f(T) \in A[T]$ and $j \in \mathbb{N}$,*

$$D^j(f(s)) = f^{(j)}(s)$$

where $D^j = \underbrace{D \circ \cdots \circ D}_{j}$ and $f^{(j)}(T) = (\frac{\partial}{\partial T})^j (f(T)) \in A[T]$.

Proof. By induction on j and using Lemma 2.1.15-1). □

Example 2.1.17. Let $B = \mathbb{Z}[X, Y] = \mathbb{Z}^{[2]}$ and $D = \dfrac{\partial}{\partial Y} + Y\dfrac{\partial}{\partial X} \in \mathrm{Der}\, B$. Let us prove that $\ker(D) = \mathbb{Z}[2X - Y^2]$. In fact let $\mathcal{D} : \mathbb{Q}[X, Y] \longrightarrow \mathbb{Q}[X, Y]$ be the extension of D to $\mathbb{Q}[X, Y]$, we first show that $\ker(\mathcal{D}) = \mathbb{Q}[2X - Y^2]$. Clearly $\mathbb{Q}[X, Y] = \mathbb{Q}[2X - Y^2, Y]$ and $\mathbb{Q}[2X - Y^2] \subseteq \ker \mathcal{D}$. Let $h \in \ker(\mathcal{D}) \setminus \{0\}$, then $h \in \mathbb{Q}[X, Y] = \mathbb{Q}[2X - Y^2, Y]$ and $\mathcal{D}(h) = 0$. Hence there is a nonzero polynomial $F \in \mathbb{Q}[U, V]$ such that $h = F(2X - Y^2, Y)$. Furthermore,

$$\begin{aligned} \mathcal{D}(h) = 0 &\Rightarrow \mathcal{D}(F(2X - Y^2, Y)) = 0 \\ &\Rightarrow F_U(2X - Y^2, Y)\mathcal{D}(2X - Y^2) + F_V(2X - Y^2, Y)\mathcal{D}(Y) = 0 \quad \text{by Lemma 2.1.15.} \\ &\Rightarrow F_V(2X - Y^2, Y) = 0, \text{ because } \mathcal{D}(2X - Y^2) = 0 \text{ and } \mathcal{D}(Y) = 1. \end{aligned}$$

Since $(2X - Y^2, Y)$ is algebraically independent over $\mathbb{Q}$, it follows that $F_V(U, V) = 0$ and then $F(U, V) = T(U)$, $T(U) \in \mathbb{Q}[U]$. So $h = T(2X - Y^2) \in \mathbb{Q}[2X - Y^2]$ and $\ker(\mathcal{D}) = \mathbb{Q}[2X - Y^2]$. Moreover, $\ker D = \mathbb{Z}[X, Y] \cap \ker(\mathcal{D}) = \mathbb{Z}[X, Y] \cap \mathbb{Q}[2X - Y^2]$. Clearly $\mathbb{Z}[2X - Y^2] \subseteq \mathbb{Z}[X, Y] \cap \mathbb{Q}[2X - Y^2]$. Given $P \in \mathbb{Z}[X, Y] \cap \mathbb{Q}[2X - Y^2]$ we have $P(X, Y) = a_0 + a_1(2X - Y^2) + \cdots + a_n(2X - Y^2)^n$, where $a_i \in \mathbb{Q}$.
Since $P(X, Y) \in \mathbb{Z}[X, Y]$, then

$$P(0, Y) \in \mathbb{Z}[Y] \Longrightarrow a_0 - a_1Y^2 + a_2Y^4 + \cdots + (-1)^n a_n Y^{2n} \in \mathbb{Z}[Y].$$

Hence $a_i \in \mathbb{Z}$ and so $P(X, Y) \in \mathbb{Z}[2X - Y^2]$; thus $\mathbb{Z}[X, Y] \cap \mathbb{Q}[2X - Y^2] \subseteq \mathbb{Z}[2X - Y^2]$. Therefore $\mathbb{Z}[2X - Y^2] = \mathbb{Z}[X, Y] \cap \mathbb{Q}[2X - Y^2]$, we thus have $\ker D = \mathbb{Z}[2X - Y^2]$.

The following useful result is Lemma 1.17 of [3].

Proposition 2.1.18. *If B is a domain of characteristic zero and $D \in \mathrm{Der}(B)$, then $\ker D$ is algebraically closed in B.*

Proof. Consider $b \in B$ such that b is algebraic over $\ker D$. Set $A = \ker D$ and let $f \in A[T]$ be a nonzero polynomial of minimal degree such that $f(b) = 0$. Note that $\deg(f) \geq 1$. Then we have,

$$0 = D(f(b)) = f^{(D)}(b) + f'(b)D(b) = f'(b)D(b).$$

Since $\deg(f) \geq 1$ and B is a domain of characteristic zero, we have $f' \neq 0$. As f' is a nonzero polynomial and $\deg(f') < \deg(f)$, then $f'(b) \neq 0$ by minimality of $\deg(f)$, and so $D(b) = 0$ (since B is a domain). Therefore b algebraic over $\ker D$ implies that $b \in \ker D$; that is $\ker D$ is algebraically closed in B. □

Remark 2.1.19. If B is a ring of characteristic $p > 1$, it is easy to observe that for $D \in \mathrm{Der}(B)$ a nonzero derivation, $\ker D$ is not algebraically closed in B. In fact for all $x \in B$, we have $D(x^p) = px^{p-1}D(x) = 0$ so $x^p \in \ker D$. Set $A = \ker D$ and take $z \in B \setminus A$, consider the polynomial $P(X) = X^p - z^p$; $P(X) \in A[X] \setminus \{0\}$ (since $z^p \in A$) and $P(z) = 0$. Hence z is algebraic over $A = \ker D$. Therefore $\ker D$ is not algebraically closed in B.

Lemma 2.1.20. *Let $B = A[X_1, \cdots, X_n]$ where A is a ring and $f = (f_1, \cdots, f_n)$ a system of variables in B. Then*

$$M_f = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial X_1} & \cdots & \frac{\partial f_n}{\partial X_n} \end{pmatrix} \in \mathrm{M}_n(B) \quad \textit{is} \quad \textit{invertible.}$$

Proof. We have $A[f] = A[X_1, \cdots, X_n]$, so $X_i \in A[f]$ for each $i \in \{1, \cdots, n\}$. Hence there is $P_i(U_1, \cdots, U_n) \in A[U_1, \cdots, U_n]$ such that $X_i = P_i(f) = P_i(f_1, \cdots, f_n)$ for each $i \in \{1, \cdots, n\}$. Moreover, $\delta_{ij} = \dfrac{\partial X_i}{\partial X_j} = \dfrac{\partial P_i(f_1, \cdots, f_n)}{\partial X_j} = \sum_{k=1}^{n} \dfrac{\partial P_i}{\partial U_k}(f_1, \cdots, f_n) \dfrac{\partial f_k}{\partial X_j}$ (by Lemma 2.1.15). Set $Q_{ik} = \dfrac{\partial P_i}{\partial U_k}(f_1, \cdots, f_n) \in B$, thus $\delta_{ij} = (Q_{i1}, \cdots, Q_{in}) \begin{pmatrix} \frac{\partial f_1}{\partial X_j} \\ \vdots \\ \frac{\partial f_n}{\partial X_j} \end{pmatrix}$ which is the (i, j)-element of the matrix

$$\begin{pmatrix} Q_{11} & \cdots & Q_{1n} \\ \vdots & \cdots & \vdots \\ Q_{n1} & \cdots & Q_{nn} \end{pmatrix} \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \cdots & \vdots \\ \frac{\partial f_n}{\partial X_1} & \cdots & \frac{\partial f_n}{\partial X_n} \end{pmatrix}$$

So this matrix product is equal to I_n. Thus $\det(M_f) \in B^\times$, and so M_f is invertible. □

Remark 2.1.21. When A is domain, $\det(M_f) \in A^\times = B^\times$.

The next proposition is Exercise 1.15 of [3].

Proposition 2.1.22. *Let B be a ring, $D \in \mathrm{Der}(B)$ and let S be a multiplicative subset of B and $S^{-1}B$ the ring of fractions of B. The map $S^{-1}D : S^{-1}B \longrightarrow S^{-1}B$ defined by*

$$(S^{-1}D)(b/s) = \frac{sD(b) - bD(s)}{s^2} \quad \textit{for all } b \in B \textit{ and } s \in S.$$

is a derivation of $S^{-1}B$.

Proof. First we need to show that the map $S^{-1}D$ is well defined. Let $b_1, b_2 \in B$ and $s_1, s_2 \in S$ be such that $\frac{b_1}{s_1} = \frac{b_2}{s_2}$ in $S^{-1}B$, we have to show that $S^{-1}D(\frac{b_1}{s_1}) = S^{-1}D(\frac{b_2}{s_2})$ in $S^{-1}B$.

Recall that: $\frac{b_1}{s_1} = \frac{b_2}{s_2}$ in $S^{-1}B \Longrightarrow (b_1s_2 - b_2s_1)u = 0$ for some $u \in S$.

We have

$$
\begin{aligned}
&(s_1D(b_1) - b_1D(s_1))s_2^2 - (s_2D(b_2) - b_2D(s_2))s_1^2 \\
&= s_1s_2^2D(b_1) - s_2^2b_1D(s_1) - s_1^2s_2D(b_2) + s_1^2b_2D(s_2) \\
&= s_1s_2^2D(b_1) - s_2^2b_1D(s_1) - s_1^2s_2D(b_2) + s_1^2b_2D(s_2) + s_1s_2b_2D(s_1) - s_1s_2b_2D(s_1) + s_1s_2b_1D(s_2) \\
&\qquad\qquad - s_1s_2b_1D(s_2) \\
&= s_1s_2(s_2D(b_1) + b_1D(s_2) - s_1D(b_2) - b_2D(s_1)) - b_1s_2(s_1D(s_2) + s_2D(s_1)) \\
&\qquad\qquad + b_2s_1(s_1D(s_2) + s_2D(s_1)) \\
&= s_1s_2(D(b_1s_2) - D(s_1b_2)) - b_1s_2(D(s_1s_2)) + b_2s_1(D(s_1s_2)) \\
&= s_1s_2(D(b_1s_2) - D(s_1b_2)) + D(s_1s_2)(b_2s_1 - b_1s_2) \\
&= s_1s_2D(b_1s_2 - s_1b_2) + D(s_1s_2)(b_2s_1 - b_1s_2).
\end{aligned}
$$

Now $u \in S \Longrightarrow u^2 \in S$ and we have:

$$((s_1D(b_1)-b_1D(s_1))s_2^2-(s_2D(b_2)-b_2D(s_2))s_1^2)u^2 = s_1s_2D(b_1s_2-s_1b_2)u^2+D(s_1s_2)(b_2s_1-b_1s_2)u^2.$$

But $(b_2s_1 - b_1s_2)u = 0 \Longrightarrow (b_2s_1 - b_1s_2)u^2 = 0$ and

$$
\begin{aligned}
(b_2s_1 - b_1s_2)u = 0 &\Longrightarrow D((b_2s_1 - b_1s_2)u) = 0 \\
&\Longrightarrow D(s_2b_1 - b_2s_1)u + (b_2s_1 - b_2s_1)D(u) = 0 \\
&\Longrightarrow D(s_2b_1 - b_2s_1)u^2 = 0 \text{ (by multiplying by } u \text{ both terms of the equality).}
\end{aligned}
$$

Therefore $((s_1D(b_1) - b_1D(s_1))s_2^2 - (s_2D(b_2) - b_2D(s_2))s_1^2)u^2 = 0$. That is

$$\frac{s_1D(b_1) - b_1D(s_1)}{s_1^2} = \frac{s_2D(b_2) - b_2D(s_2)}{s_2^2} \quad \text{in } S^{-1}B.$$

So $S^{-1}D$ is well defined, now we show that it is a derivation. Let $x_1, x_2 \in S^{-1}B$.

Then there exist $b_1, b_2 \in B$ and $s \in S$ such that $x_1 = \frac{b_1}{s}$ and $x_2 = \frac{b_2}{s}$. Then

$$\begin{aligned} S^{-1}D(x_1) + S^{-1}D(x_2) &= S^{-1}D\left(\frac{b_1}{s}\right) + S^{-1}D\left(\frac{b_2}{s}\right) = \frac{D(b_1)s - b_1Ds}{s^2} + \frac{D(b_2)s - b_2Ds}{s^2} \\ &= \frac{D(b_1)s - b_1Ds + D(b_2)s - b_2Ds}{s^2} = \frac{D(b_1+b_2)s - (b_1+b_2)Ds}{s^2} \\ &= S^{-1}D\left(\frac{b_1+b_2}{s}\right) = S^{-1}D(x_1+x_2), \end{aligned}$$

and

$$\begin{aligned} &S^{-1}D(x_1)\cdot x_2 + x_1S^{-1}D(x_2) = S^{-1}D\left(\frac{b_1}{s}\right)\cdot\left(\frac{b_2}{s}\right) + \left(\frac{b_1}{s}\right)S^{-1}D\left(\frac{b_2}{s}\right) \\ &= \frac{D(b_1)s - b_1Ds}{s^2}\cdot\frac{b_2}{s} + \frac{b_1}{s}\cdot\frac{D(b_2)s - b_2Ds}{s^2} = \frac{(D(b_1)s - b_1Ds)b_2s}{s^4} + \frac{b_1s(D(b_2)s - b_2Ds)}{s^4} \\ &= \frac{(D(b_1)b_2 + b_1D(b_2))s^2 - 2b_1b_2sDs}{s^4} = \frac{D(b_1b_2)s^2 - b_1b_2D(s^2)}{s^4} = S^{-1}D\left(\frac{b_1b_2}{s^2}\right) \\ &= S^{-1}D\left(\frac{b_1}{s}\cdot\frac{b_2}{s}\right) = S^{-1}D(x_1x_2). \end{aligned}$$

□

Remark 2.1.23. Let B be a ring, $D \in \mathrm{Der}(B)$, S be a multiplicative subset of B and $S^{-1}B$ the ring of fractions of B.

1. Proposition 2.1.22 allows us to define a map

$$\mathrm{Der}(B) \longrightarrow \mathrm{Der}(S^{-1}B),\ D \longmapsto S^{-1}D.$$

   By this we say that every derivation of B can be extended to a derivation of $S^{-1}B$.

2. If B is a domain and $0 \notin S$, then the canonical homomorphism $B \longrightarrow S^{-1}B$ is injective and we may consider that $B \subseteq S^{-1}B$. Then we have $\ker(D) = \ker(S^{-1}D) \cap B$.

3. In the special case where S is included in $\ker D$, the definition of $S^{-1}D$ simplifies as follows:

$$S^{-1}D(b/s) = \frac{D(b)}{s} \quad \text{for all } b \in B \text{ and } s \in S.$$

Example 2.1.24. Let $B = \mathbb{C}[X,Y] = \mathbb{C}^{[2]}$ and $S = B \setminus \{0\}$. Then $S^{-1}B = \mathbb{C}(X,Y)$ is the field of rational functions in two variables over $\mathbb{C}$. Consider the $\mathbb{C}$-derivation $\dfrac{\partial}{\partial X} : \mathbb{C}[X,Y] \longrightarrow \mathbb{C}[X,Y]$ and its extension to a derivation of $\mathbb{C}(X,Y)$,

$$S^{-1}\frac{\partial}{\partial X} : \mathbb{C}(X,Y) \longrightarrow \mathbb{C}(X,Y).$$

Then for $\dfrac{XY}{X^2+Y^2} \in \mathbb{C}(X,Y)$ we have $S^{-1}\dfrac{\partial}{\partial X}\left(\dfrac{XY}{X^2+Y^2}\right) = \dfrac{Y^3 - X^2Y}{(X^2+Y^2)^2}$.

Definition 2.1.25. Let $B = A^{[n]}$ where A is a ring and $\gamma = (X_1, \cdots, X_n)$ a system of variables of B. Given $f = (f_1, \cdots, f_{n-1}) \in B^{n-1}$, we define the map $\Delta_f^\gamma : B \longrightarrow B$ by $\Delta_f^\gamma(g) = \det\left(\dfrac{\partial(f_1, \cdots, f_{n-1}, g)}{\partial(X_1, \cdots, X_n)}\right)$, for all $g \in B$. By using some basic properties of the determinant function it is not difficult to show that $\Delta_f^\gamma \in \mathrm{Der}_A(B)$ and that $A[f_1, \cdots, f_{n-1}] \subseteq \ker(\Delta_f^\gamma)$.

We say that Δ_f^γ is a *Jacobian derivation.*

Remark 2.1.26. Let $B = A^{[2]}$ and $\gamma = (X,Y)$ a system of variables of B, we have $\Delta_X^\gamma = \dfrac{\partial}{\partial Y}$ and $\Delta_Y^\gamma = -\dfrac{\partial}{\partial X}$.

2.2 Locally nilpotent derivations

Given a ring B, $D \in \mathrm{Der}(B)$ and $n > 0$, we denote by $D^n : B \longrightarrow B$ the composition of D with itself n times; also we define $D^0 : B \longrightarrow B$ to be the identity map (even in the case where $D = 0$). Note that D^n is usually not a derivation when $n \neq 1$.

Definition 2.2.1. Given a ring B and $D \in \mathrm{Der}\, B$, we define

$$\mathrm{Nil}(D) = \{x \in B \mid \exists n \in \mathbb{N} \textit{ such that } D^n(x) = 0\}.$$

Clearly $\ker D \subseteq \mathrm{Nil}(D) \subseteq B$.

The following Lemma is known as the *Leibnitz Rule* and can be found in [3] as Exercise 1.19.

Lemma 2.2.2. *Let B be a ring and $D \in \mathrm{Der}(B)$. For all $x, y \in B$ and $n \in \mathbb{N}$ we have:*

$$D^n(xy) = \sum_{i=0}^{n} \binom{n}{i} D^{n-i}(x) D^i(y).$$

Proof. By induction on n; for $n = 0$ the result is trivial. Now we consider $n \in \mathbb{N}$ such that $D^n(xy) = \sum_{i=0}^{n} \binom{n}{i} D^{n-i}(x) D^i(y)$ is true and we show that

$$D^{n+1}(xy) = \sum_{i=0}^{n+1} \binom{n+1}{i} D^{n+1-i}(x) D^i(y).$$

We have:

$$\begin{aligned}
D^{n+1}(xy) = D(D^n(xy)) &= D\left(\sum_{i=0}^{n} \binom{n}{i} D^{n-i}(x) D^i(y) \right) \\
&= \sum_{i=0}^{n} \binom{n}{i} D^{n+1-i}(x) D^i(y) + \sum_{i=0}^{n} \binom{n}{i} D^{n-i}(x) D^{i+1}(y) \\
&= \sum_{i=0}^{n} \binom{n}{i} D^{n+1-i}(x) D^i(y) + \sum_{i=0}^{n-1} \binom{n}{i} D^{n-i}(x) D^{i+1}(y) + x D^{n+1}(y) \\
&= \sum_{i=0}^{n} \binom{n+1}{i} D^{n+1-i}(x) D^i(y) - \sum_{i=1}^{n} \binom{n}{i-1} D^{n+1-i}(x) D^i(y) \\
&\qquad + \sum_{i=0}^{n-1} \binom{n}{i} D^{n-i}(x) D^{i+1}(y) + x D^{n+1}(y) \\
&= \sum_{i=0}^{n} \binom{n+1}{i} D^{n+1-i}(x) D^i(y) + x D^{n+1}(y) = \sum_{i=0}^{n+1} \binom{n+1}{i} D^{n+1-i}(x) D^i(y)
\end{aligned}$$

where the second equality is true by assumption and the fifth follows from $\binom{n+1}{i} = \binom{n}{i-1} + \binom{n}{i}$. □

The next proposition is Exercise 1.21 of [3].

