Polynomial Endomorphisms and Kernels of Derivations

Stefan Maubach

Polynomial Endomorphisms and Kernels of Derivations

een wetenschappelijke proeve op het gebied
van de Natuurwetenschappen, Wiskunde en Informatica

Proefschrift

ter verkrijging van de graad van doctor
aan de Katholieke Universiteit Nijmegen,
volgens besluit van het College van Decanen,
op gezag van de Rector Magnificus Prof.dr. C.W.P.M. Blom,
in het openbaar te verdedigen op
maandag 22 september 2003
des namiddags om 1:30 precies
door

Stefan jean Maubach

geboren op 29 december 1974 te Heerlen

Promotor:
Prof. dr. F.Keune
Copromotor:
Dr. A.van den Essen

Manuscriptcommissie:
Prof.dr. L.Makar-Limanov (Wayne State University, Detriot)
Prof.dr. A.Nowicki (Nicolas Copernicus University, Toruń)
Prof.dr. J-Ph.Furter (Université de La Rochelle, La Rochelle)

Contents

Preface

Teteretetèèè! Here it is, my thesis ! It feels really good to have finished it, and I am very proud with the result. But- I could have never done it without a lot of help !

First of all, I thank Arno van den Essen. I feel very, very lucky to have had him as my supervisor, he invested loads of time in me, and I could ask him any question I felt like at any time I wanted. He has the ability to really get the best out of people, and I am certain he got the best out of me.

Then I'd like to thank the reading committee consisting of professor Makar-Limanov, professor Furter, and professor Nowicki, who read the thesis and sent me numerous corrections. Tony Crachiola, who was no official member of the reading committe, should also be added to this list. Also I'd like to thank professor Makar-Limanov for giving me the opportunity to study several months under his supervision in Detriot.

I would also like to thank some of my colleagues: Joost Berson, Peter van Rossum, Engelbert Hubbers, Jan-Willem Bikker, Martijn Grooten, Daan Holtackers, Roel Willems, Luc Bouten, and all those I forget to mention now for the many interesting and stimulating conversations on my research topics.

Also I would like to thank my friends who have made my life wonderful outside of mathematics: since I am so afraid of forgetting anyone and regretting it for the rest of my life, I don't say any name (contrary

to what I promised), but you know I mean you, yes, you !

I would like to thank my family members, especially both my parents, for doing the things which parents do- you are not taken for granted !

I would like to thank the cats Sara and Pluisje for, eh- scratching my foot, eating the plants, or something.

And finally, words do not exist to express my gratitude on her support, mathematically and non-mathematically: Joyce, who has stolen my heart. You may keep it !

Summary

The title of this thesis is "Polynomial Endomorphisms and Kernels of Derivations" and, as it should be with titles, this is the shortest description of the subject of this thesis. So actually, there are two main subjects: "Polynomial Endomorphisms" on one side and "Kernels of Derivations" on the other. Let us start to talk about the latter.

Derivations itself are quite important in the theory of polynomial mappings. Many problems and conjectures can be stated in some way using derivations. For example the Cancellation Conjecture, the Linearisation Conjecture, and the infamous Jacobian Conjecture can all be reformulated in terms of derivations.

Often it is the kernel of a locally nilpotent derivation which is the object of interest. However, given a certain locally nilpotent derivation D on $k[X_1, , \ldots, X_n]$ (k is a field) it is hard to calculate the kernel. The kernel is rather simple and easy to find if such a derivation has a slice, i.e. an element s such that $D(s) = 1$. Such derivations are very well understood, and the calculation of their kernel is a piece of cake. Obviously, one is interested if a derivation has a slice. One of the requirements is that the ideal $(D(X_1), \ldots, D(X_n))$ equals (1). In dimension 2 this is a necessary and sufficient condition; in [BEM01] J.Berson, A. van den Essen and the author generalise this result to polynomial rings over arbitrary $\mathbb{Q}$-algebras. The result is very, very

general, as one can see in section 3.3.2: If R is just any $\mathbb{Q}$-algebra, D a locally nilpotent derivation on $R[X,Y]$, and $(D(X), D(Y)) = (1)$, then D has a slice S and $ker(D) = R[P]$ for some P.

But, life is more difficult than that any locally nilpotent derivation has a slice ! What to do if there is no slice, or one doesn't find one? Luckily, there exists an algorithm, the Essen-algorithm, which is able to calculate the kernel of any such locally nilpotent derivation. If such a derivation is finitely generated, then this algorithm gives generators of the kernel within finite time. Unfortunately, this "finite time" in practice turns out to be "impossibly long" if the derivation is not too easy, mainly due to the use of Gröbner bases. But, for a long time this was the only alternative to calculating a kernel.

In paragraph 3.2.2 and further another algorithm is presented (published in [Mau00b]), the homogeneous kernel algorithm. In some sense it is more general, since one doesn't need "locally nilpotent", only "derivation" (and even that can be weakened). At first there seems to be an offset in the fact that the algorithm can only be used on "homogeneous" derivations, but with a trick described in section 3.2.4 one is able to calculate kernels of general derivations (again locally nilpotent is not needed). Then, a big offset is that this algorithm is unable to decide whether one has calculated generators of the entire kernel or only a part of it. But, the nice thing is that a segment of the Essen-algorithm can be used for this.

There are two big advantages to the homogeneous algorithm. The first one is a practical one: calculations of generators tend to be much, much faster. A striking example of this is given in 3.2.5. The second one is that the algorithm, applied to a homogeneous derivation, calculates a *minimal number* of generators for the kernel. To explain the importance of such a thing, if one would be able to do the same for any (nonhomogeneous) locally nilpotent derivation, this would have strong consequences for the cancellation conjecture, very probably solving it

!

There is one thing both algorithms cannot help us with much: a derivation having infinitely generated kernel. Both algorithms cannot spew out an infinite list within a finite timeframe. Therefore these derivations are notorious objects, and a lot of work has gone in discerning in which dimensions they can occur. (Also since such derivations give negative answers to Hilbert's fourteenth problem.) It is known that derivations in dimension three and below always have finitely generated kernel. Examples in dimension five and higher exist of derivations having an infinitely generated kernel. All examples found first are of a rather simple form, they are triangular and monomial (sending monomials to monomials). The weird thing is that in the dimension four case no examples can be found which have this very simple form. In section 3.4.2 it is shown that their kernels have no more than four generators (published in [Mau00a]). The dimension four case is at the moment of writing still open.

Another very important use for locally nilpotent derivations is in distinguishing algebraic surfaces. To distinguish some algebraic subsets of some $\mathbb{C}^n$, say V and W, one has to determine whether the rings $\mathbb{C}[X_1, \ldots, X_n]/I(V)$ and $\mathbb{C}[X_1, \ldots, X_n]/I(W)$ are not isomorphic. In order to do this, one can define the ML invariant of a $\mathbb{C}$-algebra R as the intersection of all kernels of all nonzero locally nilpotent derivations, and the HD invariant as the smallest algebra containing the kernels of all nonzero locally nilpotent derivations. In formula:

$$ML(R) := \bigcap_{D \in \mathrm{LND}(R), D \neq 0} ker(D),\ HD(R) := \mathbb{C}[\bigcup_{D \in \mathrm{LND}(R), D \neq 0} ker(D)].$$

These invariants have succesfully been used to prove that certain surfaces are not isomorphic to some $\mathbb{C}^n$, as for example the surface $X_1^2 X_2 + X_1 + X_3^2 + X_4^3$ which is not isomorphic to $\mathbb{C}^3$.

Maybe at first sight it seems that the ML and HD invariant are equally strong, in the sense that both invariants are able to discern of the same surfaces whether they are isomorphic to some $\mathbb{C}^n$. Somewhat surprising (for the author) this is not the case: in section 3.7 joint work of T. Crachiola and the author shows that both invariants are different: sometimes the ML invariant is better, sometimes the HD invariant.

Ofcourse there are cases where both the ML and HD invariants are not strong enough, for example the ring $\mathbb{C}[X,Y,Z,T]/(XY+ZT-1)$ (or surface $XY+ZT-1$) has trivial ML as well as HD invariant. The search for stronger invariants is still on, but as one can easily make up a new invariant, it is often very difficult to calculate them.

An other approach to discern surfaces using derivations can be through the use of commuting locally nilpotent derivations. The first time the author heard from this idea was in a conversation with professor Makar-Limanov. In [Mau] and here in section 3.5 a conjecture is introduced, the Commuting Derivations Conjecture, short $CD(n)$: Let $D_1,\ldots,D_{n-1}$ be locally nilpotent derivations which are linearly independent over $C[X_1,\ldots,X_n]$ and which commute each other, then

$$\bigcap_{i=1}^{n-1} ker(D_i) = \mathbb{C}[f]$$

where f is a coordinate in $\mathbb{C}[X_1,\ldots,X_n]$. This conjecture is proved for $n=3$ in section 3.5. To stress the usefulness of this result, one can see that $XY+ZT-1$ is not isomorphic to $\mathbb{C}^3$, where the ML and HD invariants are unable to help you here. (A short proofsketch: suppose $R := \mathbb{C}[X,Y,Z,T]/(XY+ZT-1)$ is isomorphic to $\mathbb{C}[X_1,X_2,X_3]$. Now $X\partial_Y - Z\partial_T$ and $X\partial_Y - T\partial_Z$ are two commuting, locally nilpotent derivations, linearly independent over R, and the intersection of their kernel is $\mathbb{C}[X]$, and by $CD(3)$ we have that X is a coordinate in R, therefore $\mathbb{C}[Y,Z,T]/(ZT-1) = R/(X) \cong \mathbb{C}[X_1,X_2]$, a contradiction.)

Also, $CD(3)$ is used in section 3.5.3 to show that $p(X)Y+q(X,Z,T)$

is a coordinate if and only if $q(a, Z, T)$ is a coordinate for every a such that $P(a) = 0$. This result and the research involving it lead the author to the following notion: if $P(X)Y + q(X, Z, T)$ is a coordinate, this is almost something like saying that "$q(X, Z, T)$ is a coordinate modulo $P(X)$". In general, could one define the notion of "coordinate" for quotient rings $\mathbb{C}[X_1, \ldots, X_n]/I$ where I is some ideal? More on this interesting question is in section 3.6.

That on the first subject of the thesis, kernels of derivations. Let us proceed with the subject of polynomial endomorphisms. The simplest polynomial endomorphisms are linear maps, and they are the greatest inspiration for the theory of polynomial maps. Many mathematicians have wondered if lots of theorems which are true for linear maps are true for polynomial maps. Sometimes they cannot be generalized, sometimes they can, and sometimes it's unclear. For example, if we consider the coefficients of a linear map, then we can determine if the linear map is invertible by looking at a polynomial in the coefficients: the determinant of a linear map. If one attempts to generalize this result to general polynomial endomorphisms, one notices that it is exactly the Jacobian Conjecture.

A similar thing: for linear maps we have the Cayley-Hamilton theorem. We have a formula which has as input 1) the size of the linear map 2) the coefficients of the linear map, and then we get a polynomial $P(T)$ and if we put our map L "into" the polynomial we get $P(L) = 0$. Just as the determinant, Cayley-Hamilton is a magic formula. The author wondered if one can generalize this to (some) polynomial endomorphisms. So, if one has a polynomial map $F \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}[X_1, \ldots, X_n]$ satisfying $F(0) = 0$, can we find a polynomial $P(T)$ such that $P(F) = 0$?

For many polynomial maps we cannot find such a $P(T)$. If we can, we call them *dynamically trivial*, they are the subject of section 4.3. The results in this section are joint work of J.P.Furter and the

author. Dynamically trivial polynomial maps are reasonably "understandable", as the fact that the Jacobian Conjecture holds for these maps indicates. All two-dimensional dynamically trivial maps are classified in section 4.3.7, and apparently they all are conjugate to a triangular map. In this two-dimensional case, an actual generalisation of Cayley-Hamilton is given: Let $F \in \mathrm{End}_{\mathbb{C}}$ be a dynamically trivial map. This fact alone gives us a formula for a polynomial $P_F(T)$ such that $P_F(F) = 0$ (See theorem 4.3.22). Surprisingly, the formula only involves the linear part L of F, and its degree d:

$$P_F(T) := \prod_{\substack{0 \leq k \leq d-1 \\ 0 \leq m \leq d \\ (k,m) \neq (0,0)}} \left(T^2 - (detL^k)(TrL^m)T + det(L^{2k+m})\right).$$

Dynamically trivial maps in higher dimensions are not completely classified, though section 4.3.4 gives us some holds, linking exponents of locally finite derivations to invertible dynamically trivial maps.

A different topic is the group of automorphisms. Most of the time the group $Aut_{\mathbb{C}}\mathbb{C}[X_1, \ldots, X_n]$ is considered, and most of the time people want to see answers to questions about this group. However, in order to solve problems over $\mathbb{C}$, it is a good idea to look at more general $\mathbb{Q}$-algebras R and their automorphism groups $Aut_R R[X_1, \ldots, X_n]$. Why? If one is interested in a certain statements on the automorphism group over $\mathbb{C}$, it is often the case that this statement is true for low dimensions, but not true for general dimensions. So, finding a counterexample might be difficult. But, looking at low dimensional cases over more general rings R, can give a clue: first, find a counterexample for an unreduced $\mathbb{Q}$-algebra. If this works, see if you can generalize this to unreduced $\mathbb{Q}$-algebras. If that works, can you do it for a domain. And then, can you generalize to a field, like $\mathbb{C}$?

All in all, this motivates to consider problems over unreduced rings. So, one could attempt to consider the Linearisation Conjecture and the Cancellation Conjecture over unreduced rings. However, in section 4.1.1 and 4.1.2 it is shown that for both these conjectures one shouldn't bother to look at unreduced rings, as the statements are equivalent.

One other reason to look at unreduced rings, is an equivalent formulation of the Jacobian Conjecture in terms of the ring $R_m := \mathbb{C}[T]/(T^m)$. If one could understand the automorphism group of the ring $R_m[X_1, \ldots, X_n]$ well enough, the Jacobian Conjecture would be solved as a conesquence. Well, that big goal wasn't achieved, but a step was taken, showing that the automorphism group of $R_m[X_1, \ldots, X_n]$ is generated by the union of the three sets:
1) $Aut_{\mathbb{C}}(\mathbb{C}[X_1, \ldots, X_n])$ (a true subset of $Aut_{R_m} R_m[X_1, \ldots, X_n]$),
2) the set $\{\ (X_1 + c\bar{T}X_1, X_2, \ldots, X_n) \mid c \in \mathbb{C}\ \}$,
3) the set $\{\ (X_1 + \bar{T}X^d, X_2, \ldots, X_n) \mid d \in \mathbb{N}\ \}$.
(The result is a bit more general on the third set.) This result is given in section 4.1.3 and was published in [Mau02a].

Finally we will discuss the only paragraph that "doesn't contain $\mathbb{Q}$": paragraph 4.2. In this we look at the automorphism group $Aut_{\mathbb{F}}\mathbb{F}[X_1, \ldots, X_n]$ for $n \geq 2$ where $\mathbb{F}$ is a finite field. This group may actually have some applications in the Real World, as one may be able to encrypt data using such polynomial maps. We are interested in the bijections $\mathbb{F}^n \longrightarrow \mathbb{F}^n$ induced by these polynomial maps, like, do all bijections occur as a polynomial automorphism? In case $char(\mathbb{F}) \neq 2$ we can answer this question: yes, all bijections can occur as a polynomial automorphism, even as a tame map. In $char(\mathbb{F}) = 2$ we consider all bijections occuring as a tame polynomial automorphism. Surprisingly, we can only get *half* of the bijections: only the even ones. Note, this result is only for *tame* automorphisms. It is unclear if a polynomial automorphism in this $char(\mathbb{F}) = 2$ case is also always even, but no

odd[1] examples have been found up yet. But- there could be some very weird polynomial automorphism which could induce an odd bijection. If such a map would be found, this would give an extremely easy way to prove that this map is a counterexample to the Tame Generators Conjecture over a finite field.

[1] "Odd" has a double meaning here. Even mathematicians can be poets sometimes.

Samenvatting

De titel van dit proefschrift is "Polynomial Endomorphisms and Kernels of Derivations" (vertaald "Polynomiale Endomorfismen en Kernen van Derivaties"), en, zoals het hoort bij titels, is dit de kortste beschrijving van de inhoud van het proefschrift. Dus, er zijn twee onderwerpen: "Polynomiale Endomorfismen" en "Kernen van Derivaties". Laten we beginnen met het laatste.

Derivaties zijn erg belangrijk binnen het onderwerp Veeltermafbeeldingen. Veel problemen en vermoedens kunnen op de een of andere manier vertaald worden in "iets met derivaties[2]". Bijvoorbeeld, het Cancellation Vermoeden, het Linearisatie Vermoeden, en het beruchte Jacobi Vermoeden kunnen allemaal herformuleerd worden in termen van derivaties.

Vaak is de kern van een derivatie het onderwerp van interesse. Maar, gegeven een derivatie D op $k[X_1, , \ldots, X_n]$ (k een lichaam), is het in het algemeen moelijk om de kern uit te rekenen. In het geval dat de derivatie een slice heeft (i.e. een element s zodat $D(s) = 1$) valt het allemaal erg mee. Dus, het is duidelijk dat men geinteresseerd is of een derivatie een slice heeft. Een van de eisen hiervoor is dat het ideaal $(D(X_1), \ldots, D(X_n))$ gelijk is aan (1). In 2 variabelen is dit een nodig en voldoende eigenschap; in [BEM01] J.Berson, A. van den Essen en de schrijver veralgemeniseren dit resultaat naar veeltermringen

[2]In het algemeen heeft men het over *locaal nilpotente* derivaties.

over een willekeurige $\mathbb{Q}$-algebra. Dit resultaat is erg algemeen, zoals men kan zien in sectie 3.3.2: Als R een willekeurige $\mathbb{Q}$-algebra is, D een locaal nilpotente derivatie op $R[X,Y]$, en $(D(X), D(Y)) = (1)$, dan heeft D een slice S en $ker(D) = R[P]$ voor een zekere P.

Maar- het leven is moeilijker: niet elke locaal nilpotente derivatie heeft een slice. Wat als er geen slice is (of als je er geen vindt)? Gelukkig, er bestaat een algorithme, het Essen-algorithme, dat de kern van elke locaal nilpotente derivatie kan uitrekenen. Als een derivatie eindig veel voortbrengers heeft, dan geeft het Essen-algorithme voortbrengers van de kern binnen "Eindige Tijd". Echter, deze "Eindige Tijd" is in de praktijk nogal eens "Ongelooflijk Lang" als het een niet te eenvoudige derivatie is, vooral doordat het algorithme Gröbner bases in zijn berekeningen betrekt. Maar, voor een lange tijd was dit practisch de enige mogelijkheid om de kern uit te rekenen.

In paragraaf 3.2.2 en verder wordt een ander algorithme geintroduceerd (gepubliceerd in [Mau00b]), het homogene kern algorithme. In zeker zin is dit algorithme algemener, omdat men niet "locaal nilpotent" eist, alleen "derivatie" (en zelfs dat laatste kan verzwakt worden). Op het eerste gezicht lijkt er een behoorlijk nadeel te zijn omdat dit algorithme alleen homogene derivaties aankan, maar met een truuk beschreven in 3.2.4 kan men algemene derivaties aanpakken (wederom, locaal nilpotent is niet nodig). Nog een nadeel is dat het homogene algorithme niet kan beslissen of alle voortbrengers van een kern zijn gevonden. Maar, het mooie is dat een segment van het Essen-algorithme dit probleem kan verhelpen.

Er zijn twee grote voordelen van het homogene algorithme. Het eerste is een practisch voordeel: berekeningen zijn meestal veel, veel sneller. Een treffend voorbeeld is beschreven in 3.2.5. Het tweede is dat het algorithme, toegepast op homogene derivaties, als zij-effect een *minimaal aantal* voortbrengers van de kern berekent. Om het belang van zulks te benadrukken, als je zulks zou kunnen doen voor elke (niet-

homogene) locaal nilpotente derivatie, dan zou dit sterke consequenties voor het Cancellation Probleem hebben, en het hoogstwaarschijnlijk oplossen.

Er is een ding waar beide algorithmes redelijk machteloos zijn: een derivatie met een oneindig voortgebrachte kern. Beide algorithmes kunnen niet een oneindige lijst binnen een eindig tijdsbestek uitspugen. Daarom zijn deze derivaties beruchte objecten, en een boel werk is eraan besteed om te bepalen in welke dimensies ze kunnen voorkomen. (Ook, omdat zulke derivaties tegenvoorbeelden tegen Hilbert's 14e probleem geven.) Het is bekend dat derivaties in dimensie drie en lager altijd eindig voortgebrachte kern hebben. Voorbeelden van locaal nilpotente derivaties in dimensies vijf en hoger met oneindig voortgebrachte kern bestaan. Alle gevonden voorbeelden hebben een vrij simpele vorm, ze zijn namelijk op driehoeksvorm, en monomiaal (ze sturen monomen naar monomen). Het vreemde is dat in dimensie vier er niet zulke eenvoudige tegenvoorbeelden kunnen bestaan: in sectie 3.4.2 word bewezen dat de kernen van zulke derivaties niet meer dan vier voortbrengers kunnen hebben (gepubliceerd in [Mau00a]). Het algemene vierdimensionale geval is op het moment van schrijven nog steeds open.

Nog een onderwerp waar locaal nilpotente derivaties nuttig zijn is in het van elkaar onderscheiden van algebraische oppervlakten. Om twee algebraische oppervlakken in $\mathbb{C}^n$, zeg V en W, van elkaar te onderscheiden, moet men bepalen of de ringen $\mathbb{C}[X_1, \ldots, X_n]/I(V)$ en $\mathbb{C}[X_1, \ldots, X_n]/I(W)$ isomorf zijn. Om dit voor elkaar te krijgen, kan men de ML invariant van een $\mathbb{C}$-algebra R definieren als de doorsnijding van alle kernen van alle locaal nilpotente derivaties op R, en de HD invariant van een $\mathbb{C}$-algebra R als de kleinste deelalgebra die alle kernen van locaal nilpotente derivaties (ongelijk aan 0) bevat. In

formules:

$$ML(R) := \bigcap_{D\in \mathrm{LND}(R), D\neq 0} ker(D),\ HD(R) := \mathbb{C}[\bigcup_{D\in \mathrm{LND}(R), D\neq 0} ker(D)].$$

De invarianten waren succesvol in het bewijzen dat bepaalde oppervlakken niet isomorf waren met een $\mathbb{C}^n$, zoals bijvoorbeeld het oppervlak $X_1^2X_2 + X_1 + X_3^2 + X_4^3$ hetgeen niet gelijk is aan $\mathbb{C}^3$.

Misschien zou je op het eerste gezicht denken dat de ML invariant en de HD invariant even sterk zijn, in de zin dat ze van dezelfde oppervlakken zouden kunnen bepalen of ze gelijk zijn of niet. Maar enigszins verassend (voor de auteur) was dit niet het geval: in sectie 3.7 liet gemeenschappelijk werk van T. Crachiola en de auteur zien dat de invarianten verschillen: soms is de ML invariant beter, soms de HD invariant.

Natuurlijk zijn er gevallen waar de ML invariant en de HD invariant niet sterk genoeg zijn, bijvoorbeeld de ring $\mathbb{C}[X, Y, Z, T]/(XY + ZT - 1)$ (of oppervlak $XY + ZT - 1$) heeft een triviale ML en HD invariant. De zoektocht naar sterkere invarianten is nog steeds aan de gang. Het is vaak eenvoudig om een nieuwe invariant te verzinnen, maar het is erg lastig deze in practische gevallen uit te rekenen.

Een andere aanpak om oppervlaktes te onderscheiden door het gebruik van derivaties kan door het gebruik van commuterende locaal nilpotente derivaties. De eerste keer dat de auteur hiervan hoorde was in een gesprek met professor Makar-Limanov. In [Mau], en hier in sectie 3.5 een vermoeden is geintroduceerd, het Commuterende Derivaties Vermoeden, kort $CD(n)$: Zij $D_1, \ldots, D_{n-1}$locaal nilpotente derivaties die lineair onafhankelijk zijn over $C[X_1, \ldots, X_n]$ en die met elkaar commuteren. Dan

$$\bigcap_{i=1}^{n-1} ker(D_i) = \mathbb{C}[f]$$

waar f een coordinaat is in $\mathbb{C}[X_1, \ldots, X_n]$. Dit vermoeden is bewezen

voor $n = 3$ in sectie 3.5. Om het nut van dit resultaat aan te tonen, men kan zien dat $XY + ZT - 1$ niet isomorf is met $\mathbb{C}^3$, waar de ML en HD invariant tekort schieten. (Een korte bewijsschets: stel $R := \mathbb{C}[X, Y, Z, T]/(XY + ZT - 1)$ is isomorf met $\mathbb{C}[X_1, X_2, X_3]$. Nu, $X\partial_Y - Z\partial_T$ en $X\partial_Y - T\partial_Z$ zijn twee commuterende, locaal nilpotente derivaties, lineair onafhankelijk over R, en de intersectie van hun kernen zijn $\mathbb{C}[X]$. Gebruik makend van $CD(3)$ zien we dat X een coordinaat is in R, waardoor $\mathbb{C}[Y, Z, T]/(ZT-1) = R/(X) \cong \mathbb{C}[X_1, X_2]$, tegenspraak.)

Daarnaast, $CD(3)$ word gebruikt in sectie 3.5.3 om te laten zien dat $p(X)Y + q(X, Z, T)$ een coordinaat is d.e.s.d.a. $q(a, Z, T)$ is een coordinaat voor elke a die voldoet aan $P(a) = 0$. Dit resultaat, en het onderzoek dat eraan vooraf ging, leidde de auteur naar de volgende opmerking: als $p(X)Y + q(X, Z, T)$ een coordinaat is, dan is dat zoiets als zeggen dat "$q(X, Z, T)$ is een coordinaat modulo $p(X)$". In het algemeen, zou men een betekenis aan het begrip "coordinaat" voor quotient ringen $\mathbb{C}[X_1, \ldots, X_n]/I$ waar I een ideaal is maken? Meer over deze interessante vraag in sectie 3.6.

Dat over het eerste onderwerp van het proefschrift, kernen van derivaties. Laten we ons nu bezig houden met het onderwerp van veeltermafbeeldingen. De simpelste veeltermafbeeldingen zijn lineaire afbeeldingen (matrices), en deze zijn de grootste inspiratie voor het onderwerp veeltermafbeeldingen. Veel wiskundigen hebben zich van stellingen over lineaire afbeeldingen afgevraagd of ze op de een of andere wijze kunnen worden veralgemeniseerd voor veeltermafbeeldingen. Soms kan dat niet, soms wel, en soms is het niet duidelijk. Bijvoorbeeld, als je de coefficienten van een lineaire afbeelding bekijkt dan kun je de inverteerbaarheid van zo'n afbeelding bepalen door een bepaald polynoom in deze coefficienten uit te rekenen: de determinant van een lineaire afbeelding. Als iemand dit resultaat veralgemeniseert voor veeltermafbeeldingen, dan kom je bij het Jacobi Vermoeden uit.

Nog zoiets: voor lineaire afbeeldingen heb je de Cayley-Hamilton stelling. Dat is een formule met als invoer 1) de grootte van de lineaire afbeelding en 2) de coefficienten van de afbeelding. Dan is de uitvoer een polynoom $P(T)$ en als je je lineaire afbeelding daar "in" stopt, dan komt er 0 uit. Net zoals de determinant, Cayley-Hamilton is een magische formule. De auteur vroeg zich hiervan af of je dit kunt generaliseren voor (sommige) veeltermafbeeldingen. Dus, als iemand een veeltermafbeelding $F \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}[X_1, \ldots, X_n]$ met $F(0) = 0$, kunnen we een polynoom $P(T)$ vinden zodat $P(F) = 0$?

Voor veel veeltermafbeeldingen kan dat niet. Als dat wel kan, noemen we ze *dynamisch triviaal*, en ze zijn het onderwerp van studie in sectie 4.3. Het resultaat van deze sectie is werk van J.P.Furter en de auteur . Dynamisch triviale veeltermafbeeldingen zijn redelijk "begrijpelijk", zoals het feit dat het Jacobi Vermoeden waar is voor deze afbeeldingen beaccentueert. Alle tweedimensionale dynamisch triviale veeltermafbeeldingen zijn geclassificeerd in sectie 4.3.7, en blijkbaar zijn ze allen geconjugeerd aan een driehoeksafbeelding. In dit tweedimensionale geval word ook een echte generalisatie van Cayley-Hamilton gegeven: Zij $F \in \mathrm{End}_{\mathbb{C}}$ een dynamisch triviale afbeelding. Dit feit alleen al geeft ons een formule voor een polynoom $P_F(T)$ zodat $P_F(F) = 0$ (zie stelling 4.3.22). Verassenderwijs bevat de formule alleen de graad d van F en het lineaire deel L:

$$P_F(T) := \prod_{\substack{0 \leq k \leq d-1 \\ 0 \leq m \leq d \\ (k,m) \neq (0,0)}} \big(T^2 - (detL^k)(TrL^m)T + det(L^{2k+m})\big).$$

Dynamisch triviale afbeeldingen in hogere dimensies zijn niet geheel geklassificeerd, maar sectie 4.3.4 geeft wat aanknopingspunten: er worden links gelegd met exponenten van derivaties.

Een ander onderwerp is de automorfismen groep van een veeltermring. Meestal bekijkt men $Aut_{\mathbb{C}}\mathbb{C}[X_1, \ldots, X_n]$, en het is hierin dat men ook het meest in is geinteresseerd. Maar, om problemen voor deze automorfismengroep over $\mathbb{C}$ op te lossen, is het vaak een goed idee om naar meer algemene $\mathbb{Q}$-algebra's R en hun automorfismengroep $Aut_R R[X_1, \ldots, X_n]$ te kijken. Waarom? Als iemand geinteresseerd is in een bepaalde eigenschap van de automorfismen groep over $\mathbb{C}$, dan is het vaak het geval dat de groep deze eigenschap heeft in lagere dimensies, maar niet in hogere. Vaak is het dan ook moeilijk een tegenvoorbeeld te vinden. Maar, het bekijken van deze eigenschap in lage dimensies over algemenere ringen kan een idee geven: allereerst, vind een tegenvoorbeeld voor deze eigenschap over een ongereduceerde $\mathbb{Q}$-algebra. Als dat lukt, kijk of je dat naar een ongereduceerde $\mathbb{Q}$-algebra kunt terugbrengen. Als ook dat werkt, kun je het doen voor een domein misschien. En dan, generaliseer naar een lichaam, bv. $\mathbb{C}$.

Alles bijelkaar genomen motiveert dit om naar problemen over ongereduceerde ringen te kijken. Bijvoorbeeld zou je het Linearisatie Vermoeden en het Cancellatie Vermoeden over ongereduceerde ringen kunnen bekijken. Maar, in secties 4.1.1 en 4.1.2 word bewezen dat het in verband met deze twee problemen niet nodig is naar ongereduceerde ringen te kijken, want de betreffende beweringen zijn equivalent met de gereduceerde problemen.

Een andere reden om naar ongereduceerde ringen te kijken is een equivalente formulering van het Jacobi Vermoeden in termen van de ring $R_m := \mathbb{C}[T]/(T^m)$. Als je de automorfismen groep van de ring $R_m[X_1, \ldots, X_n]$ goed genoeg begrijpt, dan zou als gevolg het Jacobi Vermoeden opgelost kunnen worden. Welnu, dat doel was niet bereikt, maar een stap in de goede richting was gezet, door te laten zien dat de automorfisme groep van $R_m[X_1, \ldots, X_n]$ voortgebracht word door de vereniging van de drie verzamelingen:
1) $Aut_{\mathbb{C}}(\mathbb{C}[X_1, \ldots, X_n])$ (een deelverzameling van de automorfismengroep van $R_m[X_1, \ldots, X_n]$),

2) de verzameling $\{ (X_1 + c\bar{T}X_1, X_2, \ldots, X_n) \mid c \in \mathbb{C} \}$,
3) de verzameling$\{ (X_1 + \bar{T}X^d, X_2, \ldots, X_n) \mid d \in \mathbb{N} \}$.
(Het eigenlijke resultaat is iets meer algemeen, de derde verzameling mag anders zijn). Dit resultaat is beschreven in sectie 4.1.3 en is gepubliceerd in [Mau02a].

Als laatste behandelen we de enige sectie die "niet $\mathbb{Q}$ bevat": sectie 4.2. In deze bekijken we de automorfismen groep $Aut_{\mathbb{F}}\mathbb{F}[X_1, \ldots, X_n]$ waar $n \geq 2$ en $\mathbb{F}$ een eindig lichaam is. Deze groep zou toepassingen kunnen hebben in de Echte Wereld, daar zulke afbeeldingen gebruikt zouden kunnen worden om data te versleutelen. We zijn geinteresseerd in de bijecties $\mathbb{F}^n \longrightarrow \mathbb{F}^n$ die door zulke afbeeldingen geinduceerd worden. Kunnen alle bijecties eigenlijk voorkomen? In het geval dat $kar(\mathbb{F}) \neq 2$ kunnen we dit beantwoorden: ja, ze kunnen allen gemaakt worden, zelfs als tamme afbeelding. In $kar(\mathbb{F}) = 2$ bekijken we alle bijecties geinduceerd door tamme afbeeldingen. Verassenderwijs kunnen we nu slechts de *helft* van de bijecties maken: alleen de even bijecties. Merk op dat dit resultaat slechts voor tamme afbeeldingen geldt. Het is niet duidelijk of een willekeurige inverteerbare veeltermafbeelding in deze $kar(\mathbb{F}) = 2$ altijd een even bijectie is, maar geen oneven voorbeelden zijn gevonden op het moment van schrijven. Zo'n automorfisme zou ook erg vreemde eigenschappen hebben, het zou een eenvoudig tegenvoorbeeld geven voor het Tamme Voortbrengers Vermoeden over een eindig lichaam.

Chapter 1

Preliminaries

We assume that the reader has some affinity with commutative algebra. **Definitions** will be given **in bold text**.

1.1 Notations and definitions

In this thesis we will, unless stated otherwise, use the following notations:
R will be a commutative $\mathbb{Q}$-algebra. A will be an R-algebra. If we say that A is an R-domain, then we mean it to be an R-algebra which is a domain. k will often be used for a field. $R^{[n]}$ is an abbreviation of $R[X_1, \ldots, X_n]$; in this thesis it will be generally a real abbreviation of this, i.e. $R^{[3]} \cong R[Y_1, Y_2, Y_3]$ but not $R^{[3]} = R[Y_1, Y_2, Y_3]$. However, sometimes we will write down $R^{[2]}$ for $R[X, Y]$ and $R^{[3]}$ for $R[X, Y, Z]$. We will use the notation $\partial_X, \partial_Y, \ldots$ etc. for the maps $f \longrightarrow \frac{\partial f}{\partial X}, f \longrightarrow \frac{\partial f}{\partial Y}, \ldots$ In particular, we will also write ∂_i for ∂_{X_i}. Also, we will write $\mathcal{X}$ for $X_1, \ldots, X_n$, and $\hat{\mathcal{X}}_i$ as $X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n$, i.e. the list without X_i. Sometimes we will write small letters for big letters modulo something: if $\mathfrak{i}$ is some

ideal of $k[U,V]$, then $k[u,v] := k[U,V]/\mathfrak{i}$ and $u := U + \mathfrak{i}, v := V + \mathfrak{i}$. When $\alpha \in \mathbb{N}^n$ (or $\mathbb{Z}^n$) then $\mathcal{X}^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n}$. Elements of the form $r\mathcal{X}^\alpha$ for some $r \in R$ are called **monomials**.The elements of $R^{[n]}$ of the form X^α are called **terms**, but often they will be named monomials.

We will use the gothic letters $\mathfrak{p}, \mathfrak{q}$ etc. for ideals of some ring. Moreover, we will denote the nilradical of a ring R (i.e. the set of all nilpotent elements of a ring R) by $\mathfrak{n}(R)$ or just $\mathfrak{n}$.

A ring $A \subset B$ is called **factorially closed in B** if for any $b_1, b_2 \in B$ satisfying $b_1 b_2 \in A\{0\}$ we have $b_1 \in A$ as well as $b_2 \in A$.

If A is an R-algebra domain, K the fraction field of R, then $trdeg_R(A)$ is defined as $trdeg_K(Q(A))$.

1.2 Graded rings

Let k be a field, and A a k-algebra. A graded k-algebra A is a decomposition of A of the form $A = \oplus_{n\in\mathbb{Z}} A_n$ such that each A_n is a k-vector space and $A_n A_m \subseteq A_{n+m}$. If $A_n = \{0\}$ for each $n < 0$, we say that A is **positively graded**. On such a graded ring we have a **degree function**, *deg*, which sends each non-zero $a \in A$ to the unique integer d such that $a \in \oplus_{i=0}^{d} A_i$ but $a \notin \oplus_{i=0}^{d-1} A_i$. Sometimes d will be called the **weight** of a.

