Some problems and methods of Affine Algebraic Geometry

Daniel Daigle (U. Ottawa, Canada)

Affine Algebraic Geometry is the study of affine spaces $\mathbb{A}^n$ and of algebraic varieties which resemble $\mathbb{A}^n$. The objective of these lectures is to give an introduction to this field by presenting some of its open problems and by developing some algebraic tools which are used for investigating these problems.

- All rings and algebras are tacitly assumed to be commutative and associative and to have an identity element 1.
- If A is a ring, $A^{[n]}$ = polynomial ring in n variables over A.
- If $\Bbbk$ is a field, $\Bbbk^{(n)} = \operatorname{Frac} \Bbbk^{[n]}$ = field of fractions of $\Bbbk^{[n]}$.
- If A is a ring, A^* is the set of units of A.
- "Domain" means integral domain. "$\Bbbk$-affine" means finitely generated as a $\Bbbk$-algebra. An "affine $\Bbbk$-domain" is an integral domain which is finitely generated as a $\Bbbk$-algebra.

1. Introduction: Some famous open problems

Cancellation Problem. (Zariski, $<$ 1950)

$$\mathrm{CP}(n): \quad \textit{For an algebra } A \textit{ over a field } \Bbbk, \quad A^{[1]} \cong \Bbbk^{[n+1]} \overset{?}{\implies} A \cong \Bbbk^{[n]}$$

where "$\cong$" means isomorphism of $\Bbbk$-algebras. The problem can be formulated in geometric terms:

$$\mathrm{CP}(n): \quad \textit{For an affine variety } V, \quad V \times \mathbb{A}^1 \cong \mathbb{A}^{n+1} \overset{?}{\implies} V \cong \mathbb{A}^n$$

where "$\cong$" means isomorphism of varieties.

Status: $\mathrm{CP}(n)$ is open when $n > 2$. We will prove $\mathrm{CP}(1)$ and $\mathrm{CP}(2)$ in these lectures.

Our first attempt to prove $\mathrm{CP}(n)$ begins with:

1.1. **Observation.** *Let A be an algebra over a field $\Bbbk$.*
If $A^{[1]} \cong \Bbbk^{[n+1]}$ (or more generally, if $A^{[m]} \cong \Bbbk^{[n+m]}$ for some m) then:

- *A is an affine $\Bbbk$-domain and* $\dim A = n$
- *A is a UFD*
- $A^* = \Bbbk^*$

Do these conditions (or perhaps a longer list of conditions) imply that $A \cong \Bbbk^{[n]}$? To answer, we need to solve the second problem in our list:

Problem: Characterizations of $\Bbbk^{[n]}$.
How can we decide whether a given $\Bbbk$-algebra is $\Bbbk^{[n]}$? To illustrate this problem, here are three characterizations of $\Bbbk^{[1]}$:

1.2. **Theorem.** *Let A be an integral domain containing a field $\mathbb{k}$.*

(a) $\operatorname{Frac} A = \mathbb{k}^{(1)}$*, A is $\mathbb{k}$-affine, A is a UFD,* $A^* = \mathbb{k}^* \iff A = \mathbb{k}^{[1]}$

(b) $(\mathbb{k} = \bar{\mathbb{k}})$ $\operatorname{Frac} A = \mathbb{k}^{(1)}$*, A is normal,* $A^* = \mathbb{k}^* \iff A = \mathbb{k}^{[1]}$

(c) $(\mathbb{k} = \bar{\mathbb{k}})$ *A is $\mathbb{k}$-affine,* $\dim A = 1$*, A is a UFD,* $A^* = \mathbb{k}^* \iff A = \mathbb{k}^{[1]}$

Let us prove part (c) of the theorem (only part (c) will be needed later). The proof requires the following result from the theory of curves:[1]

1.3. **Proposition.** *Let C be a nonsingular projective curve over an algebraically closed field. If the divisor class group* $\operatorname{Cl}(C)$ *of C is finitely generated, then C is rational (so $C = \mathbb{P}^1$).*

We give two proofs of 1.3. The first one is only valid when $\mathbb{k}$ is uncountable. The second one is valid in general, but is more difficult.

First proof. To prove that $C = \mathbb{P}^1$, it suffices to show that there exist distinct points $P, Q \in C$ such that $P \sim Q$ (where $\sim$ is linear equivalence of divisors). Consider the map $f : C \to \operatorname{Cl}(C)$ defined by $f(P) = [P]$, where $[P] \in \operatorname{Cl}(C)$ is the linear equivalence class of $P \in C$. Since $\mathbb{k}$ is assumed to be uncountable, it follows that C is an uncountable set of points; since $\operatorname{Cl}(C)$ is a finitely generated abelian group, it is a countable set; so f is not injective. Consider distinct points $P, Q \in C$ such that $f(P) = f(Q)$. Then $P \sim Q$, so $C = \mathbb{P}^1$. □

Second proof. Let C be any nonsingular projective curve over an algebraically closed field and let $\operatorname{Cl}^0(C)$ denote the kernel of the degree homomorphism $\deg : \operatorname{Cl}(C) \to \mathbb{Z}$. Also consider the jacobian variety $J(C)$ of C. Refer to [5, 6.10.3, p. 140] for the following claims:

- $J(C)$ is an abelian variety (i.e., an algebraic group whose underlying algebraic variety is projective)
- the dimension of the variety $J(C)$ is equal to the genus g of C
- the group $\operatorname{Cl}^0(C)$ is isomorphic to the underlying group of $J(C)$.

Since any abelian variety is a divisible group (cf. [9], p. 62), it follows that $\operatorname{Cl}^0(C)$ is divisible. (Definition: an abelian group $(G, +)$ is *divisible* if given any $y \in G$ and any integer $n > 0$ the equation $nx = y$ has a solution $x \in G$.)

If we assume that $\operatorname{Cl}(C)$ is finitely generated then $\operatorname{Cl}^0(C)$ is also finitely generated. Being both divisible and finitely generated, $\operatorname{Cl}^0(C)$ is the trivial group. So $\operatorname{Cl}^0(C)$ has only one element and consequently $J(C)$ consists of only one point. Thus $g = \dim J(C) = 0$ and C is rational. □

We deduce the characterization 1.2 (c) of $\mathbb{k}^{[1]}$:

1.4. **Theorem.** $(\mathbb{k} = \bar{\mathbb{k}})$ *Let A be an affine $\mathbb{k}$-domain of dimension 1.*
If A is a UFD and $A^* = \mathbb{k}^*$, then $A = \mathbb{k}^{[1]}$.

---

[1]Parts (a) and (b) of the theorem can be proved by algebra but part (c) requires geometry.

Proof. A is the coordinate ring of an affine curve U over the algebraically closed field $\mathbb{k}$. Moreover, U is nonsingular because A is a normal ring. The curve U can be embedded as an open subset of a nonsingular projective curve C, and the complement of U in C is a finite set of points $\{P_1, \dots, P_n\}$. Then $\mathrm{Cl}(U) \cong \mathrm{Cl}(C)/H$ where H is the subgroup of $\mathrm{Cl}(C)$ generated by $[P_1], \dots, [P_n]$. As A is factorial, $\mathrm{Cl}(U) = 0$ and consequently $\mathrm{Cl}(C)$ is finitely generated. By 1.3 it follows that $C = \mathbb{P}^1$, so U is $\mathbb{P}^1$ minus n points. The assumption $A^* = \mathbb{k}^*$ implies that $n = 1$, so $U = \mathbb{A}^1$, so $A = \mathbb{k}^{[1]}$. □

So 1.2 (c) is true, and it follows that CP(1) is true when $\mathbb{k}$ is algebraically closed:

1.5. **Corollary.** *($\mathbb{k} = \bar{\mathbb{k}}$) If A is a $\mathbb{k}$-algebra such that $A^{[m]} = \mathbb{k}^{[m+1]}$ for some m, then $A = \mathbb{k}^{[1]}$.*

Proof. Immediate consequence of 1.2 (c) and of Observation 1.1. □

Actually, 1.5 is valid without the assumption that $\mathbb{k} = \bar{\mathbb{k}}$. To prove this, we use part (a) of 1.2 instead of part (c), and we also need the Theorem of Lüroth. Since we did not prove 1.2 (a), we give this only as a remark:

Corollary. *Let $\mathbb{k}$ be any field. If A is a $\mathbb{k}$-algebra such that $A^{[m]} = \mathbb{k}^{[m+1]}$ for some m, then $A = \mathbb{k}^{[1]}$.*

Proof. We have $\mathbb{k} \subset \mathrm{Frac}\, A \subseteq \mathbb{k}^{(m+1)}$ where the transcendence degree of $\mathrm{Frac}\, A$ over $\mathbb{k}$ is equal to 1, so by the "Generalized Lüroth Theorem" we get $\mathrm{Frac}\, A = \mathbb{k}^{(1)}$. Then part (a) of Theorem 1.2 (together with Observation 1.1) implies that $A = \mathbb{k}^{[1]}$. □

Overview of the two dimensional case

Good characterizations of $\mathbb{k}^{[2]}$ are known, and can be used to prove CP(2). We present an outline now, and we give the proofs later.

First consider the problem of characterizing $\mathbb{k}^{[2]}$. The following example shows that for a two-dimensional affine $\mathbb{C}$-domain A,

$$A \text{ is a UFD, } A^* = \mathbb{C}^*, \text{ Frac}\, A = \mathbb{C}^{(2)}, A \text{ is regular } \not\Longrightarrow A = \mathbb{C}^{[2]}.$$

1.6. **Example.** Let C be an irreducible curve in $\mathbb{A}^2_{\mathbb{C}}$, let P be a nonsingular point of C, let $S \to \mathbb{A}^2_{\mathbb{C}}$ be the blowing-up of $\mathbb{A}^2_{\mathbb{C}}$ at P and let $\tilde{C} \subset S$ be the strict transform of C. Then $U = S \setminus \tilde{C}$ is a nonsingular affine surface, is factorial and has trivial units. Moreover, one can show that $U \cong \mathbb{A}^2_{\mathbb{C}}$ if and only if $C \cong \mathbb{A}^1_{\mathbb{C}}$.

In order to formulate a characterization of $\mathbb{k}^{[2]}$, we need:

1.7. **Definition.** A *derivation* of a ring B is a map $D : B \to B$ satisfying:

$$\text{for all } f, g \in B, \qquad D(f+g) = D(f) + D(g) \quad \text{and} \quad D(fg) = D(f)g + fD(g).$$

The derivation $D : B \to B$ is *locally nilpotent* if for each $b \in B$ there exists $n > 0$ such that $D^n(b) = 0$.

1.8. **Example.** Let $\mathbb{k}$ be a field and let $B = \mathbb{k}[X_1, \dots, X_n] = \mathbb{k}^{[n]}$. Then $\frac{\partial}{\partial X_i} : B \to B$ is a locally nilpotent derivation of B (for each $i = 1, \dots, n$).

One can extend these derivations $\frac{\partial}{\partial X_i}$ to the field $\operatorname{Frac} B = \Bbbk(X_1, \dots, X_n)$. Then

$$\frac{\partial}{\partial X_i} \;:\; \Bbbk(X_1, \dots, X_n) \to \Bbbk(X_1, \dots, X_n)$$

is a derivation but is not locally nilpotent: $(\frac{\partial}{\partial X_i})^m(\frac{1}{X_i}) \neq 0$ for all $m > 0$.

1.9. **Definition.** Let B be a domain of characteristic zero. We say that B is *rigid* if the only locally nilpotent derivation $D : B \to B$ is the zero derivation.