Proposition 2.2.3. *If B is a ring and $D \in \mathrm{Der}(B)$, then $\mathrm{Nil}(D)$ is a subring of B.*

Proof. Clearly 1 belongs to $\mathrm{Nil}(D)$. Now let $x, y \in \mathrm{Nil}(D)$; there exist $m, n \in \mathbb{N}$ such that $D^n(x) = 0$ and $D^m(y) = 0$. Take $l = m + n + 1$, it is easy to check by the lemma above that $D^l(xy) = 0$ and $D^l(x - y) = 0$. Hence $\mathrm{Nil}(D)$ is a subring of B. □

Definition 2.2.4. Let B be any ring. A derivation $D : B \longrightarrow B$ is *locally nilpotent* if it satisfies $\mathrm{Nil}(D) = B$, that is if $\forall b \in B \ \ \exists n \in \mathbb{N}$ such that $D^n(b) = 0$.

The set of all locally nilpotent derivations of a ring B is denoted by $\mathrm{LND}(B)$.

Example 2.2.5.

- Let A be a ring and $B = A[X_1, \cdots, X_n] = A^{[n]}$. Then $\dfrac{\partial}{\partial X_i} \in \mathrm{LND}(B)$ for each $i = 1, \cdots, n$.
- Let $B = \mathbb{C}[T] = \mathbb{C}^{[1]}$, we know that $d/dT \in \mathrm{Der}_{\mathbb{C}}(B)$ and for each $P(T) \in B$, $D = P(T)\dfrac{d}{dT} \in \mathrm{Der}_{\mathbb{C}}(B)$. In particular in the case where $P(T) \in \mathbb{C}$ we have $D \in \mathrm{LND}(B)$.

Definition 2.2.6. Let A be a ring and $B = A[X_1, \cdots, X_n]$. A derivation $D : B \longrightarrow B$ is *triangular* if $D(A) = \{0\}$ and:

$$\forall i \ \ D(X_i) \in A[X_1, \cdots, X_{i-1}]; \quad \text{in particular } D(X_1) \in A.$$

Example 2.2.7. Let $B = \mathbb{C}[X, Y, Z] = \mathbb{C}^{[3]}$, the element $D = X^2\dfrac{\partial}{\partial Y} + (X^2 + Y^3)\dfrac{\partial}{\partial Z}$ of $\mathrm{Der}_{\mathbb{C}}(B)$ is a triangular derivation.

Remark 2.2.8. Let D be a derivation and $f \in B$, if $D(f) \in \mathrm{Nil}(D)$ then $f \in \mathrm{Nil}(D)$. Moreover, if D is triangular it is in particular an A-derivation, thus $A \subseteq \ker(D)$ and so $A \subseteq \mathrm{Nil}(D)$.

The next result is Lemma 2.6 of [3].

Lemma 2.2.9. *Let A be a ring and $B = A[X_1, \cdots, X_n] = A^{[n]}$. Then every triangular derivation of B is a locally nilpotent derivation.*

Proof. Let $D : B \longrightarrow B$ be a triangular derivation. We show by induction on i that

$$A[X_1, \cdots, X_i] \subseteq \mathrm{Nil}(D), \quad \text{for all } i = 1, \cdots, n.$$

Since D is triangular we have $D(X_1) \in A \subseteq \mathrm{Nil}(D)$, by the previous remark we have $X_1 \in \mathrm{Nil}(D)$. By Proposition 2.2.3 $\mathrm{Nil}(D)$ is a subring of B and $A \subseteq \mathrm{Nil}(D)$ imply $A[X_1] \subseteq \mathrm{Nil}(D)$.
Suppose now that $i < n$ is such that $A[X_1, \cdots, X_i] \subseteq \mathrm{Nil}(D)$; we have to show that

$A[X_1, \cdots, X_{i+1}] \subseteq \mathrm{Nil}(D)$. Since $D(X_{i+1}) \in A[X_1, \cdots, X_i] \subseteq \mathrm{Nil}(D)$ it follows that $X_{i+1} \in \mathrm{Nil}(D)$. Using the fact that $\mathrm{Nil}(D)$ is a subring we get $A[X_1, \cdots, X_{i+1}] \subseteq \mathrm{Nil}(D)$. Therefore $A[X_1, \cdots, X_i] \subseteq \mathrm{Nil}(D)$, for all $i = 1, \cdots, n$. In particular for $i = n$, we have $B \subseteq \mathrm{Nil}(D)$ that is $\mathrm{Nil}(D) = B$. Thus D is locally nilpotent. □

Example 2.2.10. Let $B = \mathbb{C}[X, Y] = \mathbb{C}[Y, X] = \mathbb{C}^{[2]}$ and let $D_1 = Y\dfrac{\partial}{\partial X}$, $D_2 = X\dfrac{\partial}{\partial Y}$ be two derivations of B such that $D_1 : \mathbb{C}[Y, X] \longrightarrow \mathbb{C}[Y, X]$ and $D_2 : \mathbb{C}[X, Y] \longrightarrow \mathbb{C}[X, Y]$. The derivations D_1 and D_2 are triangular, hence $D_1, D_2 \in \mathrm{LND}(B)$. However $(D_1 + D_2)^2(X) = X$, hence $D_1 + D_2 \notin \mathrm{LND}(B)$. Also, $\dfrac{\partial}{\partial X} \in \mathrm{LND}(B)$, but $X\dfrac{\partial}{\partial X} \notin \mathrm{LND}(B)$. This shows that the set $\mathrm{LND}(B)$ does not have any algebraic structure; it is just a set.

The following Lemma is Exercise 2.9 of [3].

Lemma 2.2.11. *Let B be a ring, $D \in \mathrm{LND}(B)$ and $A = \ker D$. The following hold:*

1. *If $a \in A$, then $(aD)^n = a^n D^n$ for all $n \in \mathbb{N}$.*
2. *If $a \in A$, then $aD \in \mathrm{LND}(B)$.*
3. *Let $S \subseteq A$ be a multiplicatively closed subset of A. Then the map*

$$S^{-1}D : S^{-1}B \longrightarrow S^{-1}B, \quad x/s \longmapsto D(x)/s,$$

is a locally nilpotent derivation of $S^{-1}B$. Furthermore, $\ker(S^{-1}D) = S^{-1}A$.

Proof. 1. By induction on n.

2. It is a consequence of 1.

3. By Proposition 2.1.22 and part (3) of Remark 2.1.23, $S^{-1}D$ is well defined and is an element of $\mathrm{Der}(S^{-1}B)$. Let $x/s \in S^{-1}B$ ($x \in B$, $s \in S$); since $\mathrm{Nil}(D) = B$ there exists $m \in \mathbb{N}$ such that $D^m(x) = 0$. Now we have

$$(S^{-1}D)^m(x/s) = \underbrace{S^{-1}D \circ S^{-1}D \circ \cdots \circ S^{-1}D}_{m}(x/s) = D^m(x)/s = 0/s = 0 \text{ in } S^{-1}B.$$

Thus $S^{-1}D \in \mathrm{LND}(S^{-1}B)$. Observe that if $i : A \longrightarrow B$ is the inclusion map then $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{D} B$ is an exact sequence of A-modules and A-linear maps. By Proposition 1.5.11 the sequence

$$0 \longrightarrow S^{-1}A \xrightarrow{S^{-1}i} S^{-1}B \xrightarrow{S^{-1}D} S^{-1}B$$

is an exact sequence of $S^{-1}A$-modules. Hence $\ker(S^{-1}D) = \mathrm{Im}(S^{-1}i) = S^{-1}A$.

□

Definition 2.2.12. Let B be a ring. We define the set

$$\mathrm{KLND}(B) = \{\ker D \mid D \in \mathrm{LND}(B),\ D \neq 0\}.$$

Example 2.2.13. Let $B = \mathbb{C}[X, Y]$. We have $\dfrac{\partial}{\partial X} \in \mathrm{LND}(B)$ and $\dfrac{\partial}{\partial X} \neq 0, \ker\left(\dfrac{\partial}{\partial X}\right) \in \mathrm{KLND}(B)$. Since $\ker\left(\dfrac{\partial}{\partial X}\right) = \mathbb{C}[Y]$, we have $\mathbb{C}[Y] \in \mathrm{KLND}(B)$.
Similarly we have $\mathbb{C}[X] \in \mathrm{KLND}(B)$. More generally, if (U, V) is a system of variables of B then $\mathbb{C}[U], \mathbb{C}[V] \in \mathrm{KLND}(B)$.

Definition 2.2.14. Given a $\mathbb{Q}$-algebra B and $D \in \mathrm{LND}(B)$, we define the map

$$\xi_D : B \longrightarrow B[T],\ b \longmapsto \sum_{n\in\mathbb{N}} \frac{1}{n!} D^n(b) T^n.$$

The map ξ_D is called the *exponential map associated to* D.

The following theorem can be found in [3] as Theorem 3.3.

Theorem 2.2.15. *Let B be a $\mathbb{Q}$-algebra and $D \in \mathrm{LND}(B)$. Then the map $\xi_D : B \longrightarrow B[T]$ is an injective homomorphism of A-algebras, where $A = \ker(D)$.*

Proof. Let $\mathrm{ev}_0 : B[T] \longrightarrow B,\ f \longmapsto f(0)$. Then we have $\mathrm{ev}_0 \circ \xi_D = \mathrm{id}_B$, hence ξ_D is injective. It is clear that ξ_D preserves addition and restricts to the identity map on A, hence by Remark 1.1.18 it suffices to verify that $\xi_D(x)\xi_D(y) = \xi_D(xy)$. By Lemma

2.2.2 we have:

$$\begin{aligned}\xi_D(x)\xi_D(y) = \Big(\sum_{i\in\mathbb{N}} \frac{1}{i!}D^i(x)T^i\Big)\Big(\sum_{j\in\mathbb{N}} \frac{1}{j!}D^j(y)T^j\Big) &= \sum_{n\in\mathbb{N}}\Big(\sum_{i+j=n} \frac{1}{i!j!}D^i(x)D^j(y)\Big)T^n \\ &= \sum_{n\in\mathbb{N}} \frac{1}{n!}\Big(\sum_{i+j=n} \frac{n!}{i!j!}D^i(x)D^j(y)\Big)T^n \\ &= \sum_{n\in\mathbb{N}} \frac{1}{n!}D^n(xy)T^n \\ &= \xi_D(xy).\end{aligned}$$

Therefore ξ_D is an injective A-homomorphism. □

Remark 2.2.16. The A-homomorphism ξ_D is the inclusion map if and only if $D = 0$.

Example 2.2.17. Let $B = \mathbb{C}[X, Y, Z]$ and $B[T] = \mathbb{C}[X, Y, Z, T]$, and consider $D = X\dfrac{\partial}{\partial Y} + Y\dfrac{\partial}{\partial Z}$, $D \in \mathrm{LND}(B)$. The map ξ_D is an homomorphism of $\mathbb{C}$-algebras and we have: $\xi_D(X) = X$, $\xi_D(Y) = Y + XT$ and $\xi_D(Z) = Z + YT + \dfrac{1}{2}XT^2$.

Definition 2.2.18. Let B be a ring. Each element $D \in \mathrm{LND}(B)$ determines a map $\deg_D : B \longrightarrow \mathbb{N} \cup \{-\infty\}$ defined as follows:

$$\deg_D(x) = \begin{cases} \max\{\, n \in \mathbb{N} \mid D^n x \neq 0\} & \text{if } x \neq 0 \\ -\infty & \text{if } x = 0. \end{cases}$$

Note that $\ker D = \{\, x \in B \mid \deg_D(x) \leq 0\}$.

Example 2.2.19. Let A a domain of characteristic zero and $B = A[t]$. The derivative $D = \dfrac{d}{dt} : B \longrightarrow B$ is an element of the set $\mathrm{LND}(B)$; so D determines the map $\deg_D : A[t] \longrightarrow \mathbb{N} \cup \{-\infty\}$. The map $\deg_D$ in this case is the usual t-degree.

The following proposition can be found in [3] as Proposition 4.8.

Proposition 2.2.20. *If B be a domain of characteristic zero and $D \in \mathrm{LND}(B)$, then $\deg_D$ is a degree function.*

Proof. We begin by proving the special case where $\mathbb{Q} \subseteq B$. In this case we may consider the map $\xi_D : B \longrightarrow B[T]$, which is injective by Theorem 2.2.15, and the function $\deg_T : B[T] \longrightarrow \mathbb{N} \cup \{-\infty\}$, which is a degree function (since $B[T]$ is a domain). We have $\deg_T \circ \xi_D = \deg_D$ so by Lemma 1.3.5, $\deg_D$ is a degree function. In the general case we have $\mathbb{Z} \subseteq B$ and so $\mathbb{Z} \subseteq \ker D$. Let $S = \mathbb{Z} \setminus \{0\}$ and consider $S^{-1}D : S^{-1}B \longrightarrow S^{-1}B$, $S^{-1}D \in \mathrm{LND}(S^{-1}B)$ by Lemma 2.2.11. As $\mathbb{Q} \subseteq S^{-1}B$, the first part of the proof implies that $\deg_{S^{-1}D} : S^{-1}B \longrightarrow \mathbb{N} \cup \{\infty\}$ is a degree function. Now consider the following commutative diagrams:

$$\begin{array}{ccc} S^{-1}B & \xrightarrow{S^{-1}D} & S^{-1}B \\ \uparrow & \circlearrowleft & \uparrow \\ B & \xrightarrow{D} & B \end{array} \qquad\qquad \begin{array}{ccc} S^{-1}B & \xrightarrow{\deg_{S^{-1}D}} & \mathbb{N} \cup \{-\infty\} \\ \uparrow & \nearrow_{\deg_D} & \\ B & & \end{array}$$

Note that the map $B \longrightarrow S^{-1}B$, $x \longmapsto \dfrac{x}{1}$ is injective since B is a domain and $0 \notin S$. So D is the restriction of $S^{-1}D$ and consequently $\deg_D$ is the restriction of $\deg_{S^{-1}D}$; it follows that $\deg_D$ is a degree function. □

The next result is Corollary 5.3 of [3].

Proposition 2.2.21. *Let B be a domain of characteristic zero and $D \in \mathrm{LND}(B)$. Then $\ker(D)$ is a factorially closed subring of B.*

Proof. By Proposition 2.2.20 $\deg_D$ is a degree function and $\ker D = \{x \in B \mid \deg_D x \leq 0\}$; since $\{x \in B \mid \deg_D x \leq 0\}$ is factorially closed by Lemma 1.3.9, the result follows. □

The next corollary is Corollary 5.5 of [3].

Corollary 2.2.22. *Let B be a domain of characteristic zero, $D \in \mathrm{LND}(B)$ and $A = \ker(D)$. The following hold:*

1. *$A^\times = B^\times$.*
2. *If k is any field included in B, then D is a k-derivation.*
3. *If B is a UFD then so is A.*

Proof. By applying Proposition 2.2.21 and Lemma 1.3.17 we obtain the result. □

Corollary 2.2.23. *Let k be a field of characteristic zero and let B be a domain such that $k \subseteq B$. Then we have $k \subseteq A$ for each element A of* $\mathrm{KLND}(B)$.

Proof. This follows from part (2) of Corollary 2.2.22. □

Example 2.2.24. Let $B = \mathbb{C}[X,Y] = \mathbb{C}^{[2]}$ and $f = XY \in B$. If A is a factorially closed subring of B satisfying $f \in A$, then we have $X, Y \in A$. Thus $\mathbb{C}[X,Y] \subseteq A$ and so $B = A$. Therefore, if $D \in \mathrm{LND}(B)$ and $f \in \ker(D)$ then we have $D = 0$.

Consider Δ_f defined in Definition 2.1.25. Then $\Delta_f(X) = -X$, so Δ_f is not locally nilpotent. Since $f \in \ker(\Delta_f)$ and $\ker(\Delta_f) \neq B$, the above paragraph implies that $\ker(\Delta_f)$ is not factorially closed in B. Note, however, that $\ker(\Delta_f)$ is algebraically closed in B, by Proposition 2.1.18.

The next result can be found in [3] as Exercise 4.9.

Corollary 2.2.25. *Let B be a domain of characteristic zero. If $D \in \mathrm{Der}(B)$ is such that $D^n = 0$ for some $n > 0$, then $D = 0$.*

Proof. By contradiction, assume that $D \neq 0$. Since $D^n = 0$ for some $n > 0$, then $D \in \mathrm{LND}(B)$. By Proposition 2.2.20, $\deg_D$ exists and is a degree function. Now since $D \neq 0$ there exists some $x \in B$ such that $\deg_D(x) \geq 1$. Furthermore, $\deg_D(x^n) = n \deg_D(x)$ (because $\deg_D$ is a degree function) and $D^n = 0$ imply $D^n(x^n) = 0$. Thus $\max\{k \in \mathbb{N} : D^k(x^n) \neq 0\} < n$; that is $\deg_D(x^n) < n$. Hence we have $n \deg_D(x) < n$, a contradiction (since $\deg_D(x) \geq 1$). Therefore we must have $D = 0$. □

The next useful result can be found in [6] as Principle 5.

