Polynomial endomorphisms having coefficients in finitely generated \( \mathbb{Z} \)-algebras.

by

Abdul Rauf

a Thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Mathematics

Approved Dissertation Committee

Prof. Dr. Ivan Penkov
Chair, Jacobs University Bremen

Prof. Dr. Stefan Maubach
Hogeschool Rotterdam, Netherlands

Prof. Dr. Alan Huckleberry
Jacobs University/Ruhr Universität Bochum

Prof. Dr. David Finston
New Mexico State University, USA

Date of Defense: 03 May 2016
Declaration of Authorship

I, Abdul RAUF, hereby declare that I have written this PhD thesis independently, unless where clearly stated otherwise. I have used only the sources, the data and the support that I have clearly mentioned. This PhD thesis has not been submitted for conferral of degree elsewhere.

I confirm that no rights of third parties will be infringed by the publication of this thesis.
Signed:

________________________________________

Date: ____________________________________
Acknowledgements

I am very grateful to my PhD adviser Prof. Dr. Stefan Maubach, who has supported me throughout my thesis with his patience and knowledge whilst allowing me the room to work in my own way. His guidance helped me in all the time of research and life in general.

I am very thankful to Prof. Dr. Ivan Penkov, Prof. Dr. Alan Huckleberry and Prof. Dr. David Finston who agreed to review my thesis and also for accepting to be in my defense committee.

I would like to thank to Prof. Dr. Arno van den Essen for answering various questions through emails and reading initial version of a part of chapter 4. In addition I would like to thank Prof. Dr. Keivan Mallahi Karai for many useful discussion on various mathematical questions. I thank also the whole math department at Jacobs University for the opportunity to have nice discussions on various topics of mathematics.

I would like to acknowledge the DAAD (German Academic Exchange Service) for giving me financial support during my studies for PhD program, without which this work would not have been possible.

In the end I am also thankful to my family for their constant support throughout my studies.
# Contents

Declaration of Authorship iii  
Acknowledgements v  
Introduction/Summary 1  

1 Preliminaries 7  
1.1 Definitions and Notations 7  
Polynomial mappings 7  
Profinite group 8  
Degree function 9  
The graded ring associated to a filtration 9  
Locally Nilpotent Derivations 10  
Exponential maps, the AK invariant, locally iterative higher derivations 12  
1.2 Some conjectures 13  
The Jacobian conjecture 13  
The Cancellation Conjecture 14  

2 The profinite polynomial automorphism group 15  
2.1 Introduction 15  
2.2 Profinite endomorphisms 15  
2.3 Automorphisms fixing a variable 17  
2.4 The profinite permutations induced by endomorphisms 20  
2.5 The profinite tame automorphism group acting on orbits of a fixed size 21  
2.6 The case when $m$ is a prime integer 29  
2.7 A bound on the index of $\pi_{qm}(\text{TA}_n(\mathbb{F}_q))$ in $\pi_{qm}(\text{GA}_n(\mathbb{F}_q))$ 31  

3 A new formulation of the Jacobian Conjecture in characteristic $p$ 35  
3.1 Introduction 35  
3.2 Initial considerations 35  
3.3 A new formulation of the Jacobian Conjecture in characteristic $p$ 36  
3.4 Basic facts 37  
3.5 Two surjectivity conjectures 38  
3.6 Some computations indicating the correctness of conjecture $JC(k,n)$ 40  
3.7 Implications of the Jacobian Conjecture among various fields 42  
3.8 Some results related to $JC(k,n)$ 44  
Invertible polynomial maps and $JC(k,n)$ 44  
Closure property of $\text{SKE}_n(k)$ 45  
Connections between $JC(\mathbb{F}_p,n)$ and $JC(\mathbb{Z},n)$ 45
Boundedness .............................................. 46

4 Counter example to the cancellation problem in characteristic $p$ 49
  4.1 Introduction ........................................ 49
  4.2 Preliminaries ....................................... 49
  4.3 Main theorem of Gupta ............................. 51
  4.4 An important example of Asanuma ................ 55
  4.5 Cancellation counterexamples ..................... 58

5 On surjectivity of quotient maps 59
  5.1 Introduction ........................................ 59
  5.2 Surjectivity theorem ............................... 59
  Obstructions for being a group homomorphism .... 62
  Special case ......................................... 63
  5.3 More general situations ......................... 64
  5.4 Non-surjectivity ................................. 65

Bibliography 67
List of Symbols

\begin{align*}
R^{[n]}, \, R[X] & \quad \text{R}[X_1 \ldots , X_n] \\
\text{\text{MA}}_n(R) & \quad \text{The set of polynomial endomorphisms on } R^{[n]} \\
\text{Maps}(R^n, R^n) & \quad \text{The set of all maps } R^n \rightarrow R^n \\
\text{GA}_n(R), \text{Aut}_R(R[X]) & \quad \text{The group of } R\text{-automorphisms of } R^{[n]} \\
\text{Aff}_n(R) & \quad \text{The group of affine automorphisms on } R^{[n]} \\
\text{BA}_n(R) & \quad \text{The group of triangular automorphisms on } R^{[n]} \\
\text{TA}_n(R) & \quad \text{The tame automorphisms group on } R^{[n]} \\
\text{SA}_n(R) & \quad \text{The special automorphism group on } R^{[n]} \\
\text{MA}_n(\mathbb{F}_q) & \quad \text{The profinite polynomial endomorphism monoid over } \mathbb{F}_q \\
\hat{\text{MA}}_n(\mathbb{F}_q) & \quad \text{The profinite polynomial automorphism group over } \mathbb{F}_q \\
\hat{\text{TA}}_n(\mathbb{F}_q) & \quad \text{The profinite polynomial tame automorphism group over } \mathbb{F}_q \\
\text{M}_n(\mathbb{F}_q) & \quad \hat{\text{MA}}_n(\mathbb{F}_q) \cap \text{Perm}(\mathbb{F}_q^n) \\
\text{M}_n^m(\mathbb{F}_q) & \quad \pi_q^m(\text{MA}_n(\mathbb{F}_q)) \cap \text{Perm}(\mathbb{F}_q^{nm}) \\
\text{MA}^d_n(R) & \quad \{ F \in \text{MA}_n(R) \mid \text{deg}(F) \leq d \} \\
\text{GA}^d_n(R) & \quad \text{GA}_n(R) \cap \text{MA}^d_n(R) \\
\text{JC}(R, n) & \quad \text{The Jacobian conjecture in characteristic zero} \\
\text{AJC}(R, n) & \quad \text{The Adjamagbo Jacobian conjecture in dimension } n
\end{align*}
This thesis is divided into five chapters. Except for the last chapter we focused on prime characteristic. Let $k$ be a field. Understanding the automorphism group of affine $k$-varieties, in particular the automorphism group $GA_n(k)$ of affine $n$-space $k^n$, is a key problem in algebraic geometry. In order to understand $GA_n(k)$ it turns out to be useful (due to reduction-mod-$p$ techniques) to understand $GA_n(F_q)$, which is an important object in itself. In dimension 2 Jung proved that if $\text{char}(k) = 0$, every polynomial automorphism is tame [Jun42]. Later Van der Kulk [Kul53] generalized this result for all characteristic. More precisely, they proved that $GA_2(k)$ is the amalgamated free product of the set of affine automorphisms $\text{Aff}_2(k)$ and the set of triangular automorphisms $\text{BA}_2(k)$ over their intersection. Since then, many other proofs of this result have been given.