In 1975, Miyanishi proved the following **characterization of $\Bbbk^{[2]}$**:

1.10. **Theorem.** *Let $\Bbbk$ be an algebraically closed field of characteristic zero. For a two-dimensional affine $\Bbbk$-domain A,*

$$A \text{ is a UFD, } A^* = \Bbbk^* \text{ and } A \text{ is not rigid} \iff A = \Bbbk^{[2]}.$$

We will prove this theorem later; its proof is purely algebraic and is based on properties of locally nilpotent derivations.

In view of 1.10 and of Observation 1.1, then, to prove CP(2), there only remains to prove:

$$(*) \qquad A^{[1]} = \Bbbk^{[3]} \implies A \text{ is not rigid.}$$

The proof of $(*)$ required 4 years, and made use of sophisticated algebraic geometry (theory of open algebraic surfaces, theory of logarithmic Kodaira dimension of algebraic varieties, etc). The last step of the proof was done by Fujita in 1979 (cf. [4]) and was generalized to arbitrary characteristic in 1981 (cf. [11]). The conclusion is that the following strong version of CP(2) is true (CP(2) is the case $m = 1$):

1.11. **Theorem.** *Let $\Bbbk$ be a perfect field. If A is a $\Bbbk$-algebra such that $A^{[m]} = \Bbbk^{[m+2]}$ for some m, then $A = \Bbbk^{[2]}$.*

More than 20 years after the geometric proof, Makar-Limanov found an algebraic proof of $(*)$ which is considerably simpler than the the geometric one (it is based on properties of locally nilpotent derivations and is valid in characteristic zero). We will see this proof later, so we will have a complete algebraic proof of CP(2) in characteristic zero.

It is shown in [2] that the algebraic approach can be generalized to arbitrary characteristic by replacing locally nilpotent derivations by another device, and that this gives an algebraic proof of the case $m = 1$ of 1.11 for any perfect field. However we will restrict ourselves to characteristic zero in these notes.

Higher dimension

Problem posed by Russell in 1992. (Cf. [12])

> $(\star)$ *Let $V = \{X + X^2Y + Z^2 + T^3 = 0\} \subset \mathbb{C}^4$.*
> *Prove that $V \ncong \mathbb{C}^3$ as algebraic varieties.*

This V is now called "Russell's Threefold". It is a smooth irreducible threefold, diffeomorphic to $\mathbb{R}^6$. It is rational and factorial and admits a dominant morphism $\mathbb{C}^3 \to V$.

The problem is equivalent to:

> $(\star)$ *Let $A = \mathbb{C}[X, Y, Z, T]/(X + X^2Y + Z^2 + T^3)$.*
> *Prove that $A \ncong \mathbb{C}^{[3]}$ as $\mathbb{C}$-algebras.*

Note that A looks very much like $\mathbb{C}^{[3]}$:

- $\operatorname{Frac} A = \mathbb{C}(x, z, t) = \mathbb{C}^{(3)}$
- A is a UFD
- $A^* = \mathbb{C}^*$
- A is not rigid

The characterizations of $\Bbbk^{[3]}$ known at that moment did not allow to solve ($\star$). Two years later Makar-Limanov proved that $A \not\cong \mathbb{C}^{[3]}$ by using locally nilpotent derivations.

A recent characterization of $\Bbbk^{[3]}$ due to Kaliman (2002) allows an easy solution of ($\star$), but CP(3) is still open.

No characterization of $\Bbbk^{[4]}$ is known. For instance, the following is currently an open question:

Let V be the Russell threefold. Is $V \times \mathbb{C}$ isomorphic to $\mathbb{C}^4$?

More problems

We briefly mention four more problems.

Automorphisms. *Let $\Bbbk$ be a field. Describe the $\Bbbk$-algebra automorphisms of $\Bbbk^{[n]}$ (or the automorphisms of $\mathbb{A}^n$ as an algebraic variety).*

Open for $n \geq 3$. The structure of $\operatorname{Aut}_{\Bbbk}(\Bbbk^{[2]})$ was described by Jung (1942) and van der Kulk (1953) (plus a contribution by Serre in 1977).

Locally nilpotent derivations of $\Bbbk^{[n]}$. ($\operatorname{char} \Bbbk = 0$)
Describe the locally nilpotent derivations of $\Bbbk^{[n]}$ (or the G_a-actions on $\mathbb{A}^n$).

Open for $n \geq 3$. This is closely related to the Automorphism Problem.

1.12. **Definition.** Let $A \cong \Bbbk^{[n]}$. A *variable* of A is an element $f \in A$ satisfying

$$\exists\ f_2, \dots, f_n \text{ such that } A = \Bbbk[f, f_2, \dots, f_n].$$

Remark. If $A = \Bbbk[X_1, \dots, X_n] = \Bbbk^{[n]}$ then the set of variables of A is equal to:

$$\{\ \theta(X_1) \mid \theta \in \operatorname{Aut}_{\Bbbk}(A)\ \}.$$

Recognition/characterization of variables.
Given $f \in A \cong \Bbbk^{[n]}$, decide whether f is a variable of A.

Embeddings of $\mathbb{A}^m$ in $\mathbb{A}^n$. *Suppose that V is a closed subvariety of $\mathbb{A}^n = \mathbb{A}^n_{\Bbbk}$. If $V \cong \mathbb{A}^m$ (where $m < n$), does there necessarely exist $\theta \in \operatorname{Aut}_{\Bbbk}(\mathbb{A}^n)$ such that*

$$\theta(V) = \{\,(x_1, \dots, x_m, 0, \dots, 0) \mid x_1, \dots, x_m \in \Bbbk\}?$$

2. Locally nilpotent derivations

Recall that a *derivation* of a ring B is a map $D : B \to B$ satisfying

$$\text{for all } f, g \in B, \qquad D(f+g) = D(f) + D(g) \quad \text{and} \quad D(fg) = D(f)g + fD(g).$$

If $D : B \to B$ is a derivation, we define $\ker D = \{x \in B \mid D(x) = 0\}$.

2.1. **Exercise.** Let B be a ring and $D : B \to B$ a derivation. Verify the following claims.

(i) $\ker(D)$ is a **subring** of B.

(ii) $D(b^n) = nb^{n-1}D(b)$, for all $b \in B$ and $n \in \mathbb{N}$.

(iii) Let $f(T) = \sum_{i=0}^n a_i T^i \in B[T]$ be a polynomial ($a_i \in B$ and T is an indeterminate). If $b \in B$ then $f(b) \in B$, so it makes sense to evaluate D at $f(b)$. Show that

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

where we define the polynomial $f^{(D)}(T) \in B[T]$ by $f^{(D)}(T) = \sum_{i=0}^n D(a_i)T^i$, and where $f'(T) \in B[T]$ is the derivative of f, defined by $f'(T) = \sum_{i=1}^n i a_i T^{i-1}$. Note that if all a_i belong to $\ker(D)$ then this formula simplifies to $D\big(f(b)\big) = f'(b)D(b)$.

(iv) More generally, show that if $f \in B[T_1, \dots, T_n]$ and $b_1, \dots, b_n \in B$ then

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

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

The sum of two derivations is a derivation. If $D : B \to B$ is a derivation and $b \in B$ then the map

$$bD : B \to B, \qquad x \mapsto bD(x)$$

is a derivation of B. It follows that the set

$$\mathrm{Der}(B) = \text{ set of all derivations of } B$$

is a B-module. If $A \subseteq B$ are rings then by an *A-derivation* of B we mean a derivation $D : B \to B$ satisfying $D(A) = \{0\}$. Then the set

$$\mathrm{Der}_A(B) = \text{ set of all } A\text{-derivations of } B$$

is a B-submodule of $\mathrm{Der}(B)$.

2.2. **Example.** Let $\Bbbk$ be a field and $B = \Bbbk[X_1, \dots, X_n] = \Bbbk^{[n]}$. Here are some examples of elements of $\mathrm{Der}_{\Bbbk}(B)$.

(1) We have $\frac{\partial}{\partial X_i} \in \mathrm{Der}_{\Bbbk}(B)$ for all $i = 1, \dots, n$.

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

Proof. As $\mathrm{Der}_{\Bbbk}(B)$ is a B-module, it makes sense to define

$$D := \sum_{i=1}^n f_i \, \frac{\partial}{\partial X_i} \; \in \; \mathrm{Der}_{\Bbbk}(B).$$

Clearly, $D(X_i) = f_i$ for all $i \in \{1, \dots, n\}$. If also $D' \in \mathrm{Der}_{\Bbbk}(B)$ satisfies $D'(X_i) = f_i$ for all i, then consider $D_0 = D - D' \in \mathrm{Der}_{\Bbbk}(B)$; then $D_0(X_i) = 0$ for all i, so $D_0 = 0$ and hence $D = D'$. So D is the unique element of $\mathrm{Der}_{\Bbbk}(B)$ satisfying $D(X_i) = f_i$ for all $i \in \{1, \dots, n\}$. □

Remark. (2) implies that $\mathrm{Der}_{\Bbbk}(B)$ is a free B-module with basis $\{\frac{\partial}{\partial X_1}, \dots, \frac{\partial}{\partial X_n}\}$.

(3) Given $f = (f_1, \dots, f_{n-1}) \in B^{n-1}$, define the *jacobian derivation* $\Delta_f \in \mathrm{Der}_{\Bbbk}(B)$ by $\Delta_f(g) = \det\left(\frac{\partial(f_1, \dots, f_{n-1}, g)}{\partial(X_1, \dots, X_n)}\right)$, for each $g \in B$. Note that $\Bbbk[f_1, \dots, f_{n-1}] \subseteq \ker(\Delta_f)$.

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

Proof. Let $A = \ker D$ and consider $b \in B$ algebraic over A. Let $f \in A[T]$ be a nonzero polynomial of minimal degree such that $f(b) = 0$. Note that $\deg(f) > 0$. Then

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

We have $f' \neq 0$, so $f'(b) \neq 0$ by minimality of $\deg f$, so $D(b) = 0$. □

2.4. **Exercise.** Prove **Leibnitz Rule**: *If B is a ring, $D \in \text{Der}(B)$, $x, y \in B$ and $n \in \mathbb{N}$,*

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

Remark. $D^0 : B \to B$ is defined to be the identity map (even in the case $D = 0$).

2.5. **Definition.** Given a ring B and $D \in \text{Der}(B)$, define the set

$$\text{Nil}(D) = \{ x \in B \mid \exists_{n \in \mathbb{N}}\ D^n(x) = 0 \}.$$

So $\ker(D) \subseteq \text{Nil}(D) \subseteq B$. By exercise 2.6, $\text{Nil}(D)$ is a subring of B.

2.6. **Exercise.** Use Leibnitz Rule to show that the subset $\text{Nil}(D)$ of B is closed under multiplication. Deduce that $\text{Nil}(D)$ is a subring of B.

2.7. **Example.** Let $B = \mathbb{C}[[T]]$ and $D = d/dT : B \to B$. Then $\ker(D) = \mathbb{C}$ and $\text{Nil}(D) = \mathbb{C}[T]$. Note that $\text{Nil}(D)$ is not integrally closed in B: let $b = \sqrt{1+T} \in B$, then $b \notin \text{Nil}(D)$ but $b^2 \in \text{Nil}(D)$.

2.8. **Definition.** Let B be any ring. A derivation $D : B \to B$ is *locally nilpotent* if it satisfies $\text{Nil}(D) = B$, i.e., if $\forall_{b \in B} \exists_{n \in \mathbb{N}}\, D^n(b) = 0$. Notations:

$$\text{LND}(B) = \text{set of locally nilpotent derivations } B \to B$$
$$\text{KLND}(B) = \{ \ker D \mid D \in \text{LND}(B) \text{ and } D \neq 0 \}.$$

2.9. **Examples.** Let $\Bbbk$ be a field and $B = \Bbbk[X_1, \dots, X_n] = \Bbbk^{[n]}$.

(1) $\frac{\partial}{\partial X_i} \in \text{LND}(B)$ for each $i = 1, \dots, n$.