Proposition 2.2.26. *Let B be a domain of characteristic zero, $D \in \mathrm{LND}(B)$ and $f, g \in B$. If $Df \in gB$ and $Dg \in fB$, then either $f \in \ker(D)$ or $g \in \ker(D)$.*

Proof. Assume that $Df \neq 0$ and $Dg \neq 0$. Then $\deg_D(f) \geq 1$ and $Df = gb$ for some $b \in B \setminus \{0\}$. Thus $\deg_D(b) \geq 0$ and $\deg_D(Df) = \deg_D(f) - 1 = \deg_D(g) + \deg_D(b) \geq \deg_D(g)$. By the same argument, we show that $\deg_D(g) - 1 \geq \deg_D(f)$. Adding this two inequalities, we obtain that $\deg_D(f) + \deg_D(g) - 2 \geq \deg_D(f) + \deg_D(g)$, a contradiction. Therefore either $f \in \ker(D)$ or $g \in \ker(D)$. □

Corollary 2.2.27. *Let B be a domain of characteristic zero, $D \in \mathrm{LND}(B)$ and $f \in B$. If $Df \in fB$, then $f \in \ker(D)$.*

Proof. Take $f = g$ in Proposition 2.2.26. □

Lemma 2.2.28. *Let K/k be a field extension of characteristic zero and let $B = k[X, Y]$ and $\tilde{B} = K[X, Y]$. For each $D \in \mathrm{LND}(B)$, there exists a unique $\delta \in \mathrm{LND}(\tilde{B})$ that is an extension of D.*

Proof. Since $D : B \longrightarrow B$ is locally nilpotent, it is a k-derivation. So there exist $f, g \in B$ such that $D = f\frac{\partial}{\partial X} + g\frac{\partial}{\partial Y}$. Now we may define $\delta \in \mathrm{Der}_K(\tilde{B})$ by $\delta = f\frac{\partial}{\partial X} + g\frac{\partial}{\partial Y}$. Then δ is an extension of D and we have $\delta^n(X) = D^n(X)$ and $\delta^n(Y) = D^n(Y)$ for all $n \in \mathbb{N}$, so $X, Y \in \mathrm{Nil}(\delta)$. Since δ is a K-derivation we have $K \subseteq \mathrm{Nil}(\delta)$, so $\mathrm{Nil}(\delta) = \tilde{B}$ and $\delta \in \mathrm{LND}(\tilde{B})$. So there exists at least one $\delta \in \mathrm{LND}(\tilde{B})$ that extends D.

Suppose that $\delta_1, \delta_2 \in \mathrm{LND}(\tilde{B})$ are extensions of D. Since δ_1, δ_2 are locally nilpotent, they are K-derivations; so $\delta_1 - \delta_2 \in \mathrm{Der}_K(\tilde{B})$. Moreover, $\delta_1(X) = D(X) = \delta_2(X)$ and $\delta_1(Y) = D(Y) = \delta_2(Y)$, so $X, Y \in \ker(\delta_1 - \delta_2)$ and hence $\delta_1 - \delta_2 = 0$. □

2.3 Slices and preslices

Definition 2.3.1. Let B be a ring and $D \in \mathrm{LND}(B)$. A *slice* of D is an element $s \in B$ satisfying $D(s) = 1$.

Example 2.3.2. Let $B = \mathbb{C}[X, Y, Z] = \mathbb{C}^{[3]}$.

1. Clearly, X is a slice of $\dfrac{\partial}{\partial X} \in \mathrm{LND}(B)$.
2. Define $D \in \mathrm{LND}(B)$ by $D(Z) = Y$, $D(Y) = X$ and $D(X) = 0$, that is $D = X\dfrac{\partial}{\partial Y} + Y\dfrac{\partial}{\partial Z}$. Then given $f \in B$, we have $D(f) = f_Y X + f_Z Y$. Thus $D(B) \subseteq (X, Y)B$ and so D does not have a slice. (Here, $(X, Y)B$ denotes the ideal of B generated by X, Y.)

When a slice exists, the situation is very special. (The following result is Theorem 7.3 of [3].)

Theorem 2.3.3. *Let B be a $\mathbb{Q}$-algebra, $D \in \mathrm{LND}(B)$ and $A = \ker(D)$. If $s \in B$ is a slice of D, then $B = A[s] = A^{[1]}$ and $D = \dfrac{d}{ds} : A[s] \longrightarrow A[s]$.*

Proof. Consider $f(T) = \sum_{i=0}^{n} a_i T^i \in A[T] \setminus \{0\}$ where $n \geq 0$, $a_i \in A$ and $a_n \neq 0$. By Corollary 2.1.16 we have $D^j(f(s)) = f^{(j)}(s)$ for all $j \geq 0$, where $f^{(j)}$ denotes the j-th derivative of f; so $D^n(f(s)) = n!a_n \neq 0$ (because $n! \in \mathbb{Q}^\times \subseteq B^\times$) and in particular $f(s) \neq 0$. So s is transcendental over A, that is $A[s] = A^{[1]}$.

We show that $B = A[s]$. Consider the homomorphism of A-algebras $\xi : B \longrightarrow B$ defined by $\xi = \mathrm{ev}_{-s} \circ \xi_D$ where $\xi_D : B \longrightarrow B[T]$ is defined in Definition 2.2.14 and $\mathrm{ev}_{-s} : B[T] \longrightarrow B$ is defined in Definition 1.2.3. Hence $\xi(x) = \sum_{j=0}^{\infty} \dfrac{D^j(x)}{j!}(-s)^j$. For each $x \in B$,

$$D(\xi(x)) = \sum_{j=0}^{\infty} \frac{D^{j+1}(x)}{j!}(-s)^j + \sum_{j=1}^{\infty} \frac{D^j(x)}{j!} j(-s)^{j-1}(-1) = 0,$$

so $\xi(B) \subseteq A$; moreover for $x \in A \subseteq B$ we have $x = \xi(x) \in \xi(B)$ hence $A \subseteq \xi(B)$ and $\xi(B) = A$.

By induction on $\deg_D(x)$ we show that $\forall x \in B$, $x \in A[s]$.

If $\deg_D(x) \leq 0$ it is obvious. Now assume that $\deg_D(x) \geq 1$ and that $y \in A[s]$ is true for all $y \in B$ of degree $\deg_D(y) < \deg_D(x)$.

Since $x = \xi(x) + (x - \xi(x))$ where $\xi(x) \in A$ and $x - \xi(x) \in sB$, we have

$$x = a + x's, \quad \text{for some } a \in A \text{ and } x' \in B. \tag{1}$$

This implies that $D(x) = D(x')s + x'$ and it easily follows by induction that

$$\forall\, m \geq 1 \quad D^m(x) = D^m(x')s + mD^{m-1}(x'). \tag{2}$$

Since $\deg_D(x) \geq 1$ we have $x \notin A$ and $x' \neq 0$. Now the fact that $D \in \mathrm{LND}(B)$ implies that there is $m \geq 1$ such that $D^{m-1}(x') \neq 0$ and $D^m(x') = 0$, so $\deg_D(x') = m - 1$. Then (2) gives $D^m(x) = mD^{m-1}(x') \neq 0$ and $D^{m+1}(x) = 0$, so $\deg_D(x) = m$ and so $\deg_D(x') = \deg_D(x) - 1$. By inductive hypothesis, we have $x' \in A[s]$; then (1) gives $x \in A[s]$. So $B = A[s] = A^{[1]}$. □

Remark 2.3.4. Let $B = \mathbb{Z}[Y, X] = \mathbb{Z}^{[2]}$ and $D = \dfrac{\partial}{\partial Y} + Y\dfrac{\partial}{\partial X} \in \mathrm{Der}(B)$. Note that D is a nonzero triangular derivation (hence locally nilpotent derivation). We have $D(Y) = 1$ and we have shown in Example 2.1.17 that $A = \ker(D) = \mathbb{Z}[2X - Y^2]$. We claim that B is not a polynomial ring over A. In fact assume that $B = A^{[1]}$, then there is a $g \in B$ ($\deg(g) > 0$) such that $B = \mathbb{Z}[2X - Y^2, g]$. Hence $(2X - Y^2, g)$ is a system of variables of $\mathbb{Z}[X, Y]$; thus by Lemma 2.1.20 we must have $2(g_Y + Yg_X) \in \{1, -1\}$, a contradiction. Therefore $B \neq A^{[1]}$. Thus the hypothesis that B is a $\mathbb{Q}$-algebra in Theorem 2.3.3 is not superfluous.

The following three corollaries are Corollary 7.4, 7.5 and 7.12 of [3].

Corollary 2.3.5. *Let B be a $\mathbb{Q}$-algebra, $D \in \mathrm{LND}(B)$ and $A = \ker(D)$. If $s \in B$ satisfies $Ds \in A^\times$, then $B = A[s] = A^{[1]}$.*

Proof. Let $a \in A$ be such that $aD(s) = 1$. Then as is a slice of D; so by Theorem 2.3.3 $B = A[as] = A[s]$ and s is transcendental over A (since as is and $a \in A^\times$). □

Definition 2.3.6. Let B be a ring and $D \in \mathrm{LND}(B)$. A *preslice* of D is an element s of B satisfying $D(s) \neq 0$ and $D^2(s) = 0$ (that is $\deg_D(s) = 1$).

Lemma 2.3.7. *Let B be a ring and $D \in \mathrm{LND}(B) \setminus \{0\}$. Then there exists a preslice of D.*

Proof. Since $D \neq 0$, there exists $b \in B$ such that $D(b) \neq 0$. Set $m = \deg_D(b)$ and $s = D^{m-1}(b)$. Then $D(s) \neq 0$ and $D^2(s) = 0$, so s is a preslice of D. □

Corollary 2.3.8. *Let B be a domain of characteristic zero and $A \in \mathrm{KLND}(B)$. Then $S^{-1}B = (\mathrm{Frac}\, A)^{[1]}$, where $S = A \setminus \{0\}$. In particular* $\mathrm{trdeg}_A(B) = 1$.

Proof. Let $A \in \mathrm{KLND}(B)$, then we have $A = \ker(D)$ where $D \in \mathrm{LND}(B) \setminus \{0\}$. By Lemma 2.3.7 there is $x \in B$ such that $D(x) \neq 0$ and $D^2(x) = 0$. Set $a = D(x)$, we have $a \in S$, $S^{-1}D(x/a) = 1$ and $\mathbb{Q} \subseteq S^{-1}B$ (since B is of characteristic zero). Moreover, by Lemma 2.2.11 we have $S^{-1}D \in \mathrm{LND}(S^{-1}B)$ and $\ker(S^{-1}D) = S^{-1}A = \mathrm{Frac}(A)$. We thus have by Theorem 2.3.3 $S^{-1}B = (\mathrm{Frac}\, A)^{[1]}$. Furthermore, $\mathrm{Frac}(S^{-1}B) = \mathrm{Frac}(B)$, hence $1 = \mathrm{trdeg}_{\mathrm{Frac}(A)} S^{-1}B = \mathrm{trdeg}_{\mathrm{Frac}(A)} \mathrm{Frac}(B) = \mathrm{trdeg}_A(B)$. □

Corollary 2.3.9. *Let B be a $\mathbb{Q}$-algebra, $D \in \mathrm{LND}(B)$ and $A = \ker(D)$. If $s \in B$ satisfies $D(s) \neq 0$ and $D^2 s = 0$, then $B_\alpha = A_\alpha[s] = (A_\alpha)^{[1]}$ where $\alpha = D(s) \in A \setminus \{0\}$.*

Proof. Let $S = \{1, \alpha, \alpha^2, \cdots\}$, then $B_\alpha = S^{-1}B$ and $A_\alpha = S^{-1}A$. Consider $S^{-1}D : B_\alpha \longrightarrow B_\alpha$, then $S^{-1}D \in \mathrm{LND}(B_\alpha)$ and $\ker(S^{-1}D) = A_\alpha$ (by Lemma 2.2.11). As $S^{-1}D(s) = \alpha \in (A_\alpha)^\times$, the result follows from Corollary 2.3.5. □

The next lemma is Exercise 7.6 of [3].

Lemma 2.3.10. *Let B be a domain of characteristic zero. If $A, A' \in \mathrm{KLND}(B)$ and $A \subseteq A'$, then $A = A'$.*

Proof. We have $A \subseteq A' \subseteq B$ and A is algebraically closed in B by Proposition 2.1.18. Corollary 2.3.8 implies $\mathrm{trdeg}_A B = 1 = \mathrm{trdeg}_{A'} B$, so by Corollary 1.5.26 we have $A = A'$. □

The following lemma will be very helpful in the next chapter.

Lemma 2.3.11. *Let k be a field of characteristic zero, $B = k[X, Y] = k^{[2]}$ and $D \in \mathrm{LND}(B)$. Then some nonconstant polynomial belongs to $\ker(D)$.*

Proof. If $D = 0$ then $\ker(D) = B$, so the claim is true.
If $D \neq 0$ then $\mathrm{trdeg}_{\ker(D)}(B) = 1$ by Corollary 2.3.8, so $\mathrm{trdeg}_k(\ker D) = 1$, so again the claim is true. □

Example 2.3.12. Let k and B be like in Lemma 2.3.11. Consider $D = X\frac{\partial}{\partial X} + Y\frac{\partial}{\partial Y}$, it can be shown that $\ker(D) = k$, hence D is not locally nilpotent.

Definition 2.3.13. Let B be a domain of characteristic zero. We say that B is *rigid* if it satisfies the following equivalent conditions:

(i) $\mathrm{LND}(B) = \{0\}$

(ii) $\mathrm{KLND}(B) = \emptyset$.

The lemma below can be found in [3] as Exercise 7.8.

Lemma 2.3.14. *Let B be a domain of characteristic zero that is not rigid. If k_0 is a field such that $k_0 \subseteq B$ and $\mathrm{trdeg}_{k_0} B = 1$, then $B = k^{[1]}$ for some field k such that $k_0 \subseteq k \subseteq B$.*

Proof. Since B is not rigid, there is $D \in \mathrm{LND}(B) \setminus \{0\}$. Set $k = \ker D$, then k is factorially closed in B and since k_0 is a field, we have $k_0 \subseteq k \subseteq B$ (by Corollary 2.2.22-(2)). Furthermore Corollary 2.3.8 implies that $\mathrm{trdeg}_k B = 1$, so $\mathrm{trdeg}_{k_0} k = 0$, that is k is algebraic over k_0 and thus k is a field (indeed, k is a domain and an integral extension of the field k_0, so k is a field by Proposition 5.7 of [1]). Since $D \in \mathrm{LND} \setminus \{0\}$, Lemma 2.3.7 implies that there exists $s \in B$ satisfying $D(s) \neq 0$ and $D^2(s) = 0$. Then we have $D(s) \in k^\times$, so Corollary 2.3.5 implies that $B = k^{[1]}$. □

Example 2.3.15. Let us prove that the subring $B = \mathbb{C}[T^2, T^3]$ of $\mathbb{C}[T] = \mathbb{C}^{[1]}$ is rigid. We have $B \neq \mathbb{C}^{[1]}$. In fact T^2 is an irreducible element of B, however it is not prime in B because $T^2 | (T^3 \cdot T^3)$ in B but $T^2 \nmid T^3$ in B. Hence by Proposition 1.1.12 B is not an UFD, therefore $B \neq \mathbb{C}^{[1]}$. Furthermore, $\mathbb{C} \subseteq B \subseteq \mathbb{C}[T]$ hence $1 = \mathrm{trdeg}_{\mathbb{C}}(\mathbb{C}[T]) = \mathrm{trdeg}_B(\mathbb{C}[T]) + \mathrm{trdeg}_{\mathbb{C}}(B)$. Since $T^2 \in B$, then T is algebraic over B and by Corollary 1.5.28 $\mathbb{C}[T]$ is algebraic over B, so $\mathrm{trdeg}_B(\mathbb{C}[T]) = 0$. Hence $\mathrm{trdeg}_{\mathbb{C}}(B) = 1$. If B is not rigid, then by Lemma 2.3.14 there exists a field K such that $\mathbb{C} \subseteq K \subseteq B$ and $B = K^{[1]}$, thus $\mathrm{trdeg}_{\mathbb{C}} K = 0$; since $\mathbb{C}$ is algebraically closed we have $K = \mathbb{C}$, a contradiction (because $B \neq \mathbb{C}^{[1]}$).

The following is an improved version of Lemma 2.2.11.

Corollary 2.3.16. *Let B be a domain of characteristic zero, $D \in \mathrm{Der}(B) \setminus \{0\}$ and $b \in B \setminus \{0\}$, and let S be a multiplicatively closed subset of B such that $0 \notin S$.*

1. *We have $bD \in \mathrm{LND}(B)$ if and only if $D \in \mathrm{LND}(D)$ and $b \in \ker(D)$.*
2. *We have $S^{-1}D \in \mathrm{LND}(S^{-1}B)$ if and only if $D \in \mathrm{LND}(B)$ and $S \subseteq \ker(D)$.*

Proof. 1. $\Longleftarrow$) Lemma 2.2.11.

$\Longrightarrow$) We know that $\ker(bD) = \ker(D)$ is factorially closed in B (since $bD \in \mathrm{LND}(B) \setminus \{0\}$). Moreover there is $x \in B$ such that $(bD)(x) \neq 0$ and $(bD)^2(x) = 0$ (bD has a preslice). Hence $bD(x) = (bD)(x) \in \ker(bD) \setminus \{0\}$ and so $b, D(x) \in$

$\ker(D)$ since $\ker(D)$ is factorially closed. Moreover, $b \in \ker(D)$ implies that $(bD)^n = b^n D^n$ for all $n \geq 1$, thus $bD \in \mathrm{LND}(B)$ implies that $D \in \mathrm{LND}(B)$.

2. $\Longleftarrow$) Lemma 2.2.11.
   $\Longrightarrow$) The canonical homomorphism $B \longrightarrow S^{-1}B$ is injective, so we may consider that $B \subseteq S^{-1}B$. Since D is the restriction of $S^{-1}D$, we have $D^n(b) = (S^{-1}D)^n(b)$ for all $b \in B$ and $n \in \mathbb{N}$, so $S^{-1}D \in \mathrm{LND}(S^{-1}B)$ implies $D \in \mathrm{LND}(B)$. Since $S^{-1}D \in \mathrm{LND}(S^{-1}B)$, part (1) of Corollary 2.2.22 implies that $(S^{-1}B)^\times = \ker(S^{-1}D)^\times$. Since $S \subseteq (S^{-1}B)^\times$, we have $S \subseteq \ker(S^{-1}D)^\times$ and hence $S \subseteq B \cap \ker(S^{-1}D) = \ker(D)$.

□

Example 2.3.17. Let $B = \mathbb{C}[X, Y]$ and $D = \dfrac{\partial}{\partial X} \in \mathrm{LND}(B)$; consider $S = B \setminus \{0\}$, $S^{-1}B = \mathbb{C}(X, Y)$ and $S^{-1}D \in \mathrm{Der}(S^{-1}B)$. Since $S \nsubseteq \ker(D)$, Corollary 2.3.16 implies that $S^{-1}D$ is not locally nilpotent. We can see this directly by noting that $\frac{1}{X} \in S^{-1}B$ and $(S^{-1}D)^n(\frac{1}{X}) \neq 0$ for all $n \geq 1$.

Notation. If $A \subseteq B$ are rings, define $\mathrm{LND}_A(B) = \mathrm{LND}(B) \cap \mathrm{Der}_A(B)$.

The following proposition can be found in Principle 8 of [6].

Proposition 2.3.18. *Given a domain A of characteristic zero and $B = A[T] = A^{[1]}$, we have* $\mathrm{LND}_A(B) = A \cdot \frac{d}{dT}$.