Similarly, we can define a multi-graded ring as a k-algebra A which has a decomposition of the form $A = \oplus_{\alpha\in\mathbb{Z}^q} A_\alpha$ where q is some positive integer. If we want to emphasise the integer q, then we can say A is a q-graded ring, or q-multi-graded ring. I.e. a 1-graded ring is just a "classical" graded ring. A **positively multi-graded ring** is a multi-graded ring A such that $A_\alpha = 0$ for all $\alpha \notin \mathbb{N}^q$. In case $a \in A_\alpha$ for some $\alpha \in \mathbb{Z}^q$ then we say that a is **homogeneous of (multi-)degree** α. We define the function **grad**, which is only defined on homogeneous components, as the mapping sending $a \in A_\alpha$ to α. In case $q = 1$ (i.e.

a normal grading) the function *grad* coincides with the function *deg* restricted to homogeneous elements.

Notice that if a ring A has two (different) gradings $A = \oplus A_i$ and $A = \oplus A_j$, then we can define a multi-grading on A by defining $A_{(i,j)} := A_i \cap A_j$. Similarly, one can join up several gradings to a multi-grading, or even several multi-gradings to a new multi-grading. And, of course, given a certain multi-grading on a ring, we can decompose it into several gradings on that ring.

In case $\beta \in \mathbb{N}^q$, we say $\alpha \leq \beta$ if $\alpha_i \leq \beta_i$ for every $i \in \{1, \ldots, q\}$. We define $\alpha < \beta \iff \alpha \leq \beta$ and $\alpha \neq \beta$; i.e. it does NOT mean "$\alpha_i < \beta_i$ for all $i \in \{1, \ldots, 1\}$".

Assuming that we have a multi-graded ring $A := \sum_{\alpha \in \mathbb{N}^q}$, and $\beta \in \mathbb{Z}^q$, we define the following notations:

$$\begin{aligned} A_{\leq \beta} &:= \textstyle\sum_{\alpha \leq \beta} A_\alpha, \\ A_{< \beta} &:= \textstyle\sum_{\alpha < \beta} A_\alpha. \end{aligned}$$

Example 1.2.1. If k is a field, then one can assign a grading to the ring $k^{[n]}$ by giving X_i weight $d_i \in \mathbb{Z}$; each monomial $\mathcal{X}^\alpha$ then is homogeneous of degree $\alpha_1 d_1 + \ldots + \alpha_n d_n$ (and this fixes the grading). Joining up several such gradings one gets a multi-grading which is fixed by the multi-degrees of the X_i. Here we also have that each monomial $\mathcal{X}^\alpha$ is homogeneous.

The case that all X_i have weight 1 we call the **standard grading** on $R^{[n]}$. ; if we talk about an unspecified grading on $R^{[n]}$, we mean the standard grading.

We say that a (multi-)grading on $k^{[n]}$ is a **monomial grading** if each $\mathcal{X}^\alpha$ is homogeneous.

1.3 Polynomial mappings

Let $F := (F_1, F_2, \ldots, F_m) \in R^{[n]^m}$. We call such an element in $R^{[n]^m}$ a **polynomial morphism** or **polynomial mapping**. . Such an element $F \in End(n)$ can also be seen as a mapping $R^n \longrightarrow R^m$ given by $(r_1, \ldots, r_n) \longrightarrow (F_1(r_1, \ldots, r_n), \ldots, F_m(r_1, \ldots, r_n))$. This mapping is also denoted by F, which may cause problems if $F \neq G$ in the first meaning, and $F = G$ in the second meaning. (For example (X, Y) and $(X^p, Y^p) \in \mathbb{F}_p[X, Y]^2$.) Another mapping, denoted by F^*, is the mapping $R^{[n]} \longrightarrow R^{[m]}$ sending $p(X_1, \ldots, X_n)$ to $p(F_1, \ldots, F_m)$.

In the literature the map "F^*" is often denoted by "F" too; in this theses we will occasionally make the same abuse of notation. However, caution is needed, since we actually have three maps, all denoted by F !

In case $n = m$ we can say **polynomial endomorphism**; the collection of polynomial endomorphisms we will denote by $\mathrm{End}_R(R^{[n]})$, $\mathrm{End}_R(n)$ or $\mathrm{End}(n)$ if there is no confusion about R. Notice thus that we identify $(R^{[n]})^n$ with $\mathrm{End}(n)$.

If $F \in R^{[n]^n}$ is such that there exists $G \in R^{[n]^n}$ which satisfies $F \circ G$ is the identity mapping, we say that F is a **polynomial automorphism**. The set of these mappings is denoted by $Aut_R(R^{[n]})$, or short, $Aut(n)$ if there is no confusion about R. An $F_1 \in R^{[n]}$ is called a **coordinate** if there exist $F_2, \ldots, F_n \in R^{[n]}$ such that $F := (F_1, \ldots, F_n) \in Aut_R(R^{[n]})$. Not everything is a coordinate, for example X_1^2 is not.

Furthermore, $Aff_R(R^{[n]^m})$ is the set of affine maps in $R^{[n]^m}$, i.e. maps of the form $L + r$ where L is a linear map $R^n \longrightarrow R^n$ and r is a vector in R^n.

1.4 The great conjectures

This section gives a few famous, or sometimes notorious, conjectures.

1.4.1 The jacobian conjecture

The jacobian conjecture is the most famous conjecture in the theory of polynomial mappings, and it is very very notorious in the sense that on a regular basis wrong proofs appear, some with obvious flaws, but some ingenious with a small error, but still wrong. In some sense it is the Big, Hulking Monster which lures Knights from everywhere to the Land of Polynomial Mappings, in an attempt to achieve fame and fortune by trying to defeat it. Well- with no further delay, we introduce:

The jacobian conjecture: Let $F \in \mathbb{C}^{[n]}$. Suppose $det(jac(F)) \in \mathbb{C}^*$. Then F is invertible.

We will denote the jacobian conjecture in dimension n by **JC(n)** . Thus the jacobian conjecture, if affirmatively answered, would give a rather easy test for a polynomial mapping if it is invertible or not. More on the jacobian conjecture can be found in the book [Ess00] and [BCW82] There are loads of equivalent formulations of the jacobian conjecture. One of them we will give now, taken from [Ess98] (or see [Ess00] corollary 2.3.8). Define $R_m := \mathbb{C}[t] = \mathbb{C}[T]/(T^m)$, and denote $T + (T^m)$ by t.

Theorem 1.4.1. *There is equivalence between:*

1. *$JC(n)$ is true.*
2. *For any $d \in \mathbb{N}$ there exists a bound $C(d)$ such that for any $m \in \mathbb{N}$ and any $F \in Aut_{R_m} R_m[X]$ satisfying $deg(F) = d$, $det(JF) = 1$ we have $deg(F^{-1}) \leq C(d)$.*

3. *For any $d, e \in \mathbb{N}$ there exists a bound $C(d, e)$ such that for any $m \in \mathbb{N}$ and any $F \in Aut_{R_m} R_m^{[n]}$ satisfying $deg(F) = d$, $det(JF) = 1 + N$ and $N^e = 0$ we have $deg(F^{-1}) \leq C(d, e)$.*

4. *For any $d \in \mathbb{N}$ there exists a bound $C(d)$ such that for any R_m-derivation $D \in \mathfrak{n}Der_{R_m} R_m^{[n]}$ satisfying $div(D) = 0$ and $deg(exp(D)) \leq d$ we have $deg(exp(-D)) \leq C(d)$.*

For the definition of $Der_R R^{[n]}$, $div(D)$, and the term "derivation", we refer to the beginning of the next chapter.

1.4.2 The linearisation conjecture

The linearisation conjecture is the following:

The linearisation conjecture: (LC(n)) Let $F \in \mathbb{C}^{[n]}$ such that $F^m = I$ for some m. Then there exists some $\varphi \in Aut(\mathbb{C}^{[n]})$ such that $\varphi F \varphi^{-1}$ is a linear map.

The linearisation conjecture has been affirmatively answered for n=2 (an easy consequence of the Jung-van der Kulk-theorem) but $n \geq 3$ is still open. For more information, see [Kra95] or [Ess00] chapter 9.

1.4.3 The Cancellation Conjecture

The cancellation conjecture, more oftenly referred to as "the cancellation problem", is the following:

The cancellation conjecture (algebraic formulation): (CC(n)) Let R be a ring such that $R[T] \cong \mathbb{C}^{[n]}$ some n. Then $R \cong \mathbb{C}^{[n-1]}$.

Another formulation is the following, which involves derivations.

The cancellation conjecture (derivation formulation): Let $D \in \mathrm{LND}(R^{[n]})$ having a slice. Then there exists $\varphi \in Aut_R(R^{[n]})$ and $f \in R^*$ such that $\varphi D \varphi^{-1} = f\partial_1$.

For more information on this conjecture, see [Ess00] or [Miy85].

1.5 Linear recurrent sequences

Let V be a $\mathbb{C}$-vectorspace. Let $\mathcal{U} := \{u_k\}_{k\in\mathbb{N}}$ be a sequence of elements $u_k \in V$. We say that $\mathcal{U} := \{u_k\}_{k\in\mathbb{N}}$ is a **linear recurrent sequence** (of V), short **l.r.s.** , if there exists $n \in \mathbb{N}^*$, and $a_0, \ldots a_{n-1} \in \mathbb{C}$, such that for all $k \in \mathbb{N}$

$$u_{k+n} = a_{n-1}u_{k+n-1} + \ldots + a_1 u_{k+1} + a_0 u_k.$$

With this in hand, one can define a **characteristic polynomial**[1] with respect to this l.r.s. :

$$P(T) := T^n - a_{n-1}T^{n-1} - \ldots - a_1 T - a_0.$$

Notice that a characteristic polynomial in should be monic, and that it doesn't has to be unique for a certain l.r.s. : if $a_{k+1} = a_k$ for all $k \in \mathbb{N}$ then also $a_{k+2} = -2a_{k-1} + 3a_k$, therefore $T - 1$ as well as $T^2 + 2T - 3$ are characteristic polynomials. The following lemma is well-known (see [CMP87] for details):

Lemma 1.5.1. *Let $P(T) := T^n - a_{n-1}T^{n-1} - \ldots - a_1 T - a_0$ be a monic polynomial in $\mathbb{C}[T]$ and let $P(T) := \Pi_{i=1}^m (T-\omega_i)^{r_i}$ be the decomposition into irreducible factors. If $\mathcal{U} := \{u_i\}_{i\in\mathbb{N}}$ is a l.r.s. then the following assertions are equivalent:*

[1] sometimes called "associated polynomial"

(i) *$P(T)$ is a characteristic polynomial for $\mathcal{U}$,*

(ii) *The sequence $\mathcal{U}$ is an element of the vectorspace spanned by the n l.r.s. $\{k^j\omega_i^k\}_{k\in\mathbb{N}}$ where $i \in \{0, 1, \ldots, m\}$ and $j \in \{0, 1, \ldots, r_i - 1\}$.*

In particular, if $P(T)$ has only single roots, $\{u_k\}_{k\in\mathbb{N}}$ is a $\mathbb{C}$-linear combination of the sequences $\{\omega_i^k\}_{k\in\mathbb{N}}$.

Define the term **semi-characteristic polynomial** $S(T)$ as a polynomial which is a $\mathbb{C}$-multiple of a characteristic polynomial, i.e. $S(T) = \lambda P(T)$ for some $\lambda \in \mathbb{C}$ and some characteristic polynomial $P(T)$. (i.e. "semi-characteristic" means "non-monic characteristic"). There are a few easy things which can be said about these (semi-)characteristic polynomials:

Lemma 1.5.2. *Let $\mathcal{U}$ be a l.r.s.*

(i) *If $P(T)$ is a (semi-)characteristic polynomial of $\mathcal{U}$, and $Q(T)$ any polynomial, then $P(T)Q(T)$ is also a semi-characteristic polynomial.*

(ii) *If $P(T)$ and $Q(T)$ are both (semi-)characteristic polynomials, then $\gcd(P(T), Q(T))$ is also a (semi-)characteristic polynomial for $\mathcal{U}$.*

A corollary of lemma 1.5.2 is:

Corollary 1.5.3. *If $\mathcal{U}$ is a l.r.s. , then the set of semi-characteristic polynomials for $\mathcal{U}$ form an ideal in $\mathbb{C}[T]$.*

A short proofsketch of the above: Take (one of) the lowest degree characteristic polynomial in this set of semi-characteristic polynomials, call it $P_{\mathcal{U}}$. By 1.5.2 part (ii) taking the g.c.d. of $P_{\mathcal{U}}$ with any other (semi-)characteristic polynomial will have the same number of roots

(counting multiplicity) as $P_{\mathcal{U}}$ has, by the minimality of $P_{\mathcal{U}}$. In the same way one can see that $P_{\mathcal{U}}$ is unique, and divides any semi-characteristic polynomial, and therefore it's an ideal.

A corollary of 1.5.3 is that there is a unique minimal characteristic polynomial.

Definition 1.5.4. Write $P_{\mathcal{U}}(T)$ for the minimal characteristic polynomial.

Now let us restrict ourselves to the case where we have a characteristic polynomial having no double roots.

Definition 1.5.5. We will say that $\mathcal{U} := \{u_k\}_{k\in\mathbb{N}}$ is a l.r.s. of type $\Omega = \{\omega_1, \ldots, \omega_m\}$ if there exist $\lambda_1, \ldots, \lambda_m \in V$ such that

$$u_k = \sum_{i=1}^{m} \lambda_i \omega_i^k.$$

If $\mathcal{U} := \{u_k\}_{k\in\mathbb{N}}$ and $\mathcal{V} := \{v_k\}_{k\in\mathbb{N}}$ are l.r.s, define $\mathcal{U} + \mathcal{V} := \{u_k + v_k\}_{k\in\mathbb{N}}$ and $\mathcal{U}\mathcal{V} := \{u_k v_k\}_{k\in\mathbb{N}}$. If Ω, Σ are two sets of elements in $\mathbb{C}$, define $\Omega\Sigma := \{\omega\sigma \mid \omega \in \Omega, \sigma \in \Sigma\}$. The following result is obvious.

Lemma 1.5.6. *If $\mathcal{U} := \{u_k\}_{k\in\mathbb{N}}$ (resp. $\mathcal{V} := \{v_k\}_{k\in\mathbb{N}}$) is a l.r.s. over $\mathbb{C}$ of type $\Omega = \{\omega_1, \ldots, \omega_m\}$ (resp. $\Sigma = \{\sigma_1, \ldots, \sigma_d\}$) then $\mathcal{U}+\mathcal{V}$ (resp. $\mathcal{U}\mathcal{V}$) is a l.r.s. of type $\Omega \cup \Sigma$ (resp. $\Omega\Sigma$). In particular, if $\mathcal{U}_1, \ldots, \mathcal{U}_r$ are of type Ω, then $\mathcal{U}_1\mathcal{U}_2\cdots\mathcal{U}_r$ is of type Ω^r.*

Chapter 2

Derivations

The aim of this chapter is threefold:
First, it is meant as a preparation for chapter 3.
Second, it contains some new results of its own.
Thirdly, it is meant as a (by no means complete) collection of interesting facts, known theorems, and entertaining things about derivations, especially locally nilpotent derivations.

Derivations are for a polynomial mappings researcher as a tennisracket for a tennisplayer. It is very difficult to score without them.

2.1 General derivations

2.1.1 Notations and preliminaries

A **derivation** on a ring A is an additive map $D : A \longrightarrow A$ satisfying the Leibniz rule: $D(ab) = aD(b) + bD(a)$ for all $a, b \in A$. If A is an R-algebra then an **R-derivation** on A is a derivation on A satisfying

$D(R) = 0$.

A derivation is called **locally nilpotent** if for all $a \in A$ there exists some $n \in \mathbb{N}$ such that $D^n(a) = 0$. A derivation is called **locally finite** if $\sum_{i\in\mathbb{N}} D^i(a)R$ is a finite R-algebra module for each $a \in A$. (i.e. in case R is a field, $\sum_{i\in\mathbb{N}} D^i(a)R$ is a finite dimensional R-vectorspace.) An element $s \in R$ is called a **slice** of a derivation D if $D(s) = 1$. The standard example of a locally nilpotent derivation having a slice is $\partial_{X_i} := \partial_i$ on $R^{[n]}$.

We will denote the set of all derivations on A by $\mathbf{DER(A)}$, and denote the set of R-derivations on A by $\mathbf{DER_R(A)}$. Similarly, we will define $\mathbf{LND(A)}$, $\mathbf{SLND(A)}$ as the set of all locally nilpotent derivations resp. all locally nilpotent derivations having a slice.

It is not very difficult to see that an R-derivation on $R^{[n]}$ can be written in the form $\sum_{i=0}^{n} a_i\partial_i$ where $a_i = D(X_i)$. In case $a_i \in R[X_{i+1}, \ldots, X_n]$ for all $i \in \{1, \ldots, n\}$ we say that the derivation is a **triangular derivation**.

Notice that it is very easy to extend a derivation on A to a polynomial ring over A, for example $A[X, Y]$, by defining $D(X) = D(Y) = 0$.

We define the **divergence** of a derivation $D \in \mathrm{DER}_R(R^{[n]})$, denoted $div(D)$, as

$$div(D) := \sum_{i=1}^{n} \frac{\partial D(X_i)}{\partial X_i}.$$

.

2.1.2 The $\exp TD$ map

Let $D \in \mathrm{DER}_R(A)$ for some R-algebra A. Define the map $\exp TD : A[[T]] \longrightarrow A[[T]]$ as the map sending a to $\sum_{n=0}^{\infty} \frac{1}{n!} D^n(a)T^n$.

Proposition 2.1.1.

1. $\exp TD$ *is a ring automorphism of* $A[[T]]$ *having inverse* $\exp T(-D)$.

2. *If D is locally nilpotent, then* $\exp TD$ *induces a ring automorphism of* $A[T]$ *having inverse* $\exp T(-D)$.

Proof. For a proof of (1) we refer to [Ess00] prop. 1.2.14. To prove case (2), notice that $\exp TD$ is a ring homomorphism, since for every $a \in A$ $\sum_{n=0}^{\infty} \frac{1}{n!} D^n(a)T^n$ is a finite sum since $D^n(a) = 0$ for high enough n. The same holds for $\exp T(-D)$, which is the inverse of $\exp TD$ on $A[[T]]$, but hence also on $A[T]$. Thus $\exp TD$ is invertible, hence an automorphism. □

2.1.3 Properties of $D_{\mathfrak{pq}}$ derived from $D_{\mathfrak{p}}$ and $D_{\mathfrak{q}}$

Let $\mathfrak{p}$ be an ideal in R. We introduce some notations: the element $a + A\mathfrak{p}$ in $A/A\mathfrak{p}$ will be denoted by $a_{\mathfrak{p}}$ and the induced derivation on $A/A\mathfrak{p}$ by $D_{\mathfrak{p}}$.

Lemma 2.1.2. *Let D be an R-derivation on A. Let $\mathfrak{p}, \mathfrak{q} \subset R$ be ideals of R and suppose $D_{\mathfrak{p}}$ has a slice and $D_{\mathfrak{q}}$ is surjective. Then $D_{\mathfrak{pq}}$ has a slice.*

Proof. There exists $s \in A$ such that $D_{\mathfrak{p}}(s_{\mathfrak{p}}) = 1$ and hence $D(s) = 1+f$ for some $f \in \mathfrak{p}A$. Write $f = \sum f_i a_i$, where $f_i \in \mathfrak{p}$ and $a_i \in A$. Since $D_{\mathfrak{q}}$ is surjective there exists $F_i \in A$ such that $D(F_i) = a_i + h_i$, where $h_i \in \mathfrak{q}A$. Denote $S := s - \sum f_i F_i$.Then

$$\begin{aligned} D(S) = &\ D(s - \textstyle\sum f_i F_i) \\ = &\ D(s) - \textstyle\sum f_i D(F_i) \\ = &\ 1 + f - \textstyle\sum (f_i a_i + f_i h_i) \\ = &\ 1 - \textstyle\sum f_i h_i, \end{aligned}$$

and since $f_i h_i \in \mathfrak{pq}A$ we have $D_{\mathfrak{pq}}(S_{\mathfrak{pq}}) = 1$. □

Lemma 2.1.3. *Let $D_{\mathfrak{p}_i}$ be surjective for the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset R$. Then $D_{\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n}$ is also surjective.*

Proof. It is enough to show that if $D_{\mathfrak{p}}, D_{\mathfrak{q}}$ are surjective then $\mathcal{D}_{\mathfrak{pq}}$ is too. Let $a \in A$ be arbitrary. There exists $b \in A$ such that $D_{\mathfrak{p}}(b_{\mathfrak{p}}) = a_{\mathfrak{p}}$, hence $D(b) = a + i$ where $i \in \mathfrak{p}A$. Write $i = \sum i_k c_k$ where $i_k \in \mathfrak{p}$, $c_k \in A$. Then for every c_k there exists some d_k such that $D(d_k) = c_k + j_k$ for some $j_k \in \mathfrak{q}A$ since $D_{\mathfrak{q}}$ is surjective. Now $D(b - \sum i_k d_k) = a - \sum i_k j_k$. Since $\sum i_k j_k \in \mathfrak{pq}A$ we are done. □

Lemma 2.1.4. *Let D be a locally nilpotent R-derivation on A. If $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_n \subset R$ are ideals of R and $D_{\mathfrak{p}_i}$ has a slice for all i, then $D_{\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n}$ has a slice too.*

Proof. It is enough to show that if $D_{\mathfrak{p}}, D_{\mathfrak{q}}$ both have a slice then $D_{\mathfrak{pq}}$ has one too. By corollary 2.2.5, $D_{\mathfrak{p}}$ and $D_{\mathfrak{q}}$ are surjective. By lemma 2.1.4 $D_{\mathfrak{pq}}$ is surjective. In particular, $D_{\mathfrak{pq}}$ has a slice. □

Lemma 2.1.5. *If $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n \subset R$ are ideals of R and $D_{\mathfrak{p}_i}$ is locally nilpotent for all i, then $D_{\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n}$ is locally nilpotent too.*

Proof. It is enough to show that if $D_{\mathfrak{p}}, D_{\mathfrak{q}}$ are locally nilpotent, then $D_{\mathfrak{pq}}$ is locally nilpotent. Let $a \in A$. One knows there exists $N \in \mathbb{N}$ such that $D^N_{\mathfrak{p}}(a_{\mathfrak{p}}) = 0$, hence $D^N(a) = \sum i_k b_k$ where $i_k \in \mathfrak{p}, b_k \in A$. Now there exists $M_k \in \mathbb{N}$ such that $D^{M_k}(b_k) \in \mathfrak{q}A$. Let $M := \max_k(M_k)$. Then $D^{N+M}(a) = D^M(\sum i_k b_k) = \sum i_k D^M(b_k) \in \mathfrak{pq}A$. □

Lemma 2.1.6. *Let $\mathfrak{p} \subset R$ be an ideal of R and $D \in \mathrm{DER}_R(R^{[n]})$. Suppose that D is surjective and that $r \in R^{[n]}$ is such that $D_{\mathfrak{p}}(r \mod \mathfrak{p}) = 0$. Then there exists $\tilde{a}$ such that $\tilde{a} \equiv a \mod p$ and $D(\tilde{a}) = 0$.*

Proof. There exists $p_i \in \mathfrak{p}$ and $r_i \in R^{[n]}$ such that $D(a) = \sum p_i r_i$. Since D is surjective, we find some $h_i \in R^{[n]}$ such that $D(h_i) = r_i$. We can now take $\tilde{a} := a - \sum p_i h_i$. □

In the lemma below write η for the nilradical of some ring R, and $\bar{D}, \bar{p}$ etc. as abbreviations of $D \mod \eta R^{[n]}, p \mod \eta R^{[n]}$.

Lemma 2.1.7. *Let R be a noetherian ring, and $D \in \mathrm{DER}_R(R^{[n]})$. Suppose that D is surjective, and that $p \in R$ such that $\bar{D}(\bar{p}) = 0$. Then there exists $\tilde{p} \in R$ such that $\bar{\tilde{p}} = \bar{p}$ and $D(\tilde{p}) = 0$.*

Proof. An easy corollary of the previous lemma. □

2.1.4 Derivations on graded rings

Let D be an R-derivation on a graded R-algebra A. A derivation is called a **homogeneous derivation** of degree d if $D(A_n) \subseteq A_{n+d}$ for all $n \in \mathbb{Z}$. If A is multi-graded, D is homogeneous if it is homogeneous on every grading derived from the multi-grading. On the other hand, if one starts with a derivation D on an R-algebra A, one may try to find a grading on A such that D is homogeneous. Such a grading is called a D-grading and we can split them into three cases:

- A **D-invariant grading** satisfies $D(A_n) \subseteq A_n$. For example $X\partial_X$ on $R[X]$.
- A **D-decreasing grading** satisfies $D(A_n) \subseteq A_{n-m}$ for some positive integer m. For example ∂_X on $R[X]$ with the standard grading.
- A **D-increasing grading** satisfies $D(A_n) \subseteq A_{n+m}$ for some positive integer m. For example $X^2\partial_X$ on $R[X]$ with the standard grading.

2.2 Locally nilpotent derivations

2.2.1 Locally finite derivations

Let k be a field, and $A := k^{[n]}$. Let $D \in \mathrm{DER}(A)$. Define V_a as the k-vectorspace spanned by $a, D(a), D^2(a), \ldots$. As we already defined,

D is a locally finite derivation if and only if V_a is a finite k-vectorspace for all $a \in A$.

Example 2.2.1. $D := (X + f(Y,Z))\partial_X + (Y + g(Z))\partial_Y + Z\partial_Z$ is a locally finite derivation on $k[X,Y,Z]$ for any $f \in k[Y,Z], g \in k[Z]$.

A locally finite derivation is rather handable, for one can always restrict the derivation to the finite dimensional vectorspaces V_a. For example, the map $\exp(D) : A \longrightarrow A$ is well-defined:

Lemma 2.2.2. *Let D be a locally finite derivation. Then $\exp(D) : A \longrightarrow A$ is an invertible polynomial map.*

Proof. Let $a \in A$. Then D is a linear map on the finite vectorspace V_a; denote the restriction of D to V_a by D_a. Then $\exp(D_a)$ is a well-defined map on V_a. Hence $\exp(D)$ is a well-defined map on A. The same holds for $\exp(-D)$. Notice that $\exp TD$ is an automorphism of $A[[T]]$ having inverse $\exp -TD$. Substituting $T = 1$ in $\exp TD$ and $\exp T(-D)$ gives the well-defined maps $\exp(D)$ and $\exp(-D)$. Furthermore, 2.1.1 tells us that $\exp TD \circ \exp T(-D)$ is the identity on $A[[T]]$. Now since the homomorphism $A[[T]] \longrightarrow A$ sending $T \longrightarrow 1$ commutes with $\exp TD$ and $\exp T(-D)$, it is easy to see that

$$\exp TD|_{T=1} \circ \exp T(-D)|_{T=1} = \big(\exp TD \circ \exp T(-D)\big)|_{T=1},$$

which shows the desired statement. □

Notice that a locally nilpotent derivation is a locally finite derivation. Just to mention here, there is another special type of locally finite derivation, the semisimple derivation, which is also often studied. We will refrain from giving a precise definition, and just give the typical example: $\lambda_1 X_1\partial_1 + \ldots + \lambda_n X_n\partial_n$ on $k^{[n]}$, where $\lambda_i \in k$. Any locally finite derivation D can be uniquely written as a sum of a locally nilpotent derivation and a semisimple derivation.

2.2.2 Kernels of locally nilpotent derivations

An important object connected with derivations, especially locally nilpotent derivations, is the **kernel of a derivation**, the set of all elements mapped to zero. It is denoted by $\mathbf{A^D}$, or occasionally by $ker(D)$. If one has a set of derivations $\mathcal{D} := \{D_1, \ldots, D_m\}$, then we denote $\mathbf{ker}(\mathcal{D}) = \mathbf{A}^{\mathcal{D}} := A^{D_1} \cap \ldots \cap A^{D_m}$.

Lemma 2.2.3. *Let A be a k-algebra where k is a field.*

1. *If D is a locally nilpotent k-derivation, then A^D is factorially closed in A.*

2. *If $\mathcal{D}$ is a finite set of locally nilpotent k-derivations on A then $A^{\mathcal{D}}$ is factorially closed in A.*

Proof. Part (1) can be found in [Ess00] 1.3.32.3. Part (2) follows from the following remark: if $A_1, A_2 \subset B$ are two rings factorially closed in B then $A_1 \cap A_2$ is also factorially closed in B , since if $b_1, b_2 \in B$ satisfying $b_1 b_2 \in A_1 \cap A_2$ implies $b_1 b_2 \in A_1$ as well as $b_1 b_2 \in A_2$, thus implies $b_1, b_2 \in A_1$ as well as $b_1, b_2 \in A_2$, thus $b_1, b_2 \in A_1 \cap A_2$. □

2.2.3 Locally nilpotent derivations having a slice

Some simple examples of locally nilpotent derivations are ∂_X on $R[X]$ and $Y\partial_X$ on $R[X, Y]$. A large class of locally nilpotent derivations is the set of triangular derivations.

For locally nilpotent derivations, the property of having a slice is a very nice property, as the following proposition suggests.

Proposition 2.2.4. *Let D be a locally nilpotent R-derivation on A having a slice $s \in A$. Then $A = A^D[s]$, a polynomial ring in s over A^D and $D = \partial/\partial s$ on $A^D[s]$.*

For a proof we refer to [GN67], [Wri81] or to [Ess00], proposition 1.3.21.

Corollary 2.2.5. *Let D be a locally nilpotent R-derivation on A. Then D has a slice in A if and only if D is surjective.*

Proof. Follows immediately from Proposition 2.2.4 since $\partial/\partial s$ on $A^D[s]$ is surjective. □

By the way, notice that not all locally nilpotent derivations have a slice: the derivation $Y\partial_X$ on $k[X,Y]$, for one, doesn't have a slice since $\mathrm{Im}(D) \subset Yk[X,Y]$ and thus is not surjective, misses 1 in its image, or one of your own favorite reasons. But, even if a derivation doesn't have a slice, one can use properties of derivations having a slice. Let A be some R-algebra and let D be a derivation on A. Suppose $p \in A$ such that $q := D(p)$ is no zero divisor and $D(q) = D^2(p) = 0$. Then p is called a **preslice** of D. A very appropriate name, considering we can "do something simple" to find a slice:

Lemma 2.2.6. *Suppose D is a locally nilpotent derivation on an R-algebra A having a preslice p. Let $q := D(p)$. Let $\tilde{A} := A[q^{-1}]$. Then D can be extended to $\tilde{A}$ and $\tilde{A}^D[p] = \tilde{A}$ and $D = q\partial/\partial p$.*

Proof. Since $D(q) = 0$ and q is no zero divisor it is easy to extend the derivation to $\tilde{A}$. Let $s := q^{-1}p$. Now s is a slice for D on $\tilde{A}$, namely $D(q^{-1}p) = q^{-1}D(p) = q^{-1}q = 1$. Thus we can use proposition 2.2.4 and we have $\tilde{A}^D[s] = \tilde{A}$ and $D = \partial/\partial s$. Now notice that $\tilde{A}^D[p] = \tilde{A}^D[s]$ and $\partial/\partial s = q\partial/\partial p$. □

2.2.4 Locally nilpotent derivations on domains

Notice that a nonzero locally nilpotent R-derivation on an R-domain A always has a preslice; since $D \neq 0$ we have $A^D \neq A$, and thus there exists an element $a \in A \backslash A^D$. Now $D(a) \neq 0$, but since D is locally

nilpotent, $D^n(a) = 0$ for some $n \geq 2$. Thus $D^{n-2}(a)$ is a preslice (since $D^{n-1}(a)$ is never a zero-divisor). Thus, for a locally nilpotent derivation on a domain we can always use the trick described in lemma 2.2.6.

Lemma 2.2.7. *Let D be a locally nilpotent derivation on an R-domain A containing $\mathbb{Q}$.*

1. *If $D(a) = \lambda a$ for some $\lambda, a \in A$ then either $a = 0$ or $\lambda = 0$.*
2. *If $D(ab) = 0$ then $D(a) = D(b) = 0$.*
3. *If $a, b \in A$ and $m, n \in \mathbb{N}$, $n, m \geq 2$, such that $c_1 a^n + c_2 b^m \in A^D \backslash \{0\}$ for some $c_i \in A^D$. Then $a \in A^D$ as well as $b \in A^D$.*
4. *If D is some derivation and $a \in A$. Then aD is locally nilpotent if and only if D is locally nilpotent and $D(a) = 0$.*

Proof. Part 1 and 2 are proven in [Ess00] proposition 1.3.32. Notice that part 2 is the same as saying A^D is factorially closed. Part 4 is proven in [Ess00] corollary 1.3.34. Part 3: We can find a preslice p. Let $q := D(p)$ and define $\tilde{A} := A[q^{-1}]$, $s := p/q$. Then $D = \partial/\partial s$, and $a = f(s), b = g(s)$ for some polynomials $f(T), g(T) \in \tilde{A}^D[T]$. We may assume that both degrees are ≥ 1. We also may assume that f and g have no common factor (for this common factor must be in A^D by part 2 and thus may be divided out). Now we need to reach a contradiction. Since

$$\begin{aligned} 0 = &\ D(c_1 a^n + c_2 b^m) \\ = &\ \tfrac{\partial}{\partial s}(c_1 f(s)^n + c_2 g(s)^m) \\ = &\ c_1 n f'(s) f(s)^{n-1} + c_2 m g'(s) g(s)^{m-1} \end{aligned}$$

we thus find that $f(s)^{n-1}$ divides $g'(s)$ and $g(s)^{m-1}$ divides $f'(s)$. Therefore $deg(g') \geq (n-1)deg(f)$ and $deg(f') \geq (m-1)deg(g)$. But now $deg(f) = deg(f')+1 \geq (m-1)deg(g)+1 \geq (m-1)((n-1)deg(f)+1)+1 = (m-1)(n-1)deg(f)+m$, which gives a contradiction. □

Proposition 2.2.8. (Vasconcelos) *Let $A \subset B$ be an integral extension where B is a domain and $\mathbb{Q} \subset A$. If D is a derivation on B such that $DA \subset A$ and the restriction $D|_A$ of D to A is locally nilpotent, then D is locally nilpotent on B.*

For the proof we refer to [Ess00], proposition 1.3.37.

2.2.5 Locally nilpotent derivations on $k^{[n]}$

The $k^{[2]}$ case:

Theorem 2.2.9. (Rentschler's theorem) *Let D be a non-zero locally nilpotent derivation on $k[X,Y]$ (k some field of characteristic 0). Then*

1. *there exists some $\varphi \in Aut_k k[X,Y]$ such that $\varphi^{-1} D \varphi = f(Y)\partial_X$ where $f(Y) \in k[Y]$,*
2. *$k[X,Y]^D = k[P]$ for some $P \in k[X,Y]$.*

For the proof, see [Ess00] theorem 1.3.48. Now, the $k^{[3]}$ case:

Theorem 2.2.10. (Miyanishi) *Let k be a field of characteristic 0. Let D be a non-zero locally nilpotent derivation on $k^{[3]}$. Then $ker(D) = k[f,g]$ for some $f, g \in k^{[3]}$ which are algebraically independent over k.*

See [Miy85] for a proof. Such theorems do not exist in $k^{[4]}$ and up, as the following example shows:

2.2.6 Equivalent derivations

We say that two derivations D_1, D_2 are **equivalent** if their kernels are equal: $A^{D_1} = A^{D_2}$. We will denote $\mathbf{D_1 \sim D_2}$.

Question 2.2.11. When are two locally nilpotent derivations equivalent?

Let us define a derivation D on a ring A to be an **irreducible derivation** if there exists no derivation D_1 and $a \in A$, $a \notin A^*$, such that $D = aD_1$. Now it is clear that:

Corollary 2.2.12. *Suppose D is a locally nilpotent derivation on a domain A. If there exists $a \in A, D_1 \in \mathrm{DER}(A)$ such that $D = aD_1$ then $D \sim D_1$ (and D_1 is locally nilpotent).*

The above corollary may imply that it is possible to find some irreducible D_1 such that $D \sim D_1$. However, we do need the properties "noetherian" and "domain", as the following two examples show (without going into much detail):

Example 2.2.13.
1. (domain necessary) Let $R := \mathbb{C}[e]/(e^2 - e)$ (a noetherian ring) and $D = e\partial_X$ on $R[X]$. Then D is reducible, but one can prove that there is no irreducible equivalent derivation.
2. (noetherian necessary) Let $S := \mathbb{C}[Y, Z, X_1, X_2, \ldots]$, and let

$$R := S\left[\begin{array}{c} \frac{Y}{X_1}, \frac{Y}{X_1X_2}, \frac{Y}{X_1X_2X_3}, \ldots \\ \\ \frac{Z}{X_1}, \frac{Z}{X_1X_2}, \frac{Z}{X_1X_2X_3}, \ldots \end{array}\right] \subseteq Q(S)$$

(a domain) and consider $D := Y\partial_{W_1} + Z\partial_{W_2}$ on $R[W_1, W_2]$. Then D is reducible, but there is no irreducible derivation $\tilde{D}$ such that $D = r\tilde{D}$ for some $r \in R$.