(2) **Definition:** A derivation $D : B \to B$ is *triangular* if $D(\Bbbk) = \{0\}$ and:

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

We claim that *every triangular derivation is locally nilpotent.* Indeed, if $D : B \to B$ is triangular then $\Bbbk \subseteq \ker(D) \subseteq \text{Nil}(D)$, so $\text{Nil}(D)$ is a $\Bbbk$-subalgebra of B, and it is easy to see (by induction on i) that

$$\forall\, i \quad \Bbbk[X_1, \dots, X_i] \subseteq \text{Nil}(D);$$

so $\text{Nil}(D) = B$, i.e., D is locally nilpotent.

The subset $\text{LND}(B)$ of the B-module $\text{Der}(B)$ is usually not closed under addition and not closed under multiplication by elements of B. For instance, let $B = \mathbb{C}[X, Y] = \mathbb{C}^{[2]}$, $D_1 = Y \frac{\partial}{\partial X}$ and $D_2 = X \frac{\partial}{\partial Y}$; then $D_1, D_2 \in \text{LND}(B)$ (because they are triangular) but $D_1 + D_2 \notin \text{LND}(B)$ (because $(D_1 + D_2)^2(X) = X$). Also, $\frac{\partial}{\partial X} \in \text{LND}(B)$ but $X \frac{\partial}{\partial X} \notin \text{LND}(B)$.

2.10. **Exercise.** Let B be a ring, $D \in \text{LND}(B)$ and $A = \ker D$.

(1) If $a \in A$ then $(aD)^n = a^n D^n$ holds for all $n \in \mathbb{N}$.

(2) If $a \in A$ then $aD \in \text{LND}(B)$.

(3) Observe that $D : B \to B$ is (in particular) a homomorphism of A-modules. If $S \subset A$ is a multiplicatively closed set, consider the homomorphism of $S^{-1}A$-modules $S^{-1}D : S^{-1}B \to S^{-1}B$ defined by $(S^{-1}D)(x/s) = (Dx)/s$ ($x \in B$, $s \in S$). Show that $S^{-1}D$ is an element of $\text{LND}(S^{-1}B)$ and $\ker(S^{-1}D) = S^{-1}A$.

The exponential map associated to a locally nilpotent derivation

2.11. **Exercise.** If B is a $\mathbb{Q}$-algebra then $\text{Der}(B) = \text{Der}_{\mathbb{Q}}(B)$.

2.12. **Definition.** Let B be a $\mathbb{Q}$-algebra. Given $D \in \text{LND}(B)$, define the map

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

We call ξ_D the *exponential map associated to* D (not to be confused with the exponential of D, $\exp(D) : B \to B$, to be defined later).

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

Proof. If $e_0 : B[T] \to B$ is the map $f(T) \mapsto f(0)$, then the composite $B \xrightarrow{\xi_D} B[T] \xrightarrow{e_0} B$ is the identity map, so ξ_D is injective. It is clear that ξ_D preserves addition and restricts to the identity map on A, so it suffices to verify that

$$\left(\sum_{i\in\mathbb{N}} \frac{1}{i!} D^i(x)\, T^i\right)\left(\sum_{j\in\mathbb{N}} \frac{1}{j!} D^j(y)\, T^j\right) = \sum_{n\in\mathbb{N}} \frac{1}{n!} D^n(xy)\, T^n \tag{1}$$

holds for all $x, y \in B$. In the left hand side of (1), the coefficient of T^n is

$$\sum_{i+j=n} \frac{1}{i!\,j!} D^i(x) D^j(y) = \frac{1}{n!} \sum_{i+j=n} \frac{n!}{i!\,j!} D^i(x) D^j(y),$$

which is equal to $\frac{1}{n!} D^n(xy)$ by Leibnitz Rule. □

Theorem 2.13 has many consequences. We will see some of them.

Degree functions

2.14. **Definition.** A *degree function* on a ring B is a map $\deg : B \to \mathbb{N} \cup \{-\infty\}$ satisfying:

(1) $\forall\, x \in B \quad \deg x = -\infty \iff x = 0$

(2) $\forall\, x, y \in B \quad \deg(xy) = \deg x + \deg y$

(3) $\forall\, x, y \in B \quad \deg(x + y) \le \max(\deg x, \deg y)$.

Note that if B admits a degree function then it is a domain, by (1) and (2). Also note that if $B \xrightarrow{\varphi} B'$ is an injective ring homomorphism and $B' \xrightarrow{d} \mathbb{N} \cup \{-\infty\}$ is a degree function then $B \xrightarrow{d\circ\varphi} \mathbb{N} \cup \{-\infty\}$ is a degree function.

2.15. **Definition.** Let B be a ring. Then each $D \in \text{LND}(B)$ determines a map

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

defined as follows: $\deg_D(x) = \max\{n \in \mathbb{N} \mid D^n x \neq 0\}$ for $x \in B \setminus \{0\}$, and $\deg_D(0) = -\infty$. Note that $\ker D = \{x \in B \mid \deg_D(x) \leq 0\}$.

Although we defined $\deg_D$ for any ring B, it is useful mostly in the case of integral domains of characteristic zero:

2.16. **Proposition.** *Let B be a domain of characteristic zero and $D \in \text{LND}(B)$. Then the map $\deg_D : B \to \mathbb{N} \cup \{-\infty\}$ is a degree function.*

Proof. We first prove the special case where $\mathbb{Q} \subseteq B$. In this case we may consider the map $\xi_D : B \to B[T]$, $\xi_D(b) = \sum_{i=0}^{\infty} \frac{D^n(b)}{n!} T^n$, which is an injective ring homomorphism by 2.13. As B is a domain, $B[T] \xrightarrow{\deg_T} \mathbb{N} \cup \{-\infty\}$ is a degree function and consequently the composite $B \xrightarrow{\xi_D} B[T] \xrightarrow{\deg_T} \mathbb{N} \cup \{-\infty\}$ is a degree function. As this composite map is equal to $\deg_D$, $\deg_D$ is a degree function.

Now the general case. Since B has characteristic zero and $\ker D$ is a subring of B, we have $\mathbb{Z} \subseteq \ker D$. Let $S = \mathbb{Z} \setminus \{0\}$ and consider $S^{-1}D : S^{-1}B \to S^{-1}B$, which belongs to $\text{LND}(S^{-1}B)$ by Exercise 2.10. As $\mathbb{Q} \subseteq S^{-1}B$, the first part of the proof implies that $\deg_{S^{-1}D} : S^{-1}B \to \mathbb{N} \cup \{-\infty\}$ is a degree function. We have:

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

As $\deg_D$ is the restriction of $\deg_{S^{-1}D}$, it follows that $\deg_D$ is a degree function. □

2.17. **Exercise.** Let B be a domain of characteristic zero and suppose that $D \in \text{Der}(B)$ satisfies $D^n = 0$ for some $n > 0$. Show that $D = 0$. (*Hint.* Note that D is locally nilpotent. If $D \neq 0$ then we can choose $x \in B$ such that $\deg_D(x) \geq 1$; what is $\deg_D(x^n)$? can $D^n(x^n)$ be zero?)

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

$$\forall\, x, y \in B \setminus \{0\} \qquad xy \in A \implies x, y \in A.$$

For instance, consider the polynomial ring $R[T]$ in one variable over an integral domain R. Then R is factorially closed in $R[T]$. Note that this example is a special case of:

2.19. **Lemma.** *If B is a domain and $\deg : B \to \mathbb{N} \cup \{-\infty\}$ is a degree function then $\{x \in B \mid \deg x \leq 0\}$ is a factorially closed subring of B.*

Proof. Obvious. (Remark: if we replace $\mathbb{N}$ by $\mathbb{Z}$ in the statement, then the conclusion is not necessarely true.) □

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

Proof. $\{x \in B \mid \deg_D(x) \leq 0\}$ is factorially closed in B by 2.16 and 2.19. As $\ker D = \{x \in B \mid \deg_D(x) \leq 0\}$, we are done. $\square$

Recall the following definitions. Let R be an integral domain and let $p \in R$. We say that p is *irreducible* if $p \notin R^* \cup \{0\}$ and if the condition $p = xy$ (where $x, y \in R$) implies that $\{x, y\} \cap R^* \neq \varnothing$. We say that p is *prime* if $p \notin R^* \cup \{0\}$ and if the condition $p \mid xy$ (where $x, y \in R$) implies that p divides one of x, y (i.e., p is prime if and only if the principal ideal pR is a nonzero prime ideal of R). Recall that every prime element is irreducible but that the converse is not necessarely true. However, if R is a UFD then "irreducible" is equivalent to "prime".

2.21. **Exercise.** Suppose that A is a factorially closed subring of a domain B. Then:

(1) $A^* = B^*$.

(2) An element of A is irreducible in A iff it is irreducible in B.

(3) If B is a UFD then so is A.

Remark. For domains $A \subseteq B$,

$$\begin{aligned} A \text{ is factorially closed in } B &\implies A \text{ is algebraically closed in } B \\ &\implies A \text{ is integrally closed in } B. \end{aligned}$$

2.22. **Corollary.** *Let B be a domain of characteristic zero, $D \in \text{LND}(B)$ and $A = \ker(D)$. Then $A^* = B^*$, and if $\Bbbk$ is any field contained in B then D is a $\Bbbk$-derivation. Moreover, if B is a UFD then so is A.*

Slice theorem and consequences

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

2.24. **Examples.** Let $B = \mathbb{C}[X, Y, Z] = \mathbb{C}^{[3]}$.

(1) X is a slice of $\frac{\partial}{\partial X} \in \text{LND}(B)$.

(2) Define $D \in \text{LND}(B)$ by $DZ = Y$, $DY = X$, $DX = 0$. Then given $f \in B$,

$$D(f) = f_X D(X) + f_Y D(Y) + f_Z D(Z) = f_Y X + f_Z Y,$$

thus $D(B) \subseteq (X, Y)B$, so D does not have a slice.

When a slice exists, the situation is very special:

2.25. **Theorem** ([14, Prop. 2.1]). *Let B be a $\mathbb{Q}$-algebra, $D \in \text{LND}(B)$ and $A = \ker(D)$. If $s \in B$ satisfies $Ds = 1$ then $B = A[s] = A^{[1]}$ and $D = \frac{d}{ds} : A[s] \to A[s]$.*

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 $a_n \neq 0$). Then $D^j(f(s)) = f^{(j)}(s)$ for all $j \geq 0$, where $f^{(j)}(T) \in A[T]$ denotes the j-th derivative of f; so $D^n(f(s)) = n!\, a_n \neq 0$ and in particular $f(s) \neq 0$. So s is transcendental over A, i.e., $A[s] = A^{[1]}$.

To show that $B = A[s]$, consider the homomorphism of A-algebra $\xi : B \to B$ obtained by composing the homomorphism $\xi_D : B \to B[T]$ of 2.13 with the evaluation map $B[T] \to B$, $f(T) \mapsto f(-s)$. Explicitely, if $x \in B$ then $\xi(x) = \sum_{j=0}^{\infty} \frac{D^j x}{j!}(-s)^j$. For each $x \in B$,

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

so $\xi(B) \subseteq A$; since ξ is a A-homomorphism, $\xi(B) = A$.