Proof. By Example 2.2.5 $\frac{d}{dT} \in \mathrm{LND}(B)$, and it is easy to show that $\ker(\frac{d}{dT}) = A$ (since we are in characteristic zero). Therefore by Corollary 2.3.16 part (1) we have $A \cdot \frac{d}{dT} \subseteq \mathrm{LND}_A(B)$. Conversely for all $D \in \mathrm{LND}_A(B)$ we have $\mathrm{LND}_A(B) \ni D = D(T)\frac{d}{dT}$ (by the proof of Lemma 2.1.13), thus by part (1) of Corollary 2.3.16 we have $D(T) \in \ker D = A$. Therefore $\mathrm{LND}_A(B) \subseteq A \cdot \frac{d}{dT}$. □

2.4 Degree and Homogenization of Derivations

Throughout this section, let $B = \oplus_{n \in \mathbb{Z}} B_n$ be a $\mathbb{Z}$-graded domain and let $\deg : B \longrightarrow \mathbb{Z} \cup \{-\infty\}$ be the degree function determined by the grading (see Remark 1.4.8).

Definition 2.4.1. Let $D \in \mathrm{Der}(B)$ and consider the nonempty subset

$$U = \{\deg(D(f)) - \deg(f) \mid f \in B \setminus \{0\}\}$$

of $\mathbb{Z} \cup \{-\infty\}$. If U has a greatest element, then we say that the *degree of* D *exists* and we define $\deg(D)$ to be that element.
Note that $\deg(D) = -\infty \iff D = 0$. Furthermore if $\deg(D)$ exists and $D \neq 0$ then there is $f \in B \setminus \ker(D)$ such that $\deg(D) = \deg(D(f)) - \deg(f)$.

Definition 2.4.2. Given $D \in \mathrm{Der}(B)$, the *defect function* of D is the map

$$\begin{aligned} \mathrm{def}_D : B &\longrightarrow \mathbb{Z} \cup \{-\infty\} \\ f &\longmapsto \begin{cases} \deg(D(f)) - \deg(f) & \text{if } f \neq 0 \\ -\infty & \text{if } f = 0. \end{cases} \end{aligned}$$

The proofs of results from 2.4.3-2.4.15 follow the reasoning given in section 2.6 of [17].

Lemma 2.4.3. *Let* $D \in \mathrm{Der}(B)$.

(*i*) $\mathrm{def}_D(fg) \leq \max\{\mathrm{def}_D(f), \mathrm{def}_D(g)\}$ *for all* $f, g \in B$.

(*ii*) *If* $f_1, \ldots, f_m \in B$ *are such that* $\deg(\sum_{i=1}^m f_i) = \max_{1 \leq i \leq m} \deg(f_i)$, *then* $\mathrm{def}_D(\sum_{i=1}^m f_i) \leq \max_{1 \leq i \leq m} \mathrm{def}_D(f_i)$.

Proof. (i) If $f = 0$ or $g = 0$ the result is clear. Assume that $f \neq 0$ and $g \neq 0$. We have

$$\begin{aligned} \mathrm{def}_D(fg) &= \deg(D(fg)) - \deg(fg) \\ &= \deg(fD(g) + gD(f)) - (\deg(f) + \deg(g)) \\ &\leq \max\{\deg(fD(g)), \deg(gD(f))\} - (\deg(f) + \deg(g)) \\ &= \max\{\deg(f) + \deg(D(g)), \deg(g) + \deg(D(f))\} - (\deg(f) + \deg(g)) \end{aligned}$$

In the case that

$$\max\{\deg(f) + \deg(D(g)), \deg(g) + \deg(D(f))\} = \deg(f) + \deg(D(g)),$$

we have $\mathrm{def}_D(fg) \leq \deg(D(g)) - \deg(g) = \mathrm{def}_D(g)$.
Otherwise,

$$\max\{\deg(f) + \deg(D(g)), \deg(g) + \deg(D(f))\} = \deg(g) + \deg(D(f)),$$

so $\mathrm{def}_D(fg) \leq \deg(D(f)) - \deg(f) = \mathrm{def}_D(f)$.

Therefore $\mathrm{def}_D(fg) \leq \max\{\mathrm{def}_D(f), \mathrm{def}_D(g)\}$.

(ii) Observe that

$$\begin{aligned}
\mathrm{def}_D(\sum_{i=1}^{n} f_i) &= \deg(D(\sum_{i=1}^{m} f_i)) - \deg(\sum_{i=1}^{m} f_i) \\
&= \deg(\sum_{i=1}^{m} D(f_i)) - \max\{\deg(f_i) \mid 1 \leq i \leq m\} \\
&\leq \max\{\deg(D(f_i)) \mid 1 \leq i \leq m\} - \max\{\deg(f_i) \mid 1 \leq i \leq m\} \\
&\leq \max\{\deg(D(f_i)) - \deg(f_i) \mid 1 \leq i \leq m\} \\
&= \max\{\mathrm{def}_D(f_i) \mid 1 \leq i \leq m\}.
\end{aligned}$$

□

Proposition 2.4.4. *Let k be a field of characteristic zero. Assume that the $\mathbb{Z}$-graded domain B is a finitely generated k-algebra. Then $\deg(D)$ exists for every $D \in \mathrm{Der}_k(B)$.*
More precisely, if $h_1, h_2, \cdots, h_n$ are homogeneous elements of B which generate B as a k-algebra, then

$$\deg(D) = \max\{\deg(D(h_i)) - \deg(h_i) \mid 1 \leq i \leq n\}.$$

Proof. It is clear that there exist homogeneous elements $h_1, \cdots, h_n \in B$ such that $B = k[h_1, \cdots, h_n]$. Let $\mathrm{def} = \mathrm{def}_D : B \longrightarrow \mathbb{Z} \cup \{-\infty\}$ be the defect function of D and $K = \max\{\mathrm{def}(h_1), \cdots, \mathrm{def}(h_n)\}$. To prove the proposition, we have to show that $\mathrm{def}(f) \leq K$ for all $f \in B \setminus \{0\}$.
From Lemma 2.4.3 (i) we know that if $f_1, \cdots, f_s \in B$ then $\mathrm{def}(f_1 \cdots f_s) \leq \max_{1 \leq i \leq s} \mathrm{def}(f_i)$. In particular, it is easy to show that $\mathrm{def}(h_1^{e_1} \cdots h_n^{e_n}) \leq K$ for any $e_1, \cdots, e_n \in \mathbb{N}$.

Furthermore $\operatorname{def}(\lambda h_1^{e_1}\cdots h_n^{e_n}) \leq K$ for any $\lambda \in k^\times$ and $e_1, \cdots, e_n \in \mathbb{N}$. In fact since D is a k-derivation and $\lambda \in k^\times$ we have $\operatorname{def}(\lambda) = -\infty$. Thus

$$\operatorname{def}(\lambda h_1^{e_1}\cdots h_n^{e_n}) \leq \max\{\operatorname{def}(\lambda), \operatorname{def}(h_1^{e_1}\cdots h_n^{e_n})\} \leq K. \qquad (*)$$

Claim: If $h \in B$ is homogeneous, then $\operatorname{def}(h) \leq K$.
Proof: If $h = 0$, then $\operatorname{def}(h) = -\infty \leq K$, so suppose $h \neq 0$ and h is homogeneous of degree r. We can write $h = \sum_{i=1}^m f_i$ where $f_i = \lambda_i h_1^{e_{i1}}\cdots h_n^{e_{in}}$ and $\sum_{j=1}^n e_{ij}\deg(h_j) = r$ for all $1 \leq i \leq m$. So $\deg(f_i) = \deg(h)$ for all $1 \leq i \leq m$ and $h = \sum_{j=1}^m f_i$ satisfies the condition in Lemma 2.4.3 (ii). Then $\operatorname{def}(h) \leq \max\{\operatorname{def}(f_1), \cdots, \operatorname{def}(f_m)\}$. But $\operatorname{def}(f_i) \leq K$ for all $1 \leq i \leq m$ by $(*)$, so $\operatorname{def}(h) \leq K$ and the claim is proved.

Now let $f \in B \setminus \{0\}$, then $f = f_1 + \cdots + f_m$ where f_i are homogeneous elements of distinct degrees. Then $\deg(f) = \deg(\sum_{i=1}^m f_i) = \max\{\deg(f_i) \mid 1 \leq i \leq m\}$ so by Lemma 2.4.3 (ii) $\operatorname{def}(f) \leq \max\{\operatorname{def}(f_1), \cdots, \operatorname{def}(f_n)\}$. But by the claim above we have $\operatorname{def}(f_i) \leq K$ for all $1 \leq i \leq m$. So $\operatorname{def}(f) \leq K$. □

Example 2.4.5. Regard $B = k[X, Y, Z]$ as a graded ring (with standard $\mathbb{Z}$-grading) and let $D = X\frac{\partial}{\partial Y} + Y^3\frac{\partial}{\partial Z}$. We have $D(X) = 0$, $D(Y) = X$ and $D(Z) = Y^3$. Thus

$$\begin{aligned}\deg(D) &= \max\{\deg(DX) - \deg(X), \deg(DY) - \deg(Y), \deg(DZ) - \deg(Z)\}\\ &= \max\{-\infty, \deg(X) - \deg(Y), \deg(Y^3) - \deg(Z)\}\\ &= \max\{-\infty, 1-1, 3-1\}\\ &= 2.\end{aligned}$$

Definition 2.4.6. Let $D \in \operatorname{Der}(B)$ and $D \neq 0$. If there exists $d \in \mathbb{Z}$ such that $D(B_i) \subseteq B_{i+d}$ for all $i \in \mathbb{Z}$, then d is unique and we say that D is *homogeneous of degree* d. We adopt the convention that the zero derivation is homogeneous of degree $-\infty$.

Example 2.4.7. Let $B = k[X] = \oplus_{n\in\mathbb{N}} B_n$, where the B_n are defined as in Example 1.4.3. The derivation $D = \frac{d}{dX}$, defined in Example 2.1.2, is homogeneous of degree -1.

Lemma 2.4.8. *Let $D \in \mathrm{Der}(B)$ be such that D is homogeneous of degree d, then $\deg(D)$ exists and $\deg(D) = d$.*

Proof. Trivial. □

Definition 2.4.9. Let $D \in \mathrm{Der}(B)$ be such that $\deg(D)$ exists. Define the *homogenization* of D, $\tilde{D} : B \longrightarrow B$, as follows:
If $D = 0$, then $\tilde{D} = 0$.
If $D \neq 0$, let $d = \deg(D) \in \mathbb{Z}$, and for all $i \in \mathbb{Z}$, define:

$$\begin{aligned} \tilde{D}_i : B_i &\longrightarrow B_{i+d} \\ f_i &\longmapsto P_{i+d}(D(f_i)) \end{aligned}$$

where $P_j : B \longrightarrow B_j$ is the canonical projection for all $j \in \mathbb{Z}$.

Now given $f \in B$, $f = \sum_{i \in \mathbb{Z}} f_i$ (where all the $f_i \in B_i$ are zero expect for finitely many of them), we define

$$\tilde{D}(f) = \sum_{i \in \mathbb{Z}} \tilde{D}_i(f_i).$$

Remark 2.4.10. If $D \in \mathrm{Der}(B)$ is homogeneous, then $D = \tilde{D}$.

Proposition 2.4.11. *Let $D \in \mathrm{Der}(B)$. If $\deg(D)$ exists, then*

(*i*) *$\tilde{D} : B \longrightarrow B$ is a homogeneous derivation of degree $\deg(D)$,*

(*ii*) *$\tilde{D} = 0 \Longleftrightarrow D = 0$,*

(*iii*) *$\deg(\tilde{D}) = \deg(D)$.*

Proof. Assertion (i) is clear if $D = 0$, so assume that $D \neq 0$ and let $d = \deg(D) \in \mathbb{Z}$. We leave it to the reader to verify that $\tilde{D} : B \longrightarrow B$ is a derivation. It is clear from the definition of $\tilde{D}$ that $\tilde{D}(B_i) \subseteq B_{i+d}$ for all $i \in \mathbb{Z}$, so if $\tilde{D} \neq 0$ then $\tilde{D}$ is homogeneous of degree $\deg(D)$. So the proof of (i) will be complete once we show that $\tilde{D} \neq 0$ (we show it in the proof of (ii)).

(ii) If $D = 0$, then $\tilde{D} = 0$. Now assume that $D \neq 0$ and let us prove that $\tilde{D} \neq 0$. Let $d = \deg(D) \in \mathbb{Z}$. Then there is $f \in B \setminus \{0\}$ such that $d = \deg(D(f)) - \deg(f)$. Set $\deg(f) = n$ and write $f = f_n + \sum_{i<n} f_i$; we have

$$\deg(D(f)) \leq \max\{\deg(D(f_n)), \deg(\sum_{i<n} D(f_i))\}.$$

If $\max\{\deg(D(f_n)), \deg(\sum_{i<n} D(f_i))\} = \deg(\sum_{i<n} D(f_i))$, then there is an $i_0 < n$ such that $\deg(D(f_{i_0})) \geq \deg(D(f)) = n + d$, so
$d \leq \deg(D(f_{i_0})) - n < \deg(D(f_{i_0})) - i_0 = \deg(D(f_{i_0})) - \deg(f_{i_0})$, a contradiction.
Thus $\max\{\deg(D(f_n)), \deg(\sum_{i<n} f_i)\} = \deg(D(f_n))$, which implies that $\deg(D(f_n)) \geq \deg(D(f)) = n + d$. As $\deg(D(f_n)) \leq n + d$ is clear, we have $\deg(D(f_n)) = d + n$ and $P_{n+d}(D(f_n)) \neq 0$.
Therefore $\tilde{D}(f_n) = \tilde{D}_n(f_n) = P_{n+d}(D(f_n)) \neq 0$ and so $\tilde{D} \neq 0$. This proved (ii), and also completes the proof of (i).

(iii) Follows from (i) and Lemma 2.4.8. □

Example 2.4.12. Let $B = k[X, Y, Z]$ and $D = X\dfrac{\partial}{\partial Y} + Y^3\dfrac{\partial}{\partial Z}$ be like in Example 2.4.5. We have $\tilde{D}_1(X) = P_{1+2}(DX) = P_3(0) = 0$, $\tilde{D}_1(Y) = P_{1+2}(DY) = P_3(X) = 0$ and $\tilde{D}_1(Z) = P_{1+2}(DZ) = P_3(Y^3) = Y^3$. So $\tilde{D} : B \longrightarrow B$ is the derivation $Y^3\frac{\partial}{\partial Z}$.

Lemma 2.4.13. *Let $D \in \mathrm{Der}(B) \setminus \{0\}$ be such that $\deg(D)$ exists. Set $d = \deg(D) \in \mathbb{Z}$.*

- (i) *$\tilde{D}(P_{j+nd}(D^n(f))) = P_{j+(n+1)d}(D^{n+1}(f))$ for all $f \in B$, $n \in \mathbb{N}$ and all $j \geq \deg(f)$.*
- (ii) *If $h \in B_j$ for some j, then for all $n \in \mathbb{N}$ we have $\tilde{D}^n(h) = P_{j+nd}(D^n(h))$.*

Proof. (i) For $f \in B$, write f as $f = \sum_{i \leq j} f_i = \sum_{i<j} f_i + f_j$. For $n = 0$ we have

$$\begin{aligned}
\tilde{D}(P_j(D^0(f))) = \tilde{D}(P_j(f)) &= \tilde{D}(f_j) \text{ (since } D^0 = \mathrm{id}_B), \\
&= \tilde{D}_j(f_j) \\
&= P_{j+d}(D(f_j)) \\
&= P_{j+d}(D(f)) \text{ (since for } i < j \text{ we have } \deg(D(f_i)) < j + d).
\end{aligned}$$

Now given $n \in \mathbb{N}$, set $g = D^n(f)$ and $i = j + nd$. Observe that $\deg(D^n(f)) \leq \deg(f) + nd \leq j + nd$. Then $i \geq \deg(g)$ and by the previous argument, we get

$$\begin{aligned}\tilde{D}(P_{j+nd}(D^n(f))) &= \tilde{D}(P_i(g)) \\ &= P_{i+d}(D(g)) \\ &= P_{j+(n+1)d}(D^{n+1}(f)).\end{aligned}$$

(ii) By induction on n. Let $h \in B_j$ for some $j \in \mathbb{Z}$.
For $n = 0$, $\tilde{D}^n(h) = \tilde{D}^0(h) = h$ and $P_{j+nd}(D^n(h)) = P_j(h) = h$.
Suppose $\tilde{D}^n(h) = P_{j+nd}(D^n(h))$ for some $n \in \mathbb{N}$. Then

$$\begin{aligned}\tilde{D}^{n+1}(h) = \tilde{D}(\tilde{D}^n(h)) &= \tilde{D}(P_{j+nd}(D^n(h))) \\ &= P_{j+(n+1)d}(D^{n+1}(h))\end{aligned}$$

where the last equality follows from (i). Thus $\tilde{D}^n(h) = P_{j+nd}(D^n(h))$ for all $n \in \mathbb{N}$. □

Proposition 2.4.14. *Let $D \in \mathrm{Der}(B)$ be such that $\deg(D)$ exists. If $D \in \mathrm{LND}(B)$ then $\tilde{D} \in \mathrm{LND}(B)$.*

Proof. If $D \in \mathrm{LND}(B) \setminus \{0\}$ then Lemma 2.4.13 (ii) implies that all homogeneous elements of B belong to $\mathrm{Nil}(\tilde{D})$, so $\mathrm{Nil}(\tilde{D}) = B$. □

Proposition 2.4.15. *Let $D \in \mathrm{Der}(B)$ be such that $\deg(D)$ exists. If $f = \sum_{i \leq n} f_i \in \ker(D)$, then $f_n \in \ker(\tilde{D})$.*

Proof. We may assume that $D \neq 0$. Let $d = \deg(D)$ then Lemma 2.4.13 (i) implies that $\tilde{D}(f_n) = \tilde{D}(P_n(f)) = P_{n+d}(D(f)) = 0$. □

Chapter 3

Locally Nilpotent Derivations and Automorphisms of $k[X, Y]$

In this chapter we present how the theory of locally nilpotent derivations can be used to describe the structure of the polynomial ring $k[X, Y]$. We begin by giving some useful results about polynomial rings over a field which will help us later in our work.

3.1 Some facts on polynomial rings

Lemma 3.1.1. *Let $B = k^{[n]}$ where k is a field. Then we have $B^\times = k^\times$. Furthermore, if K is a field which is a subring of B, then $K \subseteq k$.*

Proof. By Lemma 1.3.10, k is factorially closed in B. So $B^\times = k^\times$ follows from Lemma 1.3.17. Moreover, if $K \subseteq B$ then $K^\times \subseteq B^\times = k^\times$ so $K \subseteq k$. □

Proposition 3.1.2. *Let A be a domain and $U \in A[X]$. The following are equivalent:*

(*i*) $A[X] = A[U]$,

(*ii*) $U = aX + b, \quad a \in A^\times, b \in A$.