We define $TA_n(R) := \langle \text{BA}_n(R), \text{Aff}_n(R) \rangle$, the tame automorphism group. A highly sought-after question (posed by Nagata in 1974) asked whether $TA_n(k)$ equals $GA_n(k)$ for some $k$ and $n \geq 3$. It took about 30 years till Umirbaev and Shestakov proved that if $\text{char}(k) = 0$ then $TA_3(k) \neq GA_3(k)$ [See; SU04a; SU04b]. The problem is still open in higher dimensions and in characteristic $p$ - the latter being the topic in this thesis (chapter 2). Note that a polynomial map indeed induces a map $k^n \to k^n$. Thus, in general, we have a map from the set of polynomial endomorphisms $MA_n(k)$ to $\text{Maps}(k^n, k^n)$, the set of all maps on $k^n$. This map is injective unless $k$ is a finite field - and it's exactly the latter case we'll be discussing in chapter 2. Thus, we define

$$\pi_{q^m} : MA_n(F_q) \to \text{Maps}(F_{q^m}, F_{q^m})$$

for each $m \geq 1$. For $m = 1$, we write $\pi_q$ instead of $\pi_{q^1}$. In fact, one of the motivations for chapter 2 is in trying to see whether $\pi_{q^m}(TA_n(F_q))$ can be different from $\pi_{q^m}(GA_n(F_q))$, which would imply that the groups are not equal and show the existence of wild maps over $F_q$.

This question is even interesting in case $m = 1$ and $q = 2^l$ in light of the following theorem of Maubach [Mau01]:

**Theorem 0.0.1.** If $n \geq 2$, then $\pi_q(TA_n(F_q)) = \text{Sym}(F_q^n)$ if $q$ is odd or $q = 2$. If $q = 2^l$ where $l \geq 2$ then $\pi_q(TA_n(F_q)) = \text{Alt}(F_q^n)$.

The following question was posed in the same paper:

**Question 0.0.2.** Is there an automorphism $F \in GA_n(F_q)$ where $l \geq 2$ such that $\pi_{q^l}(F)$ is odd?

Such an example would then automatically have to be a non-tame automorphism. The above question, even though getting reasonable attention, is unsettled for more than ten years now. But, then the next step is:

**Question 0.0.3.** Is there an automorphism $F \in GA_n(F_q)$ such that $\pi_{q^m}(F) \notin \pi_{q^m}(TA_n(F_q))$?
We address this question for a large class of candidate wild maps in section 2.3 of Chapter 2.

Another important problem which forms the motivation for much of the research concerning polynomial automorphism is the Jacobian conjecture. It is a quite notorious conjecture in the field of Affine Algebraic Geometry. One formulation is:

\[(JC(R,n)): \text{If } F \in MA_n(R) \text{ where } R \text{ is a domain of characteristic zero, then } \det(\text{Jac}(F)) \in R^* \text{ implies that } F \in GA_n(R).\]

For many details we can refer to the book [Ess00]. The conjecture is open even in the case \(n = 2\) and \(R = \mathbb{C}\) (and trivial in dimension 1). Proving \(JC(R,n)\) for any \(R\) of characteristic zero yields \(JC(R,n)\) true for all domains \(R\) of characteristic zero.

Naively translating the Jacobian Conjecture into characteristic \(p\) yields counterexamples, already in dimension 1: the map \(x - x^p\) is not injective but has \(\det(\text{Jac}(x - x^p)) = 1\). Therefore, Adjamagbo defined in [ADE92] a possible version of the Jacobian Conjecture for fields \(k\) with characteristic \(\text{char}(k) = p\):

\[(AJC(k,n,p)): \text{Let } F = (F_1,\ldots,F_n) \text{ where } F_i \in k[x_1,\ldots,x_n] \text{ and } k \text{ a field of characteristic } p. \text{ Assume that } \det(\text{Jac}(F)) \in k^* \text{ and additionally assume that } p \text{ does not divide } \left[ k(x_1,\ldots,x_n) : k(F_1,\ldots,F_n) \right]. \text{ Then } F \text{ has a polynomial inverse.}\]

The \(\text{char}(k)\) does not divide \(\left[ k(x_1,\ldots,x_n) : k(F_1,\ldots,F_n) \right]\) requirement seems to exclude all pathological counterexamples to the Jacobian Conjecture, but adds another difficult requirement to the (deceptively simple looking but) difficult equation \(\det(\text{Jac}(F)) \in k^*\). Adjamagbo showed that knowing \(AJC(k,n,p)\) for all \(p\) implies \(JC(n,k)\) for all \(k\).

In this thesis (chapter 3) we approach the JC in characteristic \(p\) from a different perspective: let us write down a generic polynomial automorphism of degree 2, having the identity as affine part:

\[F = (x + a_1x^2 + a_2xy + a_3y^2, y + b_1x^2 + b_2xy + b_3y^2)\]

Then, in characteristic zero, the equation \(1 = \det(\text{Jac}(F))\) yields several equations on the coefficients:

\[1 = \det(Jac(F)) = 1 + (2a_1 + b_2)x + (a_2 + 2b_3)y + (2a_1b_2 + 2a_2b_1)x^2 + (2b_2a_3 + 4a_1b_3 + 4a_3b_1)xy + (2a_2b_3 + 2a_3b_2)y^2\]

Then apparently, the equations \(2a_1 + b_2 = 0, a_2 + 2b_3 = 0, \) etc. are exactly the equations one needs to ensure that \(F\) is invertible in characteristic zero. However, in characteristic 2 the above equations are not enough to conclude that \(F\) is invertible (in fact, some equations completely vanish), as the example \((x + x^2, y)\) shows. Therefore, one needs extra equations in characteristic \(p\). In fact, thinking a little deeper, we know that such equations must exist. (Without going into detail, the set of automorphisms of determinant
Jacobian 1 is a subset of $\mathcal{M}^{d\times n}(k)$ which is endowed with a so-called ind-topology, and its closure can be described by equations (see [Sha66; Sha81; Sta12] for details)). We only have to find them. In chapter 3 we claim that we have found them (at least conjecturally). In fact, what we are doing is refining the regular Jacobian Conjecture so that it makes sense in characteristic $p$ also.