By induction on $\deg_D(x)$, we show that $\forall_{x \in B}\ x \in A[s]$. This is clear if $\deg_D(x) \leq 0$, so assume that $\deg_D(x) \geq 1$. Since $x = \xi(x) + (x - \xi(x))$ where $\xi(x) \in A$ and $x - \xi(x) \in sB$,

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

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

(3) $$\forall_{m \geq 1}\ \ D^m(x) = D^m(x')s + mD^{m-1}(x').$$

Choose $m \geq 1$ such that $D^{m-1}(x') \neq 0$ and $D^m(x') = 0$ (such an m exists because $\deg_D(x) \geq 1$, so $x \notin A$, so $x' \neq 0$). Then (3) gives $D^m(x) = mD^{m-1}(x') \neq 0$ and $D^{m+1}(x) = 0$, so $\deg_D(x') = \deg_D(x) - 1$. By the inductive hypothesis we have $x' \in A[s]$; then (2) gives $x \in A[s]$. So $B = A[s] = A^{[1]}$. ☐

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

Proof. Let $A \in \text{KLND}(B)$. Choose $D \in \text{LND}(B)$ such that $\ker D = A$ (then $D \neq 0$). If we write $S = A \setminus \{0\}$ and $K = \operatorname{Frac}(A)$ then exercise 2.10 gives $S^{-1}D \in \text{LND}(S^{-1}B)$ and $\ker(S^{-1}D) = K$. Note that $S^{-1}D$ has a slice (indeed, choose a preslice $s \in B$ of D and let $a = Ds$, then $a \in S$, so $s/a \in S^{-1}B$, and it is clear that $S^{-1}D(s/a) = 1$). So 2.25 implies that $S^{-1}B = K^{[1]}$, which proves the assertion. ☐

2.27. **Exercise.** Let B be a domain such that: (1) B has transcendence degree 1 over some field $\mathbb{k}_0 \subseteq B$ of characteristic zero; (2) $\text{LND}(B) \neq \{0\}$. Show that $B = \mathbb{k}^{[1]}$ for some field $\mathbb{k}$ such that $\mathbb{k}_0 \subseteq \mathbb{k} \subseteq B$. (Hint: let $D \in \text{LND}(B)$, $D \neq 0$, define $\mathbb{k} = \ker D$ and consider $\mathbb{k}_0 \subseteq \mathbb{k} \subseteq B$. Show that $\mathbb{k}$ is integral over $\mathbb{k}_0$ and hence must be a field. So D has a slice and $B = \mathbb{k}^{[1]}$.)

2.28. **Exercise.** Consider the subring $B = \mathbb{C}[T^2, T^3]$ of $\mathbb{C}[T] = \mathbb{C}^{[1]}$. Show that the only locally nilpotent derivation $B \to B$ is the zero derivation.

2.29. **Exercise.** Let $B = \mathbb{Z}[X, Y] = \mathbb{Z}^{[2]}$ and $D = \frac{\partial}{\partial Y} + Y\frac{\partial}{\partial X}$. Since D is triangular, we have $D \in \text{LND}(B)$. Moreover, $DY = 1$. Show that $\ker D = \mathbb{Z}[2X - Y^2]$ and that B is not a polynomial ring over $\ker D$. (So in 2.25 the hypothesis that B is a $\mathbb{Q}$-algebra is not superfluous.)

A finer analysis: preslices

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

Remark. It is clear that if $D \in \text{LND}(B)$ and $D \neq 0$ then D has a preslice.

Preslices are important because they always exist, and because they have the following nice property:

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

Proof. Let $S = \{1, \alpha, \alpha^2, \dots\}$ and consider $S^{-1}D : S^{-1}B \to S^{-1}B$. By exercise 2.10, $S^{-1}D \in \text{LND}(S^{-1}B)$, $\ker(S^{-1}D) = S^{-1}A$ and $(S^{-1}D)(s/\alpha) = 1$, so the result follows from 2.25. □

Geometric interpretation. Given $A \in \text{KLND}(B)$, the inclusion map $A \hookrightarrow B$ is a ring homomorphism and hence determines a morphism of schemes $\pi : \text{Spec}(B) \to \text{Spec}(A)$. It is natural to ask what are the properties of this morphism π. Result 2.31 implies that the general fiber of π is an affine line. More precisely:

2.32. **Corollary.** *Let B be a domain containing $\mathbb{Q}$ and let $A \in \text{KLND}(B)$. Consider the map $\pi : \operatorname{Spec} B \to \operatorname{Spec} A$ determined by $A \hookrightarrow B$.*

Then there exists a dense open set $U \subseteq \operatorname{Spec} A$ with the following property:

$$\begin{array}{ccc} \pi^{-1}(U) & \xrightarrow{\;\cong\;} & U \times \mathbb{A}^1 \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\text{projection}} & \\ & U & \end{array}$$

In particular, the general fiber of $\pi : \operatorname{Spec} B \to \operatorname{Spec} A$ is an $\mathbb{A}^1$.

Proof. Choose $D \in \text{LND}(B)$ such that $\ker D = A$. Since $D \neq 0$, there exists a preslice $s \in B$ of D. Let $\alpha = D(s) \in A \setminus \{0\}$ and define $U = \operatorname{Spec} A \setminus V(\alpha)$. As A is a domain and $\alpha \neq 0$, U is dense in $\text{Spec}(A)$. We have:

$$\begin{array}{ccc} B & \longrightarrow & B_\alpha \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_\alpha \end{array} \quad \Longleftrightarrow \quad \begin{array}{ccccc} \operatorname{Spec} B & \hookleftarrow & \pi^{-1}(U) & \xleftarrow{\;\cong\;} & \operatorname{Spec} B_\alpha \\ {\scriptstyle\pi}\downarrow & & {\scriptstyle\pi}\downarrow & & \downarrow \\ \operatorname{Spec} A & \hookleftarrow & U & \xleftarrow{\;\cong\;} & \operatorname{Spec} A_\alpha \end{array}$$

As $B_\alpha = (A_\alpha)^{[1]}$ by 2.31, we also have

$$\begin{array}{ccc} \text{Spec}(B_\alpha) & \xrightarrow{\;\cong\;} & \text{Spec}(A_\alpha) \times \mathbb{A}^1 \\ & \searrow \quad \swarrow{\scriptstyle\text{projection}} & \\ & \text{Spec}(A_\alpha) & \end{array}$$

so we obtain the desired conclusion. □

2.33. **Example.** Let $B = \mathbb{C}[X, Y, Z] = \mathbb{C}^{[3]}$ and $D \in \text{Der}_{\mathbb{C}}(B)$ defined by $D(X) = 0$, $D(Y) = X$ and $D(Z) = -2Y$. Then D is triangular, so $D \in \text{LND}(B)$. Let $A = \ker(D)$.

Observe that $D(B)$ is included in the ideal (X, Y) of B, so in particular D does not have a slice. However Y is a preslice of D, since $D(Y) = X \neq 0$ and $D^2(Y) = 0$. Then, according to 2.31, we have $B_X = (A_X)[Y] = (A_X)^{[1]}$. We would like to study the morphism $\pi : \operatorname{Spec} B \to \operatorname{Spec} A$ determined by $A \hookrightarrow B$, but for that we need to know exactly what A is. We claim:

$$A = \mathbb{C}[X, XZ + Y^2]$$

but we omit the proof ("$\supseteq$" is easy, "$\subseteq$" is more difficult). Observe that $A \cong \mathbb{C}^{[2]}$, since it is a $\mathbb{C}$-algebra generated by two elements, and since these two generators are algebraically independent over $\mathbb{C}$. So we have $\operatorname{Spec}(B) = \mathbb{A}^3$, $\operatorname{Spec}(A) = \mathbb{A}^2$ and

$$\pi : \mathbb{A}^3 \to \mathbb{A}^2, \qquad \pi(x, y, z) = (x, xz + y^2).$$

Now it is easy to calculate $\pi^{-1}(a, b)$ for any $(a, b) \in \mathbb{C}^2$, and we find:

$$\pi^{-1}(a,b) = \begin{cases} \text{an affine line,} & \text{if } a \neq 0 \\ \text{a union of two affine lines,} & \text{if } a = 0 \text{ and } b \neq 0 \\ \text{a nonreduced scheme,} & \text{if } (a,b) = (0,0). \end{cases}$$

Also observe that the open subset $U \subseteq \operatorname{Spec} A$ of 2.32 is the set $\{X \neq 0\}$ in $\mathbb{A}^2$ (see how U is obtained in the proof of 2.32).

As a final remark, note that $B \neq A^{[1]}$. Indeed, if B were a polynomial ring in one variable over A then *every* fiber of π would be an affine line, but we have seen that this is not the case. In particular, note the following obvious but important remark:

$$A \subset B,\ A = \Bbbk^{[2]} \text{ and } B = \Bbbk^{[3]} \quad \not\Longrightarrow \quad B = A^{[1]}.$$

3. Characterization of $\Bbbk^{[2]}$

Before proving the characterization we need to see two results. The first one can be found in standard textbooks on Commutative Algebra, and we omit the proof:

3.1. **Proposition.** *Let A be a domain containing a field $\Bbbk$ and such that* $\operatorname{trdeg}_{\Bbbk}(A) = 1$*. If A is contained in some $\Bbbk$-affine domain, then A is $\Bbbk$-affine.*

3.2. **Lemma.** *Let $A \subset B$ be integral domains, where B is finitely generated as an A-algebra. Suppose that $S^{-1}B = (S^{-1}A)^{[1]}$ where S is a multiplicative set of A satisfying the following condition: each element of S is a product of units of A and of prime elements p of A such that*

(i) *p is a prime element of B*
(ii) *$A \cap pB = pA$*
(iii) *A/pA is algebraically closed in B/pB.*

Then $B = A^{[1]}$.

Proof. Let $\mathbb{P}$ be the set of prime elements p of A satisfying (i), (ii), (iii) and let S_* be the multiplicative set of A whose elements are the finite products of elements of $\mathbb{P}$ (including the empty product $1 \in S_*$). The hypothesis implies that $S_*^{-1}B = (S_*^{-1}A)^{[1]}$. In other words, we may assume that $S = S_*$. Then each $s \in S$ is a product $s = p_1 \cdots p_k$ where $p_1, \dots, p_k \in \mathbb{P}$; the natural number k is uniquely determined by s, and is denoted $\ell(s)$ (by convention, $\ell(1) = 0$). This defines a set map $\ell : S \to \mathbb{N}$.

By assumption, the set $\mathcal{F} = \{ f \in B \mid S^{-1}B = (S^{-1}A)[f] \}$ is nonempty. Given $f \in \mathcal{F}$, we define for each $b \in B$ the natural number

$$\|b\|_f = \min \{ \ell(s) \mid s \in S \text{ and } sb \in A[f] \}.$$

This defines a map $\|\_\|_f : B \to \mathbb{N}$ with the following property: for any $b \in B$, $\|b\|_f = 0 \iff b \in A[f]$. Let us prove the following assertion :

(4) If $f \in \mathcal{F}$ and $b \in B$ are such that $\|b\|_f > 0$, then there exists $f_1 \in \mathcal{F}$ such that $\|b\|_{f_1} < \|b\|_f$ and $\forall_{\beta \in B}\ \|\beta\|_{f_1} \leq \|\beta\|_f$.