Proof. *ii*) $\Longrightarrow$ *i*) Trivial.
i) $\Longrightarrow$ *ii*) We have $X \in A[U]$; so there exists $P = \sum_{i=0}^{n} a_i T^i \in A[T] \setminus \{0\}$ such that

$X = P(U)$. Let $n = \deg_T(P)$, $m = \deg_X(U)$ and observe that $n > 0$ and $m > 0$. It is easy to see that $\deg_X(P(U)) = mn = \deg_X(U)\deg_T(P)$. We thus have

$$X = P(U) \Rightarrow \deg_T(P)\deg_X(U) = 1 \Rightarrow \deg_X(U) = 1 = \deg_T(P).$$

Therefore $U = aX + b, \quad a \in A \setminus \{0\}$, $b \in A$. Furthermore, $\deg_T(P) = 1$ then $P(T) = cT + d, \quad c \in A \setminus \{0\}$, $d \in A$; so $X = P(U) = cU + d = caX + bc + d$. Therefore $ca = 1$ and we thus have $a \in A^\times$. □

Corollary 3.1.3. *Let $B = k[X,Y]$ and F be an element of B such that $k[X,Y] = k[X,F]$. Then we have $F = aY + b, \quad a \in k \setminus \{0\}$ and $b \in k[X]$.*

Proof. Apply Proposition 3.1.2 to $B = A[Y] = A[F]$, $A = k[X]$. □

Lemma 3.1.4. *Let k be an algebraically closed field and $B = k[X,Y]$. If $g(X,Y)$ is a nonconstant standard homogeneous polynomial, then $g = L_1L_2\cdots L_N$, where $L_i = a_iX + b_iY, \quad a_i, b_i \in k$, $(a_i,b_i) \neq (0,0)$ and $N = \deg(g)$.*

Proof. Since g is standard homogeneous, it can be written as:

$$g(X,Y) = \sum_{i=0}^{N} b_iX^iY^{N-i} = Y^NP(\frac{X}{Y}), \text{ where } P(t) \in k[t].$$

Let $M = \deg(P(t))$ then we have $M \leq N$ and $P(t) = \sum_{i=0}^{M} b_it^i$. Moreover, k is algebraically closed, so the polynomial $P(t) \in k[t]$ can be factored as $P(t) = c\prod_{i=1}^{M}(t-c_i)$, for some $c \in k^\times, \quad c_i \in k$ and so $g(X,Y) = Y^Nc\prod_{i=1}^{M}(\frac{X}{Y} - c_i) = cY^{N-M}\Pi_{i=1}^{M}(X - c_iY) = L_1L_2\cdots L_N$, with $L_i = a_iX + b_iY \;\; a_i, b_i \in k$, $(a_i,b_i) \neq (0,0)$. □

Lemma 3.1.5. *Let $B = k[X,Y] = k^{[2]}$ where k is a field. Then there are infinitely many subrings A of B such that $B = A^{[1]}$.*

Proof. In fact let m, n be two elements of $\mathbb{N} \setminus \{0\}$ such that $n \neq m$; assume without loss of generality that $0 < m < n$ and consider the subrings $A_n = k[X + Y^n]$ and $A_m = k[X + Y^m]$ of B. Clearly we have that $A_n[Y] = B = A_m[Y]$.

Let us prove that $A_n \neq A_m$. If $A_n = A_m$, then $X + Y^m \in k[X + Y^n]$ that is $X + Y^m = g(X + Y^n)$ where $g(T) = \sum_{i=0}^{s} a_iT^i \in k[T]$ is a nonconstant polynomial and

$a_s \neq 0$. So $\mathrm{ev}_{(0,Y)}(X+Y^m) = \mathrm{ev}_{(0,Y)}\, g(X+Y^n)$ that is $Y^m = a_0 + a_1 Y^n + \cdots + a_s Y^{ns}$, a contradiction (since $0 < m < n$). Hence $A_n \neq A_m$ for all $n \neq m$.

We show that Y is transcendental over A_n for all $n \in \mathbb{N}$. By contradiction assume Y is algebraic over A_n. Then, by Corollary 1.5.28, $B = A_n[Y]$ is algebraic over A_n and consequently $\mathrm{trdeg}_{A_n}(B) = 0$. Since $X + Y^n$ is transcendental over k by Lemma 1.3.13, we have $A_n = k[X + Y^n] = k^{[1]}$ and consequently $\mathrm{trdeg}_k(A_n) = 1$. So

$$2 = \mathrm{trdeg}_k(B) = \mathrm{trdeg}_k(A_n) + \mathrm{trdeg}_{A_n}(B) = 1 + 0 = 1,$$

a contradiction. So Y is transcendental over A_n.

Therefore $B = A_n[Y] = A_n^{[1]}$ for all $n \in \mathbb{N}$; and so there is an infinite number of subrings A of B such that $B = A^{[1]}$. □

Lemma 3.1.6. *Let $B = k^{[n]}$, where k is a field and let K be a field which is a subring of B. If there is $m \in \mathbb{N}$ such that $B = K^{[m]}$, then $K = k$ and $m = n$.*

Proof. Since K is a subring of B, by Lemma 3.1.1 we have $K \subseteq k$; and k is also a subring of B. Since $B = K^{[m]}$ we must also have $k \subseteq K$; hence $K = k$. Moreover

$$k^{[n]} = B = K^{[m]} = k^{[m]} \Longrightarrow \mathrm{trdeg}_k\, k^{[n]} = \mathrm{trdeg}_k\, k^{[m]} \Rightarrow n = m.$$

□

3.2 Preliminaries on automorphisms of $k[X,Y]$

The aim of this section is to present some particular subgroups of the group of k-automorphism of $k[X,Y]$ which we will use regularly throughout this chapter, namely in Theorems 3.3.8, 3.4.1 and 3.4.4.

In this section k is an arbitrary field.

Let $B = k[X,Y]$ and let $\mathrm{Aut}_k(B)$ be the set of all k-automorphisms of B. It is well known that $\mathrm{Aut}_k(B)$ is a group.

Definition 3.2.1. The group of k-automorphisms of B is called the *general affine group* of dimension 2 and is denoted $\mathrm{GA}_2(k)$.

Remark 3.2.2. By Theorem 1.2.4, each element $\varphi \in \mathrm{GA}_2(k)$ is completely determined by the pair $(\varphi(X), \varphi(Y)) \in B \times B$. It is customary to identify φ with $(\varphi(X), \varphi(Y))$ and to write simply $\varphi = (\varphi(X), \varphi(Y))$. Then the rule for composing elements of $\mathrm{GA}_2(k)$ is:

$$(\varphi(X), \varphi(Y)) \circ (\psi(X), \psi(Y)) = ((\varphi \circ \psi)(X), (\varphi \circ \psi)(Y)).$$

For instance, consider the automorphisms $\varphi = (Y, X + Y^2)$ and $\psi = (Y, X)$. This means that $\varphi : B \longrightarrow B$ is the k-automorphism that satisfies $\varphi(X) = Y$ and $\varphi(Y) = X + Y^2$, and that $\psi : B \longrightarrow B$ is the k-automorphism that satisfies $\psi(X) = Y$ and $\psi(Y) = X$. Then $(\varphi \circ \psi)(X) = \varphi(Y) = X + Y^2$ and $(\varphi \circ \psi)(Y) = \varphi(X) = Y$, so

$$(Y, X + Y^2) \circ (Y, X) = (X + Y^2, Y),$$

and the reader can verify that

$$(Y, X) \circ (Y, X + Y^2) = (X, Y + X^2).$$

Lemma 3.2.3. *Let $\varphi : B \longrightarrow B$ be a k-homomorphism and let $u = \varphi(X)$ and $v = \varphi(Y)$. Then we have $\varphi \in \mathrm{GA}_2(k)$ if and only if (u, v) is a system of variables of B.*

Proof. $\Longrightarrow$) Let $\alpha = (u, v) \in \mathrm{GA}_2(k)$, then the automorphism $\alpha : B \longrightarrow B$ satisfies $\alpha(X) = u$ and $\alpha(Y) = v$. By Theorem 1.2.4, $\mathrm{Im}(\alpha) = k[u, v]$. Since α is surjective, $B = k[u, v]$ so (u, v) is a system of variables of B.
$\Longleftarrow$) Assume that (u, v) is a system of variables of B. We know that there is an unique k-homomorphism such that $\alpha(X) = u$ and $\alpha(Y) = v$. Then $\mathrm{Im}(\alpha) = k[u, v]$ by Theorem 1.2.4 and $k[u, v] = B$ by hypothesis, so α is surjective and since B is Noetherian α is an automorphism. □

Affine linear subgroup

Given $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ there exists a unique k-homomorphism $\varphi_A : B \longrightarrow B$ such that $\varphi_A(X) = aX + cY$ and $\varphi_A(Y) = bX + dY$. It is easy to verify that if

$I \in \mathrm{GL}_2(k)$ is the identity matrix then φ_I is the identity map of B, and that if $A, B \in \mathrm{GL}_2(k)$ then $\varphi_A \circ \varphi_B = \varphi_{AB}$. It follows that $A \longmapsto \varphi_A$ is a group homomorphism $\mathrm{GL}_2(k) \longrightarrow \mathrm{GA}_2(k)$. The image of this homomorphism is denoted $\mathcal{GL}_2(k) = \{\varphi_A \mid A \in \mathrm{GL}_2(k)\}$.

Given $(a,b) \in k^2$, define the k-homomorphism $\varphi_{(a,b)} : B \longrightarrow B$ by $\varphi_{(a,b)}(X) = X + a$ and $\varphi_{(a,b)}(Y) = Y + b$. It is clear that $\varphi_{(0,0)}$ is the identity map of B and that if $(a,b),(c,d) \in k^2$ then $\varphi_{(a,b)} \circ \varphi_{(c,d)} = \varphi_{(a+c,b+d)}$. So $(a,b) \longmapsto \varphi_{(a,b)}$ is a group homomorphism $k^2 \longrightarrow \mathrm{GA}_2(k)$. Its image is denoted $\mathcal{T} = \left\{\varphi_{(a,b)} \,\middle|\, (a,b) \in k^2\right\}$.

Definition 3.2.4.

- The subgroup $\mathcal{GL}_2(k)$ of $\mathrm{GA}_2(k)$ is called the *subgroup of linear automorphisms.*
- The subgroup $\langle \mathcal{GL}_2(k) \cup \mathcal{T} \rangle$ of $\mathrm{GA}_2(k)$ generated by $\mathcal{GL}_2(k)$ and $\mathcal{T}$ is called the *affine linear subgroup.* It is denoted by $\mathrm{Af}_2(k)$.

Remark 3.2.5.

1. The elements of $\mathrm{Af}_2(k)$ are of the form $\varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_s$, where $\varphi_i \in \mathcal{GL}_2(k) \cup \mathcal{T}$ for $i = 1, 2, \cdots, s$. Therefore
   $\mathrm{Af}_2(k) = \{(a_1X + b_1Y + c_1, a_2X + b_2Y + c_2) \mid a_i, b_i, c_i \in k; a_1b_2 - a_2b_1 \neq 0\}$.
2. There exists a semi-commuting relation among elements of $\mathcal{GL}_2(k)$ and $\mathcal{T}$, given by:

   $$(X + c_1, Y + c_2)(a_1X + b_1Y, a_2X + b_2Y) = (a_1X + b_1Y, a_2X + b_2Y)(X + c, Y + c'),$$

   where $c = a_1c_1 + b_1c_2$ and $c' = a_2c_1 + b_2c_2$.

Subgroup of triangular automorphisms

Let $a, c \in k^\times$, $b \in k$ and $f(X) \in k[X] \subseteq k[X,Y]$; like above, define a k-homomorphism $\tau_{(a,b,c,f(X))}$ such that $\tau_{(a,b,c,f(X))}(X) = aX + b$ and $\tau_{(a,b,c,f(X))}(Y) = cY + f(X)$. Given $a', c' \in k^\times$, $b' \in k$ and $f'(X) \in k[X]$ we have

$$\tau_{(a',b',c',f'(X))} \circ \tau_{(a,b,c,f(X))}(X) = aa'X + ab' + b$$

and

$$\tau_{(a',b',c',f'(X))} \circ \tau_{(a,b,c,f(X))}(Y) = cc'Y + cf'(X) + f(a'X + b'),$$

so $\tau_{(a,b,c,f(X))} \circ \tau_{(a',b',c',f'(X))} = \tau_{(aa',ab'+b,cc',cf'(X)+f(a'X+b'))}$.

Hence $\tau_{(a,b,c,f(X))}$ has $\tau_{(a^{-1},-a^{-1}b,c^{-1},-c^{-1}f(a^{-1}X-a^{-1}b))}$ as inverse, thus $\tau_{(a,b,c,f(X))}$ is bijective and $\tau_{(a,b,c,f(X))} \in \mathrm{GA}_2(k)$.

Therefore, the set

$$\mathrm{BA}_2(k) = \left\{ \tau_{(a,b,c,f(X))} = (aX+b, cY+f(X)) \;\middle|\; a,c \in k^\times, b \in k, f \in k[X] \right\}$$

is a subgroup of $\mathrm{GA}_2(k)$.

Definition 3.2.6. The subgroup of $\mathrm{GA}_2(k)$ defined above is called the *subgroup of triangular automorphisms*. It is denoted by $\mathrm{BA}_2(k)$.

Remark 3.2.7. Observe that $\mathcal{T} \subseteq \mathrm{BA}_2(k)$ and that consequently the subgroup of $\mathrm{GA}_2(k)$ generated by $\mathcal{GL}_2(k)$ and $\mathrm{BA}_2(k)$ is equal to the subgroup generated by $\mathrm{Af}_2(k)$ and $\mathrm{BA}_2(k)$.

Subgroup of tame automorphisms

Definition 3.2.8. The *tame subgroup* of $\mathrm{GA}_2(k)$ is the subgroup $\langle \mathcal{GL}_2(k) \cup \mathrm{BA}_2(k) \rangle$ generated by the subgroups of linear and triangular automorphisms. An automorphism is *tame* if it is of the form $\varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_s$, where $\varphi_i \in \mathcal{GL}_2(k) \cup \mathrm{BA}_2(k)$ for $i = 1, 2, \cdots, s$ for some s.

3.3 Rentschler's Theorem

From now-on, k denotes a field of characteristic zero.

Proposition 3.3.1. *Let $\alpha : A \longrightarrow A$ be an automorphism of a ring A, let $D \in \mathrm{LND}(A)$, and consider the map $\delta = \alpha \circ D \circ \alpha^{-1} : A \longrightarrow A$. Then $\delta \in \mathrm{LND}(A)$ and $\ker(\delta) = \alpha(\ker D)$.*

Proof. One can verify directly that δ is a derivation of A. Since D is locally nilpotent and $\delta^n = \alpha \circ D^n \circ \alpha^{-1}$ for all $n \in \mathbb{N}$, it follows that δ is locally nilpotent. For any $x \in A$ we have

$$\delta(x) = 0 \Leftrightarrow \alpha(D(\alpha^{-1}(x))) = 0 \Leftrightarrow D(\alpha^{-1}(x)) = 0 \Leftrightarrow \alpha^{-1}(x) \in \ker D \Leftrightarrow x \in \alpha(\ker D),$$

so $\ker(\delta) = \alpha(\ker(D))$. □

Definition 3.3.2. Let $B = A[X_1, \cdots, X_n] = A^{[n]}$ where A is a ring. An element $f \in B$ is called a *variable of B over A* if $B = A[f]^{[n-1]}$. (In other words, f is a variable of B over A if there exist $f_2, \cdots, f_n \in B$ such that $B = k[f, f_2, \cdots, f_n]$.)

Proposition 3.3.3. *Let k be a field of characteristic zero and $B = k[X,Y]$. If $D \in \mathrm{LND}(B) \setminus \{0\}$ and $X \in \ker(D)$, then there exists $f \in k[X] \setminus \{0\}$ such that $D = f(X)\dfrac{\partial}{\partial Y}$.*

Proof. From Corollary 2.2.23, D is a k-derivation and by Lemma 2.1.13 we have

$$D = h(X,Y)\frac{\partial}{\partial X} + g(X,Y)\frac{\partial}{\partial Y},$$

where $h(X,Y), g(X,Y) \in B$. Since $D(X) = 0$ we have $h(X,Y) = 0$, hence $D = g(X,Y)\dfrac{\partial}{\partial Y}$ and $g(X,Y) \neq 0$ (since $D \neq 0$). It follows that $\ker D = k[X]$. Then Corollary 2.3.16 (1) implies that $g(X,Y) \in \ker D$, so $g(X,Y) = f(X) \in k[X]$ and we are done. □

Corollary 3.3.4. *Let $B = k[X,Y]$ where k is a field of characteristic zero, and $D \in \mathrm{LND}(B) \setminus \{0\}$. If there exists $f(X) \in k[X] \setminus k$ (a nonconstant polynomial) such that $f(X) \in \ker(D)$, then $D = h(X)\dfrac{\partial}{\partial Y}$, where $h \in k[X] \setminus \{0\}$.*

Proof. Since f is a non constant polynomial we have $f(X) - f(0) \neq 0$ and by Corollary 2.2.23 $D(\alpha) = 0$, for all $\alpha \in k$; hence $D(f(X) - f(0)) = D(f(X)) - D(f(0)) = 0$. Thus $f(X) - f(0) = Xg(X) \in \ker(D)$, with $g(X) \neq 0$. The fact that $\ker(D)$ is factorially closed implies that $X \in \ker(D)$ and by Proposition 3.3.3, we have $D = h(X)\dfrac{\partial}{\partial Y}$. □

Remark 3.3.5. The above results (Proposition 3.3.3 and Corollary 3.3.4) remain valid with X and Y interchanged.

The lemma below is a weak version of the Lemma 4.6 of [6].

Lemma 3.3.6. *Let $B = k[X,Y]$ and $\omega = (a,b)$ where k is a field of characteristic zero, and a, b are relatively prime positive integers, and regard B as being endowed with ω-grading (see Example 1.4.4). Then if $f \in B$ is ω-homogeneous with $\deg_\omega f = d$ and ab divides d, then there exists a standard homogeneous polynomial $g(S,T) \in k[S,T]$ such that $f = g(X^b, Y^a)$.*

Proof. If $a = b = 1$, there is nothing to prove. Assume that $ab > 1$ and let $f = \sum_{(i,j)\in\mathbb{N}\times\mathbb{N}} c_{i,j}X^iY^j$ with $ia + jb = d$. Since ab divides d we have $\frac{i}{b} + \frac{j}{a} \in \mathbb{Z}$, that is $\frac{ia+bj}{ab} \in \mathbb{Z}$, so $ia = k_1b$, $jb = k_2a$ $(k_1, k_2 \in \mathbb{N})$. Thus b divides i and a divides j (because a and b are relatively prime). Set $l = \frac{i}{b}$ and $m = \frac{j}{a}$, $l, m \in \mathbb{N}$, $f = \sum_{bl,ma} c_{bl,ma}X^{lb}Y^{ma} = g(X^b, Y^a)$, with $g(S,T) = \sum_{l,m} e_{l,m}S^lT^m$ and $l + m = \frac{d}{ab}$; therefore g is a standard homogeneous polynomial with degree $\frac{d}{ab}$. □

The next result is an important part of the proof of Theorem 4.1 in [6].