We make a remark on Adjamagbo’s formulation w.r.t. the above considerations: note that if there exists at least one counterexample $F$ to the Jacobian Conjecture in characteristic zero, then $[k(x_1, \ldots, x_n) : k(F_1, \ldots, F_n)] = d > 1$. It might very well be that $F \mod p$ is an interesting map for any prime $p$. But, if $p|d$, then Adjamagbo’s formulation excludes this example, while one could argue that a formulation of the JC in characteristic $p$ should not. One could say that in this case $p \pitchfork [k(x_1, \ldots, x_n) : k(F_1, \ldots, F_n)]$ adds too many equations, or perhaps the wrong equations.

Chapter 4 of this thesis is about a counter example to the cancellation problem in characteristic $p$. The cancellation problem was first proposed by Zariski in 1949 at the Paris Colloquium on Algebra and Numbers Theory [Seg50]. Let $k$ be an algebraically closed field. The famous cancellation problem (also known as Zariski Problem) states that “if $V$ is an affine $k$-variety and $A^n_k$ is affine $n$-space over field $k$ such that $V \times A^1_k \cong A^{k+1}_k$, does it follow that $V \cong A^n_k$? Equivalently if $A$ is an affine $k$ algebra and $A^{[1]} \cong k^{[n+1]}$, does it follow that $A^1 \cong k^n$?"

The case $n = 1$ was solved by Abhyankar, Heinzer, and Eakin in 1972 [AHE72]. For $n = 2$, Fujita et al., [Fuj79] and Miyanishi, Sugie, et al., [MS80] provided a positive solution in characteristic zero and Russell [Rus81] solved the case of positive characteristic in 1981. Recently Crachiola and Makar-Limanov presented a simplified algebraic proof for $n = 2$ [CML08]. After Russell’s work in 1981, the cancellation problem for $n \geq 3$ was open for more than three decades.

Asanuma has proved the following theorem [Asa87, Corollary 5.3]

**Theorem 0.0.4.** Let $A = k[w, x, y, z]/(G + w^m z)$ where $m \geq 1$, $G = -x^e + y + y^p s$ and $s$ is a positive integer such that $p^e \nmid sp$ and $sp \nmid p^c$. Then $A$ satisfies

1. $A \otimes k(p) \cong k(p)^{[2]}$ for each prime ideal $p \subseteq k[w]$,
2. $A^{[1]} \cong k[w]^{[3]}$.

He envisaged $A$ as a candidate the counter-example to the cancellation problem for the affine 3-space $A^3_k$ in characteristic $p$ [Asa94, Remark 2.3]. In [Gup14a], Gupta proved this result. She showed that the threefold $k[X, Y, Z, T]/(X^m Y + Z^{p^e} + T + T^{sp})$, where $m, e, s$ are positive integers such that $sp \nmid p^e$ and $p^e \nmid sp$ is not isomorphic to $k^{[3]}$ for $m \geq 2$. Thus she proved that when $\text{char}(k) = p > 0$, the cancellation problem does not hold for affine 3-space $A^3_k$. Later in [Gup14c], Gupta showed that affine $n$-space is not cancellative for any $n \geq 3$. The cancellation problem is still open for dimensions $n \geq 3$ in characteristic zero.

In this thesis we unite both the Gupta and Asanuma result for the counter example to cancellation for affine 3-space in one result. When we did this work, we were unaware of Gupta’s paper [Gup14b] in which she already did this work. However we present a different proof in this thesis.
Chapter 5 of this thesis is about the surjectivity of quotient maps of special automorphism groups. Let $A$ be a Noetherian commutative ring containing $\mathbb{Q}$ and $a$ is ideal in $A$. We define $SA_n(A) := \{ F \in GA_n(A) | \det Jac(F) = 1 \}$. In 2007, Essen, Vénéreau and Maubach proved the following theorem [VDEMV07].

**Theorem 0.0.5.** Let $R$ be a ring containing $\mathbb{Q}$, $m$ a positive integer. Then the map

$$SA_n(R[x]) \rightarrow SA_n(R[x]/(x^m))$$

is surjective.

This result is worthy of a short discussion. This seemingly innocuous result had at least 3 strong consequences: (1) in the paper [VDEMV07] itself it was used to prove for certain rings $R, S$ that if $f \in R^{[n]}$ is a coordinate in $S^{[n]}$, then it is a coordinate in $R^{[m]}$ (we will not elaborate on this), (2) it was used in the paper [DMJP14] to give smooth contractible counterexamples to the generalized cancellation problem, (3) and in the paper [BVDEW12] it was used to show stable tameness of elements in $GA_2(R)$ for some rings $R$. We define $\pi : GA_n(A) \rightarrow GA_n(A/a)$ and $\sqrt{\pi} : GA_n(A) \rightarrow GA_n(A/\sqrt{a})$ where $\sqrt{a}$ is the radical of $a$. For any element $f$ having coefficients in $A/a$ or $A$ we write $\tilde{f}$ for its image in $A/\sqrt{a}$. In the chapter 5 of this thesis we extend theorem 0.0.5. We prove that if $f \in SA_n(A/a)$ then $\tilde{f} \in \sqrt{\pi}(SA_n(A))$ is equivalent to $f \in \pi(SA_n(A))$. If we choose $a = (t^m)$ and $A = R[t]$ we can see theorem 0.0.5 as its special case. Moreover we prove proposition 5.3.2 which shows that under some assumptions the map $GA_n(k) \rightarrow Aut_k(k^{[n]}/a)$ is surjective, where $a \subset k^{[n]}$ is such that $\sqrt{a}$ is maximal ideal.

**Brief description of each chapter**

**Chapter 1:** This chapter contains definitions, notations and some preliminary results used in this thesis. In the end of this chapter we present some famous conjectures.