Indeed, choose $s \in S$ such that $sb \in A[f]$ and $\ell(s) = \|b\|_f > 0$ and choose $p \in \mathbb{P}$ such that $p \mid s$ (note that $p \mid s$ in A if and only if $p \mid s$ in B, since p satisfies (ii)). Choose $P(T) \in A[T]$ (T is an indeterminate) such that $P(f) = sb$. Then $\bar{P}(\bar{f}) = 0$ in B/pB, where $\bar{f} = f + pB \in B/pB$ and $\bar{P}(T) \in (A/pA)[T]$ is the image of $P(T)$ via the canonical epimorphism. If $\bar{P}(T)$ is the zero polynomial then p divides every coefficient of $P(T)$, so dividing $P(f) = sb$ by p both sides shows that $(s/p)b \in A[f]$, where $s/p \in S$; this contradicts the fact that $\ell(s) = \|b\|_f$, so we showed that $\bar{P}(T) \neq 0$. This together with $\bar{P}(\bar{f}) = 0$ and (iii) imply that $\bar{f} \in A/pA$, which means that there exists $a \in A$ such that $f - a \in pB$. Thus $f - a = pf_1$, where $f_1 \in B$. The obvious fact that $A[f] \subseteq A[f_1]$ has the following two consequences:

$$f_1 \in \mathcal{F} \quad \text{and} \quad \forall_{\beta \in B}\ \|\beta\|_{f_1} \leq \|\beta\|_f.$$

Moreover, $P(pT + a) = \alpha_0 + p\sum_{i=1}^{d} \alpha_i T^i$ for some $\alpha_0, \dots, \alpha_d \in A$, so $sb = P(f) = P(pf_1 + a) = \alpha_0 + p\sum_{i=1}^{d} \alpha_i f_1^i$. Since $p \mid s$ it follows that $p \mid \alpha_0$, so

$$(s/p)b = (\alpha_0/p) + \sum_{i=1}^{d} \alpha_i f_1^i \in A[f_1].$$

Consequently $\|b\|_{f_1} < \|b\|_f$ and the proof of (4) is complete.

The Lemma easily follows. Indeed, let $b_1, \dots, b_n$ be a finite set of generators for B as an A-algebra. For each $f \in \mathcal{F}$, define $N(f) = \sum_{i=1}^{n} \|b_i\|_f$. If $N(f) > 0$ then $\|b_i\|_f > 0$ for some i, and applying (4) to f and b_i shows that there exists $f_1 \in \mathcal{F}$ such that $N(f_1) < N(f)$. Thus we may consider $f_* \in \mathcal{F}$ such that $N(f_*) = 0$. Then $B = A[f_*]$. $\square$

Recall that a domain B of characteristic zero is said to be *rigid* if $\text{LND}(B) = \{0\}$. Note that B is rigid if and only if $\text{KLND}(B) = \varnothing$.

We may now prove the following result of Miyanishi:

3.3. **Theorem.** *Let $\mathbb{k}$ be an algebraically closed field of characteristic zero and let B be a $\mathbb{k}$-affine domain such that* $\text{trdeg}_{\mathbb{k}}(B) = 2$.

If B is a UFD, $B^* = \mathbb{k}^*$ and B is not rigid, then $B = \mathbb{k}^{[2]}$.

Proof. As B is not rigid, we may choose $A \in \text{KLND}(B)$. The proof consists in showing that $A = \mathbb{k}^{[1]}$ and that $B = A^{[1]}$. (So at the same time we will prove 3.4, see below.)

We have $\text{trdeg}_{\mathbb{k}}(A) = 1$ by 2.26, so A is $\mathbb{k}$-affine by 3.1.

As B is a UFD and (2.20) A is factorially closed in B, A is a UFD; as $B^* = \mathbb{k}^*$ and $A \subseteq B$, $A^* = \mathbb{k}^*$; thus 1.4 gives

$$A = \mathbb{k}^{[1]}.$$

By 2.26, we have $S^{-1}B = (S^{-1}A)^{[1]}$ where $S = A\setminus\{0\}$. We claim that each prime element p of A satisfies conditions (i–iii) of 3.2. Indeed, (i) and (ii) follow easily from the fact that A is factorially closed in B and A, B are UFDs. As $\Bbbk$ is an algebraically closed field and $A = \Bbbk^{[1]}$, we have $A/pA = \Bbbk$ and hence A/pA is algebraically closed in B/pB, i.e., (iii) holds. Thus 3.2 implies that $B = A^{[1]}$, so $B = \Bbbk^{[2]}$. ☐

The above proof has the following consequence (first proved by Rentschler, [10]):

3.4. **Corollary.** *Let $B = \Bbbk^{[2]}$ where $\Bbbk$ is an algebraically closed field of characteristic zero. Let $A \in \text{KLND}(B)$. Then:*

$$A = \Bbbk^{[1]} \quad \textit{and} \quad B = A^{[1]}.$$

In other words, there exist X, Y such that $B = \Bbbk[X, Y]$ and $A = \Bbbk[X]$.

Although our proof required that $\Bbbk = \bar{\Bbbk}$, note that 3.4 is valid for any field of characteristic zero.

4. Homogenization of locally nilpotent derivations

Throughout this section we fix a pair (B, G) where B is an integral domain and G is a $\mathbb{Z}$-grading of B (i.e., G is a direct sum decomposition $B = \oplus_{i\in\mathbb{Z}} B_i$ where each B_i is a subgroup of $(B, +)$ and where $B_i B_j \subseteq B_{i+j}$ for all $i, j \in \mathbb{Z}$).

An element of B is said to be *homogeneous* if it belongs to $\cup_i B_i$.

The grading G determines a map $\deg_G : B \to \mathbb{Z} \cup \{-\infty\}$ defined as follows. Given $f \in B$, write $f = \sum_{i\in\mathbb{Z}} f_i$ where $f_i \in B_i$ for all i ($f_i \neq 0$ for finitely many i). If $f \neq 0$, define $\deg_G(f) = \max\{\, j \in \mathbb{Z} \mid f_j \neq 0\}$; if $f = 0$, define $\deg_G(f) = -\infty$. Note that this map $\deg_G$ satisfies conditions (1), (2) and (3) of 2.14. We will often write deg instead of $\deg_G$.

The grading G also determines a map $\deg_G : \text{Der}(B) \to \mathbb{Z} \cup \{-\infty, \infty\}$, which we now define.

4.1. **Definition.** For any derivation $D : B \to B$ we define

$$\deg(D) = \deg_G(D) = \sup\{\deg(Df) - \deg(f) \mid f \in B \setminus \{0\}\} \ \in \mathbb{Z} \cup \{-\infty, \infty\}.$$

Note that $\deg(D) = -\infty$ if and only if $D = 0$, and that

$$(*) \qquad \forall_{f\in B\setminus\{0\}} \quad \deg(Df) \leq \deg(f) + \deg(D).$$

Moreover, $\deg(D)$ is the smallest element of $\mathbb{Z} \cup \{-\infty, \infty\}$ which makes $(*)$ true.

We want to understand which derivations satisfy $\deg(D) < \infty$. The next fact implies that if our graded domain B is a finitely generated algebra over a field of characteristic zero, then all $D \in \text{LND}(B)$ satisfy $\deg(D) < \infty$.

4.2. **Lemma.** *Let (B, G) be as before and suppose that $B = \Bbbk[h_1, \dots, h_n]$ where $\Bbbk$ is a field of characteristic zero and $h_1, \dots, h_n$ are nonzero homogeneous elements of B. Then for any $D \in \text{LND}(B)$ (and more generally[2] for any $D \in \text{Der}_{\Bbbk}(B)$),*

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

[2]This is more general because $\text{LND}(B) \subseteq \text{Der}_{\Bbbk}(B)$, by 2.22.

Proof. Let $D \in \mathrm{Der}_{\Bbbk}(B)$ and consider the map $\delta : B \to \mathbb{Z} \cup \{-\infty\}$ defined by $\delta(0) = -\infty$ and $\delta(f) = \deg(Df) - \deg(f)$ if $f \in B \setminus \{0\}$. Let $K = \max(\delta(h_1), \dots, \delta(h_n))$, then we have to show that $\delta(f) \le K$ for all $f \in B$.

It is easily verified that $\delta(fg) \le \max(\delta(f), \delta(g))$ for all $f, g \in B$. Consequently,

(5) $$\delta\big(\lambda h_1^{e_1} \cdots h_n^{e_n}\big) \le K, \text{ for any } \lambda \in \Bbbk^* \text{ and } e_i \in \mathbb{N}.$$

Also, if $f_1, \dots, f_m \in B$ satisfy

(6) $$\deg\big(\textstyle\sum_{i=1}^m f_i\big) = \max\{\deg f_i \mid 1 \le i \le m\}$$

then it is easy to check that

(7) $$\delta(f_1 + \cdots + f_m) \le \max(\delta(f_1), \dots, \delta(f_m)).$$

Next we claim that

(8) $$\text{if } H \text{ is a homogeneous element of } B \text{ then } \delta(H) \le K.$$

To prove this, we may assume that $H \neq 0$. Write $H = \sum_{i=1}^m f_i$ where each f_i is a monomial of the form $\lambda h_1^{e_1} \cdots h_n^{e_n}$ and where $\deg(f_i) = \deg(H)$ for all i. By (5), $\delta(f_i) \le K$ for all i. As $f_1, \dots, f_m$ satisfy (6), it follows from (7) that $\delta(H) \le \max(\delta(f_1), \dots, \delta(f_m))$, so (8) is proved.

Finally, consider an arbitrary element $f \neq 0$ of B. Write $f = f_1 + \cdots + f_m$ where the f_i are homogeneous of distinct degrees. As $f_1, \dots, f_m$ satisfy (6), (7) implies that $\delta(f) \le \max(\delta(f_1), \dots, \delta(f_m))$, and by (8) we have $\delta(f_i) \le K$ for all i. So $\delta(f) \le K$. ☐

4.3. **Exercise.** In the above proof, exactly where did we use the hypothesis that D is a $\Bbbk$-derivation?

4.4. **Example.** Let $B = \mathbb{C}[X, Y, Z] = \mathbb{C}^{[3]}$ and let G be the standard grading of B, i.e., $B_0 = \mathbb{C}$ and $X, Y, Z \in B_1$. Let $D \in \mathrm{Der}_{\mathbb{C}}(B)$ be defined by $D(X) = 0$, $D(Y) = X^3 + X + 1$, $D(Z) = Y^6 + X^2Y + X^4$. Then D is triangular, so $D \in \mathrm{LND}(B)$. By 4.2, $\deg(D) = \max\{-\infty - 1,\ 3 - 1,\ 6 - 1\} = 5$.

4.5. **Definition.** A derivation $D : B \to B$ is *G-homogeneous*, or *homogeneous with respect to G*, if there exists $d \in \mathbb{Z}$ satisfying

$$\forall_{i \in \mathbb{Z}}\ D(B_i) \subseteq B_{i+d}.$$

Since G is fixed throughout, we may simply say that D is homogeneous, without mentioning G. If D is homogeneous and $D \neq 0$ then the integer d is unique and $d = \deg(D)$. Notation:

$$\mathrm{Der}(B, G) = \{D \in \mathrm{Der}(B) \mid D \text{ is } G\text{-homogeneous}\}.$$

We now proceed to define a map

$$\{D \in \mathrm{Der}(B) \mid \deg(D) < \infty\} \longrightarrow \mathrm{Der}(B, G), \qquad D \longmapsto \tilde{D}.$$

We call $\tilde{D}$ the *homogenization* of D. The following notation is convenient: for each $j \in \mathbb{Z}$, let $p_j : B \to B_j$ be the canonical projection (if $f = \sum_{i \in \mathbb{Z}} f_i$, $f_i \in B_i$, then $p_j(f) = f_j$).

4.6. **Definition.** Let $D : B \to B$ be a derivation satisfying $\deg(D) < \infty$. Let $d = \deg(D) \in \mathbb{Z} \cup \{-\infty\}$. We define $\tilde{D} : B \to B$ as follows.
If $D = 0$ (i.e., $d = -\infty$), we simply define $\tilde{D} = 0$.
If $D \neq 0$ (i.e., $d \in \mathbb{Z}$), then for each $j \in \mathbb{Z}$ define the map

$$\tilde{D}_j : B_j \to B_{j+d}, \quad h \mapsto p_{j+d}(Dh);$$

then define $\tilde{D} : B \to B$ by $\tilde{D}(f) = \sum_j \tilde{D}_j(f_j)$ (where $f = \sum_{i\in\mathbb{Z}} f_i$, $f_i \in B_i$).