Lemma 3.3.7. *Let $B = k[X,Y]$ and let $D \in \mathrm{LND}(B) \setminus \{0\}$ be such that $D(X) \neq 0$ and $D(Y) \neq 0$. If f is a nonconstant polynomial such that $f \in \ker(D)$, then there exists an $\mathbb{N}$-grading of B relative to which the highest degree homogeneous component $\tilde{f}$ of f has the form $\tilde{f} = d(X+cY^r)^s$ or $\tilde{f} = d'(Y+c'X^t)^s$ $(c, c', d, d' \in k^\times$ and $r, s, t \in \mathbb{Z}_+)$.*

Proof. Assume without loss of generality that $f(0,0) = 0$, if it is not the case we replace f by $f(X,Y) - f(0,0)$. Thus we can write f as $f(X,Y) = P(X) + Q(Y) + XYF(X,Y)$, where $F \in B$, $P(X) \in Xk[X]$ and $Q(Y) \in Yk[Y]$.

If $P = 0$, then $f = YT(X,Y)$; since $f \neq 0$ and $\ker(D)$ is factorially closed, we must have $D(Y) = 0$, a contradiction; hence $P \neq 0$ and by the same argument we obtain that $Q \neq 0$.

Now let $m = \deg(P(X))$ and $n = \deg(Q(Y))$, and note that $m \geq 1$ and $n \geq 1$. Set $e = \gcd(m,n)$, $a = \frac{n}{e}$ and $b = \frac{m}{e}$. Let $\omega = (a,b)$ and let B be endowed with the ω-grading. Then we have $\deg_\omega(P(X)) = am = bn = \deg_\omega(Q(Y))$ and so $\deg_\omega(f) \geq am$.

Let $\tilde{f}$ and $\tilde{F}$ denote the highest degree homogeneous components of f and F respectively and $\tilde{D}$ the homogenization of D. By Proposition 2.4.14, $\tilde{D} \in \mathrm{LND}(B) \setminus \{0\}$ and by Proposition 2.4.15 $\tilde{D}(\tilde{f}) = 0$. Note that $\tilde{D} \neq 0$ by Proposition 2.4.11.

Assume that $\deg_\omega(f) > am$; then we must have $\tilde{f} = XY\tilde{F}$, $\tilde{F} \neq 0$. Since $\tilde{F} \neq 0$ and $\ker(\tilde{D})$ is factorially closed we must have $\tilde{D}(X) = 0 = \tilde{D}(Y)$ and so $\tilde{D} = 0$, a contradiction. Thus $\deg_\omega(f) \leq am$ and so $\deg_\omega(f) = am$. Therefore $\tilde{f}$ can be written

as $\tilde{f} = uX^m + vY^n + XY\tilde{F}$, for some $u, v \in k$. Furthermore, $u \neq 0$ and $v \neq 0$ since they are the highest degree coefficients of P and Q respectively. Assume that $\tilde{D}(X) = 0$, then $\tilde{D}(\tilde{f} - uX^m) = 0$ and so $(vY^n + XY\tilde{F}) = Y(vY^{n-1} + X\tilde{F}) \in \ker(\tilde{D})$, thus $\tilde{D}(Y) = 0$ (since $vY^{n-1} + X\tilde{F} \neq 0$). Therefore $\tilde{D} = 0$, a contradiction. Thus $\tilde{D}(X) \neq 0$ and by the same argument one can show that $\tilde{D}(Y) \neq 0$. Since ab divides $am = \deg_\omega(\tilde{f})$ and $\gcd(a,b) = 1$, by Lemma 3.3.6, $\tilde{f}(X,Y) = g(X^b, Y^a)$ where g is a nonconstant standard homogeneous polynomial with $\deg(g) = \dfrac{am}{ab} = e$.

Let K denote the algebraic closure of k, then by Lemma 3.1.4 $g(X,Y)$ factors in $K[X,Y]$ as a product of linear polynomials; hence we have $\tilde{f} = \prod_{i=1}^{e}(c_iX^b + d_iY^a)$ where all the $c_i, d_i \in K$, $(c_i, d_i) \neq (0,0)$. In fact $c_i, d_i \in K^\times$; if any c_i is zero we will have $\tilde{f} = YH(X,Y)$, $H \in B$, thus u must be zero, a contradiction; hence all the c_i are nonzero. By the same argument we can show that $d_i \neq 0$.

Set $\tilde{B} = K[X,Y]$ and let $\delta \in \mathrm{LND}(\tilde{B})$ be the unique extension of $\tilde{D}$ (see Lemma 2.2.28). Now $\delta(\tilde{f}) = \tilde{D}(\tilde{f}) = 0$ implies that $\tilde{f} \in \ker(\delta)$; $\tilde{f}$ can also be written as $\tilde{f} = C\prod_{i=1}^{e}(X^b + L_iY^a)$ where $C = c_1c_2\cdots c_e \in K^\times$, $L_i \in K^\times$. Hence $X^b + L_iY^a \in \ker\delta$ for all $i = 1, \cdots, e$ (since $\ker\delta$ is factorially closed and each term of the product is nonzero).

We claim that all the L_i are equal. Indeed, assume that $L_i \neq L_j$ for some $i \neq j$, then $(L_i - L_j)Y^a \in \ker\delta$ which implies that $0 = \delta(Y) = \tilde{D}(Y)$, a contradiction. So all the L_i are equal to, say L. We thus have $\tilde{f} = C(X^b + LY^a)^e$ with $C, L \in K^\times$. Since $\tilde{f}(X,Y) \in k[X,Y]$ by hypothesis, we have that $\tilde{f}(X,Y) = C\sum_{l=0}^{e}\binom{e}{l}(X^b)^{e-l}(LY^a)^l \in k[X,Y]$. Recall that k is of characteristic zero, so $\mathbb{Q} \subseteq k$. Thus for $l = 0$, we obtain that $C \in k^\times$ and for $l = 1$ we have that $CeL \in k^\times$ which implies that $L \in k^\times$. Thus $\tilde{f} = C(X^b + LY^a)^e$ with $C, L \in k^\times$; and $\tilde{f} \in \ker(\tilde{D})$ implies $X^b + LY^a \in \ker(\tilde{D})$.

Now assume that $a > 1$ and $b > 1$; then

$$\tilde{D}(X^b + LY^a) = 0 \Longrightarrow bX^{b-1}\tilde{D}(X) = -aLY^{a-1}\tilde{D}(Y).$$

Hence $\tilde{D}(X) \in YB$ and $\tilde{D}(Y) \in XB$, so Proposition 2.2.26 implies that $\tilde{D}(X) = 0$ or $\tilde{D}(Y) = 0$, a contradiction. Thus $a = 1$ or $b = 1$.

Therefore $\tilde{f} = C(X + LY^a)^e$ or $\tilde{f} = C'(Y + L'X^b)^e$ where C, C', L and $L' \in k^\times$ $a, b, e \in \mathbb{Z}_+$. $\square$

We now present Rentschler's Theorem, which is an important result in the theory of polynomial rings. Our proof follows the reasoning given in Theorem 4.1 of [6], but our use of the integer $\|D\|$ clarifies the argument.

Theorem 3.3.8 (Rentschler's Theorem). *Let k be a field of characteristic zero. If $D \in \mathrm{LND}(k[X,Y])$, then there exists $f \in k[X]$ and a tame automorphism $\alpha \in \mathrm{GA}_2(k)$ such that $\alpha D \alpha^{-1} = f(X)\partial_Y$.*

Proof. The result is trivial if $D = 0$, so assume throughout that $D \neq 0$. If $DX = 0$, the result follows from Proposition 3.3.3.

If $DY = 0$, considering the tame automorphism $\alpha = (Y, X)$, we get $\alpha \circ D \circ \alpha^{-1}(X) = 0$ and the result follows from Proposition 3.3.3.

Define an equivalence relation $\sim$ on the set $\mathrm{LND} \setminus \{0\}$ as follows: given $D, D' \in \mathrm{LND} \setminus \{0\}$, we declare that $D \sim D'$ if there exists a tame automorphism α of B satisfying $D' = \alpha \circ D \circ \alpha^{-1}$.

For each $D \in \mathrm{LND}(B) \setminus \{0\}$, note that $\ker(D) \setminus k \neq \emptyset$ by Lemma 2.3.11 and define the positive integer $\|D\| = \min\{\deg_X(f) + \deg_Y(f) \mid f \in \ker(D) \setminus k\}$.

Consider $D \in \mathrm{LND}(B) \setminus \{0\}$ such that $D(X) \neq 0$ and $D(Y) \neq 0$. We may choose $f \in \ker(D) \setminus k$ such that $\|D\| = \deg_X(f) + \deg_Y(f)$ and $f(0,0) = 0$.

By Lemma 3.3.7 there exists an $\mathbb{N}$-grading of B such that we have $\tilde{f}(X,Y) = d(Y + cX^b)^e$ or $\tilde{f}(X,Y) = d(X + cY^a)^e$ where $\tilde{f}$ is the highest degree homogeneous component of f.

Suppose $\tilde{f}(X,Y) = d(Y + cX^b)^e$, note that $\deg_X(f) = \deg_X(\tilde{f})$ and $\deg_Y(f) = \deg_Y(\tilde{f})$. Define the triangular (hence tame) automorphism $\alpha = (X, Y - cX^b)$. Clearly $\alpha(f)(0,0) = 0$. We claim:

$$\deg_X(\alpha(f)) < \deg_X(f) \text{ and } \deg_Y(\alpha(f)) = \deg_Y(f). \tag{3}$$

To prove this, we write $f = \hat{f} + \tilde{f}$, where $\hat{f} = \sum_{i+bj<be} a_{ij} X^i Y^j$ $(a_{ij} \in k)$ and $\tilde{f}$ is as before. Since $\alpha(\tilde{f}) = d(\alpha(Y) + c(X^b))^e = dY^e$, we have

$$\deg_X(\alpha(\tilde{f})) = 0 < be \text{ and } \deg_Y(\alpha(\tilde{f})) = e. \tag{4}$$

For each term $a_{ij}X^iY^j$ of $\hat{f}$ we have $\alpha(a_{ij}X^iY^j) = a_{ij}X^i(Y-cX^b)^j$, so $\deg_X(\alpha(a_{ij}X^iY^j)) = i+bj < be$ and $\deg_Y(\alpha(a_{ij}X^iY^j)) = j < e$; so

$$\deg_X(\alpha(\hat{f})) < be \text{ and } \deg_Y(\alpha(\hat{f})) < e. \tag{5}$$

Combining (4) and (5), we obtain $\deg_X \alpha(f) < be$ and $\deg_Y(\alpha(f)) = e$, so (3) is proved.

Set $D' = \alpha \circ D \circ \alpha^{-1}$; we have $D' \in \mathrm{LND}(B) \setminus \{0\}$ by Proposition 3.3.1, so $D \sim D'$. Again by Proposition 3.3.1 we have $\alpha(f) \in \ker(D')$, so (3) implies that $\|D'\| < \|D\|$.

Similarly if $\tilde{f} = d(X+cY^a)^e$, consider the tame automorphism $\beta = (X - cY^a, Y)$. Note that α is tame, because $\beta = (Y,X) \circ (X, Y - cX^a) \circ (Y,X)$; and clearly $\beta(f)(0,0) = 0$. Arguing as in the first case, we obtain

$$\deg_Y(\beta(f)) < \deg_Y(f) \text{ and } \deg_X(\beta(f)) = \deg_X(f).$$

Set $D' = \beta \circ D \circ \beta^{-1}$; then (as in the first case) $D' \sim D$ and $\|D'\| < \|D\|$.

We have shown the following:

> If $D \in \mathrm{LND}(B) \setminus \{0\}$ satisfies $D(X) \neq 0$ and $D(Y) \neq 0$, then there exists $D' \in \mathrm{LND}(B) \setminus \{0\}$ such that $D' \sim D$ and $\|D'\| < \|D\|$.

Since this process of lowering $\|D\|$ cannot continue indefinitely, there must exist $D'' \in \mathrm{LND}(B) \setminus \{0\}$ such that $D'' \sim D$ and either $D''(X) = 0$ or $D''(Y) = 0$. If $D''(Y) = 0$, then $(Y,X) \circ D'' \circ (Y,X)^{-1}$ is equivalent to D'' and maps X to 0, so in fact there exists $D'' \in \mathrm{LND}(B) \setminus \{0\}$ such that $D'' \sim D$ and $D''(X) = 0$. Proposition 3.3.3 gives $D'' = h(X)\partial_Y$ for some $h(X) \in k[X]$, so we are done. □

Corollary 3.3.9. *Given $B = k^{[2]}$ and $D \in \mathrm{LND}(B)$, there exist $X, Y \in B$ such that $B = k[X,Y]$ and $D = f(X)\dfrac{\partial}{\partial Y}$ for some $f(X) \in k[X]$.*

Proof. The case $D = 0$ is trivial.

We may assume that $B = k[Z,T]$; by Rentschler's theorem there is $\alpha \in \mathrm{GA}_2(k)$ such that $\alpha \circ D \circ \alpha^{-1} = f(Z)\dfrac{\partial}{\partial T}$, $f(Z) \in k[Z] \setminus \{0\}$. Define $X = \alpha^{-1}(Z)$ and $Y = \alpha^{-1}(T)$, and note that $B = k[X,Y]$ by Lemma 3.2.3. Now $\alpha \circ D \circ \alpha^{-1}(Z) = 0$ implies that

$\alpha(D(X)) = 0$, so $D(X) = 0$ (since α is an automorphism). Therefore by Proposition 3.3.3 we have $D = h(X)\dfrac{\partial}{\partial Y}$ for some $h(X) \in k[X] \setminus \{0\}$. □

Remark 3.3.10. Let $B = k^{[2]}$, where k is a field of characteristic zero.

(*i*) If $D \in \mathrm{LND}(B) \setminus \{0\}$ and $A = \ker D$, then Rentschler's Theorem gives us that $A = k^{[1]}$ and $B = A^{[1]}$.

(*ii*) Rentschler's Theorem implies also that if D is a locally nilpotent derivation of B then $D(v) = 0$ for some variable v of B.

Corollary 3.3.11. *Let $B = k[X,Y]$ where k is a field of characteristic zero. If f is a variable of B, then f satisfies one of the following conditions:*

(*a*) *$f = aX + b$, where $a \in k^\times$ and $b \in k$.*

(*b*) *$f = cY + d$, where $c \in k^\times$ and $d \in k$.*

(*c*) *There exists an $\mathbb{N}$-grading of B relative to which the highest degree homogeneous component $\tilde{f}$ of f has the form $\tilde{f} = d(X+cY^r)^s$ or $\tilde{f} = d'(Y+c'X^t)^s$ ($c, c', d, d' \in k^\times$ and $r, s, t \in \mathbb{Z}_+$).*

Proof. Since f is variable of B, there exists $g \in B$ such that $B = k[f,g]$. Clearly there exists $D \in \mathrm{LND}(B) \setminus \{0\}$ such that $D(f) = 0$.

If $D(X) = 0$ then $\ker(D) = k[X]$ (by Proposition 3.3.3), so $f \in k[X]$. Since (f,g) is a system of variables of B, Lemma 2.1.20 implies that $f'(X)\dfrac{\partial g}{\partial_Y} \in k^\times$, hence $f'(X) \in k^\times$ (since k is factorially closed in B). Therefore $f = aX + b$ where $a \in k^\times$ and $b \in k$.

If $D(Y) = 0$ then using Remark 3.3.5 and arguing as above, we obtain that $f = cY + d$ where $c \in k^\times$ and $d \in k$.

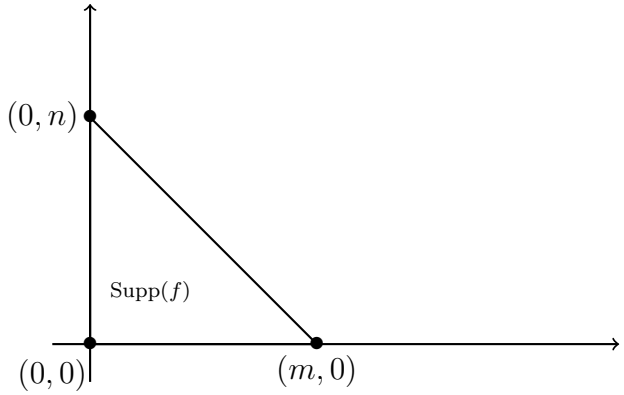
Assume that $D(X) \neq 0$ and $D(Y) \neq 0$. Since f is a nonconstant element of B (because f is a variable) and $f \in \ker(D)$ the result follows by Lemma 3.3.7. □

Definition 3.3.12. Let $B = k[X,Y] = k^{[2]}$ where k is a field of characteristic zero and $f = \sum_{i,j} a_{ij}X^iY^j \in B$, ($a_{ij} \in k$). The *support* of f is the set: $\mathrm{Supp}(f) = \{(i,j) \in \mathbb{N} \times \mathbb{N} \mid a_{ij} \neq 0\}$.

Remark 3.3.13. Let k be a field of characteristic zero, $B = k[X,Y]$ and f a variable of B. Set $m = \deg_X(f)$ and $n = \deg_Y(f)$. Then Corollary 3.3.11 implies that the following hold:

1. $n|m$ or $m|n$.

2. If f is not of the form $aX+b$ or $aY+b$ with $a \in k^\times$ and $b \in k$, then the convex hull in $\mathbb{R}^2$ of the set $\mathrm{Supp}(f) \cup \{(0,0)\}$ is the triangle with vertices $(0,0)$, $(m,0)$ and $(0,n)$.



3.4 Automorphism theorem

Observe first that the group $\mathrm{GA}_1(k)$ is well understood. Indeed, every k-automorphism ϕ of $k[X] = k^{[1]}$ is of the form $\phi(X) = aX + b$, $a \in k^\times$, $b \in k$. This follows from Proposition 3.1.2 and Remark 3.2.2.

The first step in understanding the group $\mathrm{GA}_2(k)$ was accomplished by Jung in 1942 (see [9]), when he proved that if k is a field of characteristic zero then $\mathrm{GA}_2(k)$ is generated by its subgroups $\mathcal{GL}_2(k)$ and $\mathrm{BA}_2(k)$. In 1953, van der Kulk proved that this is in fact true for k an arbitrary field. The proof that we present here is due to Rentschler, and is valid only in characteristic zero. In fact we obtain Jung's Theorem as a corollary to Rentschler's Theorem. Our proof is adapted from that of Theorem 4.8 of [6].