**Chapter 2:** In this chapter we first show that a large class of potentially non-tame maps in $GA_n(\mathbb{F}_q)$ are inside the profinite tame group $\hat{TA}_n(\mathbb{F}_q)$ (i.e. are “profinitely tame”). Then we analyze the group of invertible elements in $\hat{MA}_n(\mathbb{F}_q)$, as this is the “world” in which $\hat{GA}_n(\mathbb{F}_q)$ and $\hat{TA}_n(\mathbb{F}_q)$ live in. In sections 2.5,2.6,2.7, we study the “distance” between $\hat{TA}_n(\mathbb{F}_q)$ and $\hat{GA}_n(\mathbb{F}_q)$. Here, section 2.5 (the main bulk) is an unavoidably technical and tricky proof of a bound between $\pi_q^m(\hat{TA}_n(\mathbb{F}_q))$ and $\pi_q^m(\hat{MA}_n(\mathbb{F}_q)) \cap \text{Perm}(\mathbb{F}_q^m)^\sim)$. This bound is made explicit in section 2.7. In section 2.6 we give some examples where we compute the actual size of $\pi_q^m(\hat{TA}_n(\mathbb{F}_q))$ for some specific $q, m$. The work present in chapter 2 has been published in the Journal of Pure and Applied Algebra [MR15b].

**Chapter 3:** In this chapter we mainly give a new formulation of the Jacobian conjecture (denoted by $JC$). We do some explicit examples in order to point out that $JC$ might do what it claims. We show that this new formulation of the Jacobian conjecture coincides with the regular formulation in case the field is of characteristic zero. We also present two surjectivity conjectures. We use them to conjecturally prove various basic properties of $JC$. This work has been accepted as a publication in the Colloquium Mathematicum Journal and is present as a preprint in arxiv.org [MR15a].

**Chapter 4:** This chapter is in two parts. In the first part we define a threefold $A$ and prove that $A \neq k^{[3]}$. In the second part we prove that with
some restrictions $A^{[1]}$ is isomorphic to $k^{[4]}$. This provides a counter example to the cancellation problem in characteristic $p$. This work is based on the work of Asanuma, L. Makar-Limanov, A. Crachiola and Gupta.

**Chapter 5:** In this chapter we mainly prove two results: Theorem 5.2.2 and Proposition 5.3.2. Theorem 5.2.2 relates $\sqrt{\pi}(SA_n(A))$ with $\pi(SA_n(A))$, while proposition 5.3.2 provides a partial answer to the following question:

Let $\varphi \in Aut_k(k^{[n]}/a)$ be such that $\varphi \mod \sqrt{a} \in \sqrt{\pi}(Aut_k(k^{[n]}; \sqrt{a}))$ where $a$ is an ideal in $k^{[n]}$. Under what conditions is $\phi \in \pi(Aut_k(k^{[n]}; a))$?
Chapter 1

Preliminaries

1.1 Definitions and Notations

In this section we will list some basic definitions and notations used in this thesis. We will write definitions in bold text. Given any commutative ring $R$ and finitely many variables, say $X_1,\ldots,X_n$, we write $R[X_1,\ldots,X_n]$ for the polynomial ring in these variables, with coefficients in $R$. Often, we will use other notations $R[X]$ or $R^{[n]}$ for the ring $R[X_1,\ldots,X_n]$. Small letters however, used in this context, always represent just one variable. For example $R[x] = R[1]$ and $R[x, y] = R[2]$.

Polynomial mappings

We define a polynomial map by $F := (F_1,\ldots,F_m)$, where each $F_i \in R[X_1,\ldots,X_n]$. If $m = n$ then $F$ is called a polynomial endomorphism. The set of all polynomial endomorphisms is denoted by $\text{MA}_n(R)$. This set is a (noncommutative) ring under usual componentwise addition and as multiplication, the composition of maps, i.e.,

$$F \circ G = (F_1(G_1,\ldots,G_n),\ldots,F_n(G_1,\ldots,G_n))$$

where $G = (G_1,\ldots,G_n) \in \text{MA}_n(R)$. Any polynomial map $F \in \text{MA}_n(R)$ induces a map $R^n \rightarrow R^n$ given by

$$(a_1,\ldots,a_n) \rightarrow (F_1(a_1,\ldots,a_n),\ldots,F_n(a_1,\ldots,a_n)).$$

This induces a map $\text{MA}_n(R) \rightarrow \text{Maps}(R^n, R^n)$. In general this map need not be injective. For as a polynomial map $F := (X^p - X, Y^p - Y) \in \text{MA}_2(F_p)$ is not zero but its induced map in $\text{Maps}(F_p^2, F_p^2)$ is the zero map. However if $R$ is infinite then this map is injective. In this case the formal distinction between polynomials maps and the induced polynomial maps may be ignored.

A polynomial map $F = (F_1,\ldots,F_n)$ is said to invertible over $R$ if $R[X] = R[F_1,\ldots,F_n]$. In other words, if there exists $G_1,\ldots,G_n \in R[X]$ such that $X_i = G_i(F_1,\ldots,F_n)$ for $1 \leq i \leq n$. If $F \in R[X]^n$ is invertible then $G = (G_1,G_2,\ldots,G_n) \in R[X]^n$ in the above definition is unique and satisfies $F \circ G = X$ (proposition 1.1.6 in [Ess00]). Invertible polynomial maps are in one to one correspondence with $R$-automorphisms of the polynomial ring $R[X]$ via the map

$$F \mapsto F^*$$

where

$$F^* : h \mapsto h(F_1,\ldots,F_n).$$
The set of all invertible elements in $\text{MA}_n(R)$ is denoted by $\text{GA}_n(R)$ or $\text{Aut}_R(R[X])$ and is the group of polynomial automorphisms. This group may be viewed as an infinite dimensional algebraic group over $R$ [Kam79]. There are a few obvious groups of polynomial automorphisms:

1. The set of affine automorphisms is $\{F \in \text{GA}_n(R) \mid \deg(F) = 1\}$ where we define $\deg(F) = \max(\deg(F_1), \ldots, \deg(F_n))$ for $F \in \text{MA}_n(R)$. The set of these maps forms a group, denoted by $\text{Aff}_n(R)$.

2. A polynomial map $F \in \text{MA}_n(R)$ is triangular or Jonquières if $F_i \in R[X_1, \ldots, X_n]$. If $F$ is a triangular automorphism and $R$ is a domain, it turns out to be of the form $(r_1X_1 + f_1, \ldots, r_nX_n + f_n)$ where $r_i \in R^*$, $f_j \in R[X_{j+1}, \ldots, X_n]$. The set of these maps also forms a group, denoted by $\text{BA}_n(R)$. The set of all triangular maps such that $a_{ii} = 1$ for $1 \leq i \leq n$ is called the set of strictly triangular polynomial maps, and is a subgroup of $\text{BA}_n(R)$, denoted by $\text{BA}_n(R)$.