4.7. **Lemma.** *Let $D : B \to B$ be a derivation satisfying $\deg(D) < \infty$.*

(1) *$\tilde{D}$ exists, $\tilde{D} \in \mathrm{Der}(B, G)$ and $\deg(\tilde{D}) = \deg(D)$*
(2) *$\tilde{D} = 0 \iff D = 0$ (note in particular: $D \neq 0 \implies \tilde{D} \neq 0$)*
(3) *$D \in \mathrm{LND}(B) \implies \tilde{D} \in \mathrm{LND}(B)$.*

Proof. Exercise. □

4.8. **Example.** Let B, G and D be as in Example 4.4, then $\deg(D) = 5 < \infty$ so $\tilde{D}$ exists and $\tilde{D} \in \mathrm{LND}(B)$. The definition of $\tilde{D}$ gives:

$$\tilde{D}(X) = \tilde{D}_1(X) = p_6(DX) = 0$$
$$\tilde{D}(Y) = \tilde{D}_1(Y) = p_6(DY) = 0$$
$$\tilde{D}(Z) = \tilde{D}_1(Z) = p_6(DZ) = Y^6,$$

so $\tilde{D} = Y^6 \frac{\partial}{\partial Z}$.

5. Makar-Limanov invariant and rigid domains

For a domain B of characteristic zero, one defines the *Makar-Limanov invariant* of B to be

$$\mathrm{ML}(B) = \bigcap_{D \in \mathrm{LND}(B)} \ker D.$$

This is a factorially closed subring of B. Consequently: (i) $\mathrm{ML}(B)$ and B have the same units; (ii) if B is an algebra over a field $\mathbb{k}$ then $\mathbb{k} \subseteq \mathrm{ML}(B)$, so $\mathrm{ML}(B)$ is a subalgebra of B; (iii) if B is a UFD then so is $\mathrm{ML}(B)$.
Note that B is rigid if and only if $\mathrm{ML}(B) = B$.

5.1. **Exercise.** Verify that if $\mathbb{k}$ is a field of characteristic zero then $\mathrm{ML}(\mathbb{k}^{[n]}) = \mathbb{k}$.

We will use the technique of homogenization to prove a result of Makar-Limanov on rigid domains (5.3). For the proof we need:

5.2. **Lemma.** *Let B be a domain of characteristic zero and $D \in \mathrm{LND}(B)$. Suppose that $D(B)$ is included in the principal ideal aB, where $a \in B$. Then $a \in \ker D$ and $D = a\Delta$ for some $\Delta \in \mathrm{LND}(B)$.*

Proof. The claim is trivial if $D = 0$, so assume $D \neq 0$ (which implies $a \neq 0$). There is a unique set map $\Delta : B \to B$ which satisfies $D(x) = a\Delta(x)$ for all $x \in B$, and it is easy to see that $\Delta \in \mathrm{Der}(B)$. Write $A = \ker D$ (so $A = \ker \Delta$ as well). As D is locally nilpotent and nonzero, there exists $s \in B$ satisfying $Ds \neq 0$ and $D^2 s = 0$ (i.e., s is a preslice of D).

Then $a\Delta(s) = D(s) \in A \setminus \{0\}$, so $a \in A$ as A is factorially closed in B. The fact that $a \in \ker \Delta$ implies that $D^n(x) = a^n \Delta^n(x)$ for all $x \in B$ and $n \in \mathbb{N}$. It follows that Δ is locally nilpotent. □

5.3. **Proposition.** *Let A be an integral domain and a finitely generated algebra over a field of characteristic zero, and consider a polynomial ring $A[x]$ in one variable over A. If $\mathrm{ML}(A) = A$, then $\mathrm{ML}(A[x]) = A$.*

Proof. The inclusion $\mathrm{ML}(A[x]) \subseteq A$ is trivial, since $\ker(\frac{d}{dx}) = A$. To prove the reverse inclusion, consider $D \in \mathrm{LND}(A[x])$, $D \neq 0$; we have to show that $A \subseteq \ker D$.

Let $B = A[x]$ be endowed with its standard grading ($B_i = Ax^i$ if $i \geq 0$, $B_i = 0$ if $i < 0$) and let $d = \deg(D)$ (see 4.1). We consider two cases.

Case $\boldsymbol{d \leq 0}$. For every nonzero element $a \in A = B_0$ we have $\deg(Da) \leq \deg(a) + \deg(D) = 0 + d \leq 0$, so $Da \in A$. This shows that $D(A) \subseteq A$, so it makes sense to consider the restriction $D|_A : A \to A$, and clearly $D|_A \in \mathrm{LND}(A)$. Now the assumption $\mathrm{ML}(A) = A$ implies that $D|_A = 0$, so $A \subseteq \ker D$ and we are done in this case.

Case $\boldsymbol{d > 0}$. We show that this case is impossible. By 4.2 we have $d < \infty$, so $d \in \mathbb{Z}$ and we may consider the homogenization $\tilde{D}$ of D. By 4.7, $0 \neq \tilde{D} \in \mathrm{LND}(B)$ and $\tilde{D}$ is homogeneous of degree $d > 0$. For all $i \in \mathbb{N}$ we have $\tilde{D}(B_i) \subseteq B_{i+d} \subseteq x^d A[x]$, so $\tilde{D}(B) \subseteq x^d B$. By 5.2, $x^d \in \ker(\tilde{D})$ and $\tilde{D} = x^d \Delta$ for some $\Delta \in \mathrm{LND}(A[x])$. Since $d > 0$ and $x^d \in \ker(\tilde{D})$, we have $x \in \ker(\tilde{D})$ since $\ker(\tilde{D})$ is factorially closed in $A[x]$. Note that Δ is homogeneous of degree 0, so $\Delta(A) \subseteq A$, so $\Delta|_A \in \mathrm{LND}(A) = \{0\}$, hence $\tilde{D}(A) = 0$; this and $x \in \ker(\tilde{D})$ imply that $\tilde{D} = 0$, a contradiction. So the second case cannot occur.

This shows that $A \subseteq \mathrm{ML}(A[x])$, so $\mathrm{ML}(A[x]) = A$. □

6. Cancellation in dimension two

Result 5.3 has the following immediate consequence, which is interesting in connection with $\mathrm{CP}(n)$:

6.1. **Corollary.** *Let A be an algebra over a field $\Bbbk$ of characteristic zero. If $A^{[1]} = \Bbbk^{[n+1]}$ for some $n \geq 1$, then A is not rigid.*

Proof. $\mathrm{ML}(A^{[1]}) = \mathrm{ML}(\Bbbk^{[n+1]}) = \Bbbk$, so $\mathrm{ML}(A^{[1]}) \neq A$. By 5.3, $\mathrm{ML}(A) \neq A$. □

Observe that 6.1 proves implication (∗) of section 1 (just after 1.10). So CP(2) follows:

6.2. **Corollary.** *Let $\Bbbk$ be an algebraically closed field of characteristic zero. If B is a $\Bbbk$-algebra satisfying $B^{[1]} = \Bbbk^{[3]}$, then $B = \Bbbk^{[2]}$.*

Proof. As $B^{[1]}$ is a $\Bbbk$-affine UFD with trivial units, so is B. It is clear that $\mathrm{trdeg}_{\Bbbk}(B) = 2$ and 6.1 implies that B is not rigid. So $B = \Bbbk^{[2]}$ by 3.3. □

In the above result, the assumption that $\Bbbk$ is algebraically closed can be removed, thanks to the following result (cf. [7]):

6.3. **Kambayashi's Theorem.** *Let $K/\Bbbk$ be a separable field extension. If B is a $\Bbbk$-algebra such that $K \otimes_{\Bbbk} B = K^{[2]}$, then $B = \Bbbk^{[2]}$.*

6.4. **Corollary.** *Let* $\mathbb{k}$ *be any field of characteristic zero.*
If B *is a* $\mathbb{k}$*-algebra satisfying* $B^{[1]} = \mathbb{k}^{[3]}$*, then* $B = \mathbb{k}^{[2]}$*.*

Proof. Consider the algebraic closure $\bar{\mathbb{k}}$ of $\mathbb{k}$ and the $\bar{\mathbb{k}}$-algebra $\bar{B} = B \otimes_{\mathbb{k}} \bar{\mathbb{k}}$. Then

$$\begin{aligned}\bar{B}^{[1]} = \bar{B} \otimes_{\bar{\mathbb{k}}} \bar{\mathbb{k}}^{[1]} = B \otimes_{\mathbb{k}} \bar{\mathbb{k}} \otimes_{\bar{\mathbb{k}}} \bar{\mathbb{k}}^{[1]} = B \otimes_{\mathbb{k}} \bar{\mathbb{k}}^{[1]} \\ = B \otimes_{\mathbb{k}} \mathbb{k}^{[1]} \otimes_{\mathbb{k}} \bar{\mathbb{k}} = B^{[1]} \otimes_{\mathbb{k}} \bar{\mathbb{k}} = \mathbb{k}^{[3]} \otimes_{\mathbb{k}} \bar{\mathbb{k}} = \bar{\mathbb{k}}^{[3]},\end{aligned}$$

so $\bar{B} = \bar{\mathbb{k}}^{[2]}$ by 6.2, so $B = \mathbb{k}^{[2]}$ by Kambayashi's Theorem. □

7. Las variables

7.1. **Lema.** *Sean* $\mathbb{k}$ *un cuerpo y* $A = \mathbb{k}[X_1, \dots, X_n] = \mathbb{k}^{[n]}$*. Dados* $f_1, \dots, f_n \in A$*, las condiciones siguientes son equivalentes :*

(a) $\mathbb{k}[f_1, \dots, f_n] = A$
(b) *existe* $\theta \in \operatorname{Aut}_{\mathbb{k}}(A)$ *tal que* $\forall_i \;\; \theta(X_i) = f_i$*.*

Demostración. Dados $f_1, \dots, f_n \in A$, sea $\theta : A \to A$ el único homomorfismo de $\mathbb{k}$-álgebras tal que $\forall_i \;\; \theta(X_i) = f_i$. Si $\mathbb{k}[f_1, \dots, f_n] = A$ entonces θ es sobreyectivo, por tanto $\theta \in \operatorname{Aut}_{\mathbb{k}}(A)$ en virtud del hecho siguiente:

> *Si* R *es un anillo noetheriano y* $\varphi : R \to R$ *un homomorfismo sobreyectivo de anillos, entonces* φ *es biyectivo.*

Entonces, (a) $\Longrightarrow$ (b). El recíproco es obvio. □

7.2. **Definición.** Sea $A = \mathbb{k}^{[n]}$.

(1) Un *sistema de coordenadas* de A es un elemento $(f_1, \dots, f_n)$ de A^n tal que $\mathbb{k}[f_1, \dots, f_n] = A$.
(2) Una *variable* de A es un elemento $f \in A$ que pertenece a un sistema de coordenadas de A, es decir, un $f \in A$ satisfaciendo:

$$\text{existen } f_2, \dots, f_n \text{ tales que } A = \mathbb{k}[f, f_2, \dots, f_n].$$

Nota. Sea $f \in A = \mathbb{k}^{[n]}$. $\quad f$ es una variable de $A \Leftrightarrow A = \mathbb{k}[f]^{[n-1]}$.

7.3. **Ejemplo.** Sea $A = \mathbb{C}[X, Y, Z] = \mathbb{C}^{[3]}$. Cada uno de los triples siguientes es un ejemplo de sistema de coordenadas de A:

- (X, Y, Z)
- $(X,\ Y + X^2,\ Z + XY + Y^5)$
- $(X + (Y + X^2)^2 + (Z + XY + Y^5)^4,\ Y + X^2,\ Z + XY + Y^5)$

Entonces $X + (Y + X^2)^2 + (Z + XY + Y^5)^4$ es una variable de A.