Lemma 2.2.14. *If A is a noetherian domain and $D \in \mathrm{LND}(A)$ then there exists some irreducible locally nilpotent derivation D_1 such that $D \sim D_1$.*

Proof. If D is not irreducible itself, then we can find some $a \in A$, $a \notin A^*$, such that $D(A) \subset aA$. Now it is possible that $D = aD_1$ where D_1 is reducible. Then $D_1 = bD_2$ and we could have started with ab in stead of a. So, in some sense, we want to take a "as large as possible". Define $V := \{aA \mid D(A) \subset aA\}$ a collection of principal ideals. Now following a strictly descending path as low down as possible in this collection gives a chain of ideals $a_1A \supset a_2A \supset \ldots$. Using the following lemma 2.2.15 we see that the intersection of these ideals is a principal ideal, say aA. Now there exists no $b \in A$ such that both $aA \supset bA$ as well as $D(A) \subseteq bA$ hold. Now define a map $D_1 : A \longrightarrow Q(A)$ by defining $D_1(f) = a^{-1}D(f)$. Since $D(f) \in aA$ for all $f \in A$ we even have $D_1 : A \longrightarrow A$. We leave it to the reader to check that D_1 is a derivation. By corollary 2.2.12 we know $D_1 \sim D$ and D_1 is locally nilpotent. D_1 is irreducible, for if $D_1(A) \subset bA$ for some $b \in A$ then $aA \supset abA$ and $D(A) \subset abA$. □

Lemma 2.2.15. *Let A be a noetherian domain and $(a_1) \supset (a_2) \supset (a_3) \supset \ldots$ a descending chain of principal ideals. Then the intersection of these ideals is a principal ideal.*

Proof. Take some element $x \neq 0$ in the intersection of the ideals (which we may assume to be nonzero). Write $x = b_n a_n$ for some $b_n \in A$. Notice $(b_1, b_2, \ldots, b_n) = (b_n)$. Now consider the chain of ideals $(b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \ldots$. Since A is noetherian this chain becomes stable i.e. there is some $n \in \mathbb{N}$ such that for all $m \in \mathbb{N}$ we find $c_m \in A^*$ such that $b_n = c_m b_{n+m}$. Thus $x = a_n b_n = a_{n+m} b_{n+m}$ gives $a_{n+m} = a_n c_m$ which tells us that the chain becomes stable. □

Remark 2.2.16. The above lemma does not hold for non-noetherian rings, in example 2.2.13.2 the ring R has a descending chain $(X_1) \supset (X_1X_2) \supset \ldots$ and one can show that its intersection is (Y, Z).

A nice way to make (general) derivations on $k^{[n]}$ is by taking $n-1$

arbitrary elements $f_1, \ldots, f_{n-1}$, and then define the **Jacobian derivation** s the map sending $g \in k^{[n]}$ to $J(f_1, \ldots, f_{n-1}, g)$ where

$$J(a_1, \ldots, a_n) := \det\big(Jac(a_1, \ldots, a_n)\big) = \det\big((\partial_j a_i)\big).$$

We leave it to the reader to check that such a map indeed is a derivation. In general, such a derivation is not locally nilpotent, as the example $J(XY, -) = -X\partial_X + Y\partial_Y$ on $k[X, Y]$ shows. The following theorem shows that there is always an equivalent Jacobian derivation if you consider $k^{[n]}$. See [ML98] for a proof.

Theorem 2.2.17. (Makar-Limanov) *Let D be any non-zero locally nilpotent derivation on $k^{[n]}$ where k is a field of characteristic 0. Let $f_1 \ldots, f_{n-1}$ be $n-1$ algebraically independent elements of $ker(D)$ and D_1 the jacobian derivation defined by*

$$D_1(h) := J(f_1, \ldots, f_{n-1}, h) \quad \text{for all} \quad h \in k^{[n]}.$$

Then there exist non-zero elements $a, b \in ker(D)$ such that $aD = bD_1$. In particular D_1 is locally nilpotent and $D \sim D_1$.

2.3 *Trdeg* of kernels of sets of derivations

In this section we will assume A to be an R-domain. As said before, if A is an R-algebra domain, K the fraction field of R, then $trdeg_R(A)$ is defined as $trdeg_K(Q(A))$. If no confusion is possible, we write $trdeg(A)$. The letter $\mathcal{D}$ will mean a finite list of derivations.

In case $D \neq 0$, locally nilpotent, and A is a k-domain over a field k of characteristic 0, it is well-known that $trdeg_k(A^D)) = trdeg_k(A) - 1$. (see 1.3.32 in [Ess00])

Question 2.3.1. Let $\mathcal{D}$ be a set of m locally nilpotent derivations. Under what assumptions on $\mathcal{D}$ can we predict anything about $trdeg(A^{\mathcal{D}})$?

Let's just look at some examples.

Example 2.3.2. Let R be a domain, and K its quotient field.

1. Let $1 \leq m \leq n$ and $\mathcal{D} := \{\partial_1, \partial_2, \ldots, \partial_m\} \subset \mathrm{LND}(A)$ where $A := R^{[n]}$. Then $trdeg(A^{\mathcal{D}}) = trdeg(R[X_{m+1}, \ldots, X_n]) = n - m$.

2. Let $\mathcal{D} := \{D_1, D_2\} \subset \mathrm{LND}(A)$ where $D_1 := X\partial_Y - \partial_Z, D_2 := \partial_X, A := R[X, Y, Z]$. Then

$$\begin{aligned} A^{\mathcal{D}} &= A^{D_1} \cap A^{D_2} \\ &= R[X, Y + XZ] \cap R[Y, Z] \\ &= R \end{aligned}$$

   and thus $trdeg(A^{\mathcal{D}}) = 0$.

3. Let $\mathcal{D} := \{D_1, D_2, D_3\} \subset \mathrm{LND}(A)$ where $D_1 := \partial_1, D_2 := \partial_2, D_3 := \partial_1 - \partial_2, A := R^{[n]}$. Then $trdeg(A^{\mathcal{D}}) = trdeg(R[X_3, \ldots, X_n])$ $= n - 2$.

These examples show that there is a priori no connection between $n - \#\mathcal{D}$ and $trdeg(A^{\mathcal{D}})$. Example 2 is an example where $n - \#\mathcal{D} > trdeg(A^{\mathcal{D}})$ can occur, and example 3 shows that $n - \#\mathcal{D} < trdeg(A^{\mathcal{D}})$ can occur as well. However, in case $trdeg(A^{\mathcal{D}}) > n - \#\mathcal{D}$ then we can simplify the set $\mathcal{D}$:

Lemma 2.3.3. *Suppose $trdeg(A^{\mathcal{D}}) > n - \#\mathcal{D}$. Then there exists a subset $\tilde{\mathcal{D}} \subset \mathcal{D}$ such that $A^{\tilde{\mathcal{D}}} = A^{\mathcal{D}}$ and $trdeg(A^{\tilde{\mathcal{D}}}) = n - \#\tilde{\mathcal{D}}$.*

Proof. Suppose $trdeg(A^{\tilde{\mathcal{D}}}) > n - \#\tilde{\mathcal{D}}$. It suffices to find a strict subset $\mathcal{D}'$ of $\mathcal{D}$ which satisfies $A^{\mathcal{D}} = A^{\mathcal{D}'}$. Consider the chain $A \supseteq A^{D_1} \supseteq A^{D_1, D_2} \supseteq \ldots \supseteq A^{\mathcal{D}}$. The transcendence degree can only decrease by an integer or stay equal each step. Since $trdeg(A^{\mathcal{D}}) > n - \#\mathcal{D}$

we must have equality of transcendence degrees somewhere in this chain. In other words, for some i we must have $trdeg(B) = trdeg(B')$ where $B = A^{D_1,\ldots,D_{i-1}}$ and $B' = B \cap A^{D_i}$. Now let $b \in B$. Since $B \supseteq B'$ is algebraic, we know that there exist some relation $P(b) := c_n b^n + c_{n-1}b^{n-1} + \ldots + c_0 = 0$ where $c_i \in B'$ and $n \in \mathbb{N}^*$ as small as possible. Now

$$\begin{aligned} 0 = D_i(0) = &\ D_i(P(b)) \\ = &\ D_i(c_n b^n + c_{n-1}b^{n-1} + \ldots + c_1 b) + D_i(c_0) \\ = &\ D_i(b(c_n b^{n-1} + c_{n-1}b^{n-2} + \ldots + c_1)) \end{aligned}$$

and by lemma 2.2.7.2 we know that $D_i(b) = 0$ (for $c_n b^{n-1} + \ldots + c_1 \neq 0$, n was chosen to be as low as possible), in other words, $b \in A^{D_i}$. We had assumed $b \in B$, concluded that $b \in A^{D_i}$, thus $b \in B \cap A^{D_i} = B'$, which means $B = B'$. Thus $A^{\mathcal{D}} = A^{\mathcal{D}'}$ where $\mathcal{D}' = \mathcal{D} \backslash \{D_i\}$ □

Definition 2.3.4. $\mathcal{D} \subset \mathrm{LND}(A)$ is of *maximal rank* if for each strict subset $\mathcal{D}' \subset \mathcal{D}$ we have $A^{\mathcal{D}'} \neq A^{\mathcal{D}}$.

Using this definition we can use lemma 2.3.3 to prove the following corollary:

Corollary 2.3.5. *If $\mathcal{D} \subset \mathrm{LND}(A)$ is of maximal rank then $trdeg(A^{\mathcal{D}}) \leq n - \#\mathcal{D}$.*

So we have a property, the maximality of rank, which ensures $trdeg(A^{\mathcal{D}}) \leq n - \#\mathcal{D}$. But we still have cases (like example 2) where $trdeg(A^{\mathcal{D}}) < n - \#\mathcal{D}$ can occur. Apparently, the property that the derivations in $\mathcal{D}$ may commute is interesting:

Lemma 2.3.6. *Let $\mathcal{D} \subset \mathrm{LND}(A)$ and suppose that $DD' = D'D$ for each $D, D' \in \mathcal{D}$. Then $trdeg(A^{\mathcal{D}}) \geq n - \#\mathcal{D}$.*

Proof. We will show this by induction to $n = \#\mathcal{D}$. In case $n = 1$ we have only one derivation so there's nothing to prove. So suppose

$n > 1$ and we know the answer for sets of $n-1$ derivations. Let $D \in \mathcal{D}$ and define $\mathcal{D}' := \mathcal{D} \backslash \{D\}$. Now $trdeg(A^{\mathcal{D}'}) \geq n - \#\mathcal{D}' = n - \#\mathcal{D} + 1$. Since D commutes with all derivations on $\mathcal{D}'$, we have $D(A^{\mathcal{D}'}) \subseteq A^{\mathcal{D}'}$. Therefore, D is a well-defined LND if restricted to $A^{\mathcal{D}'}$. Thus $trdeg((A^{\mathcal{D}'})^D) \geq trdeg(A^{\mathcal{D}'}) - 1$, in other words

$$trdeg(A^{\mathcal{D}}) \geq trdeg(A^{\mathcal{D}'}) - 1 \geq (n - \#\mathcal{D} + 1) - 1 = n - \#\mathcal{D}.$$

□

Corollary 2.3.7. *Suppose that $\mathcal{D} \subset \mathrm{LND}(A)$ is of maximal rank, and all derivations in $\mathcal{D}$ commute. Then $A^{\mathcal{D}} = n - \#\mathcal{D}$.*

Remark 2.3.8. "$\mathcal{D} \subseteq \mathrm{LND}(\mathbb{C}^{[n]})$ is of maximal rank and all elements of $\mathcal{D}$ commute" is the same as "all elements of $\mathcal{D} \subseteq \mathrm{LND}(\mathbb{C}^{[n]})$ commute and are linearly independent over $\mathbb{C}^{[n]}$".

2.4 The ML and HD invariants

In this section, R denotes a commutative finitely generated $\mathbb{C}$-algebra and $\mathbb{N}$ the non-negative integers.

Definition 2.4.1.

(i). $ML(R) := \cap_{D \in LND(R)} R^D$, the Makar-Limanov invariant of R. [1]

(ii). $HD(R)$ is the $\mathbb{C}$-algebra generated by $\cup_{D \in LND^*(R)} R^D$. [2]

[1] The original notation introduced by Makar-Limanov himself was $AK(R)$, "absolute kernel" and this notation is sometimes used too.

[2] This invariant is often denoted by "$D(R)$" but since D is a very common notation for a derivation, the notation "HD" (for Harm Derksen) got into fashion.

The Makar-Limanov invariant was introduced by Makar-Limanov in [ML96] to prove that the variety in $\mathbb{C}^4$ given by the equation $X^2Y + X + Z^2 + T^3$ is not isomorphic to $\mathbb{C}^3$. Later on, Derksen gave an alternative proof in [Der97] by introducing a different invariant.

Example 2.4.2. If $R = \mathbb{C}[X_1, \ldots, X_n]$ then $ML(R) = \mathbb{C}$, and in case $n \geq 2$ $HD(R) = R$. In case $n = 1$, $HD(R) = \mathbb{C}$ (a small exception).

Corollary 2.4.3. *If $ML(R) \neq \mathbb{C}$ (i.e. $ML(R)$ is larger than $\mathbb{C}$) then R is not a polynomial ring. If $dim(R) \geq 2$ and $HD(R) \neq R$ then R is not a polynomial ring.*

The above corollary was exactly what Makar-Limanov used to prove that $X^2Y+X+Z^2+T^3$ is not isomorphic to $\mathbb{C}^3$, for if that would be the case, then $\mathbb{C}[X, Y, Z, T]/(X^2Y+X+Z^2+T^3)$ would be isomorphic to $\mathbb{C}^{[3]}$, but since $ML(\mathbb{C}[X, Y, Z, T]/(X^2Y + X + Z^2 + T^3)) \neq \mathbb{C}$ (it is equal to $\mathbb{C}[X]$) this is not the case.

Chapter 3

Kernels of derivations

3.1 How to compute the kernel of a derivation

3.1.1 Introduction

This chapter will deal with kernels of derivations, and we will consider several questions on them. First of all, how does one compute such a kernel? We will discuss algorithms for this problem in this section. Any known algorithms produce a list of generators for the kernel algebra. They are only able to provide finite lists, so these algorithms obviously will never work on a derivation whose kernel is not finitely generated. So the obvious second question is, can kernels be infinitely generated, and when can this occur? This will be studied in section 3.3.

This section gives methods on how to find generators of kernels of derivations. It describes two different methods, the Essen kernel algorithm and the homogeneous kernel algorithm.

3.1.2 The Essen kernel algorithm

In this section we will describe the Essen kernel algorithm. It will be explained quite briefly, giving the algorithm without too much detail to proof. The basis of the algorithm is the following lemma.

Definition 3.1.1. Define $\exp_f(D) := \exp(TD)|_{T=f}$.

Lemma 3.1.2. *Let $A = k[x_1, \ldots, x_n]$ be a finitely generated k-algebra where k is a field containing $\mathbb{Q}$, and D a locally nilpotent derivation on A having a slice $s \in A$. Then $A^D = k[\exp_{-s}(D)(x_1), \ldots, \exp_{-s}(D)(x_n)]$.*

Proof. Write φ_{-s} for the homomorphism $f \longrightarrow \exp_{-s}(D)(f)$. It is not very difficult to check that $D(\varphi_{-s}(f)) = 0$ for all f, which proves "$\supseteq$". Conversely, if $a \in A^D$, then $\varphi_{-s}(a) = a$. Thus $A^D \subseteq \varphi_{-s}(A) = k[\varphi_{-s}(x_1), \ldots, \varphi_{-s}(x_n)]$. □

The Essen kernel algorithm will in this thesis be only used on finitely generated k-domains where k is a field containing $\mathbb{Q}$. [1] So let us assume:

1. $A := k[x_1, \ldots, x_n] := k[X_1, \ldots, X_n]/I$ where I is some prime ideal, is a finitely generated k-domain,

2. D is a nonzero locally nilpotent derivation on A,

3. $p \in A$ is a preslice for D (i.e. $D(p) \neq 0, D^2(p) = 0$).

Actually, we only need to assume the first two points for then by 2 there exists some $a \in A \backslash A^D$. Consequently since D is locally nilpotent, we have some $n \in \mathbb{N}$ such that $D^n(a) = 0$. Then take $p := D^{n-2}(a)$, and you have the third requirement. Write $q := D(p)$ and define $\tilde{A} :=$

[1] The algorithm can be partially generalized to finitely generated R-algebras, if one restricts oneself to derivations D having a preslice p such that $D(p)$ is not a zero divisor.

$A[q^{-1}]$. D extends naturally to the ring $\tilde{A}$, and it has a slice $s := q^{-1}p$. Thus we can compute $\tilde{A}^D = k[\exp_{-s}(D)(x_1), \ldots, \exp_{-s}(D)x_n, q^{-1}]$. Now we know that $A^D = \tilde{A}^D \cap A$, therefore we only need to compute $\tilde{A}^D \cap A$. We will give this part of the algorithm in some kind of pseudo-code:

ESSEN-KERNEL-ALGORITHM;
Input: $A := k[X_1, \ldots, X_n]/I$ a domain, $D \in LND(A)$ nonzero, p a preslice of D.
Output: $f_1, \ldots, f_m \in A$ which generate the kernel.

1. $q := D(p)$.

2. Find $n_i \in \mathbb{N}$ such that $q^{n_i} \exp_{-s}(D)(x_i) \in A$, $q^{n_i-1} \exp_{-s}(D)(x_i) \notin A$.

3. Define m:=n, and define for all $1 \leq i \leq m$: $y_i := q^{n_i} \exp_{-s}(D)(x_i)$.

4. Find generators $P_1, \ldots, P_r$ for the ideal $J := \{P \in k^{[m]} \mid P(y_1, \ldots, y_m) \in qA\}$ (by using for example Gröbner bases).

5. SET M:=m
   FOR i=1 to r DO
   IF $q^{-1}P_i(y_1, \ldots, y_m) \notin k[y_1, \ldots, y_m]$
   THEN M:=M+1; $y_M := q^{-1}P_i(y_1, \ldots, y_m)$.
   FI;
   OD;
   IF $M = m$ THEN we are done, and $y_1, \ldots, y_M$ generate the kernel. END.
   FI
   IF $M \neq m$ THEN SET $m := M$.
   FI

6. GOTO 4.

We will not prove the correctness of the algorithm here; we refer the interested reader to [Ess93] or to [Ess00] pages 37-39.

Remark 3.1.3. It is very well possible that the algorithm never stops; if A^D is not finitely generated as a k-algebra then the algorithm will keep on calculating generators forever.

On the other hand, the algorithm *will* stop if sufficient generators are found.

One of the great strengths of the algorithm is to be able to determine if one has sufficient generators. The algorithm can be modified to suit only this purpose:

KERNEL-CHECK-ALGORITHM;
Input $A := k[X_1, \ldots, X_n]/I$ a domain, $D \in LND(A)$ nonzero, p a preslice of D, and $f_1, \ldots, f_m \in A^D$.
Output: YES if $f_1, \ldots, f_m$ generate the kernel, NO otherwise.

1. $q := D(p)$.
2. Find generators $P_1, \ldots, P_r$ for the ideal $J := \{P \in k^{[m]} \mid P(f_1, \ldots, f_m) \in qI\}$ (by using for example Gröbner bases).
3. FOR i=1 to r DO
   IF $q^{-1}P_i(f_1, \ldots, f_m) \notin k[f_1, \ldots, f_m]$
   THEN output NO; END.
   FI;
   OD;
4. Output YES; END.

3.1.3 The homogeneous kernel algorithm

The algorithm described in this section is more general, in the sense that the mapping doesn't have to be a derivation. This algorithm calculates generators of the kernel of a homogeneous derivation up to a certain predetermined degree. In fact, the algorithm works for non-locally nilpotent derivations as well, and even for some mappings slightly more general than derivations.

In some sense the algorithm is *less* general, for the derivation has to be homogeneous. But there's a way around that, see section 3.1.5.

Assumptions: Let k be some field, and let $A := \oplus A_\alpha$ be a positively multi-graded algebra domain such that A_α is a finite dimensional k-vectorspace for all $\alpha \in \mathbb{N}^q$, and that $A_0 := A_{(0,\ldots,0)} := k$. We assume that we have an additive mapping $E : A \longrightarrow A$ which has the property "$E(a) = E(b) = 0 \Rightarrow E(ab) = 0$", i.e. the property that the kernel of the mapping E is an algebra. We assume that there exists an *injective* function $f : \mathbb{N}^q \longrightarrow \mathbb{N}^q$ satisfying $E(A_\alpha) \subset A_{f(\alpha)}$. In other words: E is a homogeneous mapping (sending homogeneous elements to homogeneous elements), which does not send homogeneous elements of different degree to the same degree. We will denote E_α as the restriction of E to A_α.

We will assume $E \neq 0$. In case E is a derivation we only need to assume that it is homogeneous with respect to the multi-grading. We will also use notations for E which we, if we would be precise, have only defined for derivations, like A^E and such. Also, note that we use the injectivity of f in the following lemma:

Lemma 3.1.4. *Let $F \in A$ such that $E(F) = 0$. Split $F := \bigoplus F_\beta$ into homogeneous components. Then $E(F_\beta) = 0$.*

Proof. Let $G := \bigoplus G_\beta \in A$ be a decomposition of some G into homogeneous components. Because of additivity of E we know that

$E(\bigoplus G_\beta) = \sum E(G_\beta)$. But since each $E(G_\beta)$ is homogeneous of a different degree $f(\beta)$, we know that we may replace "$\sum$" in the previous formula by "$\bigoplus$", and therefore

$$E(\bigoplus G_\beta) = \bigoplus E(G_\beta).$$

Thus $0 = E(F) = \bigoplus E(F_\beta)$, and therefore $E(F_\beta) = 0$. □

Remark 3.1.5. $A_\alpha^{E_\alpha} = A^E \cap A_\alpha$.

Definition 3.1.6. We call $\mathcal{F} = \{F_1, \ldots, F_s\} \subset A_{\leq\alpha}$ a "good set for (α, E)" when

1. Each $F_i \in A_\beta$ for some $\beta \leq \alpha$,
2. $k[\mathcal{F}] \cap A_{\leq\alpha} = A^E \cap A_{\leq\alpha}$,
3. For every i one has $F_i \notin k[\hat{\mathcal{F}}_i]$.

We also define $\mathcal{F} = \{F_1, \ldots, F_s\} \subset A_{\leq\alpha}$ a "good set for $(< \alpha, E)$" when

1. Each $F_i \in A_\beta$ for some $\beta < \alpha$,
2. $k[\mathcal{F}] \cap A_{<\alpha} = A^E \cap A_{<\alpha}$,
3. For every i one has $F_i \notin k[\hat{\mathcal{F}}_i]$.

How does the algorithm work? Given a certain predetermined bound α, the algorithm calculates finite sets $\mathcal{F}_\beta \subset A_\beta$ such that their union gives a good set for (α, E). The main tool is an induction step 3.1.7, which, given a good set $\mathcal{F}$ for $(< \alpha, E)$, calculates a set $\mathcal{F}_\alpha \subset A_\alpha$ such that $\mathcal{F}_\alpha \cup \mathcal{F}$ is a good set for (α, E). Notice that this "good set"-thing is what we're looking for: generators up to a certain degree.

Lemma 3.1.7. *Let $\alpha \in \mathbb{N}^q$. Suppose we have finite sets $\mathcal{F}_\beta \subset A_\beta$ for all $\beta < \alpha$ such that $\bigcup_{\beta<\alpha} \mathcal{F}_\beta$ is a good set for $(< \alpha, E)$. Then we can construct a finite set $\mathcal{F}_\alpha \subset A_\alpha$ such that $\bigcup_{\beta\leq\alpha} F_\beta$ is a good set for α.*

Before we prove this lemma we will show that it indeed is sufficient to prove this lemma.

Lemma 3.1.8. *Let $\alpha \in \mathbb{N}^q$. Suppose we have finite sets $\mathcal{F}_\gamma \subset A_\gamma$ for all $\gamma < \alpha$ such that for all $\beta < \alpha$: $\bigcup_{\gamma\leq\beta} \mathcal{F}_\gamma$ is a good set for β. Then $\bigcup_{\beta<\alpha} \mathcal{F}_\beta$ is a good set for $< \alpha$.*

Proof. Write $\mathcal{F} := \bigcup_{\beta<\alpha} F_\beta$. We need to prove:

1. $k[\mathcal{F}] \cap A_{<\alpha} = A^E \cap A_{<\alpha}$,
2. If $F_i \in \mathcal{F}$ then $F_i \notin k[\hat{\mathcal{F}}_i]$.

Part 1: "$\subseteq$" is trivial. "$\supseteq$": Let $G \in A^E \cap A_{<\alpha}$. Split G into homogeneous parts: $G := \sum G_\beta$. By lemma 3.1.4 we know $E(G_\beta) = 0$. Now by assumption $G_\beta \in k[\bigcup_{\gamma\leq\beta} \mathcal{F}_\gamma] \cap A^E$ which is a subset of $k[\mathcal{F}] \cap A^E$.

Part 2: Let $F_i \in \mathcal{F}$. Then $F_i \in A_\beta$ for some $\beta < \alpha$. Write $\underline{\mathcal{F}} := \bigcup_{\gamma\leq\beta} \mathcal{F}_\gamma$. Suppose $F_i \in k[\hat{\mathcal{F}}_i]$. Since $F_i \in A_{\leq\beta}$ we have $F_i \in k[\hat{\mathcal{F}}_i] \cap A_{\leq\beta} \subseteq k[\hat{\underline{\mathcal{F}}}] \cap A_{\leq\beta}$, which is a contradiction with the assumption. Therefore $F_i \notin k[\hat{\mathcal{F}}_i]$. □

By these last two lemmas we can calculate good sets for any vector α if we have a good set for $0 := (0, \ldots, 0) \in \mathbb{N}^q$. But, since $A_0 = k$ by assumption, this is easy:

Remark 3.1.9. A good set for 0 is the empty set.

So we only need to prove lemma 3.1.7.

Proof. (of lemma 3.1.7) Write $\mathcal{F} = \{F_1, \ldots, F_s\} := \bigcup_{\beta<\alpha} F_\beta$. Define

$$I := \{v \in \mathbb{N}^s \mid \mathcal{F}^v \in A_\alpha\}$$

(i.e. $\sum_{i=1}^s v_i grad(F_i) = \alpha$). $k[\mathcal{F}] \cap A_\alpha$ is a finite dimensional k-vectorspace. We know

$$k[\mathcal{F}] \cap A_\alpha = \sum_{v \in I} k \cdot F^v.$$

Notice that we did write "$\sum$", not "$\oplus$", since we do not know that $\cup_{v\in I} F^v$ is an independent set. However, we can take (and calculate!) a subset J of I such that

$$k[\mathcal{F}] \cap A_\alpha = \bigoplus_{v \in J} k \cdot F^v.$$

Hence $\dim(k[\mathcal{F}] \cap A_\alpha) = \#J$. Now we compute $A_\alpha^{E_\alpha}$. (This can be easily done since it is a linear k-map from a finite dimensional k-vector space A_α to a finite dimensional k-vector space $A_{f(\alpha)}$.) Since $k[\mathcal{F}] \cap A_v \subseteq A^E$ we have by lemma 3.1.5

$$k[\mathcal{F}] \cap A_\alpha \subseteq A^E \cap A_\alpha = A_\alpha^{E_\alpha}.$$

Hence $\oplus_{v\in J} k \cdot F^v \subseteq A_\alpha^{E_\alpha}$. Thus $\{F^v \mid v \in J\}$ are k-linearly independent elements in $A_\alpha^{E_\alpha}$. Now choose a finite set $\mathcal{F}_\alpha \subset A_\alpha^{E_\alpha}$ for which $\mathcal{F}_\alpha \cup \{F^v; v \in J\}$ forms a k-linear basis of $A_\alpha^{E_\alpha}$. Now we claim: $\mathcal{F} \cup \mathcal{F}_\alpha$ is a good set for α. For this we need two (in fact three) things to be true:

1. $A^E \cap A_{\leq\alpha} = k[\mathcal{F} \cup \mathcal{F}_\alpha] \cap A_{\leq\alpha}$,
2. (a) $F_{\alpha,i} \notin k[\mathcal{F}, \hat{\mathcal{F}}_{\alpha,i}]$ and (b) $F_i \notin k[\hat{\mathcal{F}}_i, F_\alpha]$,

where $\hat{\mathcal{F}}_{\alpha,i}$ is $\mathcal{F}$ minus the i-th element $F_{\alpha,i}$. *Proof of (1):* "$\supseteq$" is O.K. "$\subseteq$": Take $G \in A^E \cap A_{\leq\alpha}$. Decompose G into homogeneous

components and let $G := G_1 + G_2$ where $G_1 \in A_\alpha, G_2 \in A_{<\alpha}$. Then $0 = E(G) = E(G_1) + E(G_2)$ hence by lemma 3.1.4 $E(G_1) = E(G_2) = 0$. By hypothesis $G_2 \in k[\mathcal{F}] \cap A_{<\alpha} \subseteq k[\mathcal{F}, \mathcal{F}_\alpha] \cap A_{\leq\alpha}$. Furthermore

$$G_1 \in A^E \cap A_\alpha = \big(k[\mathcal{F}] \cap A_\alpha\big) \oplus \big(k[\mathcal{F}_\alpha] \cap A_\alpha\big) = k[\mathcal{F}, \mathcal{F}_\alpha] \cap A_\alpha$$

hence $G_1 + G_2 \in k[\mathcal{F}, \mathcal{F}_\alpha] \cap A_{\leq\alpha}$.
Proof of (2)(a): We know that

$$k[\mathcal{F}, \mathcal{F}_\alpha] \cap A_{\leq\alpha} = \big(\bigoplus_{v\in J} k \cdot \mathcal{F}^v\big) \oplus \big(\bigoplus_{f\in\mathcal{F}_\alpha} k \cdot f\big).$$

So $F_{\alpha,i}$ is independent of the other terms and hence

$$F_{\alpha,i} \notin \big(\bigoplus_{v\in J} k \cdot \mathcal{F}^v\big) \oplus \big(\bigoplus_{F_{\alpha,i}\neq f\in\mathcal{F}_\alpha} k \cdot f\big)$$

which equals $k[\mathcal{F}] \cap A_\alpha \oplus k[\hat{\mathcal{F}}_{\alpha,i}] \cap A_\alpha = k[\mathcal{F}, \hat{\mathcal{F}}_{\alpha,i}] \cap A_\alpha$. Since $F_{\alpha,i} \notin k[\mathcal{F}, \hat{\mathcal{F}}_{\alpha,i}] \cap A_\alpha$ we have $\hat{\mathcal{F}}_{\alpha,i} \notin k[\mathcal{F}, \hat{\mathcal{F}}_{\alpha,i}]$.

Proof of (2)(b): Suppose $F_{\alpha,i} \in k[\hat{\mathcal{F}}_i, \mathcal{F}_\alpha]$. Then there is a polynomial $P(\hat{\mathcal{F}}_i, \mathcal{F}_\alpha)$ which equals F_i. Let $\beta = grad(F_i)$. Then $\beta < \alpha$. Comparing degrees in the equation $F_i = P(\hat{\mathcal{F}}_i, \mathcal{F}_\alpha)$ shows that P is in fact a polynomial in the $\hat{\mathcal{F}}_i$ since the $\mathcal{F}_\alpha$ are of too high degree. But by hypothesis $F_i \notin k[\hat{\mathcal{F}}_i]$. Contradiction, hence $F_i \notin k[\hat{F}_i, \mathcal{F}_\alpha]$.

So now (1),(2a),(2b) all hold. These are the requirements of $\mathcal{F} \cup \mathcal{F}_\alpha$ to be a good set for (α, E), which was what we needed to prove. □

3.1.4 Minimality of the generators calculated by the homogeneous algorithm for a LND

Assume that we have $\mathcal{F} := \{F_1, \ldots, F_p\}$ given by the algorithm in section 3.1.3 as generators of $ker(E)$. (So we have used the algorithm and concluded in some way that they generate the complete kernel, for example by the technique described in section 3.1.7.

Theorem 3.1.10. *The algorithm given in section 3.1.3 gives a* minimal *set of generators in the sense that if* $k[F_1, \ldots, F_p] = k[G_1, \ldots, G_q]$ *for some* G_i *then we must have* $q \geq p$.

Proof. We may assume that $G_1(0) = \ldots = G_q(0) = 0$ (i.e. each $G_i \in (X_1, X_2, \ldots, X_n)$) by replacing '$G_i(X)$' by '$G_i(X) - G_i(0)$' if necessary. Let $\mathfrak{m} := (F_1, \ldots, F_p)$. $k[F_1, \ldots, F_p]/\mathfrak{m}$ is isomorphic to the field k, and the F_i are homogeneous; hence $\mathfrak{m}$ is a homogeneous maximal ideal. Since $G_i \in k[F_1, \ldots, F_p]$ we have $G_i = P(F_1, \ldots, F_p) + c$ for some $c \in k$ and some polynomial $P(T) \in k[T_1, \ldots, T_p]$ having no constant term. But since $F_j(0) = 0$ all j and $G_i(0) = 0$ we have $c = 0$. Hence $G_i \in \mathfrak{m}$, so $\mathfrak{m} \supset (G_1, \ldots, G_q)$. In the same way we can also prove $(G_1, \ldots, G_q) \supset \mathfrak{m}$ hence $\mathfrak{m} = (G_1, \ldots, G_q)$.
Now consider $\mathfrak{m}/\mathfrak{m}^2$. This is a k-vector space. It is generated by the $\bar{F}_i := F_i \mod \mathfrak{m}^2$; namely if $g \in \mathfrak{m}$, then

$$g = P(F_1, \ldots, F_p) = \lambda_1 F_1 + \ldots + \lambda_p F_p + \sum_{|\beta| \geq 2} \lambda_\beta F^\beta. \quad \lambda_i, \lambda_\beta \in k$$

Since each F^β with $|\beta| \geq 2$ belongs to $\mathfrak{m}^2$ we get $\bar{g} = \sum \lambda_i \bar{F}_i$.
Now we claim that these generators $\bar{F}_i$ also form a basis; suppose

$$\bar{F}_i = \lambda_1 \bar{F}_1 + \ldots + \lambda_{i-1} \bar{F}_{i-1} + \lambda_{i+1} \bar{F}_{i+1} + \ldots + \lambda_p \bar{F}_p.$$

Then

$$F_i = \lambda_1 F_1 + \ldots + \lambda_{i-1} F_{i-1} + \lambda_{i+1} F_{i+1} + \ldots + \lambda_p F_p + \sum \lambda_\beta F^\beta.$$

Let us take the homogeneous part of $grad(F_i)$ in this equation. Since all F_j are homogeneous of nonzero degree themselves we get an expression of F_i in the other F_j's which satisfy $grad(F_j) \leq grad(F_i)$. But this is in contradiction with the assumption that the F_i's are found by the algorithm ,which means that they should satisfy the properties of a

"good set". Hence the $\bar{F}_i$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$; thus $dim(\mathfrak{m}/\mathfrak{m}^2) = p$. Now since $(G_1, \ldots, G_q) = \mathfrak{m}$ the $\bar{G}_i$ generate the vector space $\mathfrak{m}/\mathfrak{m}^2$. Since $dim(\mathfrak{m}/\mathfrak{m}^2) = p$ we need at least p generators. Hence q should be larger or equal to p. □

3.1.5 Applying the homogeneous algorithm to non-homogeneous derivations

Let $A := k^n$ be a polynomial ring. The algorithm in the previous section can only be directly used for homogeneous derivations, admitting a grading on the ring A. However, very often a derivation does not admit such a grading. We still want to be able to find generators for the kernel of any derivation by making it homogeneous.

Let $D = \sum_{i=1}^{p} a_i \partial_i$ be a derivation on A. Introduce one new variable Z and extend D to the Laurent polynomial ring $A[Z, Z^{-1}]$ by defining $D(Z) = 0$. Let $\varphi : A \longrightarrow A[Z, Z^{-1}]$ be the homogenization map sending $f(X_1, \ldots, X_p) \in A$ to $f(X_1/Z, \ldots, X_p/Z)$. By π we denote the substitution homomorphism $A[Z, Z^{-1}] \longrightarrow A$ sending Z to 1. On A we consider the "usual" grading "deg" defined by $deg(X^\alpha) = \alpha_1 + \ldots + \alpha_p$. For $0 \neq g \in A$ we put $g^* := Z^{deg(g)}\varphi(g) \in A[Z]$. Obviously $\pi(g^*) = g$. Furthermore one easily verifies that

$$(*) \quad \partial_i(\varphi(g)) = \frac{1}{Z}\varphi(\partial_i g) \text{ for all } g \in A.$$

On $A[Z]$ we define the *homogenization* $\widetilde{D}$ of D by $\widetilde{D} := \sum_{i=1}^{p} Z^d \varphi(a_i)\partial_i$ where $d = max(deg(a_1), \ldots, deg(a_p))$.