It is now natural to define the set of tame automorphisms, chief subgroup of $\text{GA}_n(R)$ generated by the triangular and affine maps $\text{TA}_n(R) := < \text{BA}_n(R), \text{Aff}_n(R) >$. A polynomial automorphism which is not a tame automorphism is called a wild automorphism. An automorphism $F \in \text{GA}_n(R)$ is said to be stably tame if there exist $m \in \mathbb{N}$ and new variables $X_{n+1}, \ldots, X_{n+m}$ such that the extended map $(F, X_{n+1}, \ldots, X_{n+m})$ is tame, i.e. $(F, X_{n+1}, \ldots, X_{n+m}) \in \text{TA}_n+m(R)$. If we split a polynomial automorphism $F$ by $F = G + H$ such that $\deg(G) \leq 1$, then $G$ is called the affine part of an automorphism. For more details about polynomial automorphisms see, [Ess00].

**Profinite group**

A partially ordered set $I$ is said to be directed if given any $i_1, i_2 \in I$, there exist $i_3 \in I$ such that $i_1 \leq i_3$ and $i_2 \leq i_3$. An inverse system of groups over a directed set $I$, consists of collection $\{G_i \mid i \in I\}$ of groups indexed by $I$, and a collection of homomorphisms $f_{i_2}^{i_1} : G_{i_2} \rightarrow G_{i_1}$ defined whenever $i_2 \geq i_1$. These homomorphisms must satisfy the conditions that $f_{i_1}^{i_1} = \text{id}$ for all $i \in I$, and for any $i_1 \leq i_2 \leq i_3$, we have $f_{i_3}^{i_2} \circ f_{i_2}^{i_1} = f_{i_3}^{i_1}$. Given an inverse system $(G_i, f_{i_2}^{i_1}, I)$ of groups, we define the inverse limit $\lim_{\leftarrow i \in I} G_i$ as a subgroup of the direct product of $G_i$’s

$$\lim_{\leftarrow i \in I} G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid g_i = f_{i_j}^{i_i}(g_j) \text{ for all } i \leq j \text{ in } I\}.$$

A topological group is a set $G$ which has both the structure of a group and of a topological space, such that the group’s binary operation $G \times G \rightarrow G$ and the group’s inverse map $G \rightarrow G$ are continuous maps with respect to the topology on $G$. A profinite group is a topological group which is obtained as the inverse limit of a collection of finite groups, each given the discrete topology. For more information about profinite groups, see, [RZ00].

**Example 1.1.1.** The group of $p$-adic integers

$$\mathbb{Z}_p = \{a_0 + a_1p + a_2p^2 + \ldots | a_i \in \mathbb{Z}, 0 \leq a_i \leq p - 1\}$$
under addition is profinite. It is the inverse limit of the inverse system consisting of the finite groups \( \mathbb{Z}/p^m\mathbb{Z}, m \in \mathbb{N} \) and the natural maps \( \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} (m \geq n) \). Thus

\[
\mathbb{Z}_p = \lim_{\substack{\text{m} \to \infty \\ \text{m} \in \mathbb{N}}} \mathbb{Z}/p^m\mathbb{Z} = \{(\alpha_m)_{m \in \mathbb{N}} \in \prod_{m \in \mathbb{N}} \mathbb{Z}/p^m\mathbb{Z} : \forall m \geq n, \alpha_m \mod p^n = \alpha_n, \}
\]

Example 1.1.2. Let \( p \) be the characteristic of a finite field \( F_q \) with \( q \) elements. It is clear that the algebraic closure \( \overline{\mathbb{F}}_q \) of \( \mathbb{F}_q \) is the same as \( \overline{\mathbb{F}}_p \). The algebraic closure of \( \mathbb{F}_q \) is the union \( \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n} \). Consider the family of Galois groups \( \text{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q) \) of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \) for each \( n \in \mathbb{N} \). For \( m, n \in \mathbb{N} \), let \( m \leq n \) if and only if \( m \) divides \( n \). For each pair \((m, n) \in \mathbb{N}^2 \) with \( m \mid n \), define the homomorphism \( f_{m,n}^n : \text{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q) \to \text{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q) \) by \( \theta_n \mapsto \theta_n|_{\mathbb{F}_{q^m}} \), where \( \theta_n|_{\mathbb{F}_{q^m}} \) is the restriction of \( \theta_n \) to \( \mathbb{F}_{q^m} \). In this way we get an inverse system \( (\text{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q), f_{m,n}, \mathbb{N}) \) of the finite Galois groups and one can verify that

\[
\text{Gal}(\overline{\mathbb{F}}_q : \mathbb{F}_q) = \lim_{\substack{\text{m} \to \infty \\ \text{m} \in \mathbb{N}}} \text{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q) := \{(\theta_m)_{m \in \mathbb{N}} \in \prod_{m \in \mathbb{N}} \text{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q) : \theta_m = f_{m,n}(\theta_n) \forall m \leq n \text{ in } \mathbb{N}\}.
\]

Degree function

Let \( k \) be a field and \( A \) be a commutative \( k \)-domain. A degree function on \( A \) is a map \( \text{deg} : A \to \mathbb{Z} \cup \{\infty\} \) which satisfies the following three properties for all \( a, b \in A \)

1. \( \text{deg}(a) = -\infty \iff a = 0 \).
2. \( \text{deg}(ab) = \text{deg}(a) + \text{deg}(b) \).
3. \( \text{deg}(a + b) \leq \max\{\text{deg}(a), \text{deg}(b)\} \).

The graded ring associated to a filtration

Let \( A \) be a commutative \( k \)-domain. \( A \) is said to have a \( \mathbb{Z} \)-filtration if there exists a collection of \( k \)-linear subspaces \( \{A_n\}_{n \in \mathbb{Z}} \) of \( A \) satisfying

1. \( A_n \subseteq A_m \) for \( n \leq m \in \mathbb{Z} \),
2. \( A = \bigcup_{n \in \mathbb{Z}} A_n \),
3. \( A_n A_m \subseteq A_{n+m} \) for all \( m, n \in \mathbb{Z} \).

By a proper \( \mathbb{Z} \)-filtration on \( A \) we mean a \( \mathbb{Z} \)-filtration on \( A \) with the following two properties,

- \( 0 = \bigcap_{n \in \mathbb{Z}} A_n \),
- \( (A_n \setminus A_{n-1})(A_m \setminus A_{m-1}) \subseteq A_{n+m} \setminus A_{n+m-1} \) for all \( n, m \in \mathbb{Z} \).