Problema : Reconocimiento de las variables.
Dado $f \in A = \mathbb{k}^{[n]}$*, decidir si* f *es una variable de* A*.*

Sabemos que $\mathbb{k}[X_1, \dots, X_n]/(X_n) = \mathbb{k}^{[n-1]}$. Entonces:

7.4. **Observación.** *Dado* $f \in A = \Bbbk^{[n]}$,

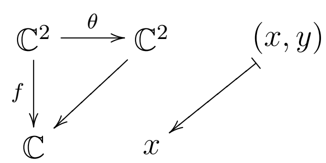
$$f \text{ es una variable de } A \implies A/(f) = \Bbbk^{[n-1]}.$$

Es interesante preguntar si el recíproco es válido :

7.5**. Teorema de Abhyankar-Moh-Suzuki.** (1975, véanse [1], [13])
Sea $\Bbbk$ *un cuerpo de característica* 0 *y sea* $f \in \Bbbk[X,Y] = \Bbbk^{[2]}$.
$\Bbbk[X,Y]/(f) = \Bbbk^{[1]} \implies f$ *es una variable de* $\Bbbk[X,Y]$.

Formulaciones geométricas del teorema de AMS ($\Bbbk = \mathbb{C}$)

- *Sea* $C \subset \mathbb{C}^2$ *una curva algebraica. Si* $C \cong \mathbb{C}^1$, *entonces existe un automorfismo de* $\mathbb{C}^2$ *que transforma* C *en el eje "*$x = 0$*".*
- *Cada inmersión* $\mathbb{A}^1 \to \mathbb{A}^2$ *es rectificable.*
- *Sea* $f : \mathbb{C}^2 \to \mathbb{C}$ *una aplicación algebraica. Si* $f^{-1}(0) \cong \mathbb{C}$, *entonces* $\exists$ *un automorfismo* θ *de* $\mathbb{C}^2$ *tal que*



Nota. El teorema de AMS no es válido en característica positiva. Por ejemplo, si $\mathrm{car}(\Bbbk) = 2$,

$$f = X + X^6 + Y^4$$

satisface $\Bbbk[X,Y]/(f) = \Bbbk^{[1]}$ pero no existe g tal que $\Bbbk[X,Y] = \Bbbk[f,g]$. La curva $C \subset \mathbb{A}^2_{\Bbbk}$ definida por $x + x^6 + y^4 = 0$ satisface $C \cong \mathbb{A}^1_{\Bbbk}$, pero no es rectificable. Decimos que C es una "recta salvaje". La clasificación de ésas es un problema abierto (véase [8]).

Conjetura de Abhyankar-Sathaye.
Sea $\Bbbk$ *un cuerpo de característica* 0 *y sea* $f \in A = \Bbbk^{[n]}$ $(n \geq 3)$.
$A/(f) = \Bbbk^{[n-1]} \implies f$ *es una variable de* A.

La conjetura todavía está abierta, para todo $n \geq 3$. El resultado siguiente es una solución parcial del caso $n = 3$.

7.6**. Teorema de Kaliman.** (2002, véanse [6], [3])
Sea $\Bbbk$ *un cuerpo de característica* 0 *y sea* $f \in \Bbbk[X,Y,Z]$. *Si*

$$\Bbbk[X,Y,Z]/(f - \lambda) = \Bbbk^{[2]} \text{ para un número infinito de } \lambda \in \Bbbk,$$

entonces f *es una variable de* $\Bbbk[X,Y,Z]$.

Consideramos otra vez el problema planteado por Russell en 1992:

> *Sea* $A = \mathbb{C}[X,Y,Z,T]/(X + X^2Y + Z^2 + T^3)$.
> *Demostrar que* $A \not\cong \mathbb{C}^{[3]}$ *como* $\mathbb{C}$*-álgebras.*

Este problema fue resuelto en 1994 por Makar-Limanov, después de que varios expertos hubieran intentado resolverlo sin éxito. Además, la solución de Makar-Limanov era bastante complicada (demostró que $\mathrm{ML}(A) = \mathbb{C}[x] \neq \mathbb{C}$, pero éste es un resultado difícil). Ahora vamos a ver que 7.6 permite una solución muy simple del problema de Russell. Demostremos que $A \ncong \mathbb{C}^{[3]}$ por contradicción:

7.7. ***Demostración.*** Consideremos el elemento $x \in A = \mathbb{C}[X, Y, Z, T]/(X + X^2Y + Z^2 + T^3)$, es decir, x es la imagen de la indeterminada X en el anillo cociente. Un simple cálculo demuestra que :

(i) $A/(x - \lambda) = \mathbb{C}^{[2]}$ para cada $\lambda \in \mathbb{C}^*$

(ii) $A/(x) \neq \mathbb{C}^{[2]}$.

Supongamos que $A \cong \mathbb{C}^{[3]}$. Entonces la condición (i) y el Teorema de Kaliman implican que x es una variable de A ; por tanto, $A/(x)$ debe ser $\mathbb{C}^{[2]}$, pero esto contradice (ii). □

7.8. **Ejercicio.** Verifiquen las afirmaciones (i) y (ii) en la demostración anterior.

Del Teorema de Kaliman (junto con otros resultados conocidos) se deduce una caracterización de $\mathbb{k}^{[3]}$ que ahora enunciamos :

7.9. **Teorema.** *Sea* $\mathbb{k}$ *un cuerpo algebraicamente cerrado de característica* 0*. Sea A un dominio de integridad finitamente generado como $\mathbb{k}$-álgebra. Supongamos que $f \in A$ satisface*

$$(*) \qquad A/(f - \lambda) = \mathbb{k}^{[2]} \text{ para un número infinito de } \lambda \in \mathbb{k}.$$

Entonces, la condición $A = \mathbb{k}^{[3]}$ es equivalente a

$$(**) \qquad A/(f - \lambda) = \mathbb{k}^{[2]} \text{ para cada } \lambda \in \mathbb{k}.$$

7.10. **Ejercicio.** Utilicen el Teorema de Kaliman para demostrar que, en el teorema 7.9, la condition $A = \mathbb{k}^{[3]}$ implica $(**)$. (*Nota:* Para demostrar que $(**)$ implica $A = \mathbb{k}^{[3]}$, se necesitan varios resultados que no hemos visto en este curso.)

Ejemplo: el polinomio de Vénéreau.

En su tesis (2001), Vénéreau planteó el problema siguiente:

> *Sea* $v = y + x^2z + xy^2t + xyz^2 \in B = \mathbb{k}[x, y, z, t] = \mathbb{k}^{[4]}$*, donde* $\mathbb{k}$ *es un cuerpo de característica* 0.
>
> *Decidir si v es una variable de B.*

Este problema todavía está abierto, después de 7 años. El problema es importante porque está relacionado con varios problemas y conjeturas (además del reconocimiento de las variables):

- Se tiene $B/(v - \lambda) = \mathbb{k}^{[3]}$ para todo $\lambda \in \mathbb{k}$. Por tanto, o bien v es una variable de B, o es un contraejemplo de la Conjetura de Abhyankar-Sathaye.

Sea $R = B[\sqrt{v}\,]$.

- No se sabe si $R = \mathbb{k}^{[4]}$ (Problema de caracterización de $\mathbb{k}^{[4]}$).
- Se tiene $R^{[1]} = \mathbb{k}^{[5]}$. Por tanto, o bien $R = \mathbb{k}^{[4]}$, o R es un contraejemplo del Problema de cancelación.

Además,

- v es una variable de $B^{[1]}$. Por tanto, o bien v es una variable de B, o es un contraejemplo de la conjetura siguiente:

  Sea $f \in A = \Bbbk^{[n]}$. Si existe m tal que f sea una variable de $A^{[m]} = \Bbbk^{[m+n]}$, entonces f es una variable de A.

Sea $A = \Bbbk[x, v] \subset B$.

- Se tiene $B^{[1]} = A^{[3]}$, pero no se sabe si $B = A^{[2]}$ (una variante del Problema de Cancelación).

8. The relation between locally nilpotent derivations and automorphisms

If B is not an integral domain, it may happen that a nonzero polynomial $f(T) \in B[T]$ have infinitely many roots in B. However note the following fact, which is needed in the proof of 8.3, below:

8.1. **Lemma.** *Let B be a ring and $f(T) \in B[T]$, where T is an indeterminate. If there exists a field $K \subseteq B$ which contains infinitely many roots of $f(T)$, then $f(T) = 0$.*

Proof. By induction on $\deg_T(f)$. The result is trivial if $\deg_T(f) \leq 0$, so assume that $\deg_T(f) > 0$. Pick $a \in K$ such that $f(a) = 0$; since $T - a \in B[T]$ is a monic polynomial, $f(T) = (T - a)g(T)$ for some $g(T) \in B[T]$ such that $\deg_T(g) < \deg_T(f)$. If $b \in K \setminus \{a\}$ is such that $f(b) = 0$, then $(b - a)g(b) = 0$ and $b - a \in B^*$, so $g(b) = 0$. So $g(b) = 0$ holds for infinitely many $b \in K$ and, by the inductive hypothesis, $g(T) = 0$. It follows that $f(T) = 0$. □

We have seen that the subset $\text{LND}(B)$ of $\text{Der}(B)$ is usually not closed under addition. However:

8.2. **Lemma.** *Let B be a ring. If $D_1, D_2 \in \text{LND}(B)$ satisfy $D_2 \circ D_1 = D_1 \circ D_2$, then $D_1 + D_2 \in \text{LND}(B)$.*

Proof. Let $D_1, D_2 \in \text{LND}(B)$ such that $D_2 \circ D_1 = D_1 \circ D_2$ and let $b \in B$. Choose $m, n \in \mathbb{N}$ such that $D_1^m(b) = 0 = D_2^n(b)$. The hypothesis $D_2 \circ D_1 = D_1 \circ D_2$ has the following three consequences:

$$\forall_{i \in \mathbb{N}}\ \forall_{j \geq n}\ \ (D_1^i \circ D_2^j)(b) = D_1^i(0) = 0,$$

$$\forall_{i \geq m}\ \forall_{j \in \mathbb{N}}\ \ (D_1^i \circ D_2^j)(b) = (D_2^j \circ D_1^i)(b) = D_2^j(0) = 0,$$

$$(D_1 + D_2)^{m+n-1} = \textstyle\sum_{i+j=m+n-1} \binom{m+n-1}{i} D_1^i \circ D_2^j,$$

so $(D_1 + D_2)^{m+n-1}(b) = 0$. Hence, $D_1 + D_2 \in \text{LND}(B)$. □

If $\theta : B \to B$ is an automorphism of a ring B, then the set $B^\theta = \{b \in B \mid \theta(b) = b\}$ is a subring of B called the *fixed ring* of θ. The following is another consequence of 2.13.

8.3. **Proposition.** *Let B be a $\mathbb{Q}$-algebra. Given $D \in \text{LND}(B)$, define the map*

$$\exp(D) : B \to B, \qquad b \longmapsto \textstyle\sum_{n \in \mathbb{N}} \frac{D^n(b)}{n!}.$$

(a) $\exp(D)$ *is an automorphism of the* $\mathbb{Q}$*-algebra* B

(b) *the fixed ring* $B^{\exp(D)} = \{ b \in B \mid \exp(D)(b) = b \}$ *is equal to* $\ker(D)$

(c) *if* $D_1, D_2 \in \text{LND}(B)$ *are such that* $D_2 \circ D_1 = D_1 \circ D_2$*, then* $D_1 + D_2 \in \text{LND}(B)$ *and*

$$\exp(D_1 + D_2) = \exp(D_1) \circ \exp(D_2) = \exp(D_2) \circ \exp(D_1)$$

Proof. If $D \in \text{LND}(B)$ then $\exp(D)$ is equal to the composite map $B \xrightarrow{\xi_D} B[T] \xrightarrow{e_1} B$, where ξ_D is defined in 2.12 and where e_1 is the evaluation homomorphism at $T = 1$, i.e., $e_1(f) = f(1)$. Since ξ_D is a ring homomorphism by 2.13, $\exp(D)$ is a ring homomorphism. As any ring homomorphism $B \to B$ is in fact a $\mathbb{Q}$-homomorphism, it follows that $\exp(D)$ is a homomorphism of $\mathbb{Q}$-algebras. Before proving that $\exp(D)$ is bijective, we prove assertion (c).