Theorem 3.4.1 (Jung's Theorem). *Let k be a field of characteristic zero. The group $\mathrm{GA}_2(k)$ of k-automorphisms of $B = k[X,Y]$ is generated by its linear and*

triangular subgroups, $\mathcal{GL}_2(k)$ and $\mathrm{BA}_2(k)$. In other words, every automorphism of B is tame.

Proof. Let $\phi \in \mathrm{GA}_2(k)$. Let $u = \phi(X)$ and $v = \phi(Y)$. Since $B = k[u,v] = k^{[2]}$, the partial derivatives $\partial_u = \frac{\partial}{\partial_u}$ and $\partial_v = \frac{\partial}{\partial v}$ are defined and we have $\partial_v \in \mathrm{LND}(B)$ and $\ker(\partial_v) = k[u]$. Applying Rentschler's Theorem to ∂_v, we obtain that there exists a **tame** automorphism α of B such that $\alpha \circ \partial_v \circ \alpha^{-1} = f(X)\partial_Y$ for some $f(X) \in k[X]$ (where $f(X) \neq 0$ since $\partial_v \neq 0$). Moreover,

$$k[X] = \ker(\partial_Y) = \ker(f(X)\partial_Y) = \ker(\alpha \circ \partial_v \circ \alpha^{-1}) = \alpha(\ker(\partial_v)) = \alpha(k[u]),$$

so $k[X] = k[\alpha(u)]$ and consequently $\alpha(u) = aX + b$ for some $a \in k^\times$, and $b \in k$, by Proposition 3.1.2. Now

$$k[X,Y] = k[\alpha(u), \alpha(v)] = k[aX + b, \alpha(v)] = k[X, \alpha(v)]$$

and the fact that $k[X, \alpha(v)] = k[X,Y]$ implies that $\alpha(v) = cY + g(X)$ for some $c \in k^\times$ and $g(X) \in k[X]$, by Proposition 3.1.2. Now the automorphism $\theta = (aX + b, cY + g(X))$ is triangular, hence tame, so $\alpha^{-1} \circ \theta$ is tame. Now

$$(\alpha^{-1} \circ \theta)(X) = \alpha^{-1}(aX + b) = \alpha^{-1}(\alpha(u)) = u = \phi(X),$$

$$(\alpha^{-1} \circ \theta)(Y) = \alpha^{-1}(cY + g(X)) = \alpha^{-1}(\alpha(v)) = v = \phi(Y),$$

so $\alpha^{-1} \circ \theta = \phi$, so ϕ is tame.

□

As we already mentioned, van der Kulk proved in 1953 that Jung's Theorem is in fact true over an arbitrary field (see [10]). Let us state this as follows (where the last equality is Remark 3.2.7):

Theorem 3.4.2 (van der Kulk). *If k is a field then*

$$\mathrm{GA}_2(k) = \langle \mathcal{GL}_2(k) \cup \mathrm{BA}_2(k) \rangle = \langle \mathrm{Af}_2(k) \cup \mathrm{BA}_2(k) \rangle.$$

In the same article, van der Kulk also proves a unique factorization theorem for elements of $\mathrm{GA}_2(k)$. Theorem 3.4.4, below, is equivalent to van der Kulk's result.

Definition 3.4.3. Let H be a subgroup of a group G such that $H \neq G$. By a *system of nontrivial left coset representatives of H in G*, we mean a subset $\mathcal{G} \subseteq G$ satisfying:

1. $\mathcal{G} \cap H = \emptyset$;
2. for each left coset gH (where $g \in G$) such that $gH \neq H$, we have $|\mathcal{G} \cap gH| = 1$.

Theorem 3.4.4 (Structure theorem). *Let k be a field and consider the subgroups $A = \mathrm{Af}_2(k)$, $B = \mathrm{BA}_2(k)$ and $C = A \cap B$ of $\mathrm{GA}_2(k)$, that is*

$$\begin{aligned} A &= \{(a_1X + b_1Y + c_1, a_2X + b_2Y + c_2) \mid a_i, b_i, c_i \in k;\ a_1b_2 - a_2b_1 \neq 0\} \\ B &= \left\{(aX + b, cY + f(X)) \mid a, c \in k^\times,\ b \in k,\ f \in k[X]\right\} \\ C &= A \cap B = \left\{(aX + b, cX + dY + e) \mid a, d \in k^\times,\ b, c, e \in k\right\}. \end{aligned}$$

Define the sets $\mathcal{A} \subseteq A$ and $\mathcal{B} \subseteq B$ by

$$\mathcal{A} = \{(tX + Y, X) \mid t \in k\} \quad \text{and} \quad \mathcal{B} = \left\{(X, Y + X^2 f(X)) \;\middle|\; f(X) \in k[X], f \neq 0\right\}.$$

Then $\mathcal{A}$ (resp. $\mathcal{B}$) is a system of non trivial left coset representatives of C in A (resp. of C in B). Moreover, $\mathcal{A} \cap \mathcal{B} = \emptyset$ and each $\phi \in \mathrm{GA}_2(k)$ has a unique factorization of the form

$$\phi = x_1 \cdots x_n c \tag{6}$$

with $n \geq 0$, $c \in C$ and $x_i \in \mathcal{A} \cup \mathcal{B}$ for all i, where the x_i alternate between $\mathcal{A}$ and $\mathcal{B}$.

We now proceed to prove the Structure Theorem. Our proof makes use of Theorem 3.4.2, even though we only proved it for fields of characteristic zero. In fact the proof shows that if k is any field for which $\mathrm{GA}_2(k) = \langle \mathrm{Af}_2(k) \cup \mathrm{BA}_2(k) \rangle$, then the Structure Theorem is true over k.

Our initial plan was to reproduce the proof given in Freudenburg's book [6], but there is a step in that proof that we could not understand (see the introduction). Resolving this issue resulted in the proof that we give below, and that is quite different from that of [6].

There are several steps in the proof. We begin with:

Lemma 3.4.5. *Let A and B be subgroups of a group G satisfying $G = \langle A \cup B \rangle$, $A \not\subseteq B$ and $B \not\subseteq A$. Let $C = A \cap B$, and let $\mathcal{A} \subset A$ (resp. $\mathcal{B} \subset B$) be a system of nontrivial left coset representatives of C in A (resp. of C in B). Then $\mathcal{A} \cap \mathcal{B} = \emptyset$ and each $g \in G$ has a (not necessarily unique) factorization of the form*

$$g = x_1 \cdots x_n c \tag{7}$$

with $n \geq 0$, $c \in C$ and $x_i \in \mathcal{A} \cup \mathcal{B}$ for all i, where the x_i alternate between $\mathcal{A}$ and $\mathcal{B}$.

Proof. Note that $C \neq A$ and $C \neq B$, since $A \not\subseteq B$ and $B \not\subseteq A$. By Definition 3.4.3 we have $\mathcal{A} \subseteq A$ and $\mathcal{B} \subseteq B$, thus $\mathcal{A} \cap \mathcal{B} \subseteq A \cap B = C$. Assume that $\mathcal{A} \cap \mathcal{B} \neq \emptyset$. Let $g \in \mathcal{A} \cap \mathcal{B} \subseteq C$, then we have $g \in C$. Definition 3.4.3-1) implies that $g \notin C$, a contradiction. Thus we must have $\mathcal{A} \cap \mathcal{B} = \emptyset$.

Let $g \in G$. If $g \in C$ then it is trivial that g factors as in (7) (take $n = 0$). Assume now that $g \in G \setminus C$. We shall now prove that g can be factored as $g = g_1 g_2 \cdots g_n$ with $n \geq 1$, $g_i \in A \cup B$ and $g_i \notin C$ for all i, and where the g_i alternate between A and B.

Since $g \in G \setminus C$ and $G = \langle A \cup B \rangle$, g can be factored as

$$g = g_1 \cdots g_n, \text{ with } g_i \in A \cup B \text{ for all } i. \tag{8}$$

Among all these factorizations (8) of g, choose one that minimizes n. Then we cannot have consecutive factors g_{i-1} and g_i both in A or both in B, because then we could replace g_{i-1} and g_i by their product and obtain a shorter factorization (8) of g, which would violate minimality of n. Similarly, if $g_i \in C$ and $i > 1$ (resp. $i = 1$) then replacing g_{i-1} and g_i (resp. g_i and g_{i+1}) by their product would produce a shorter factorization (8) of g, which is impossible. So we obtain that the g_i alternate between A and B and that $g_i \notin C$ for all i.

Furthermore, for every element $a \in A \setminus C$ we have $a = xc$ for some $x \in \mathcal{A}$ and $c \in C$. Also for every element $b \in B \setminus C$ we have $b = xc$ for some $x \in \mathcal{B}$ and $c \in C$.

Observe that g_1 belongs to $A \setminus C$ or to $B \setminus C$. Assume now without loss of generality that $g_1 \in A \setminus C$. Then $g_1 = x_1 c_1$ with $x_1 \in \mathcal{A}$ and $c_1 \in C$. So

$$g = g_1 g_2 \cdots g_n = (x_1 c_1) g_2 \cdots g_n = x_1 (c_1 g_2) g_3 \cdots g_n = x_1 g_2' g_3 \cdots g_n$$

where $g_2' = c_1 g_2 \in B \setminus C$. Then $g_2' = x_2 c_2$, where $x_2 \in \mathcal{B}$ and $c_2 \in C$. Therefore $g = x_1 x_2 g_3' \cdots g_n$ with $g_3' \in A \setminus C$. We can repeat inductively this process to get at the end that $g = x_1 x_2 \cdots x_n c$, where the $x_i \in \mathcal{A} \cup \mathcal{B}$ alternate between $\mathcal{A}$ and $\mathcal{B}$ and $c \in C$. □

In what follows, k is any field and $\mathcal{A}$, $\mathcal{B}$ are defined as in the Structure Theorem, i.e.,

$$\mathcal{A} = \{(tX + Y, X) \mid t \in k\} \quad \text{and} \quad \mathcal{B} = \left\{(X, Y + X^2 f(X)) \,\middle|\, f(X) \in k[X],\ f \neq 0\right\}.$$

We also define

$$\mathcal{U} = \left\{(X + tY, Y) \mid t \in k^\times\right\}, \quad \mathcal{V} = \{(Y, X - tY) \mid t \in k\} \quad \text{and} \quad \bar{\mathcal{A}} = \mathcal{A} \cup \mathcal{U} \cup \mathcal{V}.$$

Definition 3.4.6. Let $\phi = (F, G) \in \mathrm{GA}_2(k)$.

- We define $\deg \phi = \max\{\deg(F), \deg(G)\}$.
- If $\deg(F) \geq \deg(G)$, we say that ϕ *is of type* 1.
- If $\deg(F) < \deg(G)$, we say that ϕ *is of type* 2.

Note that each element of $\mathrm{GA}_2(k)$ is either of type 1 or of type 2. All elements of $\bar{\mathcal{A}}$ are of type 1 and all elements of $\mathcal{B}$ are of type 2.

Lemma 3.4.7. *Let $\phi \in \mathrm{GA}_2(k)$ and $h \in \bar{\mathcal{A}} \cup \mathcal{B}$. If ϕ and h are of distinct types, then*

1. *the type of $\phi \circ h$ is the same as that of h;*
2. $\deg(\phi \circ h) = \deg \phi \deg h$.

Proof. Observe first that $\bar{\mathcal{A}} \cap \mathcal{B} = \emptyset$ and the sets $\mathcal{A}$, $\mathcal{U}$ and $\mathcal{V}$ are pairwise disjoint. Since ϕ and h are of distinct types, it suffices to show the Lemma in the following cases:

Case 1: $\phi = (F, G)$ is of type 1 and $h = (X, Y + g(X)) \in \mathcal{B}$. It is easy to show that

$$\phi \circ h = (F, G + g(F)) = (P, Q).$$

Since $\deg(F) \geq \deg(G)$ and $\deg(g) > 1$, we have $\deg(Q) = \deg(g(F)) = \deg(g)\deg(F) > \deg(F) = \deg(P)$, i.e., $\phi \circ h$ is of type 2 (the type of h) and $\deg(\phi \circ h) = \deg(Q) = \deg(F)\deg(g) = \deg \phi \deg h$.

Case 2: $\phi = (F, G)$ is of type 2 ($\deg(\phi) = \deg(G)$) and $h = (tX + Y, X) \in \mathcal{A}$. We have

$$\phi \circ h = (tF + G, F) = (P, Q),$$

so $\deg(\phi \circ h) = \deg(G) = \deg(P)$ (since $\deg(G) > \deg(F)$). Thus $\phi \circ h$ is of the same type as h and $\deg(\phi \circ h) = \deg(\phi) \deg h$.

Case 3: $\phi = (F, G)$ is of type 2 and $h = (X + tY, Y) \in \mathcal{U}$. Likewise

$$\phi \circ h = (F + tG, G) = (P, Q),$$

since $t \neq 0$ and $\deg(G) > \deg(F)$, we have $\deg(P) = \deg(Q)$. Hence $\phi \circ h$ is of the same type as h and $\deg(\phi \circ h) = \deg(G) = \deg(\phi) = \deg(\phi) \deg(h)$.

Case 4: $\phi = (F, G)$ is of type 2 and $h = (Y, X - tY) \in \mathcal{V}$. Thus

$$\phi \circ h = (G, F - tG) = (P, Q)$$

and so $\deg P \geq \deg Q$ (since $\deg G > \deg F$). Thus $\phi \circ h$ is of the same type as h and $\deg(\phi \circ h) = \deg(P) = \deg(G) = \deg(\phi) = \deg(\phi) \deg(h)$.

□

Lemma 3.4.8. *Suppose that $\phi \in \mathrm{GA}_2(k)$ satisfies*

$$\phi = h_1 \circ \cdots \circ h_n$$

where $n \geq 0$ and $h_i \in \bar{\mathcal{A}} \cup \mathcal{B}$ for all i, where the h_i alternate between $\bar{\mathcal{A}}$ and $\mathcal{B}$. Then $\deg \phi = \prod_{i=1}^{n} \deg h_i$, and if $n > 0$ then ϕ has the same type as h_n.

Proof. If $n = 0$ then "$\phi = h_1 \circ \cdots \circ h_n$" should be interpreted as $\phi = \mathrm{id}$, and the empty product $\prod_{i=1}^{n} \deg h_i$ is by convention equal to 1. Since $\deg(\mathrm{id}) = 1$, the Lemma is true when $n = 0$. From now on we assume that $n \geq 1$. Let us prove by induction on j that the following statement $P(j)$ is true for all $j = 1, \ldots, n$:

$P(j)$: $\phi_j \stackrel{\text{def}}{=} h_1 \circ \cdots \circ h_j$ *has the same type as* h_j, *and* $\deg \phi_j = \prod_{i=1}^{j} \deg h_i$.

It is obvious that $P(1)$ is true. Suppose that $1 < j \leq n$ and that $P(j-1)$ is true; let us prove that $P(j)$ is true. By $P(j-1)$, ϕ_{j-1} has the same type as h_{j-1} and $\deg \phi_{j-1} = \prod_{i=1}^{j-1} \deg h_i$. Since h_{j-1} and h_j have distinct types, it follows that ϕ_{j-1} and h_j have distinct types; this together with $h_j \in \bar{\mathcal{A}} \cup \mathcal{B}$ implies (by Lemma 3.4.7) that $\phi_j = \phi_{j-1} \circ h_j$ has the same type as h_j and that

$$\deg \phi_j = \deg \phi_{j-1} \deg h_j = \prod_{i=1}^{j} \deg h_i.$$

So $P(j)$ is true. By induction, this shows that $P(1), \ldots, P(n)$ are true.

Since $P(n)$ is true, the Lemma is proved. □

Remark 3.4.9.

1. If $h \in \mathcal{A}$ then $h^{-1} \in \mathcal{V} \subseteq \bar{\mathcal{A}}$.
2. If h, h' are distinct elements of $\mathcal{A}$ then $(h')^{-1} \circ h \in \mathcal{U} \subseteq \bar{\mathcal{A}}$.
3. If $h \in \mathcal{B}$ then $h^{-1} \in \mathcal{B}$.
4. If h, h' are distinct elements of $\mathcal{B}$ then $(h')^{-1} \circ h \in \mathcal{B}$.

Lemma 3.4.10. *If $h_1 h_2 \cdots h_n c = h'_1 h'_2 \cdots h'_m c'$, where $n, m \in \mathbb{N}$, the h_i and h'_i alternate between $\mathcal{A}$ and $\mathcal{B}$ and c, c' are elements of C, then we have $n = m$, $h_i = h'_i$ and $c = c'$.*

Proof. We show this by induction on $l = \min(n, m) \geq 0$. Let $P(l)$ be the following statement:

$P(l)$: If $\min(m, n) = l$ then the condition $h_1 \cdots h_n c = h'_1 \cdots h'_m c'$ implies that $n = m$, $h_i = h'_i$ for all i, and $c = c'$.

We begin by showing that $P(0)$ and $P(1)$ are true.

Case 1: $l = 0$.

- If $n = 0$ and $m > 0$, then we have $c = h'_1 \cdots h'_m c'$, so

$$cc'^{-1} = h'_1 \cdots h'_m.$$

If $m = 1$, then we must have $h'_1 \in C$, a contradiction (since $\mathcal{A} \cap C = \emptyset$ and $\mathcal{B} \cap C = \emptyset$).

If $m > 1$, then by Lemma 3.4.8 we have $1 = \Pi_{i=1}^{m} \deg(h'_i)$. Hence $h'_i \in \mathcal{A}$ for all i, a contradiction (since h'_i alternate between $\mathcal{A}$ and $\mathcal{B}$).

- If $n > 0$ and $m = 0$ by applying the same argument above we obtain a contradiction.

  Hence we must have $n = m = 0$ and therefore $c = c'$, so $P(0)$ is true.

Case 2: $l = 1$.

If $h_1 = h'_1$ then $h_2 \cdots h_n c = h'_2 \cdots h'_m c'$, so the fact that $P(0)$ is true implies that $n = m = 1$ and $c = c'$. This shows that $P(1)$ is true whenever $h_1 = h'_1$. We now assume that $h_1 \neq h'_1$, and we show that this leads to contradictions in all possible cases. This will complete the proof that $P(1)$ is true.

- If $n = 1$ and $m > 1$, then we have $h_1 c = h'_1 \cdots h'_m c'$, so

$$cc'^{-1} = h_1^{-1} h'_1 \cdots h'_m.$$

  If $h_1 \in \mathcal{A}$ and $h'_1 \in \mathcal{B}$, then $h_1^{-1}, h'_1, h'_2, \cdots, h'_m$ alternate between $\bar{\mathcal{A}}$ and $\mathcal{B}$. Thus we can apply the Lemma 3.4.8 and get that $1 = \deg(h_1^{-1}) \Pi_{i=1}^{m} \deg(h'_i)$. Hence we have $\deg(h'_i) = 1$ for all i and so $h'_i \in \mathcal{A}$ for all $i = 1, 2, \cdots, m$, a contradiction.