Any proper \( \mathbb{Z} \)-filtration on \( A \) determines the following \( \mathbb{Z} \)-graded integral domain

\[
\text{gr}(A) := \bigoplus_i A_i/A_{i-1}.
\]
Consider $a + A_{n-1} \in A_n/A_{n-1}$, and $b + A_{m-1} \in A_m/A_{m-1}$, where $a \in A_n$, $b \in A_m$. Then multiplication is defined by

$$(a + A_{n-1})(b + A_{m-1}) = ab + A_{n+m-1},$$

where $ab + A_{n+m-1} \in A_{n+m}/A_{n+m-1}$. Multiplication is extended to all of $gr(A)$ by the distribution law.

**Example 1.1.3.**  
- Let $B = k[x, x^{-1}]$, a Laurent polynomial ring over $k$, and let $A_n$ consist of the Laurent polynomials of degree at most $n$ ($n \in \mathbb{Z}$). Then $k[x, x^{-1}] = \bigcup_{n \in \mathbb{Z}} A_n$ is a $\mathbb{Z}$-filtration and $gr(k[x, x^{-1}]) = \oplus_{n \in \mathbb{Z}} kx^n \cong k[x, x^{-1}]$.

- The natural $\mathbb{Z}$-grading by degree on $k[x]$ yields $gr(k[x]) = \bigoplus_{n \geq 0} kx^n \cong k[x]$.

- The $\mathbb{Z}$-degree grading $k[x, y]$ yields $gr(k[x, y]) = \bigoplus_{m \geq 0} \bigoplus_{i+j=m} kx^iy^j \cong k[x, y]$.

There exists a map $\rho : A \to gr(A)$ defined by $\rho(a) = a + A_{n-1}$, if $a \in A_n \setminus A_{n-1}$.

We shall call a proper $\mathbb{Z}$-filtration $\{A_n\}_{n \in \mathbb{Z}}$ of $A$ admissible if there exists a finite generating set $\Gamma$ of $A$ such that, for any $n \in \mathbb{Z}$ and $a \in A_n$, $a$ can be written as a finite sum of monomials in elements of $\Gamma$ and each of these monomials is an element of $A_n$.

**Remark 1.1.4.**  
1. Note that $\rho$ is not a ring homomorphism. If $i < n$ and $a_1, a_2, \ldots, a_r \in A_n \setminus A_{n-1}$ such that $a_1 + a_2 + \cdots + a_r \in A_i \setminus A_{i-1}(\subset A_{n-1})$, then $\rho(a_1 + a_2 + \cdots + a_r) = a_1 + a_2 + \cdots + a_r + A_{i-1} \neq 0$ but $\rho(a_1) + \cdots + \rho(a_r) = a_1 + a_2 + \cdots + a_r + A_{n-1} = 0$ in $gr(A)$.

2. Suppose $A$ has a proper $\mathbb{Z}$-filtration and a finite generating set $\Gamma$ which makes the filtration admissible. Then $gr(A)$ is generated by $\rho(\Gamma)$, since if $a_1, \ldots, a_r \in A_n \setminus A_{n-1}$, then $\rho(a_1 + a_2 + \cdots + a_r) = \rho(a_1) + \cdots + \rho(a_r)$ and $\rho(ab) = \rho(a)\rho(b)$ for any $a, b \in A$.

3. Suppose that $A$ has $\mathbb{Z}$-graded algebra structure, say $A = \bigoplus_{i \in \mathbb{Z}} C_i$. Then there exists a proper $\mathbb{Z}$-filtration $\{A_n\}_{n \in \mathbb{Z}}$ on $A$ defined by $A_n := \bigoplus_{i \leq n} C_i$. Moreover, $gr(A) = \bigoplus_{n \in \mathbb{Z}} A_n/A_{n-1} \cong \bigoplus_{n \in \mathbb{Z}} C_n = A$ and, for any element $a \in A$, the image of $\rho(a)$ under the isomorphism $gr(A) \to A$ is the homogeneous component of $a$ in $A$ of maximum degree. If $A$ is a finitely generated $k$-algebra, then the above filtration on $A$ is admissible.

**Locally Nilpotent Derivations**

Let $A$ be a $R$-algebra, where $R$ is any commutative ring. A derivation $D$ on $A$ is a function $D : A \to A$ which satisfies the following two conditions:

For all $a, b \in A$,

- $D(a + b) = D(a) + D(b)$
- $D(ab) = D(a)b + aD(b)$
for all \( a, b \in A \). If \( D(r) = 0 \) for all \( r \in R, D \) is called an \( R \)-derivation. The **kernel of a derivation** is a subring of \( A \), denoted by \( A^D \). All derivations on the polynomial ring \( R[X_1, \ldots, X_n] \) are of the form \( f_1 \frac{\partial}{\partial X_1} + \cdots + f_n \frac{\partial}{\partial X_n} \), where \( f_i \in R[X_1, \ldots, X_n] \) for \( 1 \leq i \leq n \).

Let \( A = k[X_1, \ldots, X_n], \) where \( k \) is a field. Given a weight \( w = (w_1, \ldots, w_n) \in \mathbb{Z}^n \), ring \( A \) is naturally \( \mathbb{Z} \)-graded by \( A = \oplus_{i \in \mathbb{Z}} A_i \), where \( A_i \) is the \( k \)-vector space generated by the monomials \( X_1^{a_1} \cdots X_n^{a_n} \) with \( a_1 w_1 + \cdots + a_n w_n = i \). The next proposition describes the homogeneous decomposition of a given derivation \( D \) on \( A \) relative to a \( \mathbb{Z} \)-grading of the polynomial ring \( k[X_1, \ldots, X_n] \).

**Proposition 1.1.5.** (Prop. 3.4 in [Fre06]) Let \( 0 \neq w \in \mathbb{Z}^n \) be given and consider on \( A = k[X_1, \ldots, X_n] \) the \( w \)-grading. Let \( D \) be nonzero derivation on \( A \). Then every derivation \( D \) on the polynomial ring \( A = k[X_1, \ldots, X_n] \) admits a unique finite decomposition \( D = \sum_j D_j \) such that \( D_j(A_i) \subset A_{i+j} \) for all \( i, j \in \mathbb{Z} \).

A derivation \( D \) is said to be **locally nilpotent** if and only if for each \( a \in A \) there exists a positive integer \( n \) such \( D^n(a) = 0 \). The set of all locally nilpotent derivations on \( A \) is denoted by \( \text{LND}(A) \). For each \( i = 1, \ldots, n \), the derivation \( \frac{\partial}{\partial X_i} \) is a locally nilpotent on \( R[X_1, \ldots, X_n] \) with kernel \( R[X_1, \ldots, X_i, \ldots, X_n] \).