Lemma 3.1.11. $\pi(ker(\widetilde{D})) = ker(D)$

Proof. ($\supseteq$:) Let $g \in ker(D)$. Then $\sum a_i \partial_i(g) = 0$, so by $(*)$: $\sum \varphi(a_i) Z \partial_i(\varphi(g)) = 0$ i.e. $\widetilde{D}(\varphi(g)) = 0$. So $\widetilde{D}(g^*) = 0$. Since $g = \pi(g^*)$ we get $g \in \pi(ker(\widetilde{D}))$. So $\pi(ker(\widetilde{D})) \supseteq ker(D)$.

($\subseteq$:) Let $h \in ker(\widetilde{D})$. Then $Z^d \sum \varphi(a_i)\partial_i(h) = 0$. Applying π gives $\sum a_i \partial_i(\pi(h)) = 0$ i.e. $\pi(h) \in ker(D)$. So $\pi(ker(\widetilde{D})) \subseteq ker(D)$. □

Now one can easily verify that $\widetilde{D}$ matches the requirements of the algorithm, using the "usual" grading $grad := deg$ on $A[Z]$ as the needed "combined grading". Hence we can find generators for $ker(D)$ by calculating generators for $ker(\widetilde{D})$.

Remark 1: Perhaps a flaw in this extension is that the algorithm can not compute a minimal set of generators. Under some conditions $ker(\widetilde{D})$ might not be finitely generated while $ker(D)$ is: an example of this is the derivation $D := \partial_S + SW^2\partial_T + TW^2\partial_U + W\partial_V$. Since this derivation has a slice it is finitely generated. In this situation, $\widetilde{D} := Z^3\partial_S + SW^2\partial_T + TW^2\partial_U + Z^2W\partial_V$. This derivation cannot have finitely generated kernel: for if it has, then the derivation $Z^3\partial_S + S\partial_T + T\partial_U + Z^2\partial_V$ (substituting $W = 1$) has a finitely generated kernel too, but as we see in 3.3.2 this is not the case.
Remark 2: A different approach could be the following: suppose one has a derivation on a k-algebra A which sends $B := \{f \in A \mid deg(f) \leq n\}$ into some describable, finite dimensional k vectorspace $C \subset A$. (For example, C can be $\{f \in A \mid deg(f) \leq m\}$ for some integer m.) Then one could calculate generators of the kernel up to degree n by restricting D to the k-vectorspace of polynomials of degree smaller or equal to n. You then gain a linear map $D|_B : B \longrightarrow C$, and you can calculate its kernel, obtaining $B^{D|_B}$. Then

$$B^{D|_B} = A^D \cap B.$$

However, the 'homogenization' method described above in this section turned out to be more efficient, probably due to the fact that the size of the k-vectorspaces used in calculations are much smaller. Also, in the "homogeneous" case, if one has done calculations for degree n, then

calculating generators up to degree $n+1$ uses the known generators. By the other method one has to calculate the kernel of D restricted to the k-vectorspace of polynomials of degree smaller or equal to $n+1$, doing a lot of double work.

3.1.6 Example and efficiency of the homogeneous algorithm.

Let us consider the derivation on $An := k[X_1, \ldots, X_n]$ given by

$$D_n := X_{n-1}\partial_{X_n} + X_{n-2}\partial_{X_{n-1}} + \ldots + X_1\partial_{X_2}.$$

We can easily construct a D_n-invariant and a D_n-decreasing grading on An and combine them in a grading *grad* defined by

$$grad(X^\alpha) = (< p, \alpha >, < q, \alpha >)$$

where $p = (1, \ldots, 1)$ and $q = (0, 1, \ldots, n-2, n-1)$ (and $<,>$ denotes the standard inproduct). We are going to consider this derivation for $n = 5$ and write $A := A5$ for notational reasons. Also we denote A_α as the collection of all polynomials of $grad(F) = \alpha$, and $\mathcal{F}_\alpha$ means the set of generators of degree equal to α. Also $\mathcal{F}_{<\alpha}$ is the set of generators of degree smaller than α. Easy to check is that $A_{(n,m)}$ is finite dimensional over k for all n, m, hence the algorithm will work on this derivation with this grading. Suppose we already know that $\mathcal{F}_{(1,0)} = \{X_1\}$ and that $\mathcal{F}_{(0,0)} = \mathcal{F}_{(2,0)} = \mathcal{F}_{(0,1)} = \mathcal{F}_{(1,1)} = \mathcal{F}_{(2,1)} = \mathcal{F}_{(0,2)} = \mathcal{F}_{(1,2)} = \{\}$. (This is easily deduced.) Now we want to find a good set for the vector $(2, 2)$ using the technique described in the proof of lemma 3.1.7. Easy to see is that $A_{(2,2)} = kX_3X_1 + kX_2^2$, $A_{(2,1)} = kX_3$. Furthermore $D_\alpha(A_{(2,2)}) \subseteq A_{(2,1)}$ so the linear map $D_\alpha : A_{(2,2)} \longrightarrow A_{(2,1)}$ needs to be considered. The kernel of this map is, as one easily sees, a linear space L generated by $X_3X_1 - \frac{1}{2}X_2^2$. The generating set for $< (2, 2)$ is $\mathcal{F}_{<(2,2)} = \{X_1\}$. So we need to check if there are elements of L

in $k[\mathcal{F}_{<(2,2)}]$, hence we need to check if there are elements of L in $k[\mathcal{F}_{<(2,2)}] \cap A_{(2,2)} = \{0\}$. Hence we get $\dim(L) - \dim(\{0\}) = 1$ new generator(s). So $\mathcal{F}_{(2,2)} = \{X_3X_1 - \frac{1}{2}X_2^2\}$.

Now about efficiency. All calculations are done on a SUN ENTERPRISE 4000 (Ultrasparc 170 MHz) using the MAGMA computer algebra system. The algorithm calculates within 22 seconds the generators up to grad (10,10). These are all generators, as can be checked by the method described in the following section 3.1.7 within 2 seconds. If one solely uses the Essen-algorithm then one has to wait for 3902 seconds (65 minutes) until the answer is given.

3.1.7 The best of both worlds: joining both algorithms

The major drawback of the Essen algorithm is that in practice it is not very fast for most locally nilpotent derivations. The major drawback of the homogeneous algorithm is that it cannot answer the question if found generators are sufficient. However, if we use the homogeneous algorithm to compute generators, and then use the kernel-check-algorithm described in the section "The Essen kernel algorithm", to decide if these actually generate the whole kernel, then generally this is a fast way. The example in the previous section uses exactly this method.

3.2 Derivations on $R[X, Y]$

The two-variable case is a rather surveyable case, and that is why we are going to consider it for general rings.

3.2.1 Kernels of derivations on $R[X,Y]$

It is well-known that a locally nilpotent derivation on $k^{[2]}$ has a kernel generated by one element (i.e. Rentschler's theorem). But what's the case for $R^{[2]}$ where R is some ring? If we don't assume anything on our ring or derivation, we can have locally nilpotent derivations with kernel an infinitely generated R-algebra, as the following example on $R^{[1]}$ shows:

Example 3.2.1. Let $R := R[t] = k[T]/(T^2)$ and let $D := t\partial_X$ on $R[X]$. Then $R[X]^D = R[tX, tX^2, tX^3, \ldots]$ is an infinitely generated R-algebra.

Proof. Notice $R[X] = k[X] \oplus tk[X]$. So write a generic element c in $R[X]$ as $c := a(X) + tb(X) \in R[X]$ for some $a(X), b(X) \in k[X]$. Now $0 = D(c) = D(a(X)+tb(X)) = t\partial_X(a(X))$ if and only if $a(X) \in k$, i.e. $R[X]^D = k + tk[X] = R[tX, tX^2, tX^3, \ldots]$. This is infinitely generated as an R-algebra, since you need all of the given generators tX^n (just restrict yourself to polynomials of $deg_X \leq n$). □

So we should at least assume our ring to be reduced. But, that is not enough:

Example 3.2.2. Let $R := k[u,v] := k[U,V]/(UV)$ and consider $D := v\partial_X$ on $R[X]$. Then $R[X]^D = R[uX, uX^2, \ldots]$ is an infinitely generated R-algebra.

Proof. Notice $R[X] = k[v,X] \oplus uk[u,X]$. So write a generic element c in $R[X]$ as $c := a(v,X) + ub(u,X) \in R[X]$ for some $a(v,X), b(u,X)$. Now $0 = D(c) = D(a(v,X) + ub(u,X)) = v\partial_X(a(v,X))$ if and only if $a(v,X) \in k[v]$, i.e. $R[X]^D = k[v] + uk[u,X] = R[uX, uX^2, \ldots]$ which is infinitely generated as an R-algebra since you need all uX^n-generators. □

So we even need to assume that R is a domain. Any locally nilpotent derivation on $R[X]$ where R is a domain has a finitely generated kernel (in fact, $R[X]^D = R$ or $R[X]$). But, in two variables, we still have a counterexample:

Example 3.2.3. Let $R := k[T^2, T^3]$, and $D := T^2\partial_X + T^3\partial_Y$. Then $R[X,Y]^D$ is not finitely generated.

Proof. The derivation can be extended to $k[T][X,Y]$; on this ring we have $k[T][X,Y]^D = k[T, TX-Y]$, and thus $R[X,Y]^D = k[T][X,Y]^D \cap R[X,Y] = k[T, TX-Y] \cap R[X,Y]$ which equals $R[LT^2, L^2T^2, \ldots]$ where $L := TX - Y$. This is an infinitely generated kernel since you need all generators L^nT^2. □

So even "domain" is not enough. But, if one assumes R to be a UFD, we have the following theorem, which is an extension of Rentschler's theorem:

Theorem 3.2.4. *(Berson) Let R be a UFD containing $\mathbb{Q}$, and let D be a locally nilpotent derivation on $R[X,Y]$. Then*

1. *there exists some $\varphi \in Aut_R R[X,Y]$ such that $\varphi^{-1}D\varphi = f(Y)\partial_X$ where $f(Y) \in R[Y]$.*

2. *$R[X,Y]^D = R[P]$ for some $P \in R[X,Y]$.*

For the proof, see [Ber99].

But now, what should we assume of a locally nilpotent derivation D on $R[X,Y]$ where R is a general ring, to make sure that $R[X,Y]^D$ is finitely generated? The following section shows that a sufficient assumption is $1 \in (D(X), D(Y))$.

3.2.2 Derivations on $R[X,Y]$ satisfying $(D(X),D(Y))=(1)$

The results in this section are joint work of J.Berson, A. van den Essen, and the author, and is published in [BEM01].

In this subsection we use the following notations: $A := R[X,Y]$. $(D(X),D(Y)) = D(X)R[X,Y]+D(Y)R[X,Y]$ is the ideal in $R[X,Y]$ generated by $D(X)$ and $D(Y)$. We will write $\partial_X(P),\partial_Y(P)$ as P_X,P_Y.

Definition 3.2.5. Let R be some ring. We define $\mathcal{B}(R)$ as the statement:
"Any $D \in \mathsf{LND}_R(A)$ satisfying $1 \in (D(X),D(Y))$ has a slice S and $A^D = R[P]$."

The main aim is to show that $\mathcal{B}(R)$ holds for any $\mathbb{Q}$-algebra R (Theorem 3.2.13).

Lemma 3.2.6. *If R is a domain and $D \in \mathrm{LND}_R(R^{[n]})$, then $div(D) = 0$.*

See [Ess00] prop. 1.3.51 for a proof.

Corollary 3.2.7. *If R is a reduced ring and $D \in \mathrm{LND}_R(R^{[n]})$, then $div(D) = 0$.*

Proof. If $\mathfrak{p}$ is some prime ideal in R then $D \mod \mathfrak{p}$ is a well-defined locally nilpotent derivation over $R/\mathfrak{p}$, thus $div(D \mod \mathfrak{p}) = 0$. Thus $div(D) = 0 \mod \mathfrak{p}$ for all prime ideals $\mathfrak{p}$, thus $div(D) = 0 \mod \mathfrak{n}$ where $\mathfrak{n}$ is the intersection of all prime ideals. Since R is reduced, $\mathfrak{n} = 0$. □

The following remark follows directly from the definition of divergence.

Remark 3.2.8. Let R be a $\mathbb{Q}$-algebra and let $D \in \mathrm{DER}_R(A)$ which satisfies $div(D) = 0$, then $D = P_Y\partial_X - P_X\partial_Y$ for some $P \in A$.

To show $\mathcal{B}(R)$ for any $\mathbb{Q}$-algebra, we first reduce to the case that R is Noetherian. Therefore let R' be the $\mathbb{Q}$-subalgebra of R generated by the coefficients of the polynomials $D(X), D(Y), a$ and b where a, b are such that $1 = aD(X) + bD(Y)$. Notice that R' is noetherian, regardless of R. Write $A' = R'[X, Y]$, D' the restriction of D to A'.

Lemma 3.2.9. *If D' has a slice and $A'^{D'} = R'[P]$ then D has a slice and $A^D = R[P]$.*

Proof. Let $S \in A'$ such that $D'(S) = 1$. Then since $A' \subseteq A$ we have $S \in A$ and $D(S) = D'(S) = 1$. So let $A'^{D'} = R'[P]$. Since w have a slice we have $R'[X, Y] = A' = A'^{D'}[S] = R'[P, S]$. So there exist $F, G \in R'[X, Y]$ such that $F(P, S) = X$ and $G(P, S) = Y$. But since all is contained in $R[X, Y]$ we have

$$R[X, Y] = R[F(P, S), G(P, S)] \subseteq R[P, S] \subseteq R[X, Y].$$

Hence $A^D = R[P, S]^D = R[P]$. □

To prove $\mathcal{B}(R)$ for Noetherian domains containing $\mathbb{Q}$, we first need a lemma from [DF98]

Lemma 3.2.10. *(Daigle) Let R be a domain containing $\mathbb{Q}$ and $P \in R[X, Y]$ such that $1 \in (P_X, P_Y)$. Then $K[P] \cap R[X, Y] = R[P]$, where $K = Q(R)$, its field of fractions.*

Proof. If $K[P] \cap R[X, Y] \not\subseteq R[P]$, then there exists an $F \in K[T] \setminus R[T]$ with $F(P) \in R[X, Y]$. Choose one of minimal degree. Observe that $F(P) \in R[X, Y]$ implies that $F'(P)F_X$ and $F'(P)F_Y$ belong to $R[X, Y]$.
Since there are $g, h \in R[X, Y]$ with $P_X g + P_Y h = 1$, we deduce $F'(P) = F'(P)P_X g + F'(P)P_Y h \in R[X, Y]$. So $F'(T) \in K[T]$ and $F'(P) \in R[X, Y]$, thus by minimality of the degree of F we must conclude, that $F' \in R[T]$. Now write $F = \sum_{i=0}^{d} f_i T^i$, then $F' \in R[T]$ implies

(since R is a $\mathbb{Q}$-algebra) that $f_i \in R$ for all $i \geq 1$, thus yielding $f_0 = F(P) - \sum_{i=1}^{d} f_i P^i \in R[X,Y] \cap K = R$, contradicting the assumption, that $F \notin R[T]$. □

Now we can prove the next theorem :

Theorem 3.2.11. *Let R be a Noetherian domain containing $\mathbb{Q}$, $K = Q(R)$, and let D be a locally nilpotent derivation on $R[X,Y]$ with $1 \in (D(X), D(Y))$.*
Then $R[X,Y]^D = R[P]$ for some $P \in R[X,Y]$ and D has a slice $t \in R[X,Y]$.

Proof. Extend D to $K[X,Y]$ the natural way. We know by theorem 1.2.25 in citeEssenBoek that there is a $Q \in K[X,Y]$ with $K[X,Y]^D = K[Q]$. Because D is locally nilpotent, we know that $div(D) = 0$, so there is a $P \in R[X,Y]$ with $D(X) = P_Y$ and $D(Y) = -P_X$. This means that $D(P) = 0$, and, as a consequence, $P \in K[X,Y]^D = K[Q]$. So write $P = g(Q)$ with $g \in K[T]$. We now have $P_X = g'(Q)Q_X$ and $P_Y = g'(Q)Q_Y$. Notice that $(P_Y, P_X) = (D(X), D(Y)) = (1)$ (also in $K[X,Y]$), which means that $g'(Q) \in K^*$. Then there are $\lambda, \mu \in K, \lambda \neq 0$ satisfying $P = g(Q) = \lambda Q + \mu$, yielding $K[P] = K[Q]$. By the previous lemma, $R[X,Y]^D = K[X,Y]^D \cap R[X,Y] = K[P] \cap R[X,Y] = R[P]$.
Hence we proved our first claim. Now we can use Theorem 4.7 in [BD97] to conclude that

$$R[X,Y] = R[P][s] \text{ for some } s \in R[X,Y] \tag{3.1}$$

This means that $f : R[X,Y] \longrightarrow R[X,Y]$ defined by $f(X) = P(X,Y)$ and $f(Y) = s(X,Y)$ satisfies $f \in Aut_R R[X,Y]$. A well-known consequence is that

$$\det JF(X) \in R[X,Y]^* = R^* \tag{3.2}$$

But this determinant is equal to $-P_Y s_X + P_X s_Y = -D(s)$. So $D(s) \in R^*$, whence $t := s/D(s)$ satisfies $D(t) = 1$ and we are done. □

Combining lemma 3.2.9 and theorem 3.2.11 we have

Theorem 3.2.12. *Let R be any domain containing $\mathbb{Q}$. Then $\mathcal{B}(R)$ holds.*

Now we are able to prove the main theorem of this section:

Theorem 3.2.13. *Let R be any $\mathbb{Q}$-algebra. Then $\mathcal{B}(R)$ holds.*

Proof. Let $D = a(X,Y)\partial_X - b(X,Y)\partial_Y$ be an arbitrary locally nilpotent derivation satisfying $1 \in (a(X,Y), b(X,Y))$. We have to prove that D has a slice and that $A^D = R[P]$. By lemma 3.2.9 we may assume R to be noetherian. Thus the nilradical $\mathfrak{n}$ of R can be written as $\mathfrak{n} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$, where the $\mathfrak{p}_i$ run through all minimal prime ideals of R and $\mathfrak{n}^e = 0$ for some $e \geq 1$.

(i) First we show that D has a slice in A. Therefore observe that by theorem 3.2.12 , $D_{\mathfrak{p}_i}$ has a slice in $R/\mathfrak{p}_i[X,Y]$ for all i. So by lemma 2.1.4, $D_{\mathfrak{n}}$ has a slice in $R/\mathfrak{n}[X,Y]$. Then again by lemma 2.1.4, $D_{\mathfrak{n}^e}$ has a slice in $R/\mathfrak{n}^e[X,Y]$. Since $\mathfrak{n}^e = (0)$, this means that D has a slice, say s in $R[X,Y] = A$.

(ii) Write $\bar{D} := D \mod \mathfrak{n}R[X,Y]$ on $\bar{R}[X,Y]$. Since $\bar{R}$ is reduced and D is locally nilpotent, we know that $\bar{D} = \bar{P}_Y\partial_X - \bar{P}_X\partial_Y$ for some $\bar{P} \in \bar{R}$. Also note $\bar{D}(\bar{P}) = 0$. By lemma 2.1.7 we may even assume $D(P) = 0$. We claim: $R[P,s] = R[X,Y]$, which upon using $D(s) = 1$ and $D(P) = 0$ implies that $R[X,Y]^D = R[P]$ as desired. Use notations $P_{\mathfrak{p}_i} := P \mod \mathfrak{p}_i$ etc. To see the claim it suffices by [Ros01] theorem 3.5.3 to see that each $F_{\mathfrak{p}_i}$ is invertible over $R_{\mathfrak{p}_i}$, where $F = (P,s)$. However, by theorem 3.2.12 we know that $R/\mathfrak{p}_i[X,Y]^{D_{\mathfrak{p}_i}} = R/\mathfrak{p}_i[P_{\mathfrak{p}_i}]$ and obviously, $D_{\mathfrak{p}_i}(s_{\mathfrak{p}_i}) = 1$. So we get $R/\mathfrak{p}_i[X,Y] = R/\mathfrak{p}_i[P_{\mathfrak{p}_i}, s_{\mathfrak{p}_i}]$, i.e. $F_{\mathfrak{p}_i}$ is invertible over $R_{\mathfrak{p}_i}$. □

3.3 The number of generators of kernels

3.3.1 Infinitely generated kernels on $R^{[n]}$

Since we are interested in knowing kernels of derivations, it is an important question whether it is possible at all to "know" a kernel. It might be quite difficult to "know" a kernel in case it is not finitely generated. So, one has the question:

Question 3.3.1. When is A^D finitely generated, and when not?

This is closely related to Hilbert's 14th problem:

Hilbert 14 in n variables Does every derivation on $k^{[n]}$ have a finitely generated kernel?

The answer is NO.

Theorem 3.3.2. *(Daigle-Freudenberg) Let*

$$\begin{aligned} D_1 = &\ X_4^2\partial_1 + (X_4X_1 + X_5)\partial_2 + X_2\partial_3 \\ D_2 = &\ X_5^3\partial_1 + X_1\partial_2 + X_2\partial_3 + X_5^2\partial_4 \end{aligned}$$

on $k^{[5]}$. Then ${k^{[n]}}^{D_1}$ as well as ${k^{[n]}}^{D_2}$ are not finitely generated.

We refer to theorem 3.3 in [DF99] as proof.

We will list for various R the known facts for which dimensions n there exist locally nilpotent derivations on $R^{[n]}$ such that their kernels are finitely generated.

Properties of R	Finitely generated up and including dimension:	Infinitely generated examples exist in dimension:
$R = k$, a field	3	5 (Theorem 3.3.2)
R a domain	1	2 (Example 3.2.3)
R a reduced ring	0	1 (Example 3.2.2)

So from this table, only the $k^{[4]}$ case is still open. For several years the $k^{[5]}$ and $k^{[6]}$ cases were open too, only the $k^{[7]}$-case was settled by Robert's example. Only recently the $k^{[6]}$-case, and quickly after that, the $k^{[5]}$-case were settled by Daigle and Freudenburg in [Fre00] and [DF99]. There are some results in dimension 4, again by Daigle and Freudenburg, as for example the papers [DF01a] and [DF01b] which show that any *triangular* locally nilpotent derivation on $k^{[4]}$ has a finitely generated kernel. This implies that if derivations having not finitely generated kernels exist, then they must have a much more complicated form than the not finitely generated kernel-derivations in dimension 5 and 6 found by Daigle and Freudenburg.

In subsection 3.3.2 we will prove a special case of this, i.e. the fact that the kernel of a triangular monomial derivation is finitely generated (by simply calculating the kernel). This is interesting too, for the examples of Daigle and Freudenburg in dimension 5 and 6 are of this form (as well as Robert's example in dimension 7).

The main idea in all the examples of Daigle-Freudenburg is using the following lemma (lemma 1 on page 1013 in [Fre01], or see [DF99]).

Lemma 3.3.3. *Let $A := \oplus_{i\in\mathbb{N}} A_i$ be a graded k-domain such that $A_0 = k$, and let D be a homogeneous locally nilpotent k-derivation of A. Let $a \in A^D$, $a \notin Im(A)$. Define $\tilde{D} : A[T] \longrightarrow A[T]$ sending $T \longrightarrow a$. Suppose ϕ_n is a sequence of non-zero elements of $A[T]^{\tilde{D}}$ having leading T-coefficients $b_n \in A$. If $degb_n$ is bounded, but $deg_T(\phi_n)$*

is not bounded, then $A[T]^{\tilde{D}}$ *is not finitely generated over* k.

3.3.2 A 4-dimensional case

The results in this section have been published in [Mau00a].

In this section we will consider triangular monomial derivations on $k^{[4]}$, i.e. derivations having the following form up to a permutation of X_1, X_2, X_3, X_4:

$$D := \lambda_1 X_2^a X_3^b X_4^c \partial_{X_1} + \lambda_2 X_3^d X_4^e \partial_{X_2} + \lambda_3 X_4^f \partial_{X_3} + \lambda_{X_4} \partial_4$$

where $a, b, c, d, e, f \in \mathbb{N}$ and $\lambda_i \in k$.

The main result will be the following corollary (of theorem 3.3.5).

Corollary 3.3.4. *A triangular monomial derivation on* $k^{[4]}$ *has a kernel generated by at most four elements.*

In the theorem below we use the following notations: D is as above, a "general" triangular monomial k-derivation. Furthermore we write

$$\begin{aligned} r_1 &:= X_4^F(X_1 - \textstyle\sum_{i=0}^{a} \mu_i X_2^{a-i} X_3^{b+1+i(d+1)} X_4^{i(e-f)+c-f}) \\ r_2 &:= X_4^G(X_2 - \tfrac{1}{d+1}\tfrac{\lambda_2}{\lambda_3} X_4^{e-f} X_3^{d+1}) \\ r_5 &:= X_4^{-l}(\tfrac{1}{d+1}\tfrac{\lambda_2}{\lambda_3} r_1^{\alpha} - \mu_a r_2^{\beta}) \end{aligned}$$

where

- $G = max\{0, f-e\}$, $F = max\{0, fa+f-ae-c\}$
- $\mu_i = \prod_{j=1}^{i} \left((\frac{a-j+1}{b+1+j(d+1)})(\frac{-\lambda_2}{\lambda_3})^i \right) \frac{\lambda_1}{(b+1)\lambda_3}$
- $\alpha := \frac{1}{E}(b+1+a(d+1)), \beta = \frac{1}{E}(d+1)$ in which $E = gcd(b+1+a(d+1), d+1)$
- l is some integer.

Theorem 3.3.5. *Let $A := k[X_1, X_2, X_3, X_4]$ and let D be a monomial triangular k-derivation on A.*

1. *If $\lambda_4 \neq 0$ then $ker(D) = k[exp(-sD)(X_1), exp(-sD)(X_2), exp(-sD)(X_3)]$ where $s = \lambda_4^{-1} X_4$;*
2. *If $\lambda_4 = 0$ and $\lambda_1\lambda_2\lambda_3 = 0$ then $ker(D) = k[F_1, F_2, F_3]$ for some F_i;*
3. *If $\lambda_4 = 0$,$\lambda_1\lambda_2\lambda_3 \neq 0$, $ae + c - fa - f < 0$ and $e - f < 0$, then $ker(D) = k[X_4, r_1, r_2, r_5]$ where r_i as above;*
4. *If $\lambda_4 = 0$,$\lambda_1\lambda_2\lambda_3 \neq 0$, $ae + c - fa - f \geq 0$ or $e - f \geq 0$ then $ker(D) = k[X_4, r_1, r_2]$ where r_i as above.*

Proof. (1): We use the ESSEN-algorithm described in section 3.1.2. If $\lambda_4 \neq 0$ then take $p = X_4$, $q = \lambda_4$ (and $l = 1$) and $s = \lambda^{-1}q$. Now

$$R_0 = k[exp(-sD)(X_1), exp(-sD)(X_2), exp(-sD)(X_3), q].$$

But since q is invertible in $k[X_1, X_2, X_3, X_4]$ any new step won't introduce any new elements. Hence R_0 is the complete kernel as stated.
(2): For this result we refer to [DF98].
(3): We will apply the algorithm described in section 3.1.2 again. Note $D(X_3) = \lambda_3 X_4^f$ and define $q = X_4$ and $s = X_3/D(X_3)$. Now when we want to calculate

$$r_i := q^{e_i} \exp(-sD)(X_i).$$

We know $ae + c - fa - f < 0$ and $e - f < 0$.

Claim: In this case one has

$$\begin{aligned} r_1 &= X_4^{fa+f-ae-c} X_1 - \textstyle\sum_{i=1}^{a} \mu_i X_2^{a-i} X_3^{b+1+i(d+1)} X_4^{(a-i)(f-e)}. \\ r_2 &= X_4^{f-e} X_2 - \tfrac{1}{d+1}\tfrac{\lambda_2}{\lambda_3} X_3^{d+1} \\ r_3 &= 0 \\ r_4 &= X_4 \end{aligned}$$

where μ_i is as in the theorem. The only thing which needs to be proved of this claim is that the formula for r_1 is correct. By the lemma following this proof we are done. Let $R_0 := k[r_1, r_2, r_3, r_4] = k[r_1, r_2, X_4]$. We want to calculate any new generators. For such a generator g we must have $X_4^l g = G(r_1, r_2)$ for some $G(U_1, U_2) \in k[U_1, U_2]$, $l \geq 1$. Hence $G(r_1, r_2) = 0(mod\ X_4)$. So $G(r_1(mod\ X_4), r_2(mod\ X_4)) = 0$. Hence $G(\mu_a X_3^{b+1+a(d+1)}, \frac{1}{d+1}\frac{\lambda_2}{\lambda_3} X_3^{d+1}) = 0$. If G is taken of minimal degree then it must be of the form $(c_1U_1)^\alpha - (c_2U_2)^\beta$ where $\alpha = \frac{1}{E}(d+1), \beta = \frac{1}{E}(b+1+a(d+1))$ in which $E = gcd(b+1+a(d+1), d+1)$ and $c_1 = \frac{1}{\mu_a}$, $c_2 = (d+1)\frac{\lambda_3}{\lambda_2}$. Hence we can take a maximal $l \in \mathbb{N}$ such that $X_4^{-l} G(r_1, r_2) \in A$. Say $r_5 := X_4^{-l} G(r_1, r_2) = X_4^{-l}(c_1 r_1^\alpha - c_2 r_2^\beta)$. Since l is taken as large as possible we have $r_5(mod\ X_4) \neq 0$. We now leave it to the reader to verify that $r_5 \mod (X_4)$ depends on X_2 (a real detailed proof would be very tedious: as a hint, notice that $r_5 \mod (X_4)$ is the lowest degree term with respect to X_4 of $G(r_1, r_2)$). It is easy to see that for any $\widetilde{G} \in k[U_1, U_2]$ satisfying $\widetilde{G}(r_1(mod\ X_4), r_2(mod\ X_4)) = 0$ G divides $\widetilde{G}$. Hence $R_1 = k[X_4, r_1, r_2, r_5]$ is a subset of $k^{[4]^D}$. Now let us attempt to construct another generator. Suppose we have $H \in k[U_1, U_2, U_3]$ such that $H(r_1, r_2, r_5) = X_4 \cdot (\text{something})$. Then $H(r_1(mod\ X_4), r_2(mod\ X_4), r_5(mod\ X_4)) = 0$. But since $r_5(mod\ X_4)$ depends on X_2 this means that H is independent of U_3 and that we have a polynomial from our previous step. Hence we find no more new generators and thus $ker(D) = R_1 = k[X_4, r_3, r_4, r_5]$.

(4): This case (in fact: these 3 cases) can be handled with similar arguments as in (3). For example, $e - f \geq 0$ and $ae + c - fa - f \geq 0$ brings up the problem of finding a polynomial G such that $G(r_1, r_2) = X_4 \cdot (\text{something})$ which means $0 = G(r_1(mod\ X_4), r_2(mod\ X_4))$. But in this case r_1 depends on X_1 while r_2 doesn't. Hence in this case one has no new generators. In fact, in all remaining cases one has no new generators. □

Lemma 3.3.6.

$$X_4^{fa+f-ae-c}exp(-sD)(X_1) = \\ X_4^{fa+f-ae-c}X_1 - \sum_{i=1}^{a}\mu_i X_2^{a-i}X_3^{b+1+i(d+1)}X_4^{(a-i)(f-e)}$$

where $\mu_i = \prod_{j=1}^{i}\left((\frac{a-j+1}{b+1+j(d+1)})(\frac{\lambda_2}{\lambda_3})^i\right)\frac{\lambda_1}{(b+1)\lambda_3}$.

Proof. One can of course compute that the formula is correct, but that is not so easy. However, we can use some grading-tricks: define two degree functions on A by means of

$$deg_1(X_1^{t_1}X_2^{t_2}X_3^{t_3}X_4^{t_4}) = t_3 + (d+1)t_2 + (a(d+1)+b+1)t_1 \\ deg_2(X_1^{t_1}X_2^{t_2}X_3^{t_3}X_4^{t_4}) = t_4 + ft_3 + (df+e)t_2 + (adf+ae+bf+c)t_1.$$

and define a multidegree $grad := (deg_1, deg_2)$ on A. So if we define $A_{n,m}$ as the linear k-span of the monomials M satisfying $grad(M) = (n,m)$ then $A := \bigoplus_{(n,m)\in\mathbb{N}^2} A_{n,m}$. Furthermore, a nice property of this grading is that $D(A_{n,m}) \subseteq A_{n-1,m}$, which can be easily checked. Using these properties it is an easy exercise to prove that for every monomial M occuring in $X_4^{fa+f-ae-c}exp(sD)(X_1)$ we have $grad(M) = grad(X_4^{fa+f-ae-c}X_1)$. Now if we restrict our map D to the linear space $A_{n,m}$ where $grad(X_4^{fa+f-ae-c}X_1) = (n,m)$ then D induces a linear map l from $A_{n,m}$ to $A_{n-1,m}$. Then since $X_4^{fa+f-ae-c}exp(-sD)(X_1) \in A_{n,m}$ we have $A_{n,m}^D = ker(l)$. The matrix of l with respect to the basis

$$\{X_1X_4^{fa+f-ae-c},\ X_2^aX_3^{b+1}X_4^{a(f-e)},\ X_2^{a-1}\quad X_3^{b+1+(d+1)}X_4^{(a-1)(f-e)},\dots \\ \dots, X_3^{b+1+a(d+1)}\}$$

of $A_{n,m}$ and the basis

$$\{X_2^aX_3^bX_4^{a(f-e)}, X_2^{a-1}X_3^{b+d+1}X_4^{(a-1)(f-e)}, \dots, X_3^{b+a(d+1)}\}$$

of $A_{n-1,m}$ we denote by $\mathcal{M}$. It has entries $m_{1,1} = \lambda_1$, $m_{i,i} = (a+1-i)\lambda_2$ for $i \geq 2$, $m_{i,i+1} = (b+1+(i-1)(d+1))\lambda_3$ for $i \geq 1$ and zeros elsewhere. It has dimension $(a+2)\times(a+1)$. The matrix has

corank 1 and is of maximal rank. Hence the kernel is one dimensional. Some calculation proves that the kernel is spanned by $e_1 - \sum_{i=0}^{a} \mu_i e_{i+2}$ where $e_1, \ldots, e_{a+2}$ is the standard basis and μ_i is exactly as previously described. Hence $A^D_{n,m}$ is one dimensional and generated by $X_4^{fa+f-ae-c}X_1 - \sum_{i=1}^{a} \mu_i X_2^{a-i} X_3^{b+1+i(d+1)} X_4^{(a-i)(f-e)}$. We know that $X_4^{fa+f-ae-c} exp(-sD)(X_1)$ is in $A_{n,m}$ and also in $ker(D)$. Hence

$$X_4^{fa+f-ae-c} exp(-sD)(X_1) = X_4^{fa+f-ae-c}X_1 - \sum_{i=1}^{a} \mu_i X_2^{a-i} X_3^{b+1+i(d+1)} X_4^{(a-i)(f-e)}.$$

□

3.4 The commuting derivations conjecture

3.4.1 Useful things about commuting derivations

As we saw in section 2.3 corollary 2.3.7 it is natural to look at sets $\mathcal{D}$ of locally nilpotent derivations which commute and are of maximal rank. We are especially interested in the case that $trdeg(A^{\mathcal{D}})$ equals 1. For this case the following conjecture can be posed (using remark 2.3.8):

Commuting Derivations Conjecture (CD(n)) :
If $D_1, \ldots, D_{n-1} \in LND(\mathbb{C}^{[n]})$ linearly independent over $\mathbb{C}^{[n]}$ such that $[D_i, D_j] = 0$ for all $1 \leq i, j \leq n-1$ (i.e. they all commute) then

$$\bigcap_{i=1}^{n-1} ker(D_i) = \mathbb{C}[f]$$

where f is a coordinate in $\mathbb{C}^{[n]}$.

We will prove this conjecture for $n = 3$. The following lemma we will need later on.

Lemma 3.4.1. *Let R be a domain, and $r \in R$ such that rR is a prime ideal. Then r is irreducible in R.*

Proof. Let $I := rR$. Suppose r is reducible, i.e. $r = ab$ for some $a, b \in R$ not invertible. Since $ab \in I$, a prime ideal, we have a or b in I. We may assume $a \in I$, thus $a = rs$ for some $s \in R$, and thus $rsb = ab = r$ and since R is a domain we get $sb = 1$, which means b is invertible, a contradiction. Hence r must be irreducible. □

The following theorem is a special case of the main theorem in [Kal01].