  If $h_1 \in \mathcal{B}$ and $h'_1 \in \mathcal{A}$, then $h_1^{-1}, h'_1, h'_2, \cdots, h'_m$ alternate between $\mathcal{A}$ and $\mathcal{B}$. Thus we can apply the Lemma 3.4.8, and obtain the same contradiction.

  Hence h_1 and h'_1 must both belong to the same set $\mathcal{A}$ or $\mathcal{B}$.

  If $\{h_1, h'_1\} \subseteq \mathcal{A}$, then since $h_1 \neq h'_1$ by assumption, we have $h_1^{-1} h'_1 \in \bar{\mathcal{A}}$ by Remark 3.4.9; so $(h_1^{-1} h'_1), h'_2, \cdots, h'_m$ alternate between $\bar{\mathcal{A}}$ and $\mathcal{B}$. Thus Lemma 3.4.8 implies $1 = \deg(h_1^{-1} h'_1) \Pi_{i=2}^{m} \deg(h_i)$, and so $\deg(h'_2) = 1$, a contradiction.

  Assume that $\{h_1, h'_1\} \subseteq \mathcal{B}$. Since $h_1 \neq h'_1$ by assumption, we have $h_1^{-1} h'_1 \in \mathcal{B}$ by Remark 3.4.9. Then $(h_1^{-1} h'_1), h'_2, \cdots, h'_m$ alternate between $\mathcal{A}$ and $\mathcal{B}$.

Lemma 3.4.8 implies $1 = \deg(h_1^{-1}h_1')\Pi_{i=2}^m \deg(h_i')$, and so $1 = \deg(h_1^{-1}h_1')$, a contradiction.

- If $n > 1$ and $m = 1$ by applying the same argument above we obtain a contradiction.

  Hence we must have $n = m = 1$. We thus have $h_1c_1 = h_1'c_1'$, so

  $$cc'^{-1} = h_1^{-1}h_1'.$$

  If h_1 and h_1' alternate between $\mathcal{A}$ and $\mathcal{B}$, then h_1^{-1} and h_1' alternate between $\bar{\mathcal{A}}$ and $\mathcal{B}$. So by Lemma 3.4.8 we have $1 = \deg(h_1^{-1})\deg(h_1')$ and thus h_1 and h_1' are elements of $\mathcal{A}$, a contradiction. Therefore h_1 and h_1' must belong to the same set $\mathcal{A}$ or $\mathcal{B}$.

  Since h_1 and h_1' are distinct, we have $h_1^{-1}h_1' \in \mathcal{U} \cup \mathcal{B}$ by Remark 3.4.9 hence $cc'^{-1} \in \mathcal{U} \cup \mathcal{B}$ which is impossible since $(\mathcal{U} \cup \mathcal{B}) \cap C = \emptyset$.

  These contradictions show that $P(1)$ is true.

Let $d > 1$. Assume that $P(l)$ is true for $0 \leq l < d$. We show that $P(d)$ is true. So assume that $h_1 \cdots h_n c = h_1' \cdots h_m' c'$ with $\min(n, m) = d$.

If $h_1 = h_1'$ then $h_2 \cdots h_n c = h_2' \cdots h_m' c'$, so the fact that $P(d-1)$ is true implies that $n = m$, $c = c'$ and $h_i = h_i'$ for all i. This shows that $P(d)$ is true whenever $h_1 = h_1'$. We now assume that $h_1 \neq h_1'$, and we show that this leads to contradictions in all possible cases. This will complete the proof of the Lemma.

We have

$$cc'^{-1} = h_n^{-1} \cdots h_2^{-1}h_1^{-1}h_1' \cdots h_m'. \tag{9}$$

Consider the case where ($h_1 \in \mathcal{B}$ and $h_1' \in \mathcal{A}$) or ($h_1 \in \mathcal{A}$ and $h_1' \in \mathcal{B}$).
Then the h_i^{-1} and h_i' (in the right hand side of (9)) alternate between $\bar{\mathcal{A}}$ and $\mathcal{B}$ so we can apply Lemma 3.4.8. Equation (9) implies that

$$1 = \left(\prod_{i=1}^{n} \deg(h_i^{-1})\right)\left(\prod_{i=1}^{m} \deg(h_i')\right),$$

so $h_1, h_1' \in \mathcal{A}$, a contradiction. Hence h_1 and h_1' must both belong to one of the sets $\mathcal{A}$ or $\mathcal{B}$.

Assume that $\{h_1, h_1'\} \subseteq \mathcal{A}$. Since h_1 and h_1' are distinct then $h_1^{-1}h_1' \in \mathcal{U} \subseteq \bar{\mathcal{A}}$ (by Remark 3.4.9). So

$$h_n^{-1}, \ldots, h_2^{-1}, (h_1^{-1}h_1'), h_2', \ldots, h_m' \text{ alternate between } \bar{\mathcal{A}} \text{ and } \mathcal{B}. \tag{10}$$

Hence we can apply Lemma 3.4.8 and obtain

$$1 = \left(\prod_{i=2}^{n} \deg(h_i^{-1})\right) \deg(h_1^{-1}h_1') \left(\prod_{i=2}^{m} \deg(h_i')\right). \tag{11}$$

Hence $h_2, h_2' \in \mathcal{A}$, a contradiction. (Note that h_2 and h_2' exist since $d \geq 2$.)

Assume that $\{h_1, h_1'\} \subseteq \mathcal{B}$. Since h_1 and h_1' are distinct $h_1^{-1}h_1' \in \mathcal{B}$ (by Remark 3.4.9). Hence condition (10) is satisfied and we can apply Lemma 3.4.8 and obtain that (11) is true in this case too. Hence $\deg(h_1^{-1}h_1') = 1$, a contradiction.

These contradictions show that $P(d)$ is true and complete the proof of the Lemma. □

Proof of the Structure Theorem. We begin by verifying that the hypothesis of Lemma 3.4.5 is satisfied. It is clear that $A \not\subseteq B$ and $B \not\subseteq A$, and we have $\mathrm{GA}_2(k) = \langle A \cup B \rangle$ by Theorem 3.4.2.

Let us show that $\mathcal{A}$ (resp. $\mathcal{B}$) is a system of nontrivial left coset representatives of C in A (resp. of C in B). Clearly $\mathcal{A} \subseteq A$, $\mathcal{B} \subseteq B$, $\mathcal{A} \cap C = \emptyset$ and $\mathcal{B} \cap C = \emptyset$. Given $\alpha = (a_1X + b_1Y + c_1, a_2X + b_2Y + c_2) \in A \setminus C$ and $\beta = (aX + b, cY + f(X)) \in B \setminus C$, we have $b_1 \neq 0$, $c \neq 0$ and $f(X) = r + sX + X^2g(X)$, for some $r, s \in k$ and $g(X) \in k[X] \setminus \{0\}$. It is not difficult to check that

$$\alpha = (a_1b_1^{-1}X + Y, X)(b_1X + c_1, b_2X + (a_2b_1 - b_2a_1)b_1^{-1}Y + c_2) \tag{12}$$

and

$$\beta = (X, Y + c^{-1}X^2g(X))(aX + b, cY + r + sX). \tag{13}$$

We can now show that $|\mathcal{A} \cap \alpha C| = 1$. Set $\alpha' = (a_1b_1^{-1}X + Y, X)$, and note that $\alpha' \in \mathcal{A}$. We have $\mathcal{A} \cap \alpha C = \mathcal{A} \cap \alpha' C$ (by Equation (12)). Clearly $\alpha' \in \mathcal{A} \cap \alpha' C$. Assume that there is some $c \in C$, $c \neq 1$ such that $\alpha' c \in \mathcal{A}$, hence we must have $c \in \mathcal{U}$ (defined just before Definition 3.4.6), a contradiction. Therefore we have $\mathcal{A} \cap \alpha C = \mathcal{A} \cap \alpha' C = \{\alpha'\}$ and so $|\mathcal{A} \cap \alpha C| = 1$.

Likewise, using the same argument as above we can show that $|\mathcal{B} \cap \beta C| = 1$.

So $\mathcal{A}$ (resp. $\mathcal{B}$) is a system of nontrivial left coset representatives of C in A (resp. of C in B).

Therefore by Lemma 3.4.5, every $g \in \mathrm{GA}_2(k)$ has a factorization of the form

$$g = x_1 \cdots x_n c,$$

with $n \geq 0$, $c \in C$ and $x_i \in \mathcal{A} \cup \mathcal{B}$ for all i, where the x_i alternate between $\mathcal{A}$ and $\mathcal{B}$.

By Lemma 3.4.10, this factorization is unique. So we are done.

□

Remark 3.4.11. In group theory there is a notion of *free product with amalgamation*, which we will not define here. It turns out that the above Structure Theorem is equivalent to the statement that $\mathrm{GA}_2(k)$ is the free product of $\mathrm{Af}_2(k)$ and $\mathrm{BA}_2(k)$ with amalgamation along $C = \mathrm{Af}_2(k) \cap \mathrm{BA}_2(k)$, which is written as follows:

$$\mathrm{GA}_2(k) = \mathrm{Af}_2(k) *_C \mathrm{BA}_2(k).$$

According to [6], page 84, Nagata (in 1972) seems to be the first to have stated and proved the Structure Theorem in terms of amalgamated free product, but the statement had appeared without proof in a 1966 paper by Shafarevich.

Chapter 4

Some remarks on polynomial rings in three variables

The preceding chapter gives a complete description of the locally nilpotent derivations and automorphisms of $k[X, Y]$. In this very short chapter we make a few comments on the same problems for $k[X, Y, Z]$.

4.1 Locally nilpotent derivations

In this section, k is a field of characteristic zero.

Given any $n \geq 1$, one can state:

Problem. *Describe all locally nilpotent derivations of* $k^{[n]}$.

The case $n = 1$ of this problem is trivial, and Rentschler's Theorem completely solves the case $n = 2$. However, the problem is open for all $n \geq 3$.

Our aim, in this section, is to explain why Rentschler's Theorem cannot be extended to $n = 3$. More precisely, we will see that a certain consequence of Rentschler's Theorem is false in the case $n = 3$.

Definition 4.1.1. Let $B = k^{[n]}$ and $D \in \mathrm{Der}_k(B)$.

1. The **corank** of D is the maximum integer i such that there exists a system of variables $(X_1, \cdots, X_n)$ of B satisfying $\{X_1, \cdots, X_i\} \subseteq \ker(D)$.

2. The **rank** of D is defined by $\text{rank}(D) = n - \text{corank}(D)$.

Observe in particular that, if $B = k^{[n]}$ and $D \in \text{Der}_k(B)$,

$$\text{rank}(D) < n \iff \text{some variable of } B \text{ belongs to } \ker(D).$$

As noted in Remark 3.3.10 (ii), Rentschler's Theorem implies that every locally nilpotent derivation of $k^{[2]}$ has a variable in its kernel. So the following is a consequence of Rentschler's Theorem:

Corollary 4.1.2. *Every locally nilpotent derivation of $k^{[2]}$ has rank < 2.*

It is interesting to ask if it the case that every locally nilpotent derivation of $k^{[n]}$ has rank strictly less than n. For $n \geq 3$, the answer was not known until, in 1995, Freudenburg produced the following example on $B = k[X, Y, Z]$ having rank 3.

Theorem 4.1.3. *Let $B = k[X, Y, Z] = k^{[3]}$, $F = XZ - Y^2$ and $G = ZF^2 + 2X^2YF + X^5$. Define the k-derivation $\Delta : B \longrightarrow B$, by $\Delta = \Delta_{(F,G)}$. Then $\Delta \in \text{LND}(B)$, $\ker \Delta = k[F, G]$ and $\text{rank}(\Delta) = 3$.*

Proof. This is Theorem 5.19 of [6]. □

Remark 4.1.4. This explains the claim that we made at the beginning of this section: Rentschler's Theorem cannot be extended to $n = 3$, since one of its consequences (corollary 4.1.2) is false when $n = 3$.

4.2 Automorphisms

Definition 4.2.1. Let $B = k[X_1, \cdots, X_n] = k^{[n]}$. The group of k-automorphisms of B is called *the general affine group of dimension n*. It is denoted by $\text{GA}_n(k)$.

According to Theorem 1.2.4, Remark 3.2.2 of Section 3.2 can be extended for the case $n > 2$. Thus every element of $\varphi \in \text{GA}_n(k)$ is completely determined by the n-tuple $(\varphi(X_1), \cdots, \varphi(X_n))$.

As in Section 3.2, we define some subgroups of $\text{GA}_n(k)$.

Definition 4.2.2. Let $A = (a_{ij}) \in \mathrm{GL}_n(k)$ and $a = (a_1, \cdots, a_n) \in k^n$.

1. The element of $\varphi \in \mathrm{GA}_n(k)$ defined by $\varphi(X_i) = a_{1i}X_1 + \cdots + a_{ni}X_n$ $(1 \leq i \leq n)$ is denoted by φ_A.

   The set
   $$\mathcal{GL}_n(k) = \{\, \varphi_A \mid A \in \mathrm{GL}_n(k) \},$$
   is a subgroup of $\mathrm{GA}_n(k)$ and is called the *subgroup of linear automorphisms of dimension n*.

2. The element $\varphi \in \mathrm{GA}_n(k)$ defined by $\varphi(X_i) = X_i + a_i$ $(1 \leq i \leq n)$ is denoted by φ_a.

   The set
   $$\mathcal{T} = \{\, \varphi_a \mid a \in k^n \},$$
   is a subgroup of $\mathrm{GA}_n(k)$.

3. The subgroup $\langle \mathcal{GL}_n(k) \cup \mathcal{T} \rangle$ of $\mathrm{GA}_n(k)$, generated by $\mathcal{GL}_n(k)$ and $\mathcal{T}$, is called the *affine linear subgroup of dimension n*. It is denoted by $\mathrm{Af}_n(k)$.

Definition 4.2.3. Let $\mathrm{BA}_n(k)$ be the subgroup of $\mathrm{GA}_n(k)$ whose elements are the automorphisms $\phi \in \mathrm{GA}_n(k)$ of the form
$$\phi = \big(a_1X_1 + f_1, \ldots, a_nX_n + f_n\big),$$
where $a_1, \ldots, a_n \in k^\times$, $f_1 \in k$, and $f_i \in k[X_1, \cdots, X_{i-1}]$ for $1 < i \leq n$.

Definition 4.2.4. Let $\varphi \in \mathrm{GA}_n(k)$. One says that φ is a *tame automorphism* if φ belongs to the subgroup $\langle \mathcal{GL}_n(k) \cup \mathrm{BA}_n(k) \rangle = \langle \mathrm{Af}_n(k) \cup \mathrm{BA}_n(k) \rangle$ of $\mathrm{GA}_n(k)$. One says that φ is *wild* if it is not tame.

Therefore the following can be stated:

Problem. *Is* $\mathrm{GA}_n(k) = \langle \mathcal{GL}_n(k) \cup \mathrm{BA}_n(k) \rangle$*? In other words is every element of* $\mathrm{GA}_n(k)$ *tame?*

Jung's Theorem (Theorem 3.4.1), proved in 1942, tells us that the answer to this question is yes if $n = 2$. The case $n = 3$ remained open until 2004.

In 1972, Nagata defined the following automorphism σ of $k[X, Y, Z] = k^{[3]}$:

$$\begin{aligned}\sigma(X) &= X - 2(XZ + Y^2)Y - (XZ + Y^2)^2 Z,\\ \sigma(Y) &= Y + (XZ + Y^2)Z,\\ \sigma(Z) &= Z\end{aligned}$$

and conjectured:

Conjecture (Nagata, [15]). *σ is not tame!*

In 2004, Shestakov and Umirbaev showed in [21] that Nagata's conjecture was true (assuming that k has characteristic zero). This also proved that

$$\mathrm{GA}_3(k) \neq \langle \mathrm{Af}_3(k) \cup \mathrm{BA}_3(k) \rangle.$$

Therefore, not all automorphisms of $k^{[3]}$ are tame. It is still an open problem to describe the structure of the group $\mathrm{GA}_3(k)$.

Bibliography

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Univ. Oxford, (1969).

[2] A. Baker, *An Introduction to Galois Theory*, Lecture Notes, Univ. Glasgow, (2013).

[3] D. Daigle, *Introduction to locally nilpotent derivations*, Lecture notes (2010). Available on the website http://aix1.uottawa.ca/∼ddaigle/

[4] David S. Dummit and Richard M. Foote, *Abstract Algebra, Third edition* Wiley-Interscience, New York (1957).

[5] van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Birkhauser **190** (2000), 1-11.

[6] G. Freudenburg, *Algebraic Theory of Locally Nilpotent Derivations*, Berlin Heidelberg, Springer-Verlag **136** (2006).

[7] M. Hall, Jr., *The Theory of Groups*, Macmillan Company, (1959).

[8] A. Hatcher, *Algebraic Topology*, Cambridge University Press **2** (2002) ISBN 0-521-79160-0.

[9] H. W. E. Jung, *Über ganze birationale Transformationen der Ebene*, J. Reine Angew. Math. **184** (1942), 161-174.

[10] W. van der Kulk, *On polynomial rings in two variables*, Nieuw Arch. Wisk. **1** (1953), 33-41.

[11] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Modern Birkhauser Classics (1985).

[12] C. F. Miller, *Combinatorial Group Theory*, Lecture Notes, Univ. Melbourne (2004).

[13] J. S. Milne, *Fields and Galois Theory*, Lecture Notes. Available at www.jmilne.org/math/, **4.51** (2015).

[14] P. Morandi, *Field and Galois Theory*, Graduate Texts in Mathematics, Springer **167** (1996).

[15] N. Masayoshi, *On automorphism group of* $k[x, y]$, Department of Mathematics, Kyoto University, Lectures in Mathematics, No. 5, Kinokuniya Book-Store Co., Ltd., Tokyo, **v+53** (1972).

[16] H. Neumann, *Generalized free products with amalgamated subgroups I*, Amer. J. Math. **70** (1948), 590-625.

[17] A. Nur, *Locally nilpotent derivations and the cancellation problem in affine algebraic geometry*, M.Sc. thesis, Univ. Ottawa (2011).

[18] R. Rentschler, *OpÃ©rations du groupe additif sur le plan affine*, C.R. Acad. Sc. Paris, **267** (1968).

[19] J. Rotman, *The Theory of Groups: An Introduction*, Allyn and Bacon Series in Advanced Mathematics (1965).

[20] R. Y. Sharp, *Steps in Commutative Algebra, Second edition*, London Mathematical Society, Student Texts **51**, 2000.

[21] P. Shestakov and U. Umirbaev, *The tame and the wild automorphisms of polynomial rings in three variables*, American Mathematical Society, **17**, 197-227 (2004).