The following lemma shows that if a locally nilpotent derivation \( D \) admits a finite decomposition on a \( \mathbb{Z} \)-graded ring \( A \) then the homogeneous lowest and highest degree derivations in the decomposition are also locally nilpotent. We will use the following lemma and the proposition 1.1.5 in the proof of example 5.2.11

**Lemma 1.1.6.** (Principle 14 in [Fre06]) Suppose \( A \) be a \( \mathbb{Z} \) graded ring \( A = \oplus_{i \in \mathbb{Z}} A_i \), and let \( D \in \text{LND}(A) \) be given. Suppose that for integers \( m \leq n, D \) admits the decomposition \( D = \sum_{m \leq i \leq n} D_i \), where each \( D_i \in \text{Der}_k(A) \) is homogeneous of degree \( i \) relative to this grading, and where \( D_m \neq 0 \) and \( D_n \neq 0 \). Then \( D_m, D_n \in \text{LND}(A) \).

To check if a given derivation is locally nilpotent, the following proposition is quite useful.

**Proposition 1.1.7.** (Prop. 1.3.16 in [Ess00]) Let \( A \) be generated as an \( R \) algebra by some set \( G \), and \( D \) an \( R \)-derivation on \( A \). Then \( D \) is locally nilpotent derivation if and only if for every \( g \in G \) there exist an \( n \in \mathbb{N} \) with \( D^n(g) = 0 \).

As an example, we can use the above proposition to show that every triangular derivation on \( R[X] \) i.e. the derivation of the form

\[ D = \alpha_1(X_2, \ldots, X_n) \frac{\partial}{\partial X_1} + \cdots + \alpha_{n-1}(X_n) \frac{\partial}{\partial X_{n-1}} + \alpha_n \frac{\partial}{\partial X_n} \]

where \( \alpha_i \in R[X_{i+1}, \ldots, X_n] \) for all \( 1 \leq i \leq n-1 \) and \( \alpha_n \in R, \) is locally nilpotent.

Another useful result is corollary 1.3.34 in [Ess00]. It states

**Lemma 1.1.8.** Let \( 0 \neq D \) be any derivation on \( A \) and \( 0 \neq f \in A \). Then \( fD \) is locally nilpotent if and only if \( D \) is locally nilpotent and \( f \in A^D \).

Consider a \( \mathbb{Q} \)-algebra \( A \). Given \( D \in \text{LND}(A) \), we define the **exponential map** \( \exp(D) : A \rightarrow A \) by \( \exp(D)(f) = \sum_{n \geq 0} \frac{1}{n!} D^n(f) \) for all \( f \in A \). The sum is finite since \( D \in \text{LND}(A) \). We have the following proposition (principle 10 in [Fre06]).
Proposition 1.1.9. Let $D \in \text{LND}(A)$ then

1. $\exp(D)$ is an automorphism of the $\mathbb{Q}$-algebra $A$.

2. If $D$ and $D_0$ commutes for some $D_0 \in \text{LND}(A)$, then $D + D_0 \in \text{LND}(A)$ and $\exp(D + D_0) = \exp(D) \circ \exp(D_0)$. In particular $\exp(D)$ and $\exp(D_0)$ commute.

Here we do some instructive examples as an application of proposition 1.1.9(1). Let $A = R[X]$, where $R$ is any commutative $\mathbb{Q}$-algebra.

Example 1.1.10. 1. Let $f \in R[X_1, \ldots, X_i, \ldots, X_n]$ and $D = f \frac{\partial}{\partial X_i}$ a derivation on polynomial ring $R[X]$ for $1 \leq i \leq n$. By 1.1.7,1.1.8, $D \in \text{LND}(A)$. Also $\exp(D)(X_j) = X_j$, if $j \neq i$ and $\exp(D)(X_i) = X_i + f$. So $\exp(D) = (X_1, \ldots, X_{i-1}, X_i + f, X_{i+1}, \ldots, X_n)$, i.e. all elementary maps are polynomial automorphisms.

2. Consider the triangular derivation $D = -2X_1 \frac{\partial}{\partial X_1} + X_3 \frac{\partial}{\partial X_2}$ on $A := R[X_1, X_2, X_3]$. Then $D \in \text{LND}(A)$. If $\alpha := X_1X_3 + X_3^2$, then $D(\alpha) = 0$ and so by 1.1.8, $D_1 = \alpha D \in \text{LND}(A)$. Moreover we can verify that $D_1X_1 = -2\alpha X_2, D_1^2X_1 = -2\alpha^2X_3, D_1D_2X_1 = 0, D_1X_2 = \alpha X_3, D_2X_2 = D_1X_3 = 0$. Thus we get

$$\exp(\alpha D)(X_1, X_2, X_3) = (X_1 - 2\alpha X_2 - \alpha^2 X_3, X_2 + \alpha X_3, X_3),$$

which is the Nagata example. Hence proposition 1.1.9 verifies that the Nagata map is an automorphism of $R[X_1, X_2, X_3]$.

Exponential maps, the AK invariant, locally iterative higher derivations

Let $k$ be a field of any characteristic. Let $A$ be a commutative $k$-algebra and let $\phi : A \rightarrow A[1]$ be a $k$-algebra homomorphism. We write $\phi = \phi_U : A \rightarrow A[U]$ to emphasize an indeterminate $U$. We say that $\phi$ is an exponential map on $A$ if it satisfies the following properties

1. $\epsilon_0 \phi_U$ is the identity on $A$, where $\epsilon_0 : A[U] \rightarrow A$ is the evaluation at $U = 0$.

2. $\phi_V \phi_U = \phi_{V+U}$, where $\phi_V : A \rightarrow A[V]$ is extended to a homomorphism $\phi_V : A[U] \rightarrow [U, V]$ by setting $\phi_V(U) = U$.

Let $\text{EXP}(A)$ denote the set of all exponential maps on $A$.

Define a subring of $A$ by $A^\phi = \{ a \in A | \phi(a) = a \}$. $A^\phi$ is called the ring of $\phi$-invariants of an exponential map $\phi$ on $A$. We define the AK invariant, or the ring of absolute constants of $A$, as

$$AK(A) = \bigcap_{\phi \in \text{EXP}(A)} A^\phi.$$

Remark 1.1.11. 1. $AK(A) = A$ if and only if $\phi(A) = A$ for all $\phi \in \text{EXP}(A)$.