Theorem 3.4.2. *Let $f \in \mathbb{C}[X, Y, Z]$ such that $\mathbb{C}[X, Y, Z]/(f - \lambda) \cong \mathbb{C}^{[2]}$ for all but finitely many $\lambda \in \mathbb{C}$. Then f is a coordinate.*

Proof. In the main theorem in [Kal01] take $X' = \mathbb{C}^3$,
$U := \{\lambda \mid \mathbb{C}[X, Y, Z]/(f - \lambda) \cong \mathbb{C}^{[2]}\}$, $Z := f^{-1}(U)$, $p = f$. Then this theorem states p is a coordinate. □

The following follows from theorem 7 in [EV99]. $\eta(R)$ is the nilradical of some ring R.

Theorem 3.4.3. *Let A be a ring and let $p \in A^*$. Let $a \in A, G, F \in A[X]$ such that F is a coordinate in $A[X]$, $a \mod (pA)$ invertible, and $G(X) \mod (pA) \in \eta((A/pA)[X])$. Then $aF(X) + G(X) + pY$ is a coordinate in $A[X, Y]$.*

In the following lemma, the derivation δ_i (the restriction of D_i to A^{D_n}) is well-defined: for all $a \in A^{D_n}$ we have $0 = D_i(D_n(a)) = D_n(D_i(a))$, hence $D_i(A^{D_n}) \subseteq A^{D_n}$. We say that a $\mathbb{C}$-domain is a $\mathbb{C}$-algebra which is a domain.

Lemma 3.4.4. *Let A be a $\mathbb{C}$-domain and $D_1, \ldots, D_n$ be commuting locally nilpotent derivations which are linearly independent over A. Let $\delta_i := D_i|_{A^{D_n}}$. Then $\delta_1, \ldots, \delta_{n-1}$ are linearly independent over A^{D_n}.*

Proof. Suppose that $\sum a_i\delta_i = 0$ for some $a_i \in A^{D_n}$. Since D_n is nonzero there exists a preslice $p \in A$ for D_n, i.e. an element p which satisfies $d := D_n(p) \neq 0$ and $D_n^2(p) = 0$ (i.e. $d \in A^{D_n}$). Let $s := pd^{-1} \in A[d^{-1}]$. Then $D_n(s) = 1$. Furthermore, by [Ess00] pages 27-28, $A[d^{-1}] = A^{D_n}[d^{-1}][s]$. Let $a := \sum a_i D_i(s) \in A[d^{-1}]$, say $\tilde{a} := d^m a \in A$. So

$$(\sum_{i=1}^{n-1} a_i d^m D_i)(s) = d^m a = \tilde{a} = \tilde{a} D_n(s).$$

Also by our hypothesis

$$\sum_{i=1}^{n-1} a_i d^m D_i - \tilde{a} D_n = 0$$

on A^{D_n}. Since $A \subset A^{D_n}[d^{-1}][s]$ it follows that $\sum a_i d^m D_i = \tilde{a} D_n$. From the linear independence of the D_i over A we deduce that $d^m a_i = 0$ for all i, whence $a_i = 0$ for all i. □

Proposition 3.4.5. *Let A be a $\mathbb{C}$-domain with $trdeg_{\mathbb{C}}Q(A) = n(\geq 1)$. Let $D_1, \ldots, D_n$ be commuting locally nilpotent $\mathbb{C}$-derivations on A which are linearly independent over A. Then*

(i). There exist s_i in A such that $D_i s_j = \delta_{ij}$ for all i, j and

(ii). $A = \mathbb{C}[s_1, \ldots, s_n]$ a polynomial ring in $s_1, \ldots, s_n$ over $\mathbb{C}$.

Proof. We use induction on n. The case $n = 1$ is well-known (cor. 1.3.33 [Ess00]). So let $n \geq 2$. $trdeg_{\mathbb{C}}(A^{D_n}) = n - 1$ and according to lemma 3.4.4 the derivations $\delta_i := D_i|_{A^{D_n}}$ $1 \leq i \leq n-1$ satisfy the hypothesis of the proposition. So by induction there exist $s_i \in A^{D_n}$ such that $\delta_i s_j = \delta_{ij}$ and $A^{D_n} = \mathbb{C}[s_1, \ldots, s_{n-1}]$. So the first $n-1$ derivations have a slice in A. Similarly D_n has a slice s_n in $A^{D_1} \subset A$. Then from $A = A^{D_n}[s_n]$ the result follows. □

3.4.2 Proof of $CD(3)$

This proof will appear in [Mau].

Proposition 3.4.6. *Let A be an affine $\mathbb{C}$-domain such that $trdeg_{\mathbb{C}}Q(A) = n$ and $A^* = \mathbb{C}^*$. If A is a* UFD *and $D_1, \ldots, D_{n-1}$ are commuting locally nilpotent $\mathbb{C}$-derivations on A which are linearly independent over A, then $\cap A^{D_i} = \mathbb{C}[g]$ for some $g \in A$ which satisfies $g - c$ is irreducible in A for all $c \in \mathbb{C}$.*

Proof. Put $B := \cap A^{D_i}$. By lemma 2.3.7 we have $trdeg_{\mathbb{C}}B = n - (n - 1) = 1$. Also B is a UFD (see [Ess00] cor. 1.3.36) and $B = A \cap Q(B)$. Since $trdeg_{\mathbb{C}}Q(B) = 1$ it follows from special case of Hilbert 14 (using B is normal since it is a UFD) that B is a finitely generated $\mathbb{C}$-algebra. So B is an affine domain of krull dimension one. It is a well-known result that if $B^* = \mathbb{C}^*$, B is a UFD and B is an affine domain of krull dimension one, that $B = \mathbb{C}[g] \cong_{\mathbb{C}} \mathbb{C}^{[1]}$. (See for example [Mya78].) Since $g - c$ is irreducible in $\mathbb{C}[g]$ for all $c \in \mathbb{C}$ and B is factorially closed in A it follows that $g - c$ is also irreducible in A (see [Ess00] exercise 6, 1.3). □

The following proposition the author proved together with A. van den Essen and P.van Rossum.

Proposition 3.4.7. *Let D_1, D_2 be two linearly independent (over $\mathbb{C}[X, Y, Z]$) commuting locally nilpotent $\mathbb{C}$-derivations. Then there exists $g \in \mathbb{C}[X, Y, Z] \backslash \mathbb{C}$ such that*

(i). $\mathbb{C}[X, Y, Z]^{D_1, D_2} = \mathbb{C}[g]$

(ii). $\mathbb{C}[X, Y, Z]_{b(g)} = \mathbb{C}[f, g, p]_{b(g)}$ *for some* $f, p \in \mathbb{C}[X, Y, Z]$ *and* $b(g) \in \mathbb{C}[g] \backslash \{0\}$

(iii). $\mathbb{C}[X, Y, Z]/(g - \lambda) \cong_{\mathbb{C}} \mathbb{C}^{[2]}$ *for all* $\lambda \in \mathbb{C}$ *with* $b(\lambda) \neq 0$.

Proof. *(i)* $\mathbb{C}[X,Y,Z]^{D_1} = \mathbb{C}[f,g]$ and $\mathbb{C}[X,Y,Z]^{D_2} = \mathbb{C}[p,q]$ by [Mya78]. Since D_1, D_2 commute we have $D_2(\mathbb{C}[f,g]) \subseteq \mathbb{C}[f,g]$. Write $d_2 := D_2|_{\mathbb{C}[f,g]}$. By lemma 3.4.4 it follows that $d_2 \neq 0$ on $\mathbb{C}[f,g]$. So by Rentschler's theorem we may assume that $d_2 = a(g)\frac{\partial}{\partial f}$ i.e. $D_2(g) = 0$ and $D_2(f) = a(g) \neq 0$. So $\mathbb{C}[X,Y,Z]^{D_1,D_2} = \mathbb{C}[f,g]^{d_2} = \mathbb{C}[g]$ i.e.

$$\mathbb{C}[X,Y,Z]^{D_1,D_2} = \mathbb{C}[g]. \tag{3.3}$$

Similarly we get $D_1(\mathbb{C}[p,q]) \subset \mathbb{C}[p,q]$ and putting $d_1 := D_1|_{\mathbb{C}[p,q]}$ this gives by Rentschler that we may assume $d_1 = b(q)\frac{\partial}{\partial p}$ for some $b(q) \neq 0$. So

$$\mathbb{C}[X,Y,Z]^{D_1,D_2} = \mathbb{C}[p,q]^{d_1} = \mathbb{C}[q]. \tag{3.4}$$

From (3.3) and (3.4) we deduce that $\mathbb{C}[g] = \mathbb{C}[q]$, whence $g = \lambda q + \mu$ for some $\lambda \in \mathbb{C}^*$ and $\mu \in \mathbb{C}$. Replacing q by g (and hence $b(q) = b(\lambda^{-1}(g-\mu) = \tilde{b}(g)$ by $\tilde{b}(g)$ we get that we may assume the following

$$\begin{array}{l} \mathbb{C}[X,Y,Z]^{D_1} = \mathbb{C}[f,g], D_1 f = D_1 g = 0, D_1 p = b(g) \neq 0 \\ \mathbb{C}[X,Y,Z]^{D_2} = \mathbb{C}[p,g], D_2 f = a(g) \neq 0, D_2 g = D_2 p = 0. \end{array}$$

(ii) Also $\mathbb{C}[f,g,p] \cong_{\mathbb{C}} \mathbb{C}^{[3]}$ (for if p depends on $\mathbb{C}[f,g]$ then $D_1 p = 0$, contradiction). Observe that $D_1 p = b(g) \neq 0$ and $D_1^2 p = D_1 b(g) = 0$, so $s := p/b(g) \in \mathbb{C}[X,Y,Z]_{b(g)}$ satisfies $D_1 s = 1$, whence $\mathbb{C}[X,Y,Z]_{b(g)} = \mathbb{C}[f,g]_{b(g)}[s] = \mathbb{C}[f,g,p]_{b(g)}$.
(iii) Given $\mathbb{C}[X,Y,Z]_{b(g)} = \mathbb{C}[f,g,p]_{b(g)}$, we have

$$\big(\mathbb{C}[X,Y,Z]_{b(g)}\big)/(g-\lambda) = \big(\mathbb{C}[f,g,p]_{b(g)}\big)/(g-\lambda).$$

If $b(\lambda) \in \mathbb{C}^*$ we have $\mathbb{C}[X,Y,Z]/(g-\lambda) = \mathbb{C}[f,g,p]/(g-\lambda)$. Now $f \mod (g-\lambda), p \mod (g-\lambda)$ are generators of this algebra. Since it is of transcendence degree 2 they are algebraically independent and thus $\mathbb{C}[X,Y,Z]/(g-\lambda)$ is isomorphic to $\mathbb{C}^{[2]}$. □

Theorem 3.4.8. *CD(3) is true, i.e. let D_1, D_2 be two linearly independent (over $\mathbb{C}[X,Y,Z]$) commuting locally nilpotent $\mathbb{C}$-derivations, then $A^{D_1,D_2} = \mathbb{C}[g]$ and g is a coordinate in $\mathbb{C}[X,Y,Z]$.*

Proof. Combining 3.4.7 and 3.4.2 gives exactly this result. □

3.4.3 Coordinates $p(X)Y + q(X, Z_1, \ldots, Z_{n-1})$

Theorem 3.4.9. *Assume AS(n-1), CD(n) and CC(n-1). Let* $F := p(X)Y + q(X, Z_1, \ldots, Z_{n-1})$ *where* $p(X) \neq 0$. *Then equivalent are:*

(i). F *is a coordinate in* $\mathbb{C}[X, Y, Z_1, \ldots, Z_{n-1}]$

(ii). $\mathbb{C}[X, Y, Z_1, \ldots, Z_{n-1}]/(F) \cong_{\mathbb{C}} \mathbb{C}^{[n]}$

(iii). $q(a, Z_1, \ldots, Z_{n-1})$ *is a coordinate in* $\mathbb{C}[Z_1, \ldots, Z_{n-1}]$ *for every zero* a *of* $p(X)$.

(iv). F *is a coordinate over* $\mathbb{C}[X]$ *in* $\mathbb{C}[X, Y, Z_1, \ldots, Z_{n-1}]$

Proof. (*of theorem 3.4.9)*
From 3.4.13 we have *(iii)*$\Longrightarrow$*(iv).* *(iv)*$\Longrightarrow$*(i)* and *(i)*$\Longrightarrow$*(ii)* follow since they are weaker statements in general. *(ii)*$\Longrightarrow$*(iii)* follows from 3.4.15. □

From the fact that AS(2), CC(2) and CD(3) (see 3.4.8) are true, we can deduce the following corollaries:

Corollary 3.4.10. *The above equivalences hold for* $F = p(X)Y + q(X, Z_1, Z_2)$.

Corollary 3.4.11. *AS(4) is true if restricted to polynomials of the form* $p(X)Y + q(X, Z, T)$.

Lemma 3.4.12. *Let* $q(Z_1, \ldots, Z_{n-1}) \in \mathbb{C}[Z_1, \ldots, Z_{n-1}]$. *Suppose AS(n-1) and CC(n-1) are true. If* $\mathbb{C}[Z_1, \ldots, Z_{n-1}, Y]/(q) \cong_{\mathbb{C}} \mathbb{C}^{[n-1]}$ *then* q *is a coordinate in* $\mathbb{C}^{[n-1]}$.

Proof. $\mathbb{C}[Z_1, \ldots, Z_{n-1}]/(q)[Y] \cong_{\mathbb{C}} \mathbb{C}^{[n-1]}$ so by CC(n-1) we have $\mathbb{C}[Z_1, \ldots, Z_{n-1}]/(q) \cong_{\mathbb{C}} \mathbb{C}^{[n-2]}$ and by AS(n-1) we have q is a coordinate in $\mathbb{C}^{[n-1]}$. □

Write

$$p(X) = \Pi_{i=1}^{r}(X - \alpha_i)^{e_i}$$

for some $e_i \in \mathbb{N}$, and $F := p(X)Y + q(X, Z_1, \ldots, Z_{n-1})$ for some $q \in \mathbb{C}[X, Z_1, \ldots, Z_{n-1}]$.

Theorem 3.4.13. *Let $q(X, Z_1, \ldots, Z_{n-1})$ be such that $q(\alpha_i, Z_1, \ldots, Z_{n-1})$ is a coordinate in $\mathbb{C}[Z_1, \ldots, Z_{n-1}]$ for every $1 \leq i \leq r$. Then $F := p(X)Y + q(X, Z_1, \ldots, Z_{n-1})$ is a coordinate in $\mathbb{C}[X, Y, Z_1, \ldots, Z_{n-1}]$ over $\mathbb{C}[X]$.*

Proof. Using theorems 2.1.1 part 4 and 3.7.11 from [Ros01], we see that it suffices to prove that F is a coordinate in $\mathbb{C}[X]_{\mathfrak{m}}[Y, Z_1, \ldots, Z_{n-1}]$ over $\mathbb{C}[X]_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m} \subset \mathbb{C}[X]$. Let $\mathfrak{m} = (X - \alpha)$ for some $\alpha \in \mathbb{C}$. Notice that if $a(X) \in \mathbb{C}[X]$ we have $a \in \mathbb{C}[X]^*_{\mathfrak{m}}$ if and only if $a(\alpha) \neq 0$. In case $\alpha \neq \alpha_i$ we have $p(\alpha) \neq 0$ and hence F is a coordinate in $\mathbb{C}[X]_{\mathfrak{m}}[Y, Z_1, \ldots, Z_{n-1}]$. Left to prove the case $\alpha = \alpha_1$ ($\alpha = \alpha_i$ has the same proof). Let $q_1(Z_1, \ldots, Z_{n-1}) := q(\alpha, Z_1, \ldots, Z_{n-1})$ (hence a coordinate in $\mathbb{C}^{[n-1]}$), and define

$$\tilde{p} := \Pi_{i=2}^{r}(X - \alpha_i)^{e_i} = p(X)(X - \alpha)^{-e_1}.$$

Now

$$F = (X - \alpha)^{e_1}\tilde{p}(X)Y + q_1 + (X - \alpha)h(X, Z_1, \ldots, Z_{n-1})$$

for some h. Notice $\tilde{p} \in \mathbb{C}[X]^*_{\mathfrak{m}}$. But now, using 3.4.3 we have F is a coordinate in $\mathbb{C}[X]_{\mathfrak{m}}[Y, Z_1, \ldots, Z_{n-1}]$. □

Lemma 3.4.14. *Let $F = p(X)Y + q(X, Z_1, \ldots, Z_{n-1})$ be irreducible. Then there exists $\lambda \in \mathbb{C}$ such that $X - \lambda \mod (F)$ is irreducible in $\mathbb{C}[X, Y, Z_1, \ldots, Z_{n-1}]/(F)$.*

Proof. Take λ such that $p(\lambda) \neq 0$. Then

$$\begin{array}{rl} \mathbb{C}[X, Y, Z_1, \ldots, Z_{n-1}]/(F, X - \lambda) & = \\ \mathbb{C}[Y, Z_1, \ldots, Z_{n-1}]/(p(\lambda)Y + q(\lambda, Z_1, \ldots, Z_{n-1})) & \cong_{\mathbb{C}} \mathbb{C}^{[n-1]} \end{array}$$

which is a domain: hence $(X - \lambda, F)$ is prime, and thus $X - \lambda \mod F$ is irreducible by lemma 3.4.1. □

Lemma 3.4.15. *Assume CD(n), CC(n-1) and AS(n-1). Let $F := p(X)Y + q(X, Z_1, \ldots, Z_{n-1})$ and assume $\mathbb{C}^{[n+1]}/(F) \cong_{\mathbb{C}} \mathbb{C}^{[n]}$. Then $q(a, Z_1, \ldots, Z_{n-1})$ is a coordinate in $\mathbb{C}[Z_1, \ldots, Z_{n-1}]$ for all zeros a of $p(X)$.*

Proof. Ofcourse we assume that all Z_i occur in q for otherwise we are dealing with a lower dimensional case. Let

$$D_i := \frac{\partial q}{\partial Z_i}\frac{\partial}{\partial Y} - p\frac{\partial}{\partial Z_i}$$

be derivations on $\mathbb{C}^{[n+1]}$ for all $1 \leq i \leq n-1$. These derivations are triangular derivations since

$$\begin{array}{c} D(Y) \in \mathbb{C}[Z_1, \ldots, Z_n, X], \\ D(Z_i) \in \mathbb{C}[Z_{i+1}, \ldots, Z_n, X] \\ \text{and } D(X) \in \mathbb{C} \end{array}$$

and it is not difficult to see that a triangular derivation is locally nilpotent (see for example [Ess00], corollary 1.3.17). It is clear that $[D_i, D_j] = 0$, and that the D_i are linearly independent over $\mathbb{C}[X, Y, Z_1, \ldots, Z_{n-1}]$. Now we know

$$\mathbb{C}^{[n+1]}/(F) \cong_{\mathbb{C}} \mathbb{C}^{[n]}.$$

Furthermore $D_i(F) \subset (F)$, so the derivations $\bar{D}_i := D_i \mod (F)$ are well-defined on $\mathbb{C}^{[n+1]}/(F) \cong \mathbb{C}^{[n]}$. Also they are independent over $\mathbb{C}^{[n+1]}/(F)$. Since we assumed CD(n) we have

$$\bigcap_{i=1}^{n-1} ker(\bar{D}_i) = \mathbb{C}[g]$$

for some coordinate g. Since $ker(\bar{D}_i) \supset \mathbb{C}[\bar{X}]$ we see $\mathbb{C}[g] \supset \mathbb{C}[\bar{X}]$. By lemma 3.4.14 we see that $X - a$ is irreducible in $\mathbb{C}^{[n+1]}/(F)$ for some $a \in \mathbb{C}$. Now $X - a = Q(g)$ for some polynomial $Q(T) \in \mathbb{C}[T]$. Decomposing $Q(T)$ into linear factors $T - \lambda_i$ and observing that $g - \lambda_i$ is irreducible in $\mathbb{C}^{[n+1]}/(F)$ (since g is a coordinate in it), it follows that $g - \lambda_i$ divides the irreducible element $X - a$. So $X - a = bg + c$ for some $b \in \mathbb{C}^*, c \in \mathbb{C}$. Thus $\mathbb{C}[g] = \mathbb{C}[X]$, and $X - \alpha$ is a coordinate in $\mathbb{C}^{[n+1]}/(F) \cong_{\mathbb{C}} \mathbb{C}^{[n]}$ for every $\alpha \in \mathbb{C}$. So

$$\mathbb{C}^{[n-1]} \cong_{\mathbb{C}} \mathbb{C}^{[n+1]}/(F, X - \alpha) \text{ for all } \alpha \in \mathbb{C}.$$

In case $p(\alpha) = 0$ we have

$$\mathbb{C}^{[n-1]} \cong_{\mathbb{C}} \mathbb{C}[Y, Z_1, \ldots, Z_{n-1}]/(q(\alpha, Z_1, \ldots, Z_{n-1})$$

and thus by CC(n-1) and AS(n-1) and lemma 3.4.12 we have $q(\alpha, Z_1, \ldots, Z_{n-1})$ is a coordinate in $\mathbb{C}[Z_1, \ldots, Z_{n-1}]$. □

3.5 An extension of the concept of coordinate

This section deals with a lot of conjectures, and an attempt to generalise the concept of stable coordinate for elements in a quotient ring of a polynomial ring.

Definition 3.5.1. Let $I = (f_1, \ldots, f_m)$ be an ideal in $\mathbb{C}[X_1, \ldots, X_n] = \mathbb{C}^{[n]}$. Let $r \in \mathbb{C}^{[n]}$. Define $r + (I) \in \mathbb{C}^{[n]}/I$ is a *generalised coordinate in* $\mathbb{C}^{[n]}/I$ if $f_1Y_1 + \ldots + f_mY_m + r \in \mathbb{C}^{[n+m]}$ is a stable coordinate.

The definition does not depend on the generators of I as can be seen from

Lemma 3.5.2. *Let* $I = (f_1, \ldots, f_m) = (g_1, \ldots, g_l)$ *be an ideal in* $\mathbb{C}[X_1, \ldots, X_n] = \mathbb{C}^{[n]}$. *Let* $r \in \mathbb{C}^{[n]}$. *Then* $f_1Y_1 + \ldots + f_mY_m + r \in \mathbb{C}^{[n+m]}$ *can be mapped to* $g_1Z_1 + \ldots + g_lZ_l + r$ *by an automorphism of* $\mathbb{C}[X, Y, Z] = \mathbb{C}^{[n+m+l]}$.

Proof. Let $F := f_1Y_1 + \ldots + f_mY_m + r$ and $G := g_1Z_1 + \ldots + g_lZ_l + r$. We will show that there is an automorphism of $\mathbb{C}[X, Y, Z]$ sending F to G. Since $(g_1, \ldots, g_l) = (f_1, \ldots, f_m)$ in $\mathbb{C}[X]$ we have $g_i = a_{i1}f_1 + \ldots + a_{im}f_m$ for some $a_{ij} \in \mathbb{C}[X]$. Let $L_j := a_{1j}Z_1 + \ldots + a_{lj}Z_l$ for $1 \leq j \leq m$. Notice that

$$G = f_1L_1 + \ldots + f_mL_m + r.$$

Now let φ be the elementary automorphism sending Y_j to $Y_j + L_j$ for each j and leaving other variables invariant. Then

$$\begin{aligned} \varphi(F) &= f_1\varphi(Y_1) + \ldots + f_m\varphi(Y_m) + r \\ &= f_1(Y_1 + L_1) + \ldots + f_m(Y_m + L_m) + r \\ &= F + f_1L_1 + \ldots + f_mL_m \\ &= F + G - r \end{aligned}$$

In the same way we can make an automorphism τ sending G to $G + F - r$, so F can be mapped to G by $\tau^{-1}\varphi$. □

Conjecture 3.5.3. "Generalised coordinate" is an extension of the concept of "stable coordinate". In other words, if I is an ideal in $\mathbb{C}^{[n+m]}$ and if $r \in \mathbb{C}^{[n+m]}/I$ is a generalised coordinate, and $\mathbb{C}^{[n+m]}/I \cong_{\mathbb{C}} \mathbb{C}^{[n]}$ then r is a stable coordinate.

Trying to decide if polynomials of the form $P(X_1, \ldots, X_n)Y + Q(X_1, \ldots, X_n)$ are coordinates might be a good idea in combination with the next question to give an algorithm to decide whether a polynomial is a coordinate:

Question: Is there an algorithm which decides of (lots of) $F \in \mathbb{C}[X_1, \ldots, X_n]$ if there exists a ring automorphism φ such that $\varphi(F)$ is linear in X_n ? (

For if for some F such a φ doesn't exist then it is no coordinate, and if it does it is of the above shape.

Another possible different approach of extending the concept of (stable) coordinate to a more general ring is looking for (stable) slices in such a ring:

Definition 3.5.4.

(i). Let R be a finitely generated $\mathbb{C}$-algebra. Say $s \in R$ is a *slice in* R if there exists a locally nilpotent $\mathbb{C}$-derivation on R such that $D(s) = 1$.

(ii). Let R be a finitely generated $\mathbb{C}$-algebra. Say $s \in R$ is a *stable slice in* R if there exists some $n \in \mathbb{N}$ and a locally nilpotent $\mathbb{C}$-derivation on $R[T_1, \ldots, T_n]$ such that $D(s) = 1$.

"Slice" and "stable slice" are extensions of the concept of coordinate, since every coordinate over a polynomial ring induces a locally nilpotent derivation having the coordinate as slice. So we can ask the same question for "stable slice" as we did for "generalised coordinate" (conjecture 3.5.3):

Conjecture 3.5.5. "Stable slice" is an extension of the concept of "stable coordinate". In other words: let $(f_1, \ldots, f_m) = I \subset \mathbb{C}^{[n]}$ be an ideal. Let $s \in \mathbb{C}^{[n]}$. Then s is a stable slice in $\mathbb{C}^{[n]}/I$ if and only if $s + f_1T_1 + \ldots + f_mT_m$ is a stable coordinate in $\mathbb{C}^{[n+m]}$.

Independently of the conjectures 3.5.3 and 3.5.5 one can make the following (two) conjecture(s):

Conjecture 3.5.6. Let $s \in \mathbb{C}[X_1, \ldots, X_n]$. Then

(i). s is a stable slice $\Longrightarrow$ s is a generalised coordinate.

(ii). s is a generalised coordinate $\Longrightarrow$ s is a stable slice.

3.6 The Derksen and Makar-Limanov invariants

In this section we will compare the ML invariant and the HD invariant. The results are joint work of T.Crachiola and the author. [CM]

3.6.1 Makar-Limanov invariant trivial, Derksen invariant not

n this section we will give a ring whose Makar-Limanov invariant is trivial but its Derksen invariant is not.

Definition 3.6.1. Define the ideal $I := (X, Y) \subset \mathbb{C}[X, Y]$, and let

$$\begin{aligned} R := &\ \mathbb{C}[X^2, X^3, Y^3, Y^4, Y^5, X^{1+i}Y^{1+j} \mid i, j \in \mathbb{N}] \\ = &\ \mathbb{C}[X^2, X^3, Y^3, Y^4, Y^5, XY, X^2Y, XY^2, XY^3] \end{aligned}$$

(i.e. $R = \mathbb{C} \oplus \mathbb{C}X^2 \oplus \mathbb{C}XY \oplus I^3$).

Notice that R is finitely generated, noetherian, and a domain.

Lemma 3.6.2. $ML(R) = \mathbb{C}$.

Proof. Let $D_1 := Y^3\partial_X$ and $D_2 := X^2\partial_Y$. These are locally nilpotent derivations on R, as can be easily checked. Then $R^{D_1} = R \cap \mathbb{C}[X,Y]^{D_1} \subseteq \mathbb{C}[X,Y]^{D_1} = \mathbb{C}[Y]$. Also $R^{D_2} = R \cap \mathbb{C}[X,Y]^{D_2} \subseteq \mathbb{C}[X,Y]^{D_2} = \mathbb{C}[X]$. Thus $\mathbb{C} \subseteq ML(\mathbb{C}) \subseteq R^{D_1} \cap R^{D_2} \subseteq \mathbb{C}[X,Y]^{D_1} \cap \mathbb{C}[X,Y]^{D_2} = \mathbb{C}[Y] \cap \mathbb{C}[X] = \mathbb{C}$. □

In order to calculate $HD(R)$ we first show that every locally nilpotent derivation on R actually comes from a locally nilpotent derivation on $\mathbb{C}[X,Y]$

Lemma 3.6.3. *(i). The integral closure of R in $\mathbb{C}[X,Y]$ is $\mathbb{C}[X,Y]$.*

(ii). The integral closure of R in $Q(R)$ (the fraction field of R) is $\mathbb{C}[X,Y]$.

Proof. (i) is easy, since the integral closure of the smaller ring $\mathbb{C}[X^2,Y^3]$ in $\mathbb{C}[X,Y]$ already is $\mathbb{C}[X,Y]$. *(ii)* $Q(R) = \mathbb{C}(X,Y)$. Let $a \in Q(R)$ be integral over R. Then surely a is integral over $\mathbb{C}[X,Y]$. But $\mathbb{C}[X,Y]$ is a UFD and thus integrally closed in its fraction field i.e. $a \in \mathbb{C}[X,Y]$ already. Thus the integral closure of R in $Q(R)$ is a subset of $\mathbb{C}[X,Y]$. Finally, since $Q(R) = \mathbb{C}(X,Y)$ and by part *(i)* we are done. □

Notice that if D is a derivation (not necessarily locally nilpotent) on a domain A, then it extends uniquely to a derivation on the fraction field $Q(A)$ of A, by just forcing $D(a^{-1}b) = a^{-2}(aD(b) - D(a)b)$ for all $a \in A, b \in A\backslash\{0\}$.

Theorem 3.6.4. *(Seidenberg) Let A be a noetherian domain containing $\mathbb{Q}$, K its quotient field and $\tilde{A}$ the integral closure of A in K. Let D be a derivation on A and $\tilde{D}$ its unique extension to K. Then $\tilde{D}(\tilde{A}) \subseteq \tilde{A}$.*

This is quoted literally from [Ess00] prop. 1.2.15 page 17, but it is originally from [Sei66].

Lemma 3.6.5. *If D is a locally nilpotent derivation on R then it extends uniquely to a locally nilpotent derivation on $\mathbb{C}[X,Y] \longrightarrow \mathbb{C}[X,Y]$.*

Proof. The integral closure of R in $Q(R)$ is $\mathbb{C}[X,Y]$ (by 3.6.3). So by the above theorem of Seidenberg D extends uniquely to $\mathbb{C}[X,Y]$. By theorem 2.2.8 we see that D is locally nilpotent. □

Lemma 3.6.6. *If $f \in \mathbb{C}[X,Y]$ is a coordinate, $p(T) \in \mathbb{C}[T]$ and $p(f) \in R$ then XY does not appear as a monomial in $p(f)$.*

Proof. $f = f_0 + f_1 = f_0 + aX + bY + cX^2 + dXY + eY^2 + g$ for some $g \in I^3$ and $a \neq 0$ or $b \neq 0$. Now $p(f) = q(f_1)$ for some $q(T) \in \mathbb{C}[T]$.

$$\begin{aligned} q(f_1) = &\ \lambda_0 + \lambda_1 f_1 + \lambda_2 f_1^2 + \ldots + \lambda_n f_1^n \\ = &\ \lambda_0 + \lambda_1(aX + bY + cX^2 + dXY + eY^2) + \\ &\ \lambda_2(aX + bY + cX^2 + dXY + eY^2)^2 + g' \quad g' \in I^3 \end{aligned}$$

and since $a \neq 0$ or $b \neq 0$ and $q(f) \in R$ we must have $\lambda_1 = 0$. Thus

$$\begin{aligned} q(f) = &\ \lambda_0 + \lambda_2(aX + bY + cX^2 + dXY + eY^2)^2 + g' \quad g' \in I^3 \\ = &\ \lambda_0 + \lambda_2(a^2X^2 + 2abXY + b^2Y^2) + g'' \quad g'' \in I^3 \end{aligned}$$

but since in no element of R appears the monomial Y^2 and $q(f) \in R$ we must have $\lambda_2 b^2 = 0$ which implies $2\lambda_2 ab = 0$, which is the coefficient of XY. □

Lemma 3.6.7. *Let $D \in LND(R)$. Suppose there exists $g \in R^D$ such that the coefficient of XY of g is nonzero (XY appears in g). Then $D = 0$.*

Proof. We know by 3.6.5 that D can be extended as a locally nilpotent derivation to $\mathbb{C}[X,Y]$. Suppose $D \neq 0$. Thus $\mathbb{C}[X,Y]^D = \mathbb{C}[f]$ for some coordinate f by Rentschler's theorem. Hence $g = p(f) \in R^D$. But now by lemma 3.6.6, the coefficent of XY must be zero, a contradiction. Hence our assumption that D was nonzero was wrong, thus $D = 0$. □

Lemma 3.6.8. *$HD(R) \neq R$.*

Proof. If we show that $XY \notin HD(R)$ then we are done. Suppose $g_1, \ldots, g_n \in R$ are elements of kernels of nonzero locally nilpotent derivations such that $XY = p(g_1, \ldots, g_n)$ for some $p \in \mathbb{C}[T_1, \ldots, T_n]$. Then since $g_i \in R$ we have that $g_i = c_i + a_i X^2 + b_i XY + h_i$ for some $a_i, b_i, c_i \in \mathbb{C}, h_i \in (X^3, X^2Y, XY^2, Y^3)$. We may assume that $c_i = 0$. Furthermore by lemma 3.6.7 $b_i = 0$. Let p' be the part of p which is linear. Now $XY = p'(a_1X^2, \ldots, a_nX^2) + h'$ for some $h' \in (X^3, X^2Y, XY^2, Y^3)$. This gives a contradiction. □

3.6.2 Derksen invariant trivial, Makar-Limanov invariant not

In this section we will give a class of rings with trivial Derksen invariant but non-trivial Makar-Limanov invariant. Let A be a commutative domain over $\mathbb{C}$ with transcendence degree 1 such that A is not isomorphic to $\mathbb{C}[X]$. For example, take A to be the coordinate ring of a curve which is not isomorphic to the line. We will examine the ring $R := A[X_1, \ldots, X_n]$ for $n \geq 2$.

Lemma 3.6.9. *$HD(R) = R$.*

Proof. The kernels of the partial derivatives generate R. □

Of course, the same observation shows that a polynomial ring with at least two variables over any algebra always has trivial Derksen invariant. Lemma 3.6.9 and Example 2.4.2 are special cases. To show that $ML(R) \neq \mathbb{C}$, we will use the following

Theorem 3.6.10. *(Makar-Limanov) Suppose A is a commutative domain over $\mathbb{C}$ with transcendence degree 1. Then $ML(A[X_1, \ldots, X_n]) = ML(A)$ for each $n \geq 1$.*

This theorem provides an alternate proof of the Abhyankar-Eakin-Heinzer cancellation theorem for curves [AEH72], in the characteristic zero case. For a proof of Theorem 3.6.10, see [ML02] or [ML98].

Lemma 3.6.11. *$ML(R) = A$.*

Proof. By Theorem 3.6.10, $ML(R) = ML(A)$. Suppose $ML(A) \neq A$, so that there exists a non-zero locally nilpotent derivation D on A. But now $trdeg(A^D) = trdeg(A) - 1 = 0$ and thus $A^D = \mathbb{C}$. Take $a \in A$ such that $D(a) = \lambda \neq 0$, then $s := \lambda^{-1}a$ is a slice and thus $A = A^D[s] = \mathbb{C}[s]$. This contradicts our original assumption on A, thus $ML(A) = A$ and we are done. □

Notice that $trdeg(R) > 2$ for the class of rings R in this section. This is a necessary condition for an example of our type. Using the fact that the kernel of a locally nilpotent derivation is algebraically closed, one can show that if $trdeg(R) = 1$ or 2 and $HD(R) = R$, then $ML(R) = \mathbb{C}$.

3.6.3 Derksen and Makar-Limanov invariants equal

Finally, in this section we will give a class of rings whose Derksen and Makar-Limanov invariants are both non-trivial. Let R be the ring over $\mathbb{C}$ given by the equation $x^n y = P(z)$, where $n > 1$ and $deg(P) > 1$. Danielewski used surfaces of this type to give a negative answer to the generalized Zariski cancellation question [Dan89]. We make use of the following

Theorem 3.6.12. *$LND(R) = x^n\mathbb{C}[x]\frac{\partial}{\partial z}$, where R is viewed as a subring of $\mathbb{C}[x, x^{-1}, z]$.*

For the proof, see [ML01]. In particular, the kernel of every locally nilpotent derivation on R is $\mathbb{C}[x]$. As a result, we have

Lemma 3.6.13. $HD(R) = ML(R) = \mathbb{C}[x]$.

Chapter 4

Polynomial mappings

4.1 Problems over reduced rings

4.1.1 The linearisation conjecture over reduced rings

Introduction

The results of this section have been published in [Mau02b].