Consider $D_1, D_2 \in \text{LND}(B)$ such that $D_2 \circ D_1 = D_1 \circ D_2$. By 8.2, $D_1 + D_2 \in \text{LND}(B)$ so it makes sense to consider the ring homomorphism $\exp(D_1 + D_2) : B \to B$. As an abbreviation, we write $\epsilon_i = \exp(D_i)$ for $i = 1, 2$. If $b \in B$,

$$(\epsilon_1 \circ \epsilon_2)(b) = \epsilon_1 \Big(\textstyle\sum_{j \in \mathbb{N}} \frac{D_2^j(b)}{j!} \Big) = \sum_{j \in \mathbb{N}} \frac{1}{j!} \epsilon_1 \big(D_2^j(b) \big) = \sum_{j \in \mathbb{N}} \frac{1}{j!} \Big(\sum_{i \in \mathbb{N}} \frac{D_1^i \big(D_2^j(b) \big)}{i!} \Big)$$

$$= \textstyle\sum_{i,j \in \mathbb{N}} \frac{(D_1^i \circ D_2^j)(b)}{i!j!} = \sum_{n \in \mathbb{N}} \frac{1}{n!} \sum_{i+j=n} \binom{n}{i} (D_1^i \circ D_2^j)(b).$$

Since $D_2 \circ D_1 = D_1 \circ D_2$, we have $(D_1 + D_2)^n = \sum_{i+j=n} \binom{n}{i} D_1^i \circ D_2^j$ for each $n \in \mathbb{N}$ and consequently

$$(\epsilon_1 \circ \epsilon_2)(b) = \textstyle\sum_{n \in \mathbb{N}} \frac{1}{n!} (D_1 + D_2)^n(b) = \exp(D_1 + D_2)(b).$$

So $\exp(D_1) \circ \exp(D_2) = \exp(D_1 + D_2)$, and since $D_1 + D_2 = D_2 + D_1$ it follows that $\exp(D_1) \circ \exp(D_2) = \exp(D_2) \circ \exp(D_1)$, so assertion (c) is proved.

Consider $D \in \text{LND}(B)$. Since $(-D) \circ D = D \circ (-D)$, part (c) implies $\exp(D) \circ \exp(-D) = \exp(-D) \circ \exp(D) = \exp(0) = \text{id}_B$, so $\exp(D)$ is bijective and the proof of (a) is complete. It is clear that $\ker(D) \subseteq B^{\exp(D)}$. To prove the reverse inclusion, consider $b \in B$ such that $\exp(D)(b) = b$. Then for every integer $n > 0$ we have

$$b = (\exp D)^n(b) = \exp(nD)(b) = \textstyle\sum_{j=0}^{\infty} \frac{1}{j!} (nD)^j(b) = \sum_{j=0}^{\infty} \frac{1}{j!} D^j(b) n^j = b + f(n),$$

where we define $f(T) \in B[T]$ by $f(T) = \sum_{j=1}^{\infty} \frac{1}{j!} D^j(b) T^j$. As $\mathbb{Q} \subseteq B$ and $\mathbb{Q}$ contains infinitely many roots of $f(T)$, we have $f(T) = 0$ by 8.1, so in particular $D(b) = 0$, and we have shown that $B^{\exp(D)} \subseteq \ker(D)$. So (b) is proved. $\square$

8.4. **Exercise.** Let $B = \mathbb{C}[X, Y, Z] = \mathbb{C}^{[3]}$ and $D \in \text{Der}_{\mathbb{C}}(B)$ defined by $D(X) = 0$, $D(Y) = X$ and $D(Z) = -2Y$. Then D is triangular, so $D \in \text{LND}(B)$ and we may consider the $\mathbb{Q}$-automorphism $\exp(D) : B \to B$. Note that $\exp(D)$ is actually a $\mathbb{C}$-automorphism, because $\mathbb{C} \subset \ker(D) = B^{\exp(D)}$. Compute the images of X, Y and Z by $\exp(D)$.

8.5**.** Let B be a domain containing a field $\mathbb{k}$ of characteristic zero. Note that if $D \in \text{LND}(B)$ then $\exp(D) : B \to B$ is a $\mathbb{k}$-automorphism of B (because $\mathbb{k} \subseteq \ker(D) = B^{\exp(D)}$). So we have a well-defined set map,

$$\text{LND}(B) \longrightarrow \text{Aut}_{\mathbb{k}}(B), \qquad D \longmapsto \exp(D).$$

Of course this map is not a homomorphism, since $\text{LND}(B)$ is only a set. If we want to investigate the structure of the group $\text{Aut}_{\Bbbk}(B)$, then one possible approach would be to study the the subgroup $\langle E \rangle$ of $\text{Aut}_{\Bbbk}(B)$ generated by the set $E = \{\exp(D) \mid D \in \text{LND}(B)\}$. This explains why the two problems

- *describe the group* $\text{Aut}_{\Bbbk}(B)$
- *describe the set* $\text{LND}(B)$

are related. For instance, if $B = \Bbbk^{[n]}$ and $n > 2$ then it is an open problem to determine the structure of the group $\text{Aut}_{\Bbbk}(B)$, and it is believed that $\langle E \rangle$ is almost all of $\text{Aut}_{\Bbbk}(B)$ (it is conjectured that $\text{Aut}_{\Bbbk}(B)$ is generated by its subgroups $\langle E \rangle$ and $GL_n(\Bbbk)$); so in the case of $\Bbbk^{[n]}$ the two problems are very closely related. On the other hand if B is a ring such that $\text{LND}(B)$ is a small set (for instance if B is rigid) then, obviously, studying $\text{LND}(B)$ will not help to understand $\text{Aut}_{\Bbbk}(B)$.

8.6. **Lemma.** *Let B be a domain containing a field $\Bbbk$ of characteristic zero and consider the subgroup $\langle E \rangle$ of $\text{Aut}_{\Bbbk}(B)$ generated by the set $E = \{\exp(D) \mid D \in \text{LND}(B)\}$. Then $\langle E \rangle$ is a normal subgroup of $\text{Aut}_{\Bbbk}(B)$.*

Proof. If $\theta \in \text{Aut}_{\Bbbk}(B)$ and $D \in \text{LND}(B)$, then $\theta^{-1} \circ D \circ \theta \in \text{Der}(B)$ and $(\theta^{-1} \circ D \circ \theta)^n = \theta^{-1} \circ D^n \circ \theta$, so $\theta^{-1} \circ D \circ \theta \in \text{LND}(B)$. It is easily verified that $\theta^{-1} \circ \exp(D) \circ \theta = \exp(\theta^{-1} \circ D \circ \theta)$, so $\theta^{-1} E \theta \subseteq E$ holds for all $\theta \in \text{Aut}_{\Bbbk}(B)$. It follows that $\langle E \rangle \lhd \text{Aut}_{\Bbbk}(B)$. □

8.7. **Exercise.** Let B be a domain containing a field $\Bbbk$ of characteristic zero. Fix one particular derivation $D \in \text{LND}(B)$ and consider the map

$$\Bbbk \longrightarrow \text{Aut}_{\Bbbk}(B), \qquad \lambda \longmapsto \exp(\lambda D).$$

Show that this is a group homomorphism $(\Bbbk, +) \to \text{Aut}_{\Bbbk}(B)$. Show that this homomorphism is injective whenever $D \neq 0$.

8.8. **Exercise.** Let B be a domain containing a field $\Bbbk$ of characteristic zero. Fix one particular derivation $D \in \text{LND}(B)$ and consider the map

$$\Bbbk \times B \longrightarrow B, \qquad (\lambda, b) \longmapsto \lambda * b,$$

where we define $\lambda * b = \exp(\lambda D)(b)$ (so the operation $*$ depends on the choice of D). Show that this is an action of the group $(\Bbbk, +)$ on the $\Bbbk$-algebra B, i.e., verify the following conditions:

- $0 * b = b$ for all $b \in B$
- $(\lambda_1 + \lambda_2) * b = \lambda_1 * (\lambda_2 * b)$ for all $\lambda_1, \lambda_2 \in \Bbbk$ and all $b \in B$
- for each $\lambda \in \Bbbk$, the map $B \to B$, $b \mapsto \lambda * b$, is an automorphism of B as a $\Bbbk$-algebra.

Remark. Let $\Bbbk$ be an algebraically closed field of characteristic zero and let the symbol $G_a(\Bbbk)$ denote the group $(\Bbbk, +)$ viewed as an algebraic group. If X is an affine $\Bbbk$-variety, say $X = \text{Spec}\, B$ where B is an affine $\Bbbk$-domain, then one can consider the algebraic actions of $G_a(\Bbbk)$ on X (which are also called "G_a-actions" on X). Then one can show that there exists a bijection

$$\text{LND}(B) \longrightarrow \text{ set of actions of } G_a(\Bbbk) \text{ on } \text{Spec}(B).$$

This can be proved, essentially, by applying the functor Spec to the situation of exercises 8.7 and 8.8. Then the theory of locally nilpotent derivations of B is equivalent to that of G_a-actions on Spec(B), and one has a "dictionary" between the two theories. For instance, if $D \in \text{LND}(B)$ and α is the corresponding G_a-action on $\operatorname{Spec} B$, then the ring of invariants B^α of the action is equal to $\ker(D)$; and if I is the ideal of B generated by the set $D(B)$, then the closed subset of $\operatorname{Spec} B$ given by I is equal to set of fixed points of α.

References

1. S. Abhyankar and T.T. Moh, *Embeddings of the line in the plane*, J. reine angew. Math. **276** (1975), 148–166.
2. A. Crachiola and L. Makar-Limanov, *An algebraic proof of a cancellation theorem for surfaces*, preprint, IHES/M/05/29, 2005.
3. D. Daigle and S. Kaliman, *A note on locally nilpotent derivations and variables of* $k[x, y, z]$, to appear in Canad. Math. Bull., 2009.
4. T. Fujita, *On Zariski problem*, Proc. Japan Acad. **55A** (1979), 106–110.
5. R. Hartshorne, *Algebraic Geometry*, GTM, vol. 52, Springer-Verlag, 1977.
6. S. Kaliman, *Polynomials with general* $\mathbb{C}^2$*-fibers are variables*, Pacific J. Math. **203** (2002), 161–190.
7. T. Kambayashi, *On the absence of nontrivial separable forms of the affine plane*, J. Algebra **35** (1975), 449–456.
8. T.T. Moh, *On the classification problem of embedded lines in characteristic* p, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi NAGATA, Kinokuniya, 1987, pp. 267–279.
9. D. Mumford, *Abelian varieties*, Tata Inst. Fund. Res. Studies in Math., vol. 5, Tata Inst. Fund. Res., Bombay, 1970.
10. R. Rentschler, *Opérations du groupe additif sur le plan affine*, C. R. Acad. Sc. Paris **267** (1968), 384–387.
11. K.P. Russell, *On Affine-Ruled Rational Surfaces*, Math. Annalen **255** (1981), 287–302.
12. ______, *On a class of* $\mathbb{C}^3$*-like threefolds*, preliminary report, 1992.
13. M. Suzuki, *Propriétés topologiques des polynômes de deux variables complexes, et automorphismes algébriques de l'espace* C^2, J. Math. Soc. Japan **26** (1974), 241–257.
14. D. Wright, *On the jacobian conjecture*, Illinois J. of Math. **25** (1981), 423–440.