We introduce some notations. As always, R is a $\mathbb{Q}$-algebra, $A = R[X_1, \ldots, X_n]$, $\mathfrak{n}$ the nilradical of R, $\bar{R} = R/\mathfrak{n}$, $\bar{A} = A/\mathfrak{n}A = \bar{R}[X_1, \ldots, X_n]$. Write $I = (X_1, \ldots, X_n)$. If $F \in A^n$ write $\bar{F} = F \mod(\mathfrak{n})$. s will be some integer. If we write $F = L + H$ we mean that L is linear and H contains no linear monomials (all monomials are of degree at least 2).

Definition 4.1.1. We say that $F \in A^n$ is *linearisable in* R if there exists an R-automorphism $\varphi \in A^n$ such that $\varphi^{-1} F \varphi = L$ where L is a linear map.

Theorem 4.1.2. *Let $F^s = I$. Then the following are equivalent:*

1. *F is linearisable over R.*

2. *$\bar{F}$ is linearisable over $\bar{R}$.*

$1 \longrightarrow 2$ is clear. The following lemma's are dedicated to the proof of $2 \longrightarrow 1$.

Lemma 4.1.3. *Suppose theorem 4.1.2 has been proved for maps F satisfying*

1. *$F^s = I$,*

2. *$F = L + H$ where $H \in \mathfrak{i}A^n$ and $\mathfrak{i}$ is an ideal in R satisfying $\mathfrak{i}^2 = (0)$.*

Then theorem 4.1.2 is true in general.

Proof. Suppose $\bar{F}$ is linearisable. That is, one may assume F to be of a form such that $F^s = I$ and $F = L + H$ and $H \in \mathfrak{n}A^n$. Now we have to prove that F is linearisable. First we show that we may assume R to be noetherian. Write $F = (F_1, \ldots, F_n)$, $F_i = \sum c_{\alpha,i}\mathcal{X}^\alpha$. Define $R' := \mathbb{Q}[c_{\alpha,i}] \subseteq R$. This ring is finitely generated over $\mathbb{Q}$ hence noetherian. We are going to show that there exists $\varphi \in R'[X_1, \ldots, X_n]$ such that $\varphi^{-1}F\varphi$ is linear. So replacing R by R' we may assume R to be noetherian. Now $H \in \mathfrak{n}A^n$ and $\mathfrak{n}^N = 0$ for some integer $N \geq 1$ (since R is noetherian). Calculating modulo $\mathfrak{n}^2$ we have $\overline{F} = \overline{L} + \overline{H}$ where $\overline{H} \in \bar{\mathfrak{n}}A^n/\mathfrak{n}^2A^n$, $\bar{\mathfrak{n}}^2 = \bar{0}$. Hence there exists (by assumption) an invertible polynomial map $\bar{\varphi} \in A^n/\mathfrak{n}^2A^n$ such that $\overline{\varphi}^{-1}F\overline{\varphi}$ is linear. So there exists $\varphi \in A^n$ such that $\tilde{F} := \varphi^{-1}F\varphi = \tilde{L} + \tilde{H}$ where $\tilde{H} \in \mathfrak{n}^2$. Now calculating modulo $(\mathfrak{n}^2)^2$ we find in the same way $H' \in \mathfrak{n}^4$, and after a finite number of permutations we get $H'' \in \mathfrak{n}^N A^n = 0A^n = 0$. □

Hence this lemma says that we only need to prove theorem 4.1.2 for maps $F^s = I$, $F = L + H$ where $H \in \mathfrak{i}A^n$ and $\mathfrak{i}$ is an ideal in R satisfying $\mathfrak{i}^2 = (0)$.

Lemma 4.1.4. *Let $F = L + H$ where L linear and $H \in \mathfrak{i}A^n$ such that $\mathfrak{i}^2 = (0)$. Then are equivalent:*

1. *$F^s = I$ for some integer s*
2. *$L^s = I$ and $\sum_{i=0}^{s-1} L^{s-1-i} H L^i = 0$*

Proof. By induction we will prove $I = F^s = L^s + \sum_{i=0}^{s-1} L^{s-1-i} H L^i$. Comparing degrees gives the theorem. So suppose $F^{k-1} = L^{k-1} + \sum_{i=0}^{k-2} L^{k-2-i} H L^i$ Then

$$\begin{array}{rl} F^k = & F \circ F^{k-1} = (L+H)(L^{k-1} + \sum_{i=0}^{k-2} L^{k-2-i} H L^i) \\ = & (L^k + \sum_{i=0}^{k-2} L^{k-1-i} H L^i + H(L^{k-1} + \sum_{i=0}^{k-2} L^{k-2-i} H L^i)) \\ (*) = & (L^k + \sum_{i=0}^{k-2} L^{k-1-i} H L^i + H(L^{k-1})) \\ = & (L^k + \sum_{i=0}^{k-1} L^{k-1-i} H L^i) \end{array}$$

where $(*)$ holds since $H(L^{k-1} + \sum_{i=0}^{k-2} L^{k-2} H L^i) = H(L^{k-1})$ since $H \in \mathfrak{i}A^n$ where $\mathfrak{i}^2 = (0)$. □

Definition 4.1.5. Let $F \in A^n$. Define $\sigma_F : A^n \longrightarrow A^n$ by $\sigma_F(G) = [G, F] = GF - FG$. Define $\tau_F : A^n \longrightarrow A^n$ by $\tau_F(G) = \frac{-1}{s} \sum_{i=0}^{s-1} i F^i G F^{s-1-i}$.

Remark 4.1.6. If $H, H' \in \mathfrak{i}A^n$ where $\mathfrak{i}^2 = (0)$, then for any $G \in A^n$ we have $H(G + H') = HG$.

Lemma 4.1.7. *Let $L \in A^n$ linear, and $G \in A^n$ arbitrary.*

1. *σ_L and τ_L are R-linear maps on A^n.*
2. *$L^k \sigma_L(G) L^l = \sigma_L(L^k G L^l)$*
   $L^k \tau_L(G) L^l = \tau_L(L^k G L^l)$.
3. *$\sigma_L^2(L^k G L^l) = \sigma_L(L^k G L^{l+1}) - \sigma_L(L^{k+1} G L^l)$.*

4. $\sum_{i=0}^{s-1} \sigma_L(L^i G L^{s-i}) = 0$.

Proof. Straightforward. □

Lemma 4.1.8. *Let* $N = Im(\sigma_L)$ *for some* $L \in A^n$ *satisfying* $L^s = I$. *Then* $\sigma_L \tau_L = 1_N$.

Proof. Let $H \in N$. Then $H = \sigma_L(G)$ for some G. Now

$$\begin{aligned}
\sigma_L\tau_L(H) &= \sigma_L\tau_L\sigma_L(G) \\
&= \sigma_L(\tfrac{-1}{s}\textstyle\sum_{i=0}^{s-1} iL^i\sigma_L(G)L^{s-1-i}) \\
(4.1.7.2) &= \sigma_L(\tfrac{-1}{s}\textstyle\sum_{i=0}^{s-1} i\sigma_L(L^iGL^{s-1-i})) \\
&= \tfrac{-1}{s}\textstyle\sum_{i=0}^{s-1} i\sigma_L^2(L^iGL^{s-1-i}) \\
(4.1.7.3) &= \tfrac{-1}{s}\textstyle\sum_{i=0}^{s-1} i\sigma_L(L^iGL^{s-i}) + \tfrac{1}{s}\sum_{i=0}^{s-1} i\sigma_L(L^{i+1}GL^{s-1-i}) \\
&= \tfrac{1}{s}(-\textstyle\sum_{i=1}^{s-1} i\sigma_L(L^iGL^{s-i}) + \sum_{i=1}^{s}(i-1)\sigma_L(L^iGL^{s-i})) \\
&= \tfrac{1}{s}(-\textstyle\sum_{i=1}^{s-1} \sigma_L(L^iGL^{s-i})) + \tfrac{s-1}{s}(\sigma_L(G)) \\
(4.1.7.4) &= \tfrac{1}{s}(\sigma_L(G)) + \tfrac{s-1}{s}(\sigma_L(G)) \\
&= \sigma_L(G) = H
\end{aligned}$$

□

Lemma 4.1.9. $A^n = ker(\sigma_L) \oplus Im(\sigma_L)$ *for any* $L \in A^n$ *satisfying* $L^s = I$.

Proof. Let $K = ker(\sigma_L)$, $N = Im(\sigma_L)$. Then $0 \longrightarrow K \xrightarrow{Id.} A^n \xrightarrow{\sigma_L} N \longrightarrow 0$ is an exact sequence of R-modules. It is well-known that if there exists some map $f : N \longrightarrow A^n$ such that $\sigma_L f = 1_N$ that $A^n = K \oplus N$. By lemma 4.1.8 such a map f does exist (take $f = \tau_L$). □

Now we can finish the

Proof. (of theorem 4.1.2, 2⟶1): By lemma 4.1.3 we may assume that we have a map F satisfying $F^s = I$ and $F = L + H$ where L is linear

and $H \in \mathfrak{i}A^n$ and $\mathfrak{i}^2 = (0)$. Write $\tau := \tau_L$, $\sigma := \sigma_L$. Let $\varphi := I + \tau(H)$. Then

$$\begin{aligned}(I - \tau(H))(I + \tau(H)) &= (I + \tau(H) - \tau(H(I + \tau(H))))\\ &= (I - \tau(H) - \tau(H))\\ &= I.\end{aligned}$$

So $\varphi^{-1} = (I - \tau(H))$. Define $L + \tilde{H} := \tilde{F} := \varphi^{-1} F \varphi$.

$$\begin{aligned}\tilde{F} &= L + \tilde{H}\\ &= \varphi^{-1} F \varphi\\ &= (I - \tau(H))(L + H)(I + \tau(H))\\ &= (I - \tau(H))(L + L\tau(H) + H(I + \tau(H))\\ &= (I - \tau(H))(L + \tau(LH) + H(I))\\ &= (L + \tau(LH) + H - \tau(H(L + \tau(LH) + H)))\\ &= (L + \tau(LH) + H - \tau(HL))\\ &= L + \tau(LH - HL) + H\\ &= L - \tau\sigma(H) + H.\end{aligned}$$

Now $\sigma(H - \tau\sigma(H)) = \sigma(H) - \sigma\tau\sigma(H) = (\text{ lemma } 4.1.8)\, \sigma(H) - \sigma(H) = 0$. So $\tilde{H} := H - \tau\sigma(H) \in ker(\sigma)$. So $0 = \sigma(\tilde{H}) = \tilde{H}L - L\tilde{H}$ hence $\tilde{H}L = L\tilde{H}$. By lemma 4.1.4 we have $0 = \sum_{i=0}^{s-1} L^{s-1-i}\tilde{H}L^i = \sum_{i=0}^{s-1} \tilde{H}L^{s-1} = (s-1)\tilde{H}L^{s-1}$ hence $0 = 0 \cdot L = (s-1)\tilde{H}L^{s-1}L = (s-1)\tilde{H}L^s = (s-1)\tilde{H}$. So $\tilde{H} = 0$ and hence $\tilde{F} = L$ linear. So F is linearisable. □

4.1.2 The cancellation conjecture over reduced rings

In this section we will prove that the cancellation problem holds forsome $\mathbb{Q}$-algebra R if and only if the cancellation problem holds for $\bar{R}$, the reduced ring (R modulo its nilradical η).

Theorem 4.1.10. *The cancellation problem for a $\mathbb{Q}$-algebra R is equivalent to the cancellation problem over $\bar{R}$, where $\bar{R}$ is the reduced ring of R.*

This result follows from the proposition below and the formulation at the end of section 1.4.3.

Proposition 4.1.11. *Let R be a $\mathbb{Q}$-algebra. Let D be a locally nilpotent R-derivation having a slice on $A := R^{[n]}$. Then the following are equivalent:*

1. *There exists $\varphi \in Aut_R(A)$, $F \in R^*$ such that $\varphi^{-1} D \varphi = f\partial_1$;*
2. *There exists $\varphi_0 \in Aut_{\bar{R}} \bar{A}$, $\bar{f} \in \bar{R}$ such that $\varphi_0^{-1} \bar{D} \varphi_0 = \bar{f}\partial_1$.*

Proof. (1⇒2) is trivial: just calculate modulo the nilradical and take $\varphi_0 := \bar{\varphi}$. (2⇒1) Let $\bar{\varphi}$ be a map such that $\bar{\varphi}^{-1}\bar{D}\bar{\varphi} = \bar{f}\partial_{X_1}$ for some $f \in R$. Then $\widetilde{D} := \varphi^{-1} D \varphi = f\partial_{X_1} + \partial$ where $\partial \in \eta Der_R A$. D has a slice and hence $\widetilde{D}$ must have one too. Now write $\partial = g_1\partial_{X_1} + \ldots + g_n\partial_{X_n}$ where each g_i must be nilpotent. Now since $\widetilde{D}$ is locally nilpotent and has a slice there exist elements G_i such that $\widetilde{D}(G_i) = g_i$. (See the remarks about derivations towards the end of section 2.) Notice that these G_i are nilpotent too. Hence the map $\varphi := (X_1 - G_1, \ldots, X_n - G_n)$ defines an R-automorphism of A sending $P \in A$ to $P \circ \varphi$. Thus

$$\begin{aligned}
(\varphi^{-1}\widetilde{D}\varphi)(X_i) &= \varphi^{-1}\widetilde{D}(X_i - G_i) \\
&= \varphi^{-1}(\widetilde{D}(X_i) - \widetilde{D}(G_i)) \\
&= \varphi^{-1}(\delta_{1i} f + g_i - g_i) \\
&= \varphi^{-1}(\delta_{1i} f) \\
&= \delta_{1i} f
\end{aligned}$$

where δ_{1i} equals 1 if $i = 1$ and zero if $i \geq 2$. Hence $\varphi^{-1}\widetilde{D}\varphi = f\partial_{X_1}$. Finally, since $\varphi^{-1} D \varphi$ has a slice, it follows that $f \in R^*$. □

4.1.3 The ring $(\mathbb{C}[T]/(T^m))^{[n]}$ and its automorphisms

The results in this section have been published in [Mau02a]

Introduction

This section is about the automorphism group over $\mathbb{C}[T]/(T^m)[X_1, \ldots, X_n]$. Why this interest in this automorphism group? This is mainly motivated by several equivalent formulations of the famous Jacobian Conjecture in terms of the rings $R_m := \mathbb{C}[T]/(T^m)$, see 1.4.1 or [Ess98]. From this point of view, knowing more about the automorphisms in $R_m[X_1, \ldots, X_n]$ could be interesting. The main theorem in this section, theorem 4.1.14, is finding a sufficent set of generators for this automorphism group.

$R_m := \mathbb{C}[T]/(T^m)$. We will denote $\bar{T}$ by ϵ. $A := R_m[X_1, \ldots, X_n]$, $B_m := R_m[X_1, \ldots, X_n]$. $E_{R_m}(R_m[X_1, \ldots, X_n]) \subset Aut_{R_m}(A)$ is the collection of automorphisms of the form $(X_1, \ldots, X_{i-1}, X_i + f, X_{i+1}, \ldots, X_n)$ where $f \in R_m[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. $P_{i,j}$ is the map interchanging X_i and X_j.

The automorphism group of $R_m[X]$

First, let us consider the case $n = 2$. In the field case we have $T(\mathbb{C}, n)$ which is called the tame automorphism group of $\mathbb{C}[X, Y]$. It is generated by elementary maps $E_{\mathbb{C}}(\mathbb{C}[X_1, X_2])$ and affine maps $Aff(\mathbb{C})$. Due to the Jung - van der Kulk theorem ([Jun42],[Kul53]) we know that $Aut_{\mathbb{C}}\mathbb{C}[X, Y]$ is the amalgamated free product of $Aff(\mathbb{C})$ and $E(\mathbb{C})$ over their intersection.

For R_m in stead of $\mathbb{C}$ one could hope to extend this result. However, if we define $T(R_m, 2)$ in the same way we cannot hope to have $Aut_{R_m}R_m[X, Y] = T(R_m, 2)$ since $(X + \epsilon X^2, Y)$ is an automorphism in R_m but not in $T(R_m, 2)$ for $\det(JF) \notin R_m^*$. However, if we allow maps of the form $(X + \epsilon H, Y)$ and $(X, Y + \epsilon H)$ (let us denote the set of these maps by $N(R_m)$) to be tame we easily have:

Lemma 4.1.12. *$Aut_{R_m}R_m[X, Y] = T(R_m, 2)$, where $T(R_m, 2)$ is the group generated by $Aff(\mathbb{C})$,$E(\mathbb{C})$ and $N(R_m)$.*

Proof. "$\supseteq$" is easy. "$\subseteq$": let $F \in Aut_{R_m} R_m[X,Y]$. By the Jung-van der Kulk theorem we may assume that $F = (F_1, F_2) = (X,Y) + \epsilon^i(H_1, H_2)$ for some $i \in \mathbb{N}$. Now let $\varphi_i = (X - \epsilon^i H_1, Y)$, $\sigma_i = (X, Y - \epsilon^i H_2)$ then $\varphi_i\sigma_i F = (X,Y) + \epsilon^{i+1}(G_1, G_2)$ for some G_i. Doing this several times, we get $\varphi_{m-1}\sigma_{m-1}\cdots\varphi_i\sigma_i F = (X,Y)$, hence $F \in T(R_m, 2)$. □

There is no mentioning of an amalgamated free product over their intersection, however. We cannot hope to extend this part, as the following example indicates:

Example 4.1.13. Let $R = R_2$. Then

$$\begin{aligned}(X + \epsilon X^2, Y)(X, Y + X)(X - \epsilon X^2, Y)(X, Y - X) &= (X, Y - \epsilon X^2),\\ (Y, X)(X - \epsilon Y^2, Y)(Y, X) &= (X, Y - \epsilon X^2).\end{aligned}$$

However, one might try to find a "more unique" set of generators for the automorphism group, by not allowing all maps $(X_1, \ldots, X_i + \epsilon H_i, \ldots, X_n)$. The following theorem does this:

Theorem 4.1.14. *Let $n \geq 1$. $Aut_{R_m} B_m$ is generated by the union of the following sets:*

1. *$Aut_{\mathbb{C}}(A)$;*
2. *the maps $(X_1 + c\epsilon X_1, X_2, \ldots, X_n)$ all $c \in \mathbb{C}$;*
3. *the maps $(X_1 + \epsilon X_1^d, X_2, \ldots, X_n), (X_1 + \epsilon X_1^{d+1}, X_2, \ldots, X_n), \ldots$ where d is some positive integer.*

Here we view $Aut_{\mathbb{C}}(A)$ as a subset of $Aut_{R_m}(B_m)$; notice that $\mathbb{C} \subset R_m$. One can prove that the maps 2) of the above theorem together with $Aff_{\mathbb{C}}(A)$ generate $Aff_{R_m}(B_m)$; the lemma's 4.1.18 and 4.1.19 indicate this. These remarks give

Corollary 4.1.15. *$Aut_{R_m}R_m[X,Y]$ is generated by $Aff_{R_m}R_m[X,Y]$, $E_{R_m}R_m[X,Y]$ and the maps $(X+\epsilon X^d, Y), (X+\epsilon X^{d+1}, Y), \ldots$ where d is some positive integer.*

In this subsection we will prove the following theorem (which is stronger than theorem 4.1.14):

Theorem 4.1.16. *$Aut_{R_m}B_m$ is generated by the union of the following sets:*

1. *$Aut_{\mathbb{C}}(A)$;*
2. *the maps $(X_1 + c\epsilon X_1, X_2, \ldots, X_n)$ all $c \in \mathbb{C}$;*
3. *some maps*

$$(X_1 + \epsilon F_1(X_1), X_2, \ldots, X_n), (X_1 + \epsilon F_2(X_1), X_2, \ldots, X_n), \ldots$$

where $\lim_{i\to\infty} deg(F_i \mod \epsilon) = \infty$.

Definition 4.1.17. Denote by $\mathcal{C}_m$ the monoid generated by 1),2) and 3) from the above theorem 4.1.16.

We want to prove that $\mathcal{C}_m = Aut_{R_m}B_m$. The proof of theorem 4.1.16 will go by the use of several lemmas.

Lemma 4.1.18. *Let $\alpha \in R_m^*$. Then $(\alpha X_1, X_2, \ldots, X_n) \in \mathcal{C}_m$.*

Proof. Let $\alpha = c(1+a_1\epsilon+a_2\epsilon^2+\ldots+a_{m-1}\epsilon^{m-1})$ for some nonzero $c \in \mathbb{C}$. Let $\beta_1, \ldots, \beta_{m-1}$ be the zeros of the polynomial $Y^{m-1} + a_1Y^{m-2} + a_2Y^{m-3} + \ldots + a_{m-2}Y + a_{m-1}$. Then $(\alpha X_1) = (cX_1) \circ (X_1 - \beta_1\epsilon X_1) \circ \ldots \circ (X_1 - \beta_{m-1}\epsilon X_1)$ since for any $\lambda_1, \lambda_2 \in R_m$ one has $(\lambda_1 X) \circ (\lambda_2 X) = (\lambda_1\lambda_2 X)$. This calculation works in n variables too so we're done. □

Lemma 4.1.19. *$(\alpha X_1 + \beta, X_2, \ldots, X_n) \in \mathcal{C}_m$ for all $\alpha \in R_m^*$, $\beta \in R_m$.*

Proof. Let $\alpha^{-1}\beta = \gamma + \delta$ where $\gamma, \delta \in R_m^*$. Then

$$(\gamma X_1)(X_1{+}1)(\gamma^{-1}X_1)(\delta X_1)(X_1{+}1)(\delta^{-1}X_1) = (X_1{+}\gamma{+}\delta) = (X_1{+}\alpha^{-1}\beta).$$

Since $(\alpha X_1)(X_1 + \alpha^{-1}\beta) = (\alpha X_1 + \beta)$ it follows that $\alpha X_1 + \beta \in C_m$. This calculaton works in n variables too, so we're done. □

Lemma 4.1.20. *Let $F_1, \ldots, F_n \in R_m[X_1, \ldots, X_n]$ be such that $\mathbb{C}[\bar{F}_1, \ldots, \bar{F}_n] = \mathbb{C}[X_1, \ldots, X_n]$ then $R_m[F_1, \ldots, F_n] = R_m[X_1, \ldots, X_n]$.*

Proof. Well-known (see [Ess00] lemma 1.1.9). □

Lemma 4.1.21.

1. *Let $H, G \in (B_m)^n$ and $k \geq 1$ then $(X + \epsilon^k H) \circ (X + \epsilon^k G) = X + \epsilon^k(H + G) \mod \epsilon^{k+1}$.*
2. *Let $H, G \in B_m$ and $k \geq 1$ then $(X_1 + \epsilon^k H, X_2, \ldots, X_n) \circ (X_1 + \epsilon^k G, X_2, \ldots, X_n) = (X_1 + \epsilon^k(H + G) + \epsilon^{k+1}(\ldots), X_2, \ldots, X_n)$*

Proof. Easy since $\epsilon^k H(X + \epsilon(\ldots)) = \epsilon^k H(X) + \epsilon^{k+1}(\ldots)$. □

Lemma 4.1.22. *If $X + \epsilon H \in \mathcal{C}_m$ for all $H \in (B_m)^n$ then $\mathcal{C}_m = Aut_{R_m} A$.*

Proof. Let $F \in Aut_{R_m} B_m$. Then $\bar{F} \in Aut_{\mathbb{C}} A$. Since $\bar{F}^{-1}F = X + \epsilon H$ for some $H \in R_m[X_1, \ldots, X_n]^n$ we have $F = \bar{F} \circ (X + \epsilon H)$. Hence $F \in \mathcal{C}_m$. □

Lemma 4.1.23. *If $(X_1 + \epsilon H, X_2, \ldots, X_n) \in \mathcal{C}_m$ for all $H \in B_m$ then $\mathcal{C}_m = Aut_{R_m} B_m$.*

Proof. First notice that $P_{1,i}(X{+}\epsilon H, X_2, \ldots, X_n)P_{1,i} = (X_1, \ldots, X_{i-1}, X_i{+}$ $\epsilon H(P_{1,i})$,
$X_{i+1}, \ldots, X_n)$ so $(X_1, \ldots, X_{i-1}, X_i + \epsilon H, X_{i+1}, \ldots, X_n) \in \mathcal{C}_m$ for all $H \in B_m$. We are going to proceed by induction.

Suppose $(X_1 + \epsilon H_1, \ldots, X_i + \epsilon H_i, X_{i+1}, \ldots, X_n) \in \mathcal{C}_m$ for all $H_i \in R_m[X_1, \ldots, X_n]$. Now choose some $H_{i+1} \in R_m[X_1, \ldots, X_n]$. Let $\tilde{H} := (X_1 + \epsilon H_1, \ldots, X_i + \epsilon H_i, X_{i+1}, \ldots, X_n)$. Then $R_m[\tilde{H}] = B_m$ by lemma 4.1.20, so there exists $G_{i+1} \in B_m$ such that $H_{i+1} = G_{i+1}(\tilde{H})$. Hence $(X_1, \ldots, X_i, X_{i+1} + \epsilon G_{i+1}, X_{i+2}, \ldots, X_n) \circ \tilde{H} = (X_1 + \epsilon H_1, \ldots, X_{i+1} + \epsilon H_{i+1}, X_{i+2}, \ldots, X_n)$. By induction and lemma 4.1.22 we are done. □

Lemma 4.1.24. *Suppose for all $k \geq 1$ and any arbitrary monomial M (= cX^α for some $c \in \mathbb{C}$) we have that there exists some map $E_{k,M} \in \mathcal{C}_m$ such that $E_{k,M} = (X_1 + \epsilon^k M + \epsilon^{k+1} H, X_2, \ldots, X_n)$ for some $H \in B_m$ then $\mathcal{C}_m = Aut_{R_m} B_m$.*

Proof. by lemma 4.1.23 we only have to prove that $(X_1 + \epsilon H, X_2, \ldots, X_n) \in \mathcal{C}_m$ for all $H \in R_m[X_1, \ldots, X_n]$. We will proceed by induction on k. Suppose that for any map $F := (X_1 + \epsilon H, X_2, \ldots, X_n)$ we can construct some map $F' = (X_1 + \epsilon H', X_2, \ldots, X_n) \in \mathcal{C}_m$ such that $F - F' = (\epsilon^k H'', 0, \ldots, 0)$ some $H'' \in R_m[X_1, \ldots, X_n]$. Let $H'' = \sum_{j=1}^s M_j + \epsilon G$ where $G \in B_m$ and M_j are monomials. Now we are going to compose several maps which are the identity in all variables except the first one; therefore we write down only the first variable. Using lemma 4.1.21.2 a few times we get

$$\begin{aligned} F_1'' := &\quad F_1' \circ (E_{k,M_1})_1 \circ \ldots \circ (E_{k,M_s})_1 \mod \epsilon^{k+1} \\ = &\quad (F_1 - (\epsilon^k \textstyle\sum_{j=1}^s M_j)) \circ (X_1 + \epsilon^k \sum_{j=1}^s M_j) \mod \epsilon^{k+1} \\ = &\quad F_1 \mod \epsilon^{k+1}. \end{aligned}$$

Hence we can construct F'' which is equal to $F + (\epsilon^{k+1}\tilde{H}, 0, \ldots, 0)$ some $\tilde{H} \in B_m$. By induction we are done since $\epsilon^m = 0$. □

Lemma 4.1.25. *If for any $d \geq 2$ and $k \geq 1$ there exist $G \in \mathcal{C}_m$ such that $G \mod \epsilon^{k+1} = (X_1 + \epsilon^k X_1^d, X_2, \ldots, X_n)$, then $\mathcal{C}_m = Aut_{R_m} B_m$.*

Proof. By lemma 4.1.24 we only have to prove that for any monomial M we can construct maps $E_{k,M}$ of the form $(X_1+\epsilon^k M+\epsilon^{k+1}H, X_2, \ldots, X_n)$ for some $H \in R_m[X_1, \ldots, X_n]$. Now notice that if $c' \in \mathbb{C}$ such that $c'^{d-1} = c$ then

$$(c'^{-1}X_1, X_2, \ldots, X_n)(X_1 + \epsilon^k X_1^d, X_2, \ldots, X_n)(c'X_1, X_2, \ldots, X_n) = (X_1 + c\epsilon^k X_1^d, X_2, \ldots, X_n).$$

Furthermore defining $L := (X_1 + a_2X_2 + \ldots + a_nX_n, X_2, \ldots, X_n)$ we have

$$(*) \qquad \begin{array}{l} L^{-1}(X_1 + c\epsilon^k X_1^d, X_2, \ldots, X_n)L \\ (X_1 + c\epsilon^k(X_1 + a_2X_2 + \ldots + a_nX_n)^d, X_2, \ldots, X_n). \end{array}$$

So maps of the form $(X_1 + c\epsilon^k(X_1 + a_2X_2 + \ldots + a_nX_n)^d, X_2, \ldots, X_n)$ mod ϵ^{k+1} can be constructed (where only the first coordinate is not X_i). By lemma 4.1.21.2 we can make maps of the form $(X_1 + c\epsilon^k H + \epsilon^{k+1}(\ldots), X_2, \ldots, X_n)$ where H is any linear combination of polynomials of the form $(X_1 + a_2X_2 + \ldots + a_nX_n)^d$. Since these polynomials generate the k-vectorspace of homogeneous polynomials in n variables of degree d we can find a map $E_{k,M}$ as stated for any monomial of degree d. Since d is arbitrary ≥ 2 we are done. □

Now we will give some technical statements for the case that $n = 1$ ($B_m = R_m[X]$, one variable). These will be used in the proof of lemma 4.1.27 which will be the last step in the proof of theorem 4.1.16. This is the only lemma in which one has to do a lot of (dirty) calculations; one cannot avoid some hard work in some places. (At least, I cannot.)

Lemma 4.1.26.

1. *If there exists some map $E_{k,d} \in \mathcal{C}_m$ where $d \geq 2$ such that $E_{k,d}$ mod $\epsilon^{k+1} = (X + \epsilon^k X^d)$ then there exists a map $F \in \mathcal{C}_m$ such that*

$$F \mod \epsilon^{k+2} = (X + \epsilon^{k+1} \sum_{i=0}^{s} h_i X^i)$$

and $h_d = 1$.

2. *If there exists a map* $F \in \mathcal{C}_m$ *with*

$$F \mod \epsilon^{k+1} = (X + \epsilon^k \sum_{i=1}^{s} h_i X^i)$$

where $s > d$, $h_d = 1$ *(*$d \geq 2$*) then there exists some* $\widetilde{F} \in \mathcal{C}_m$ *satisfying*

$$\widetilde{F} \mod \epsilon^{k+1} = (X + \epsilon^k \sum_{i=1}^{s} \tilde{h_i} X^i)$$

where $\tilde{h_d} = 1$, $\tilde{h_s} = 0$ *(and if* $h_i = 0$ *then* $\tilde{h_i} = 0$*).*

Proof.

1. Choose some $c \in \mathbb{C}$. Let $a \in \mathbb{C}$ be such that $a^{d-1} = c$. Then

$$(a^{-1}X)E_{k,d}(aX) = (X + c\epsilon^k X^d) \mod \epsilon^{k+1}.$$

So we have $E_{k,d,c} \in \mathcal{C}_m$ such that $E_{k,d,c} \mod \epsilon^{k+1} = (X + c\epsilon^k X^d)$ for any $c \in \mathbb{C}$. Now choose $\alpha \in R_m$ such that $\alpha = 1 + c\epsilon$ for some $c \in \mathbb{C}$. Notice that $\alpha^d \mod \epsilon^2 = 1 + cd\epsilon$ and $\alpha^{-d} \mod \epsilon^2 = 1 - cd\epsilon$ (in fact, "analytically speaking" d could be any real number). So now we have some $F \in \mathcal{C}_m$ such that

$$\begin{aligned} & F \mod \epsilon^{k+2} \\ = \; & E_{k,d,-1}(\alpha^{-1}X)E_{k,d,1}(\alpha X) \\ = \; & (X - \epsilon^k X^d - \epsilon^{k+1}G)(\alpha^{-1}X)(X + \epsilon^k X^d + \epsilon^{k+1}H)(\alpha X) \end{aligned}$$

where G, H are certain polynomials $\in \mathbb{C}[X]$ and $c \in \mathbb{C}$ arbitrarily chosen. But writing out the last equation we get:

$$
\begin{aligned}
& F \mod \epsilon^{k+2} \\
= \; & (X - \epsilon^k X^d - \epsilon^{k+1} G(X))(\alpha^{-1} X) \\
& \qquad (X + \epsilon^k X^d + \epsilon^{k+1} H(X))(\alpha X) \\
= \; & (\alpha^{-1} X - \epsilon^k \alpha^{-d} X^d - \epsilon^{k+1} G(\alpha^{-1} X)) \\
& \qquad (\alpha X + \epsilon^k \alpha^d X^d + \epsilon^{k+1} H(\alpha X)) \\
= \; & (\alpha^{-1} X - \epsilon^k (1 - cd\epsilon) X^d - \epsilon^{k+1} G(X)) \\
& \qquad (\alpha X + \epsilon^k (1 + cd\epsilon) X^d + \epsilon^{k+1} H(X)) \\
= \; & (\alpha^{-1} X - \epsilon^k X^d + \epsilon^{k+1} (cdX^d - G(X))) \\
& \qquad (\alpha X + \epsilon^k X^d + \epsilon^{k+1} (cdX^d + H(X))) \\
= \; & (X + \alpha^{-1} \epsilon^k X^d + \alpha^{-1} \epsilon^{k+1} (cdX^d + H(X))) + \\
& \quad -\epsilon^k (\alpha X + \epsilon^k X^d)^d + \epsilon^{k+1} (cd(\alpha X)^d - G(\alpha X))) \\
= \; & (X + (1 - c\epsilon) \epsilon^k X^d + \epsilon^{k+1} (cdX^d + H(X))) + \\
& -\epsilon^k ((1 + c\epsilon) X + \epsilon^k X^d)^d + e^{k+1} (cdX^d - G(X))) \\
= \; & (X + \epsilon^k X^d + \epsilon^{k+1} ((cd - c) X^d + H(X)) + \\
& \quad -\epsilon^k (X + c\epsilon X + \epsilon^k X^d)^d + \epsilon^{k+1} (cdX^d - G(X)).
\end{aligned}
$$

Now we have to differentiate between $k = 1$ and $k > 1$ since in the latter case $\epsilon^k (X + c\epsilon X + \epsilon^k X^d)^d = \epsilon^k X^d + dc\epsilon^{k+1} X^d \mod \epsilon^{k+2}$ and in the case $k = 1$ one has $\epsilon^k (X + c\epsilon X + \epsilon^k X^d)^d = \epsilon(X + c\epsilon(X + X^d))^d = \epsilon(X^d + \epsilon d X^{d-1}(X + X^d)) \mod \epsilon^2 = \epsilon X^d +$

$\epsilon^2(dX^d + dX^{2d-1})$. Let us do the case $k > 1$:

$$\begin{aligned}
& F \mod \epsilon^{k+2} \\
= \; & (X + \epsilon^k X^d + \epsilon^{k+1}((cd-c)X^d + H(X)) + \\
& \quad -\epsilon^k(X + c\epsilon X + \epsilon^k X^d)^d + \epsilon^{k+1}(cdX^d - G(X)) \\
= \; & (X + \epsilon^k X^d + \epsilon^{k+1}((cd-c)X^d + H(X)) + \\
& \quad -(\epsilon^k X^d + dc\epsilon^{k+1}X^d) + \epsilon^{k+1}(cdX^d - G(X)) \\
= \; & (X + \epsilon^{k+1}((-c)X^d + H(X)) + \epsilon^{k+1}(cdX^d - G(X)) \\
= \; & (X + \epsilon^{k+1}((-c+cd)X^d + H(X) - G(X)).
\end{aligned}$$

Since c is completely free (and G, H are fixed) we can obtain the desired result. The case $k = 1$ is not really different: replace "$H(X) - G(X)$" by "$H(X) - G(X) - dX^{2d-1}$" and observe that the coefficient of X^d equals $\epsilon^2(2cd - c - d)$.

2. Choose some $c \in \mathbb{C}$ such that $c^{s-1} = -1$ and $c^{d-1} \neq -1$. Now let $F' := (c^{-1}X)F(cX)F$. Then

$$\begin{aligned}
& F' \mod \epsilon^{k+1} \\
= \; & (c^{-1}X)(X + \epsilon^k \textstyle\sum_{i=1}^s h_i X^i)(cX)(X + \epsilon^k \sum_{i=1}^s h_i X^i) \\
= \; & (X + \epsilon^k \textstyle\sum_{i=1}^s g_i X^i)(X + \epsilon^k \sum_{i=1}^s h_i X^i) \\
= \; & (X + \epsilon^k \textstyle\sum_{i=1}^s g_i X^i + \epsilon^k \sum_{i=1}^s h_i X^i)
\end{aligned}$$

where $g_i := c^{i-1}h_i$. Define $h'_i := g_i + h_i$ for all i. Then $h'_s = g_s + h_s = c^{s-1}h_s + h_s = -h_s + h_s = 0$. Also if $h_i = 0$ then $g_i = 0$ and hence $h'_i = 0$. Furthermore $h'_d = g_d + h_d = c^{d-1}h_d + h_d =$

$(c^{d-1}+1) \neq 0$. Choose $a \in \mathbb{C}$ such that $a^{d-1} = (c^{d-1}+1)^{-1}$. Now define $\widetilde{F} := (a^{-1}X)F'(aX)$. Then

$$\begin{aligned} \widetilde{F} \mod \epsilon^{k+1} & \\ = & (a^{-1}X)(X + \epsilon^k \textstyle\sum_{i=1}^{s-1} h'_i X^i)(aX) \\ = & (X + \epsilon^k \textstyle\sum_{i=1}^{s-1} a^{i-1} h'_i X^i) \\ = & X + \epsilon^k \textstyle\sum_{i=1}^{s-1} \tilde{h_i} X^i \end{aligned}$$

where $\tilde{h_i} := a^{i-1}h'_i$. Hence $\tilde{h_d} = 1$, and if $h'_i = 0$ then $\tilde{h_i} = 0$.

□

Lemma 4.1.27. *For the case $n = 1$ ($B_m = R_m[X]$, one variable) we have for any $k, d \in \mathbb{N}$ that there exists some $E_{k,d} \in \mathcal{C}_m$ such that $E_{k,d} = (X + \epsilon^k X^d) \mod \epsilon^{k+1}$.*

Proof. Notice that for $d = 0, 1$ we can refer to lemma 4.1.19. So let $d > 1$. This lemma will be done by induction.
Suppose for any $k' < k$ we have maps $E_{k',d}$ as in the theorem.
Suppose for any $d' < d$ we have maps $E_{k,d'}$ as in the theorem.
We have to prove that we can construct a map $E_{k,d}$. By induction we have some map $E_{k-1,d}$. So by lemma 4.1.26.1 we get some map F of the form

$$F \mod \epsilon^{k+1} = X + \epsilon^k \sum_{i=0}^{s} h_i X^i$$

where $h_d = 1$. Now by applying lemma 4.1.26.2 several times we have constructed a map F' which looks like

$$F' \mod \epsilon^{k+1} = X + \epsilon^k \sum_{i=0}^{d} h_i X^i.$$

By induction we have maps $E_{k,d-1}, \ldots, E_{k,1}, E_{k,0}$. Now define for any $c \in \mathbb{C}$ the maps $E_{k,d,c} := (X + c\epsilon^k X^d) \mod \epsilon^{k+1} = (a^{-1}X)E_{k,d}(aX)$ where $a \in \mathbb{C}$ such that $a^{d-1} = c$. Now using lemma 4.1.21 a few times we have

$$F \circ E_{k,d-1,-h_{d-1}} \circ E_{k,d-2,-h_{d-2}} \circ \cdots$$
$$\cdots \circ E_{k,2,-h_2} \circ (X - h_1\epsilon^k X) \circ (X - h_0\epsilon^k) \mod \epsilon^{k+1} = (X + \epsilon^k X^d)$$

and hence we are done by induction. □

Proof. (of theorem 2) Lemma 4.1.27 gives us the ability to construct maps as required in lemma 4.1.25. (The fact that lemma 4.1.27 is in one dimension is of no consequence, that was just to make notations easier.) Since the requirements of lemma 4.1.25 are fulfilled, we are done. □

4.2 Endomorphisms over finite fields

The results in this section have been published in [Mau01].

4.2.1 Introduction

Though many Theorems about polynomial maps are true for an arbitrary field, or an arbitrary algebraically closed field, these Theorems are mostly used for the characteristic zero case, or more specifically, the complex numbers. However, it might be interesting to study polynomial maps over characteristic $p > 0$, or even over finite fields. Some research in this direction has been done, see for example [Nou81], [Adj95], [ADE92], [Ess00] (chapter 10 paragraph 3). The case that we are considering, the automorphism group, or the tame automorphism group, over a finite field might be very useful, as can be seen in the paper [Moh99]. In fact, it might be one of the few useful applications

of polynomial mappings in the "real" world of "money, economics and data travel" : in [Moh99] a method is given on how to encrypt data using the tame automorphism group over a finite field. Therefore, a theoretical approach of the automorphism group or tame automorphism group over a finite field can give a good foundation for similar applications. Also it might induce some ideas on already standing conjectures over the complex numbers, like the tame generators conjecture. The last conjecture has recently been solved by Shestakov and Unirbaer ([SU02a], [SU02b]).

4.2.2 Bijections induced by automorphisms over $\mathbb{F}_{p^n}$

Definition 4.2.1. Let k be a field, $A := k[X_1, \ldots, X_n]$.

$\mathcal{P}(k^n)$ is the set of all maps $k^n \longrightarrow k^n$.
$\mathcal{B}(k^n) \subset \mathcal{P}(k^n)$ is the set of all bijections $k^n \longrightarrow k^n$.

$\mathcal{E} : \mathrm{End}_k(A) \longrightarrow \mathcal{P}(k^n)$ is the map sending $F \in \mathrm{End}_k(A)$ ($F = (F_1, \ldots, F_n) \in A^n$) to the map $\mathcal{E}(F) : k^n \longrightarrow k^n$ defined by

$$\mathcal{E}(F)(\alpha_1, \ldots, \alpha_n) := (F_1(\alpha_1, \ldots, \alpha_n), \ldots, F_n(\alpha_1, \ldots, \alpha_n)).$$

$\mathrm{Aut}(k, n) := \{F \in \mathrm{End}_k(A) \mid \mathcal{E}(F) \in \mathcal{B}(k^n)\}$.
$\mathrm{Aut}_k(A) :=$ the group of automorphisms of A (i.e. $\mathrm{Aut}_k(A) \subset \mathrm{End}_k(A)$).
$T(k, n)$ is the tame automorphism subgroup of $\mathrm{Aut}_k(A)$. As usual, "$\#S$" will denote the number of elements in a finite set S.

Remark: $\mathrm{Aut}(k, n)$ is in general larger than $\mathrm{Aut}_k(A)$: in case k is a finite field of p^n elements, let $\varphi := (X_1^{p^n}, X_2, \ldots, X_n)$. Then the map $\mathcal{E}((X_1^{p^n}, X_2, \ldots, X_n))$ is a bijection $k^n \longrightarrow k^n$ but φ is not an invertible element of $\mathrm{End}_k(A)$.

In this article we will try to answer the question whether $\mathcal{E}(\mathrm{Aut}_k(A)) = \mathcal{B}(k^n)$. The case that k is infinite is easy:

Lemma 4.2.2. *If k is not a finite field then $\mathcal{E}(\mathrm{Aut}(k,n))$ (and hence $\mathcal{E}(\mathrm{Aut}_k(A))$) is smaller than $\mathcal{B}(k^n)$.*

Proof. Suppose $F = (F_1, \ldots, F_n)$ is a polynomial map $k^n \longrightarrow k^n$ interchanging $(0, \ldots, 0)$ and $A := (1, 0, \ldots, 0)$, and the identity anywhere else. Then $F_i - X_i$ is a polynomial map $k^n \longrightarrow k$ which is zero everywhere in case $i \geq 2$ or zero almost everywhere in case $i = 1$; over an infinite field this implies $F_i - X_i = 0$, thus $F = I$, contradiction for $F(0, \ldots, 0) \neq (0, \ldots, 0)$. □

The case that k is a finite field has a surprising result:

Theorem 4.2.3. *Let k be a finite field.*

(i). $\#\mathcal{E}(T(k,1)) = \#\mathcal{B}(k)/(\#k - 2)!$, so only if $k = \mathbb{F}_2, \mathbb{F}_3$ then $\mathcal{E}(T(k,1)) = \mathcal{B}(k)$.

(ii). If $n \geq 2$ and $\mathrm{Char}(k) \neq 2$ or $k = \mathbb{F}_2$ then $\mathcal{E}(T(k,n)) = \mathcal{B}(k^n)$.

(iii). If $n \geq 2$ and $k = \mathbb{F}_{2^m}$ where $m \geq 2$ then $\#\mathcal{E}(T(k,n)) = \#\mathcal{B}(k^n)/2$. In fact, $\mathcal{E}(T(k,n))$ is the alternating subgroup A_l of the symmetric group $S_l \cong \mathcal{B}(k^n)$ where $l = \#k^n$.

The proof will go in several steps. First observe that $\mathcal{B}(k^n)$, with as operation composition of maps, is isomorphic to the symmetic group S_l where $l = (\#k^n)$, since every bijection $\sigma \in \mathcal{B}(k^n)$ can be seen as a permutation of elements in k^n. This enables us to use a Theorem of Jordan:

Definition 4.2.4. Let G be a transitive subgroup of S_n. G is called a *primitive* subgroup if there exist no two elements $i, j \in \{1, \ldots, n\}$ such that for any $g \in G$ we have either $\{g(i), g(j)\} = \{i, j\}$ or $\{g(i), g(j)\} \cap \{i, j\} = \emptyset$.

Theorem 4.2.5. *Let G be a primitive subgroup of S_n. Suppose G contains a 3-cycle. Then G contains the alternating subgroup A_n.*

For a proof, see [IZ95].

Definition 4.2.6. Let k be a finite field, and let $\alpha = (\alpha_1, \ldots, \alpha_n) \in k^n, b \in k$. Let

$$f_i := \prod_{\substack{a \in k \\ a \neq \alpha_i}} (X_i - a) \in k[X_i].$$

Let $\lambda := f_1(\alpha_1) \cdots f_n(\alpha_n)$. Then define

$$f_{(\alpha,b)} := b\lambda^{-1} \prod_{i=1}^{n} f_i(X_i).$$

Notice $f_{(\alpha,b)}(\alpha) = b$ and $f_{(\alpha,b)}(\beta) = 0$ for all $\beta \in k^n \backslash \{\alpha\}$.

Definition 4.2.7. Let k be a finite field.

(i). Let $\alpha \in k^{n-1}, b \in k$. Then define

$$\sigma_{(\alpha,b)} := \big(X_1 + f_{(\alpha,b)}(X_2, \ldots, X_n), X_2, \ldots, X_n\big).$$

(ii). Let $i \in \{2, \ldots, n\}$. Define

$$\sigma_i := \big(X_i, X_2, \ldots, X_{i-1}, X_1, X_{i+1}, \ldots, X_n\big),$$

the map interchanging X_i and X_1.

(iii). Choose some $a \in k^*$ such that $\{1, a, a^2, \ldots\} = k^*$. Define

$$\tau := (aX_1, X_2, \ldots, X_n).$$

(iv). Let G be the subgroup of $T(k,n)$ generated by the $\sigma_{(\alpha,b)}$, the σ_i, and τ.

Lemma 4.2.8. $\mathcal{E}(G) = \mathcal{E}(T(k,n))$.

Proof. We need to show that (1) for any $f \in k[X_2,\ldots,X_n]$ we have $\sigma \in G$ such that $\mathcal{E}(\sigma) = \mathcal{E}(X_1+f, X_2,\ldots,X_n)$, and that (2) for each linear map L we have some $\sigma \in G$ such that $\mathcal{E}(\sigma) = \mathcal{E}(L)$.
Part (1): Let $\zeta := (X_1+f, X_2,\ldots,X_n)$ for some $f \in k[X_2,\ldots,X_n]$. Notice that $\sigma_{(\alpha',b')}\sigma_{(\alpha'',b'')} = \sigma_{(\alpha'',b'')}\sigma_{(\alpha',b')} = (X_1+g, X_2,\ldots,X_n)$ where $g \in k[X_2,\ldots,X_n]$ satisfies (in case $\alpha' \neq \alpha''$) $g(\alpha') = b'$, $g(\alpha'') = b''$. In the same way we see that if we define σ to be the composition of all $\sigma_{(\alpha,f(\alpha))}$, where α runs through k^{n-1} then $\sigma = (X_1+g, X_2,\ldots,X_n)$ and $g(\alpha) = f(\alpha)$ for all $\alpha \in k^{n-1}$. Thus $\mathcal{E}(\sigma) = \mathcal{E}(\zeta)$.
Part (2): Since $\sigma_i\tau^m\sigma_i = (X_1,\ldots,X_{i-1},a^mX_i,X_{i+1},\ldots,X_n)$ and $\{1,a,a^2,\ldots\} = k^*$ we can get any map $L_{i,\lambda} :=$
$(X_1,\ldots,X_{i-1},\lambda X_i,X_{i+1},\ldots,X_n)$ where $\lambda \in k^*$ is arbitrary. It is well-known that these maps, together with the maps $\sigma_\gamma := (X_1+\gamma_2X_2+\ldots+\gamma_nX_n,X_2,\ldots,X_n)$ where $\gamma := (\gamma_2,\ldots,\gamma_n) \in k^{n-1}$, generate the linear maps. By part (1) there exists for each $\gamma \in k^{n-1}$ a map $\mu_\gamma \in G$ such that $\mathcal{E}\sigma_\gamma = \mathcal{E}\mu_\gamma$, and that suffices to prove (2). □

Lemma 4.2.9. *Let k be a finite field. Let G be as in Definition 4.2.7*(iv)*. Then*

(i). $\mathcal{E}(G)$ is a primitive group,

(ii). $\mathcal{E}(G)$ contains a 3-cycle.

Proof.
(i): The fact that $\mathcal{E}(G)$ is transitive follows from the fact that G contains all linear bijections $k^n \longrightarrow k^n$. So it suffices to show that for arbitrary $r = (r_1,\ldots,r_n), s = (s_1,\ldots,s_n) \in k^n$, $r \neq s$ there exists some $\sigma \in G$ such that $\sigma(r) \neq r$, $\sigma(s) = s$. Let $i \in \{1,\ldots,n\}$ such

that $r_i \neq s_i$. If $i \geq 2$ then we take the map $\sigma_{(\alpha,1)}$ where $\alpha \in k^{n-1}$ is the $n-1$-tuple of the last $n-1$ coordinates of $r = (r_1, \alpha) \in k^n$. Then $\sigma_{(\alpha,1)}(r) = (r_1 + 1, \alpha)$ and $\sigma_{(\alpha,1)}(s) = s$. In case $i = 1$ we can take $\sigma_2\sigma_{(\alpha,s)}\sigma_2$ for some other appropriate r, s.
(ii): Let o:$= (0, \ldots, 0) \in k^{n-1}$ and let

$$\sigma := \sigma_{(\mathrm{o},1)} = \big(X_1 + f_{(\mathrm{o},1)}(X_2, \ldots, X_n), X_2, \ldots, X_n\big),$$
$$\mu := \sigma_2\sigma\sigma_2 = \big(X_1, X_2 + f_{(\mathrm{o},1)}(X_1, X_3, \ldots, X_n), X_3, \ldots, X_n\big).$$

Then σ is the identity outside the set $V_1 := \{(a, 0, \ldots, 0) \mid a \in k\}$ and μ is the identity outside the set $V_2 := \{(0, a, 0, \ldots, 0) \mid a \in k\}$. Both σ and μ are cyclic of order $\mathrm{Char}(k)$ on V_1 resp. V_2. Let $\zeta := \sigma^{-1}\mu^{-1}\sigma\mu$. Then ζ acts trivially on $k^n \backslash (V_1 \cup V_2)$ and nontrivially only on a subset of $V_1 \cup V_2$. Now if $\alpha \notin V_2, \sigma(\alpha) \notin V_2$ then one can easily check (using the fact that μ only works on elements of V_2) that $\zeta(\alpha) = \alpha$. Also if $\alpha \notin V_1, \mu(\alpha) \notin V_1$ then one can easily check (using the fact that σ only works on elements of V_1) that $\zeta(\alpha) = \alpha$. Thus the only cases left are:
1) $\alpha \notin V_2, \sigma(\alpha) \in V_2$ (then α equals the element $A := (-1, 0, \ldots, 0)$),
2) $\alpha \notin V_1, \mu(\alpha) \in V_1$ (then α equals the element $B := (0, -1, 0, \ldots, 0)$),
3) $\alpha \in V_1$, $\alpha \in V_2$ (then α equals the element $O := 0$).
Notice $\sigma(A) = O, \sigma(B) = B, \mu(B) = O, \mu(A) = A, \sigma(O) \notin V_2, \mu(O) \notin V_1$. Using this we see that $\zeta(A) = B$, $\zeta(B) = O$, $\zeta(O) = A$, hence ζ is a 3-cycle. □

Now we are ready for the proof of the main result:

Proof. (of Theorem 4.2.3) We will use notations as in Definition 4.2.7. We will view $\mathcal{B}(k^n)$ as a subgroup of S_{q^n} where $q = \#k$. By Theorem 4.2.5, Lemma 4.2.8 and Lemma 4.2.9 we see that A_{q^n} is a subgroup of $\mathcal{E}(G) = \mathcal{E}(T(k, n))$.
(i) Case $n = 1$: $T(k, 1)$ consists only of the linear maps $x \longrightarrow bx + c$ where $b \in k^*, c \in k$. These maps are all different bijections, so these

are $\#k^* \times \#k = (q-1)q$ different maps. Since $\#\mathcal{B}(k) = (\#k)!$ the result follows.
(ii) Case $n \geq 2$, Char$(k) \neq 2$: If we can find $\sigma \in G$ such that $\mathcal{E}(\sigma) \notin A_{q^n}$, then $\mathcal{E}(G) = S_{q^n}$; in other words, find $\sigma \in G$ such that the sign of $\mathcal{E}(\sigma)$ is -1. Our claim is: τ is such an element. τ (or $\mathcal{E}(\tau)$) has order $q-1$ and consists of a number of separate $(q-1)$-cycles: for each $\alpha \in k^{n-1}$ a separate cycle in the set $V_\alpha := \{(b, \alpha) \mid b \in k^*\}$. Hence q^{n-1} cycles of order $q-1$. Now a cycle of order $q-1$ has sign -1 since $q-1$ is even. Since q is odd, q^{n-1} is odd too, hence the sign of τ is -1.
Case $n \geq 2$, $k = \mathbb{F}_2$: In this case we can find another element of sign -1, namely $\sigma_{(\mathrm{o},1)}$ where o$= (0, \ldots, 0) \in k^{n-1}$. This map acts nontrivially only on $(0, \ldots, 0)$ and $(1, 0, \ldots, 0)$; it interchanges them. Hence the sign is -1. The rest is the same as the previous case.
(iii) Case $n \geq 2$, $k = \mathbb{F}_q = \mathbb{F}_{2^r}$, $r \geq 2$: We will show that every generator of G has sign 1, so $\mathcal{E}(G) = A_{q^n}$.
1) $\sigma^2_{(\alpha,b)} = (X_1 + 2f_{(\alpha,b)}, X_2, \ldots, X_n) = Id$, (since $2 \equiv 0 \mod (2)$). Hence $\sigma_{(\alpha,b)}$ consists only of 2-cycles. If we count the number of elements which stay invariant, then we know how many 2-cycles. The set of non-invariant elements is $V := \{(a, \alpha) \mid a \in k\}$, hence we have $\#V/2 = 2^r/2 = 2^{r-1}$ 2-cycles. Since 2^{r-1} is even (for $r \geq 2$), the sign of $\sigma_{(\alpha,b)}$is 1.
2) $\sigma_i^2 = Id$, hence σ_i consists of only 2-cycles too. Let us look at σ_2. This map leaves $V := \{(a, a, \alpha) \mid a \in k, \alpha \in k^{n-2}\}$ invariant. Hence we have $(\#k^n - \#V)/2 = ((2^r)^n - (2^r)^{n-1})/2 = 2^{rn-r-1}(2^r - 1)$ 2-cycles. This number is also even (since $rn - r - 1 \geq 2$ for $n, r \geq 2$) hence the sign is 1.
3) τ has order $2^r - 1$ and consists of a number of $(2^r - 1)$-cycles. These cycles have sign 1, hence τ has sign 1. $\square$

4.2.3 Conclusions

Using Theorem 4.2.3 we can also completely define all zero sets of coordinates over finite fields. $Z(F)$ will be the zero set of F, and k a finite field of q elements. A coordinate is an element $F \in k[X_1, \ldots, X_n]$ such that there exist $F_2, \ldots, F_n \in k[X_1, \ldots, X_n]$ satisfying $k[F, F_2, \ldots, F_n] = k[X_1, \ldots, X_n]$.

Corollary 4.2.10. *A set $S \subseteq k^n$ is a zero set of a coordinate $F \in k[X_1, \ldots, X_n]$ if and only if $\#S = q^{n-1}$.*

Proof. The case $n = 1$ is trivial, since every coordinate is of the form $aX_1 + b$ where $a \in k^*$. So let $n \geq 2$ and define $V_0 := \{(0, \alpha) \mid \alpha \in k^{n-1}\}$. S being the zero set of a coordinate is equivalent to having an automorphism φ satisfying $\varphi(S) = V_0$ (the first component of φ will be the coordinate). The "only if"-part of corollary 4.2.10 follows from the fact that φ induces a bijection $k^n \longrightarrow k^n$, and thus $\#S = \#\varphi(S) = \#V_0$. Conversely we need to find an invertible polynomial map φ satisfying $\varphi(S) = V_0$. In other words, we need to find a bijection B which sends S to V_0 and is induced by an invertible polynomial map φ (i.e. $B := \mathcal{E}(\varphi)$). Using Theorem 4.2.3, in case $q = 2$ or $q = p^r$ where $p > 2$ we can find such a bijection B. In case $q = 2^r, r \geq 2$ we show that there exists an even bijection which sends S to V_0. We can achieve this by taking two elements $a, b \in k^n \backslash (S \cup V_0)$, $a \neq b$ (this is possible since $q > 2$, $n > 1$) and then taking a bijection B sending S to V_0 and the identity on $k^n \backslash (S \cup V_0 \cup \{a, b\})$ and then either interchanging a and b or sending a to a and b to b. □

Notice that the first two results of Theorem 4.2.3 are also true if we replace $T(k, n)$ by $\mathrm{Aut}_k(A)$; the third one is unclear, however: if that one is not true, it would give an easy counterexample against the -former- Tame Generators Conjecture, which stated that for any field k and any positive integer n, $Aut_k(A) = T(k, n)$:

Corollary 4.2.11. *(of Theorem4.2.3) Suppose $k = \mathbb{F}_{2^r}$ where $r \geq 2$ and $F \in \mathrm{Aut}_k(A)$ such that $\mathcal{E}(F) \in S_l \backslash A_l$, $l = \#k$. Then $Aut_k(A) \neq T(k, n)$:*

Such a counterexample over $\mathbb{F}_{2^r}$ might even induce a counterexample over $\mathbb{C}$, but that's not clear.

4.3 Dynamically trivial maps

The results in this section are joint work of J-Ph. Furter and the author.

4.3.1 Introduction

The Linearisation Conjecture asserts that if $F \in Aut_{\mathbb{C}}(\mathbb{C}^{[n]})$ and $F^s = I$ ($s \in \mathbb{N}^*$), then F is linear up to conjugation (i.e. there exists some $\varphi \in Aut_{\mathbb{C}}(\mathbb{C}^{[n]})$ such that $\varphi F \varphi^{-1}$ is linear).

One could also consider similar cases, like what polynomial endomorphisms satisfy $F^s = 0$ for some $s \in \mathbb{N}^*$, or $F^s = F$. In the case that $F^s = I$ one may say that "F is a zero of the polynomial $T^s - 1$". The other two cases, $F^s = F$ and $F^s = 0$ can also be seen as F being the zero of a polynomial $Q(T) \in \mathbb{C}[T]$. Comparing things from linear algebra, if A is a linear map, then there exists a minimum polynomial $\mathsf{m}_A \in \mathbb{C}[T]$ such that $\mathsf{m}_A(A) = 0$. From this polynomial all kinds of information about the map A can be deduced, for example, the invertibility of the map A. It is an interesting question to classify all endomorphisms which are zero of some polynomial, and also to classify which polynomials can occur as "minimum polynomial" of some endomorphism.

The minimum polynomials of such endomorphisms may be even useful in the Jacobian Conjecture, as we can conclude that an endomorphism is non-invertible if and only if T does divide the minimum

polynomial $Q(T)$. In this context it is useful to ask that if F is no zero of some polynomial, does there exist a (tame) base change (i.e. some (tame) automorphism φ) such that φF is a zero of a polynomial?

Dynamically, such endomorphisms are trivial, since their iterates are contained in a finite dimensional vectorspace. So a good name for such endomorphisms from the dynamical systems point of view can be "dynamically trivial", a name which we uphold (though purely algebraically they might be called "locally finite polynomial mappings").

This section is an attempt at tackling some of the problems occuring near the above questions.

4.3.2 Definitions and the ideal I_F

Definition 4.3.1. (i). We say that $F \in End(n)$ is a zero of $\mathsf{m}(T) = a_dT^d + \ldots + a_1T + a_0 \in \mathbb{C}[T]$ if $a_dF^d + \ldots + a_1F + a_0I = 0$. We will write $a_dF^d + \ldots + a_1F + a_0I = \mathsf{m}(F) = \mathsf{m}(T)|_{T=F}$.

(ii). If F satisfies such a relation $a_dF^d + \ldots + a_1F + a_0I = 0$ where not all a_i are zero, we say F is a **dynamically trivial** polynomial mapping.

Definition 4.3.2. If $F \in (\mathbb{C}^{[n]})^n$ then we will write $I_F := \{\mathsf{m}(T) \in \mathbb{C}[T] \mid \mathsf{m}(F) = 0\}$.

Theorem 4.3.3. *I_F is an ideal of $\mathbb{C}[T]$.*

Proof. We need to show (1) that if $\mathsf{m}_1, \mathsf{m}_2 \in I_F$ then $\mathsf{m}_1 + \mathsf{m}_2 \in I_F$ (follows from lemma 4.3.4.2) and (2) if $\mathsf{m} \in I_F$, $P \in \mathbb{C}[T]$ then $P\mathsf{m} \in I_F$. Write $P = \sum_{i=0}^{k} a_iT^i$. We know by lemma 4.3.4.1 that $a_iT^i\mathsf{m} \in I_F$. 4.3.4.2 then tells us that $\sum_{i=0}^{k} a_iT^i\mathsf{m} \in I_F$, hence $P\mathsf{m} \in I_F$. □

Lemma 4.3.4.

(i). If F is a zero of $\mathsf{m}(T)$ then F is a zero of $T^s\mathsf{m}(T)$ where $s \in \mathbb{N}$.

(ii). If F is a zero of $\mathsf{m}_1(T)$ and $\mathsf{m}_2(T)$ then F is a zero of $(\mathsf{m}_1 + \mathsf{m}_2)(T)$.

Proof. i) Take $\mathsf{m}(F) = 0$. Then $0 = (m(F)) \circ F^s = (T^s \mathsf{m}(T))|_{T=F}$. *ii)* Easy. □

Since I_F is an ideal in $\mathbb{C}[T]$, it is generated by one element, let's call it $\mathsf{m}_F(T)$. If one chooses the element to be monomial (highest coefficient equals 1), then it is unique. We can give it a nice name:

Definition 4.3.5. m_F is the minimum polynomial for F, if it exists. Define $\mathsf{m}_F = 0$ in case $I_F = \{0\}$.

Lemma 4.3.6. *Let $\varphi \in Aut(n)$. Then*

(i). $F \in \mathbb{C}^{[n]}$ dynamically trivial $\iff$ $\varphi^{-1} F \varphi$ dynamically trivial ,

(ii). if φ is linear, then $\mathsf{m}_F = \mathsf{m}_{\varphi^{-1} F \varphi}$.

Proof. (ii) is easy, and *(i)* will follow from the equivalence of (a) and (a') in theorem 4.3.11. □

4.3.3 $\det(JF)$ and $\mathsf{m}_F(0)$ of dynamically trivial maps

Lemma 4.3.7. *If $F \in End(n)$ is a dynamically trivial mapping then the following are equivalent:*

(i). F is invertible

(ii). $\mathsf{m}_F(0) \in \mathbb{C}^*$

Proof. If F is invertible and $\mathsf{m}(F) = 0$ for some $\mathsf{m} \neq 0$ satisfying $\mathsf{m}(0) = 0$, then $(T^{-1}\mathsf{m}(T))|_{T=F} = \mathsf{m}(F) \circ F^{-1} = 0$ hence the polynomial m_F must satisfy $\mathsf{m}_F(0) \neq 0$ for otherwise it would not be of lowest degree. The other way around, if $\mathsf{m}_F(0) \neq 0$ then $F^{-1} = (\mathsf{m}_F(0)T)^{-1}(\mathsf{m}_F(0) - \mathsf{m}_F(T))|_{T=F}$. □

Write JF for the Jacobian matrix of F.

Lemma 4.3.8. *If F is dynamically trivial and not invertible then $det(JF) = 0$.*

Proof. We find $\mathsf{m}_F(T)$ of lowest degree such that $\mathsf{m}_F(F) = 0$. By lemma 4.3.7 we know that $\mathsf{m}_F(0) = 0$. Thus T divides $\mathsf{m}_F(T)$. Write $Q(T) := T^{-1}\mathsf{m}_F(T)$. Then we know $0 = \mathsf{m}_F(F) = Q(F) \circ F$. Since m_F is the minimum polynomial, $Q(F) \neq 0$. This means that (writing $F = (F_1, F_2, \ldots, F_n)$) that $F_1, \ldots, F_n$ are algebraically dependent. This last statement is well-known to be equivalent to $det(JF) = 0$. □

Corollary 4.3.9. *If $F \in End(n)$ is dynamically trivial then $det(JF) \in \mathbb{C}$.*

Corollary 4.3.10. *The Jacobian Conjecture is true for dynamically trivial $F \in End(n)$.*

4.3.4 Equivalent formulations

Theorem 4.3.11. *Let $F \in End(n)$ be a polynomial map. Then the following are equivalent:*
(a) *F is a dynamically trivial map ($\mathsf{m}_F \neq 0$),*
(a') *The sequence $\{deg(F^k)\}_{k\in\mathbb{N}}$ is bounded,*
(a") *The map F is a locally finite map on the $\mathbb{C}$-vectorspace $(\mathbb{C}^{[n]})^n$,*
(a"') *The map $E_F := (F^* - I^*) \in End(n)$ sending $g \longrightarrow g(F) - g$ is a locally finite map on the $\mathbb{C}$-vectorspace $(\mathbb{C}^{[n]})^n$,*

Proof. (a)$\longleftrightarrow$(a'): Assuming (a), we can deduce that $F^n = \sum_{i=0}^{n-1} c_i F^i$ for some $n \in \mathbb{N}$, $c_i \in \mathbb{C}$. But now for any $m \in \mathbb{N}$, F^{n+m} can be expressed as a $\mathbb{C}$-linear combination of $F^{n-1}, \ldots, F, I$, which means that the sequence $\{deg(F^k)\}_{k\in\mathbb{N}}$ is bounded. On the other hand, if the sequence $\{deg(F^k)\}_{k\in\mathbb{N}}$ is bounded, then there must be some $n \in \mathbb{N}$ such

that there is a $\mathbb{C}$-linear dependence between $F^n, F^{n-1}, \ldots, F, F^0$.
(a')$\longrightarrow$(a"): we need to prove that for any $g \in \mathbb{C}^{[n]}$ the vectorspace $V_g := span\{g, g(F), g(F^2), \ldots\}$ is finite dimensional. But since $\{deg(F^k)\}_{k\in\mathbb{N}}$ is a bounded sequence, this is the case.
(a")$\longrightarrow$(a'): $V_{X_i} := span\{X_i, F_i, F_i(F), F_i(F^2), \ldots\}$ is a finite dimensional vectorspace, so $\{deg(F_i(F^k))\}_{k\in\mathbb{N}}$ is a bounded sequence. Thus $\{F^k\}$ is a bounded sequence.
(a")$\longleftrightarrow$(a"'): $W_g := span\{g, E_F(g), E_F^2(g), \ldots\} = span\{g, g-g(F), g-2g(F)+g(F^2), \ldots\}$. One can see that $W_g = V_g$ for any $g \in \mathbb{C}^{[n]}$. Since $W_g = V_g$ we have equivalence of F^* locally finite if and only if E_F is locally finite. □

The following concerns a missing link:

Conjecture 4.3.12. Let $F \in End(n)$ be a polynomial map. Then the following are equivalent:
(b) F is dynamically trivial and invertible,
(b') $F = exp(D)$ where D is some locally finite derivation D (and hence F is invertible with inverse $exp(-D)$).

Notice that $(b') \longrightarrow (b)$ is true: if D is locally finite and $V_g := span\{g, D(g), D^2(g), \ldots\}$ then $\exp(\lambda D)(g) \in V_g$ for any $\lambda \in \mathbb{C}$. Therefore, $\exp(kD)$ is a locally finite map on $\mathbb{C}^{[n]}$ for any $k \in \mathbb{N}$, and by 4.3.11 (a") we have F is dynamically trivial. F is invertible since $\exp(-D)$ is the inverse.

Lemma 4.3.13. *The following are equivalent:*
(c) *The map E_F is locally nilpotent,*
(c') *The map $D := \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i} E_F^i$ is well-defined and is locally nilpotent,*
(c") *$F^* = exp(D)$ of some locally nilpotent derivation D.*

Proof. Equivalence of (c),(c'), and (c") is shown in [Ess00] pages 44-45, in particular proposition 2.1.3 . □

Remark 4.3.14. $(c'') \longrightarrow (b') \longrightarrow (a)$ and the first and last arrow cannot be reversed.

Proof. It is clear that (c") implies (b'), but (b') does not imply (c"). Assuming (b') we also have (b), which implies (a). Now $F = (X + XY, 0)$ satisfies (a') but not (b) or (b') since F is not invertible. □

4.3.5 Nilpotent maps

Lemma 4.3.15. *If $F \in (\mathbb{C}^{[n]})^n$ satisfies $F^m = 0$ for some $m \in \mathbb{N}$, then $F^n = 0$.*

Proof. Let us endow $\mathbb{C}^n$ with the Zariski topology. If $k \geq 0$, let us set $V_k := \overline{F^k(\mathbb{C}^n)}$, the Zariski closure of $F^k(\mathbb{C}^n)$. Since F is a continuous map, $F(\mathbb{C}^n)$ is irreducible, by [Spr81] lemma 1.2.3 (ii). Thus V_k is irreducible and closed. We also have

$$V_{k+1} = \overline{F(V_k)} \subseteq \overline{F^k(F(\mathbb{C}^n))} \subseteq \overline{F^k(\mathbb{C}^n)} = V_k,$$

so we have a chain $\mathbb{C}^n = V_0 \supseteq V_1 \supseteq V_2 \supseteq \ldots \supseteq V_m = 0$. Suppose that $\dim(V_k) = \dim(V_{k+1}) \geq 1$ for some $k \in \mathbb{N}$. Since V_k as well as V_{k+1} are irreducible, $V_k = V_{k+1}$. Then $V_{k+2} = \overline{F(V_{k+1})} = \overline{F(V_k)} = V_{k+1}$ and thus the chain becomes stationary; which is a contradiction with the fact that $V_m = 0$. Therefore, the dimension of the V_k must decrease each step, which implies that $dim(V_n) = 0$. Thus $F^n = 0$. □

4.3.6 Dynamically trivial maps and l.r.s.

Dynamically trivial endomorphisms are closely linked with linear recurrence sequences. Actually, if F is dynamically trivial, then $\{F^k\}_{k\in\mathbb{N}}$

is a l.r.s. ! Furthermore, the language of linear recurrence sequences (l.r.s. for short) will be a very useful tool to handle some computations to come.

Let F be an endomorphism of $\mathbb{C}^n$. We can define complex sequences $F_{i,\alpha}$ for $1 \leq i \leq n$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, by the following equality (for each non negative integer k) :

$$F^k = \left(\sum_{\alpha \in \mathbb{N}^n} F_{1,\alpha}(k) X^\alpha, \ldots, \sum_{\alpha \in \mathbb{N}^n} F_{n,\alpha}(k) X^\alpha \right),$$

where we set $X^\alpha := X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ if $\alpha = (\alpha_1, \ldots, \alpha_n)$.

In other words, $F_{i,\alpha}(k)$ is the coefficient of X^α of the i-th coordinate of F^k.

The following theorem is straightforward.

Theorem 4.3.16. *Let F be an endomorphism of $\mathbb{C}^n$ and let $P(T)$ be a monic polynomial of $\mathbb{C}[T]$, then the three following assertions are equivalent :*

(i). $P(F) = 0$;

(ii). *the sequence $\{F^k\}_{k \in \mathbb{N}}$ of $End(n)$ is a l.r.s. with characteristic polynomial P ;*

(iii). *for each $i \in \{1, \ldots, n\}$, $\alpha \in \mathbb{N}^n$, the sequence $\{F_{i,\alpha}(k)\}_{k \in \mathbb{N}}$ is a complex l.r.s. with characteristic polynomial P.*

Lemma 4.3.17. *Let $\{F_k\}_{k \in \mathbb{N}}$ be a l.r.s. of endomorphisms $F_k \in End(n)$ of type Ω. Let $\varphi \in End(n)$ and $d := deg(\varphi)$. Then $\{F_k \varphi\}_{k \in \mathbb{N}}$ is a l.r.s. of type Ω and $\{\varphi F_k\}_{k \in \mathbb{N}}$ is a l.r.s. of type $\Sigma := \Omega \cup \Omega^2 \cup \ldots \cup \Omega^d$.*

Proof. By definition we find $k \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{C}$ such that $F_{m+k} = a_{m-1}F_{m+k-1} + \ldots + a_0F_m$ for all $m \in \mathbb{N}$. Thus $F_{m+k}\varphi = a_{m-1}F_{m+k-1}\varphi + \ldots + a_0F_m\varphi$ for all $m \in \mathbb{N}$, so $\{F_k\varphi\}_{k\in\mathbb{N}}$ is a l.r.s. of type Ω.

For the $\{\varphi F_k\}_{k\in\mathbb{N}}$ sequence: let

$$\varphi = \big(\sum \lambda_{1,\alpha}X^\alpha, \ldots, \sum \lambda_{n,\alpha}X^\alpha\big).$$

Write F_k^α for $(F_k)_1^{\alpha_1}(F_k)_2^{\alpha_2}\cdots(F_k)_n^{\alpha_n}$. Then for each $i \in \{1, \ldots, n\}, \alpha \in \mathbb{N}^n$, $\{\lambda_{i,\alpha}(F_k)^\alpha\}_{k\in\mathbb{N}}$ is a l.r.s of type $\Omega^{\#\alpha}$ by lemma 1.5.6. Sums of these l.r.s. are hence of type $\Omega \cup \Omega^2 \cup \ldots \cup \Omega^d$. Therefore, $\{\varphi F_k\}_{k\in\mathbb{N}}$ is a l.r.s. of the above type. □

4.3.7 The n=2 case

In this section we will assume that any polynomial map F which we consider will satisfy $F(0) = 0$. Also, if we say in this section that something is an automorphism, we mean it to be an element of $Aut_{\mathbb{C}}(\mathbb{C}[X, Y])$. We will try to classify all dynamically trivial $F \in (\mathbb{C}[X, Y])^2$ satisfying $F(0) = 0$ and give formulas for polynomials of which they are zeroes.

For the case $n = 2$, we can give another equivalent formulation for F to be an invertible dynamically trivial map:

Lemma 4.3.18. *In case $F \in Aut(\mathbb{C}[X, Y])$ then F is a dynamically trivial map if and only if $deg(F^2) \leq deg(F)$.*

Proof. In [Fur99] the quotient $\tau := deg(F^2)/deg(F)$ is studied, and it is shown that $\tau \leq 1$ if and only if $\{deg(F^k)\}_{k\in\mathbb{N}}$ is a bounded sequence. □

The Jung- van der Kulk theorem in connection with the above theorem gives the following corollary:

Corollary 4.3.19. *If F is invertible and dynamically trivial, and $F(0) = 0$, then F is triangularisable.*

Proof. This is a consequence of proposition 5 in [Fur99], part (ii) $\longrightarrow$ (i): it is shown that if $deg(F^2) \leq deg(F)$ then F is conjugate to an affine map or an elementary one, and both are (conjugate to) a triangular map (since $F(0) = 0$). □

Main results

In this subsection we will just give the main results. For proofs we refer to the following two subsections, "The invertible case" and "The noninvertible case".

Theorem 4.3.20. *Let F be dynamically trivial. Then*

(i). if F is invertible, there exists $\varphi \in Aut(2)$ such that $\varphi F \varphi^{-1} = (aX + f(Y), bY)$

(ii). if F is not invertible, then there exists $\varphi \in Aut(2)$ such that $\varphi F \varphi^{-1} = (aX + Y f(X, Y), 0)$

Proof. Combine corollary 4.3.19 (for (i)) and lemma 4.3.29 (for (ii)). □

Theorem 4.3.21. *If F is dynamically trivial and $F(0) = 0$, then $deg(\mathsf{m}_F(T)) \leq deg(F) + 1$ and this bound is sharp.*

Proof. Notice that remark 4.3.26 tells us that this bound is attained. We split up in the case F invertible and F not invertible.
F invertible: In case $F := (aX + f(Y), bY)$ for some F we see by lemma 4.3.25 that $deg(\mathsf{m}_F) \leq d + 1$. If F is a linear conjugate of such a map we use lemma 4.3.6 part *(ii)*. In the other cases we use corollary 4.3.19

and lemma 4.3.27 and using 4.3.24 we may assume $d_1 \geq 2$, $d = d_1^2 d_2$ for some $d_1, d_2 \in \mathbb{N}$, and $deg(\mathsf{m}_f) \leq \#\{(i,j) \in \mathbb{N}^2 \mid d_2 i + j \leq d_1 d_2\} - 1$. Now

$$\begin{array}{rl} -\frac{d_1^2 d_2}{2} - d_1(\frac{d_2}{2} - 1) - 1 \leq 0 \Longleftrightarrow & \\ d_1(d_2 d_1 + 1) - \frac{d_2 d_1 (d_1+1)}{2} - 1 - d_1^2 d_2 \leq 0 \Longleftrightarrow & \\ \left(\sum_{i=0}^{d_1} d_2(d_1 - i) + 1\right) - 1 - d_1^2 d_2 \leq 0 & \Longleftrightarrow \\ \sum_{i=0}^{d_1} \{j \in \mathbb{N} \mid 0 \leq j \leq (d_1 d_2 - d_2 i)\} - 1 - d_1^2 d_2 \leq 0 & \Longleftrightarrow \\ \#\{(i,j) \in \mathbb{N}^2 \mid d_2 i + j \leq d_1 d_2\} - 1 \leq d & \end{array}$$

and thus we are done for this case.
F not invertible: This is a direct consequence of lemma 4.3.29 and lemma 4.3.31. □

Theorem 4.3.22. *(extension of Cayley-Hamilton for dynamically trivial polynomial maps) Let F be dynamically trivial and $F(0) = 0$. Let $d := deg(F)$ and let L be the linear part of F. Then F is a zero of $P_F(T)$ where*

$$P_F(T) := \prod_{\substack{0 \leq k \leq d-1 \\ 0 \leq m \leq d \\ (k,m) \neq (0,0)}} \left(T^2 - (detL^k)(TrL^m)T + det(L^{2k+m})\right).$$

Proof. $P_F(T)$ is of degree $2(d^2 + d - 1)$. Let a, b be the eigenvalues of L. Then

$$\begin{array}{rl} & T^2 - (detL^k)(TrL^m)T + det(L^{2k+m}) \\ = & T^2 - (a^k b^k)(a^m + b^m)T + a^{2k+m} b^{2k+m} \\ = & (T - a^{k+m} b^k)(T - a^k b^{k+m}). \end{array}$$

We split up in the case F invertible and F not invertible.
F invertible: Looking at lemma 4.3.27 we see that $P_F(T)$ divides the polynomial $M_F(T)$ shown there. Notice that these a, b in lemma 4.3.27

really are the eigenvalues of the linear part of F.
F not invertible: Looking at lemma 4.3.31 we see that that $P_F(T)$ divides the polynomial $M_F(T)$ shown there. Notice that a and 0 are the only eigenvalues of the linear part of F. □

Remark 4.3.23. Notice that for $d = 1$ the above theorem indeed gives the 2-dimensional case of the Cayley-Hamilton theorem.

The invertible case

Lemma 4.3.24. *If F is invertible and triangularisable, then $F = \varphi G \varphi^{-1}$ for some triangular G and an automorphism φ, in such a way that $deg(F) = deg(\varphi)^2 deg(G)$.*

Proof. Using the well-known Jung-van der Kulk- theorem we can write $F = \lambda_0\tau_1\lambda_1\cdots\tau_l\lambda_l$ where $\lambda_i \in Aff(\mathbb{C}, 2)$ (the affine automorphism group) and $\tau_i \in J(\mathbb{C}, 2)$ (the de Jonquière group, or set of upper triangular automorphisms), and $deg(F) = \prod_i deg(\tau_i)$. Since F is triangularisable, it must be that $\lambda_0 = \lambda_l^{-1}, \tau_1 = \tau_l^{-1}, \lambda_1 = \lambda_{l-1}^{-1}$ etc. up to the middle part, which is $\lambda_{l/2}$ in case l is even or $\tau_{l/2+1/2}$ in case l is odd. In the case that l is odd, take $\varphi := \lambda_0\tau_1\lambda_1\cdots\lambda_{l/2-1/2}$, $G := \tau_{l/2+1/2}$. In case l is even, let L be a linear map such that $L\lambda_{l/2}L^{-1}$ is upper triangular, and take $\varphi := \lambda_0\tau_1\lambda_1\cdots\tau_{l/2}L^{-1}$, $G := L\lambda_{l/2}L^{-1}$ In both cases the result follows easily from the fact that $deg(\varphi^{-1}) = deg(\varphi) = \sum_i^{l/2-1 \text{ or } l/2} deg(\tau_i)$. □

Lemma 4.3.25. *Let $F_{a,b} := (aX + f(Y), bY)$ for some $a, b \in \mathbb{C}^*$ and $f(Y) \in \mathbb{C}[Y]$. Let $d := deg(f)$. Then $F_{a,b}$ is a zero of $(T - a)(T - b)(T - b^2)\cdots(T - b^d)$.*

Proof. Let us consider $F := (AX + f(Y), BY)$ where A, B are variables, and $f(Y) := \sum_{i=1}^{d} C_i Y^i$ where the C_i are variables as well. Define $Q(T) := (T - A)(T - B)(T - B^2)\cdots(T - B^d)$. We first show that

$((F^n)_1)_{n\in\mathbb{N}}$ and $((F^n)_2)_{n\in\mathbb{N}}$ are linear recurrent sequences satisfying $Q(T)$. In other words, we have to show that for $i = 1, 2$ and each $\alpha \in \mathbb{N}^2$ the sequences $((F^n)_{i,\alpha})_{n\in\mathbb{N}}$ are l.r.s of type $\omega := \{A, B, B^2, \ldots, B^d\}$. Or more precisely, defining $R := \mathbb{C}(A, B, C_1, \ldots, C_d)$, we must have for $i = 1, 2$ and each $\alpha \in \mathbb{N}^2$ that

$$\{(F^n)_{i,\alpha}\}_{n\in\mathbb{N}} \in R \cdot \big(\{A^n\}_{n\in\mathbb{N}}\big) + \sum_{j=1}^{d} R \cdot \big(\{B^{jn}\}_{n\in\mathbb{N}}\big).$$

By induction it is not difficult to prove that $F^n := (A^nX + f(B^{n-1}Y) + Af(B^{n-2}Y) + \ldots A^{n-1}f(Y), B^nY)$. Rewriting we get

$$\begin{array}{rll}
F^n := & \big(A^nX + \sum_{i=0}^{n-1} A^i f(B^{n-1-i}Y) & , B^nY\big) \\
= & \big(A^nX + \sum_{i=0}^{n-1} A^i \sum_{j=1}^{d} \big(C_j(B^{n-1-i}Y)^j\big) & , B^nY\big) \\
= & \big(A^nX + \sum_{j=1}^{d} C_jY^j \sum_{i=0}^{n-1} \big(A^i(B^j)^{n-1-i}\big) & , B^nY\big) \\
= & \big(A^nX + \sum_{j=1}^{d} C_jY^j \frac{(A^n - B^{nj})}{A-B^j} & , B^nY\big) \\
= & X\big(A^n, 0\big) & + \\
& \sum_{j=1}^{d} \frac{C_jY^j}{A-B^j}\Big(A^n, 0\Big) & + \\
& \sum_{j=1}^{d} \frac{C_jY^j}{A-B^j}\Big((B^j)^n, 0\Big) & + \\
& Y(0, B^n). &
\end{array}$$

So we are done in the case that we assume that $A, B, C_1, \ldots, C_d$ are variables. But now one can just specialise by substituting values; the lemma is proven for any specialisation $a, b, c_1, \ldots, c_d$ of $A, B, C_1, \ldots, C_d$ which has no relation $a = b^k$ for some $k \in \mathbb{N}$. Since this proves the lemma for a dense set of $(a, b, c_1, \ldots, c_d) \in \mathbb{C}^{2+d}$ the lemma follows for all $(a, b, c_1, \ldots, c_d) \in \mathbb{C}^{2+d}$. (If one appreciates it, one may also assume $A = B^k$ for some $k \in \mathbb{N}$ and recalculate the above formula for F^n.) □

Remark 4.3.26. For some $a, b \in \mathbb{C}$ the above F has $\mathsf{m}_F(T) = (T - a)(T - b)(T - b^2)\cdots(T - b^d)$, i.e. $deg(\mathsf{m}_F) = deg(F) + 1$ (for example $a = 2, b = 3$).

Lemma 4.3.27. *Let $F = \varphi G \varphi^{-1}$ where $G = (aX + f(Y), bY)$ for some $a, b \in \mathbb{C}, f(Y) \in \mathbb{C}[Y]$ and $\varphi \in Aut(\mathbb{C}[X,Y])$ with $\varphi(0) = 0$. Let $d_2 := deg(G)$, $d_1 := deg(\varphi)$. Then F is a zero of*

$$M_F(T) := \prod_{\substack{i,j \in \mathbb{N} \\ (i,j) \neq (0,0) \\ d_2 i + j \leq d_1 d_2}} (T - a^i b^j).$$

Proof. Let us begin with the case where a and the $(b^i)_{1 \leq i \leq d_2}$ are $d_2 + 1$ distinct complex numbers. Therefore, by lemma 4.3.25, $\{G^k\}_{k \in \mathbb{N}}$ is a l.r.s. of type $\Omega := \{a\} \cup \{b^i,\ 1 \leq i \leq d_2\}$. By lemma 4.3.17 $\{\varphi G^k \varphi^{-1}\}_{k \in \mathbb{N}}$ is a l.r.s. of type $\Sigma = \Omega \cup \Omega^2 \cup \ldots \cup \Omega^{d_1}$. We find that $\Sigma = \{a^i b^j,\ d_2 i + j \leq d_1 d_2,\ (i,j) \neq (0,0)\}$, so that $M_F(F) = 0$.

In the general case, we use a density argument. Let $f(Y) \in \mathbb{C}[Y]$ and $\varphi \in \mathbb{C}[X,Y]^2$ be fixed and let us call $F_{a,b}$ (resp. $M_{a,b}$) what we called before F (resp. M_F), to stress on the fact that a and b will be parameters. We have already proven that if $(a,b) \in \mathbb{C}^2$ does not belong to the hypersurface

$$\prod_{1 \leq i \leq d_2} (A - B^i) \times \prod_{1 \leq i < j < d_2} (B^i - B^j) = 0,$$

then $M_{a,b}(F_{a,b}) = 0$. Therefore, by density, this equality remains true for any $(a,b) \in \mathbb{C}^2$.

□

Note. The underlying topology expressed by the word density is the Zariski topology. However, the argument is unchanged if one takes the transcendental topology. It essentially means that if a polynomial $R(a,b)$ satisfies $R(a,b) \equiv 0$ when (a,b) is outside a given hypersurface of $\mathbb{C}^2$, then we have $R(a,b) \equiv 0$ on $\mathbb{C}^2$.

The noninvertible case

Lemma 4.3.28. *Let $F \in \mathbb{C}[X,Y]^2$ such that $F(0) = 0$, F is dynamically trivial , and F is not invertible. Then $F = (p(u), q(u))$ for some $u(X,Y) \in \mathbb{C}[X,Y]$ and $p(S), q(S) \in \mathbb{C}[S]$ satisfying $u(p,q) = \lambda S$ some $\lambda \in \mathbb{C}$.*

Proof. Assume $F \neq (0,0)$. Let $\mathsf{m}_F(T)$ be the minimum polynomial such that $\mathsf{m}_F(F) = 0$. By lemma 4.3.7 we have $\mathsf{m}_F(0) = 0$. Let $Q(T) := T^{-1}\mathsf{m}_F(T)$. Since $deg_T(Q) < deg_T(\mathsf{m}_F)$ we have $Q(F) \neq 0$. But $Q(F) \circ F = 0$, and that implies we have a polynomial relation between F_1 and F_2 (where $F = (F_1, F_2)$). Since $F_1, F_2 \in \mathbb{C}[X,Y]$ it follows from Gordon's lemma (see [Gor87]) that $F_1 = p(u), F_2 = q(u)$ for some $u \in \mathbb{C}[X,Y]$ and $p(S), q(S) \in \mathbb{C}[S]$. Since $F(0) = 0$ we may assume $u(0,0) = p(0) = q(0) = 0$. It follows that $u \notin \mathbb{C}$ (since $F(0,0) \neq 0$). Define $L(S) := u(p(S), q(S))$. Notice $u(F) = u(p(u), q(u)) = L(u)$, and thus $u(F^i) = L(u(F^{i-1})) = L^2(u(F^{i-2})) = \ldots = L^i(u)$. And this means $F^i = (p(u), q(u)) \circ F^{i-1} = (p(L^{i-1}(u)), q(L^{i-1}(u)))$.

Let $\mathsf{m}_F(T) := T^m + a_{m-1}T^{m-1} + \ldots + a_1 T$. ($m \geq 2$ since $F \neq (0,0)$) Let us look at the first component of $\mathsf{m}_F(F)$:

$$\begin{aligned} 0 = \;& p(u(F^{m-1})) + a_{m-1}p(u(F^{m-2})) + \ldots + a_1 p(u) \\ = \;& p(L^{m-1}(u)) + a_{m-1}p(L^{m-2}(u)) + \ldots + a_1 p(u) \text{ hence} \\ (*) \qquad 0 = \;& p(L^{m-1}(S)) + a_{m-1}p(L^{m-2}(S)) + \ldots + a_1 p(S). \end{aligned}$$

Looking at the second component of $\mathsf{m}_F(F)$ yields the equation $0 = q(L^{m-1}(S)) + a_{m-1}q(L^{m-2}(S)) + \ldots + a_1 q(S)$. Observe that not both p and q are constant (for then $F = 0$). Say $deg(p) \geq 1$. Then (*) gives $deg(L(S)) \leq 1$. Since $L(0) = u(p(0), q(0)) = u(0,0) = 0$ we see that $L(S) = \lambda S$ for some $\lambda \in \mathbb{C}$ in all cases. □

Lemma 4.3.29. *If $F \in \mathbb{C}[X,Y]^2$ such that $F(0) = 0$, F is dynamically trivial , and F is not invertible then there exists an automorphism φ and $G := (aX + Yf(X,Y), 0)$ such that $F = \varphi G \varphi^{-1}$.*

Proof. We may assume that $F \neq (0,0)$. By lemma 4.3.28 we know that $F = (p(u), q(u))$ and $u(p,q) = \lambda S$, (with $\lambda \neq 0$ since $F \neq (0,0)$) as stated there. Thus the Abhyankar-Moh theorem tells us there exists some automorphism φ such that $\varphi(p(S), q(S)) = (S, 0)$. Thus $\varphi F \varphi^{-1} = \varphi(p(u), q(u))\varphi^{-1} = (u, 0)\varphi^{-1} = (u(\varphi^{-1}), 0)$. Define $G := (r(X) + Yf(X,Y), 0) := (u(\varphi^{-1}), 0)$. By lemma 4.3.11 we know that $(deg(G^i))_{i\in\mathbb{N}}$ must be bounded. Since one can easily see that $G^n = (r^n(X) + Y(\ldots), 0)$ we must have $r(X)$ of degree ≤ 1, i.e. $r(X) = aX$ for some $a \in \mathbb{C}$ (since $F(0) = 0$). Thus we are done. □

Lemma 4.3.30. *$G := (aX + Yf(X,Y), 0)$ is zero of $T^2 - aT$.*

Proof. It is easy to see that $G^2 = aG$. □

Lemma 4.3.31. *Let $F := \varphi G \varphi^{-1}$ where $G := (aX + Yf(X,Y), 0)$. Then F is a zero of $M_F(T) := T(T-a)(T-a^2)\cdots(T-a^d)$ where $d = deg(F)$.*

Proof. By lemma 4.3.28 we have $F = (p(u), q(u))$ where $u(p,q) = aT$. Notice $F^n = (p(a^n u), q(a^n u))$ for all $n \geq 1$. Define $Q := T(T - a)(T - a^2)\cdots(T - a^e)$ where $e := max(deg(p(S)), deg(q(S)))$. Write $Q(T) = \sum c_i T^i$. Let $p_k(S)$ be the homogeneous part of degree k of $p(S)$ (i.e. $p_k(S) = \lambda_k S^k, q_k(S) = \mu_k S^k$, some $\lambda_k, \mu_k \in \mathbb{C}$). Then

$$\begin{array}{rl}
 & Q(a^k) = 0 \forall k \in \{1, \ldots, e\} \\
\iff & \sum c_i (a^k)^i = 0 \forall k \in \{1, \ldots, e\} \\
\Rightarrow & \sum c_i S^k (a^k)^i (\lambda_k, \mu_k) = 0 \forall k \in \{1, \ldots, e\} \\
\iff & \sum c_i S^k a^{ik} (\lambda_k, \mu_k) \forall k \in \{1, \ldots, e\} \\
\iff & \sum c_i (p_k(a^i S), q_k(a^i S)) \forall k \in \{1, \ldots, e\} \\
\iff & \sum c_i (p(a^i S), q(a^i S)) = 0 \\
\iff & \sum c_i (p(a^i u), q(a^i u)) = 0 \\
 & Q(F) = 0.
\end{array}$$

Notice that $e \leq d$. □

Remark: In this case it is actually possible to calculate the minimum polynomial (which we will not prove here). Define $\mathsf{supp}(\sum \lambda_i S^i) := \{i \mid \lambda_i \neq 0\}$, and define $U := \mathsf{supp}(p(S)) \cup \mathsf{supp}(q(S))$. Remember $u(p(S), q(S)) = aT$. Then

$$\mathsf{m}_F(T) := T \prod_{i \in U} (T - a^i).$$

4.3.8 Questions and conjectures

Other generalisations in two variables

Of course, an interesting question could be if it would be possible to find some kind of "Cayley-Hamilton" for generic polynomial maps, for example in two variables. Probably an extension should involve a "nice" set $S \subset \mathbb{C}[X,Y]^2$ such that for every $F \in \mathbb{C}[X,Y]^2$ we find $\varphi_i \in S$ such that $\sum_i \varphi_i(F^i) = 0$. What would one want as "nice" properties for this set S?

Notice that the useful thing of Cayley-Hamilton for linear maps (in which case, $S = \mathbb{C} \cdot I$) is the fact that the characteristic polynomial describes when a map is invertible by its constant part. A nice property!

Notice that if $\sum_i \varphi_i F^i = 0$ and φ_0 is an automorphism, then F is an automorphism having inverse $(-\varphi_0)^{-1} \sum_{i=1}^n \varphi_i F^{i-1}$. And if $\varphi_0 = 0$ then either F is not invertible or $\sum_i \varphi_i F^{i-1} = 0$. Aha, maybe we could let S have the property (*) that if $\varphi \in S$ then either φ is an automorphism or $\varphi = 0$!

Too bad, this doesn't work. The largest possible set satisfying (*) would be $S_1 := \{0\} \cup Aut(\mathbb{C}[X,Y])$, but it is not very difficult to see that, if $F := (X^2, Y^2)$ and $\varphi_i \in S_1$ such that $\sum_i \varphi_i F^i = 0$ then $\varphi_i = 0$ for all i. So if we would find a formula, it will not extend the property (*). But, we still can pose:

Question 4.3.32. Is there an "understandable" set $S \subset \mathbb{C}[X,Y]^2$ and a "magic formula" assigning to $F \in \mathbb{C}[X,Y]^2$ a "formal" polynomial $P_F(T) := \sum_i \varphi_i T^i$ for some $\varphi_i \in S$, such that $\sum_i \varphi_i(F^i) = 0$ and φ_0 is invertible if and only if F is?

"Understandable" would mean, among other things, that we can easily decide for polynomials in this set whether they are invertible or not. (For example, the Jacobian Conjecture should hold for this set.) The "magic formula" should only require the object 'F' and not any properties of F, just as in Cayley-Hamilton for linear maps.

Dimension 3 and up

In dimension 2 we have actually classified all dynamically trivial mappings: they are conjugates of linear maps or of triangular maps. (Theorem 4.3.20). In higher dimensions we apparently find more mappings: if D is a locally finite derivation, then $exp(D)$ is also a dynamically trivial map (See Theorem 4.3.11 part (b')), and may not be triangularisable (see [Bas84]). So a question we may ask is:

Question 4.3.33. What are the conjugacy classes of dynamically trivial maps in $\mathbb{C}[X,Y,Z]^3$?

Also, we don't have an extension of lemma 4.3.18. If $F := (X + Y^2, Y + Z^2, Z)$ then $deg(F^2) = 4 > deg(F) = 2$ but $deg(F^i) \leq 4$ all i, hence F is dynamically trivial .

On this we can ask :

Question 4.3.34. If $F \in Aut(\mathbb{C}^n)$ is dynamically trivial , and $d := deg(F)$, does there exist a bound $C(d)$ such that $deg(F^m) \leq C(d)$ all m? Is $C(d) := d^{n-1}$ a good guess?

Chapter 5

Unsolved problems

It is a rare occasion that research solves more questions than arise from it. Maybe inherent to research is asking so many questions that it is inevitable that in the end one has more unanswered questions than answered ones.

Mathematicians sometimes tend to be much more interested in questions and conjectures than in theorems and lemmas. Therefore this chapter sums up many questions and conjectures scattered through the other chapters (and a few new ones).

The difficulty of the conjectures and problems is hard to say; many of them are quite new, so an easy solution is very well possible. On the other hand, some of them could be very hard.

Problem 1. *Is the kernel of the derivation* $Y^2\partial_X + Z\partial_Y + T\partial_Z + W\partial_T$ *finitely generated?*

Conjecture 2. *Let* $D_1, \ldots, D_{n-1} \in \mathrm{LND}(\mathbb{C}^{[n]})$ *be linearly independent over* $\mathbb{C}^{[n]}$*. such that for each* $1 \leq i < j \leq n-1$ $[D_i, D_j] = 0$ *(i.e. they commute). Then* $(C^{[n]})^{D_1,\ldots,D_{n-1}} = \mathbb{C}[f]$ *where* f *is a coordinate.*

For the following conjecture, we must make some definitions. Let $I = (f_1, \ldots, f_m)$ be an ideal in $\mathbb{C}^{[n]}$. Let $r \in \mathbb{C}^{[n]}$, define $\bar{r} := r + I \in$

$\mathbb{C}^{[n]}$ and $R := r + f_1Y_1 + \ldots + f_mY_m \in \mathbb{C}^{[n]}[Y_1, \ldots, Y_m]$. Then $\bar{r}$ is a **generalized coordinate** if R is a stable coordinate. We say $\bar{r}$ is a **generalized slice** if there exist $p \in \mathbb{N}$ such that R is a slice for some derivation on $\mathbb{C}^{[n]}[Y_1, \ldots, Y_{m+p}]$.

Conjecture 3. *If $\mathbb{C}^{[n]}/I \cong \mathbb{C}^{[d]}$ some d then $\bar{r}$ is a generalised coordinate if and only if $\bar{r}$ is a stable coordinate. Furthermore, $\bar{r}$ is a generalized slice if and only if $\bar{r}$ is a generalized coordinate.*

Conjecture 4. *Let $\mathbb{F}$ be a finite field of characteristic 2. Then every $F \in Aut(\mathbb{F}^{[n]})$ is an even permutation of the set $\mathbb{F}^n$.*

Conjecture 5. *All invertible dynamically trivial maps are of the form $\exp(D)$ where D is a locally finite derivation.*

Problem 6. *What are the conjugacy classes of dynamically trivial maps in dimensions 3 and up?*

Problem 7. *Describe the polynomial maps $F \in End(\mathbb{C}^{[n]})$ for which we find no $\varphi \in Aut(\mathbb{C}^{[n]})$ such that φF is dynamically trivial.*

Problem 8. *Find a set $S \subset End(\mathbb{C}^{[n]})$ for which the Jacobian Conjecture holds, and for each $F \in End(\mathbb{C}^{[n]})$ we have a polynomial $\sum_{i=0}^{m} \varphi_i T^i$ where $\varphi_i \in S$ such that $\sum_{i=0}^{m} \varphi_i F^i = 0$ and φ_0 is invertible if and only if F is invertible.*

Conjecture 9. *If $F \in Aut(\mathbb{C}^{[n]})$ is dynamically trivial, and $d := deg(F)$, then $deg(F^m) \leq d^{n-1}$ for all $m \in \mathbb{N}$.*

List of notations

Bibliography

[ADE92] K. Adjamagbo, H. Derksen, and A. van den Essen. On polynomial maps in positive characteristic and the Jacobian Conjecture. Technical Report 9208, University Nijmegen, 1992.

[Adj95] K. Adjamagbo. On separable algebras over a U.F.D. and the Jacobian Conjecture in any characteristic. In *Proceedings of the international conference on invertible polynomial maps, Curacao, July 4-81994*, pages 89–103. Kluwer Academic Publishers, 1995.

[AEH72] S. Abhyankar, P. Eakin, and W. Heinzer. On the uniqueness of the coefficient ring in a polynomial ring. *Journal of Algebra*, 23:310–342, 1972.

[Bas84] H. Bass. A non-triangular action of G_a on A^3. *J. of Pure and Applied Algebra*, 33:1–5, 1984.

[BCW82] H. Bass, E. Connell, and D. Wright. The Jacobian Conjecture: Reduction of degree and formal expansion of the inverse. *Bulletin of the American Mathematical Society*, 7:287–330, 1982.

[BD97] A. Bhatwadekar and A. Dutta. Kernel of locally nilpotent R-derivations on $R[X, Y]$. *Transactions of the American Mathematical Society*, 349:3003–3019, 1997.

[BEM01] J. Berson, A. van den Essen, and S.J. Maubach. Derivations having divergence zero on $R[X, Y]$. *Israel journal of mathematics*, 124:115–124, 2001.

[Ber99] J. Berson. Derivations on polynomial rings over a domain. Master's thesis, University of Nijmegen, 1999.

[CM] T Crachiola and S.J. Maubach. The Derksen invariant vs. the Makar-Limanov invariant. To be published in Proceedings of the AMS.

[CMP87] L. Cerlienco, M. Mignotte, and F. Piras. Suites récurrentes linéaires, propriétés algébriques et arithmétiques. *L'Enseignement Mathématiques*, 33:67–108, 1987.

[Dan89] W Danielewski. On the cancellation problem and automorphism groups of affine algebraic varieties. preprint, 1989. Warsaw.

[Der97] H. Derksen. *Constructive Invariant Theory and the Linearisation Problem*. PhD thesis, University of Basel, 1997.

[DF98] D. Daigle and G Freudenburg. Locally nilpotent derivations over a U.F.D. and an application to rank two derivations of $k[x_1, \ldots, x_n]$. *J. Algebra*, 201:353–371, 1998.

[DF99] D. Daigle and G. Freudenburg. A counterexample to Hilbert's fourteenth problem in dimension five. *J. Algebra*, 221:528–535, 1999.

[DF01a] D. Daigle and G. Freudenburg. A note on triangular derivations of $k[x_1, x_2, x_3, x_4]$. *Proc.Amer.Math.Soc.*, 129:657–662, 2001.

[DF01b] D. Daigle and G. Freudenburg. Triangular derivations of $k[x_1, x_2, x_3, x_4]$. *J. Algebra*, 241:328–339, 2001.

[Ess93] A. van den Essen. An algorithm to compute the invariant ring of a G_a-action on an affine variety. *J. Symbolic Computation*, 16:531–555, 1993.

[Ess98] A. van den Essen. On Bass' inverse degree approach to the Jacobian Conjecture and exponential automorphisms. *Proceedings of the International Conference on Computational and Combinatorial Algebra, held at the University of Hong Kong, May 24-29*, 1998.

[Ess00] A. van den Essen. *Polynomial Automorphisms and the Jacobian Conjecture*, volume 190 of *in Progress in Mathematics*. Birkhäuser, 2000.

[EV99] E. Edo and S. Vénéreau. Length 2 variables of $A[X, Y]$ and transfer. *Proceedings of Krakow conference on polynomial automorphisms*, pages 67–76, 1999.

[Fre00] G. Freudenburg. A counterexample to hilbert's fourteenth problem in dimension six. *Transformation Groups*, 5:61–71, 2000.

[Fre01] G. Freudenburg. A survey of counterexamples to Hilbert's fourteenth problem. *Serdica Math. J.*, 27:1001–1023, 2001.

[Fur99] J-Ph. Furter. On the degree of iterates of automorphisms of the affine plane. *in Manuscripta Mathematica*, 98:183–193, 1999.

[GN67] P Gabriel and Y. Nouazé. Idéax premiers de l'algèbre envelloppante d'une algèbre de lie nilpotente. *Journal of Algebra*, 6:77–99, 1967.

[Gor87] P. Gordan. Über biquadratische Gleichungen. *Math.Annalen*, 29:318–326, 1887.

[Hos01] J.M. Hossu. Strategische overdracht van informatie. Master's thesis, University of Nijmegen, February 2001.

[IZ95] I.M. Isaacs and T. Zieschang. Generating symmetric groups. *Amer. Math. Monthly*, 102:734–739, 1995.

[Jun42] H. Jung. Uber ganze birationale Transformationen der Ebene. *J. Reine Angew. Math.*, 184:161–174, 1942.

[Kal01] S. Kaliman. Polynomials with general $\mathbb{C}^2$-fibers are variables. *preprint*, 2001.

[Kra95] H. Kraft. Challenging problems on affine n-space. *Séminaire Bourbaki*, 802, 1994-95.

[Kul53] W. van der Kulk. On polynomial rings in two variables. *Nieuw Archief voor Wiskunde*, 3(I):33–41, 1953.

[Mau] S.J. Maubach. The commuting derivations conjecture. To appear in Journal of Pure and Applied Algebra.

[Mau00a] S. Maubach. Triangular monomial derivations on $k[x_1, x_2, x_3, x_4]$ have kernel generated by at most four elements. *J. Pure Appl. Algebra*, 153:165–170, 2000.

[Mau00b] S.J. Maubach. An algorithm to compute the kernel of a derivation up to a certain degree. *Journal of Symbolic Computation*, 29:959–970, 2000.

[Mau01] S.J. Maubach. Polynomial automorphisms over finite fields. *Serdica Math.*, 27:343–350, 2001.

[Mau02a] S.J. Maubach. The automorphism group of $[t]/(t^m)[x_1, \ldots, x_n]$. *Communications in Algebra*, 30(2), 2002. 619-630.

[Mau02b] S.J. Maubach. The Linearisation Conjecture and other problems over nonreduced rings. *Communications in Algebra*, 30(4):1693–1705, 2002.

[Miy85] M. Miyanishi. Normal affine subalgebras of a polynomial ring. *Algebraic and Topological Theories- to the memory of Dr. Takehiko Miyata*, pages 37–51, 1985.

[ML96] L. Makar-Limanov. On the hypersurface $x+x^2y+z^2+t^3 = 0$ in $\mathbb{C}^4$ or a $\mathbb{C}^3$ -like threefold which is not $\mathbb{C}^3$. *Israel Journal of Mathematics*, 96:419–429, 1996.

[ML98] L. Makar-Limanov. Locally nilpotent derivations, a new ring invariant and applications. Lecture notes, 1998.

[ML01] L. Makar-Limanov. On the group of automorphisms of a surface $x^n y = p(z)$. *Israel Journal of Mathematics*, 121:113–123, 2001.

[ML02] L. Makar-Limanov. Cancellation for curves. preprint, 2002.

[Moh99] T. Moh. A public key system and master key functions. *Communications in Algebra*, 27(5):2207–2222, 1999.

[Mya78] M. Myanishi. Curves on rational and unirational surfaces. preprint, 1978.

[Nou81] P. Nousiainen. On the Jacobian Problem in positive characteristic. preprint, 1981. Pennsylvania State University.

[Ros01] P. van Rossum. *Tackling Problems on Affine Space with Locally Nilpotent Derivations on Polynomial Rings*. PhD thesis, University of Nijmegen, 2001.

[Sei66] A. Seidenberg. Derivations and integral closure. *Pacific Journal*, 16:167–173, 1966.

[Spr81] T. A. Springer. *Linear Algebraic Groups*. Birkhäuser Verlag, 1981.

[SU02a] I. P. Shestakov and U. U. Umirbaev. Poisson brackets and two-generated subalgebras of rings of polynomials. preprint, 2002.

[SU02b] I. P. Shestakov and U. U. Umirbaev. The tame and the wild automorphisms of polynomial rings in three variables. preprint, 2002.

[Vas69] W. Vasconcelos. Derivations on commutative noetherian rings. *Mathematische Zeitschrift*, 112:229–233, 1969.

[Wri81] W. Wright. On the jacobian conjecture. *Illinois Journal of Mathematics*, 15:423–440, 1981.

Index