2. $AK(A)$ is a subalgebra of $A$ which is preserved by isomorphism. Indeed, any isomorphism $f : A \rightarrow B$ of $k$-algebras restricts to an isomorphism $f : AK(A) \rightarrow AK(B)$. To understand this, observe that if $\phi \in \text{EXP}(A)$, then $f \phi f^{-1} \in \text{EXP}(B)$. 
3. $AK(k^{[n]}) = AK(k[X_1, X_2, \ldots, X_n]) = k$ for all $n \geq 1$. Since for each $i \in \{1, 2, \ldots, n\}$ we have the exponential map $\phi_i(X_1, X_2, \ldots, X_n) = (X_1, X_2, \ldots, X_i+U, \ldots, X_n)$ such that $(k^{[n]})^\phi = K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. When $n = 1$, this characterizes $k^{[1]}$ (see lemma 4.2.2).

4. If $A$ is a domain with transcendence degree $n \geq 2$ over $k$ then $AK(A) = k$ does not imply that $A = k^{[n]}$ [BML01].

It is often helpful to view a given $\phi \in \text{EXP}(A)$ as a sequence in the following way. For $n \in \mathbb{N}$, define $D^n : A \rightarrow A$ by setting $D^n(a)$ equal to the $U^n$-coefficient of $\phi(a)$ and let $D = \{D^0, D^1, D^2, \ldots\}$. To say that $\phi$ is a $k$-algebra homomorphism is equivalent to saying that the sequence $\{D^i(a)\}$ has finitely many nonzero elements for each $a \in A$, that $D^n$ is $k$-linear for each natural number $n$, and that the Leibniz rule $D^n(ab) = \sum_{i+j=n} D^i(a)D^j(b)$ holds for all natural numbers $n$ and all $a, b \in A$. The above properties (1) and (2) of the exponential map $\phi$ translate into the following properties of $D$:

1. $D^0$ is the identity map.
2. (iterative property) For all natural numbers $i, j$,
   \[ D^i D^j = \binom{i+j}{i} D^{i+j} \]

Due to all of these properties, the collection $D$ is called a **locally finite iterative higher derivation** on $A$. More generally, a higher derivation on $A$ is a collection $D = \{D^i\}$ of $k$-linear maps on $A$ such that $D^0$ is the identity and the above Leibniz rule holds. The notion of higher derivation is due to [Has37]. When the characteristic of $A$ is zero, each $D^i$ is determined by $D^1$, which is a locally nilpotent derivation on $A$. In this case, $\phi = \exp(U D^1) = \sum_i \frac{1}{i!} (U D^1)^i$ and $A^\phi$ is the kernel of $D^1$.

The above discussion of exponential maps, locally finite iterative higher derivations, and the AK invariant makes sense more generally for any (not necessarily commutative) ring. However, we will not need this generality. Most of the part about exponential maps presented above can be seen in [Cra06]; [Gup14a].

### 1.2 Some conjectures

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

#### 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, and some ingenious proofs with small errors but still wrong.
Let $R$ be commutative ring. It is well known that if $F \in R[X]^n$ is an invertible over $R$ then $\det \text{Jac}(F)$ is unit in $R[X]$, where

$$\text{Jac}(F) = \begin{pmatrix}
\frac{\partial F_1}{\partial X_1} & \frac{\partial F_1}{\partial X_2} & \cdots & \frac{\partial F_1}{\partial X_n} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{\partial F_n}{\partial X_1} & \frac{\partial F_n}{\partial X_2} & \cdots & \frac{\partial F_n}{\partial X_n}
\end{pmatrix}$$

is Jacobian matrix. The famous Jacobian conjecture states that the converse is also true, i.e.,

**The Jacobian conjecture: JC(R,n)** Let $R$ be a commutative $\mathbb{Q}$-algebra and $F \in R[X]^n$. If $\det \text{Jac}(F) \in R[X]^*$, then $F$ is invertible over $R$.

Thus the Jacobian conjecture, if affirmatively answered, would give a rather easy test of invertibility for a polynomial mapping.

As observed in the introduction, the Jacobian conjecture JC(R,n) is false in characteristic $p > 0$ due to the example $F = x^p - x$. However in this case $[F_p(x) : F_p(F)] = p$, so in particular $p$ divides $[F_p(x) : F_p(F)]$. This and other considerations led Adjamagbo to the following formulation of the Jacobian conjecture in characteristic $p > 0$.

**Adjamagbo Jacobian Conjecture: AJC(k,n,p)** Let $F \in \text{MA}_n(k)$ where $k$ is a field of characteristic $p$. If $\det \text{Jac}(F) \in k^*$ and $p$ does not divide $[k(X) : k(F)]$, then $F$ has polynomial inverse.

**The Cancellation Conjecture**

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

**The cancellation conjecture (algebraic formulation):** Let $R$ be a ring such that $R[T] \cong C^{[n+1]}$ for some $n \geq 3$. Then $R \cong C^{[n]}$.

For more information on these conjectures, see [Ess00].
Chapter 2

The profinite polynomial automorphism group

2.1 Introduction

In this chapter we introduce an extension of the (tame) polynomial automorphism group over finite fields: the profinite (tame) polynomial automorphism group, which is obtained by putting a natural topology on the automorphism group. We show that most known candidate non-tame automorphisms are inside the profinite tame polynomial automorphism group, giving another result suggesting that tame maps are potentially “dense” inside the set of automorphisms. We study the profinite tame automorphism group and show that it is not far from the set of bijections obtained by endomorphisms.

The notation \( (X_1, \ldots, \hat{X}_i, \ldots, X_n) \) means that we skip the \( i \)-th entry. Throughout \( q \) will denote a power of a prime integer.

2.2 Profinite endomorphisms

Let \( k \) be a field and \( \text{MA}_n(k) \) be the collection of polynomial maps over \( k \). Since each polynomial map induces a map \( k^n \to k^n \), thus we define

\[
\pi_q^m : \text{MA}_n(F_q) \to \text{Maps}(F_{q^m}^n, F_{q^m}^n).
\]

For \( m = 1 \) we denote this map by \( \pi_q \) instead of \( \pi_q^1 \). The map \( \pi_q^m \) is not injective. However it is not that hard to see that \( \pi_q(\text{MA}_n(F_q)) = \text{Maps}(F_q^n, F_q^n) \), i.e. that \( \pi_q \) is surjective. It becomes interesting if one wants to study \( \pi_q^m(\text{MA}_n(F_q)) \), as this will not be equal to \( \text{Maps}(F_{q^m}^n, F_{q^m}^n) \). In order to understand this, let us define the group action

\[
\text{Gal}(F_{q^m} : F_q) \times (F_{q^m})^n \to (F_{q^m})^n
\]

by

\[
\phi \cdot (a_1, \ldots, a_n) = (\phi(a_1), \ldots, \phi(a_n)).
\]

If \( \alpha \in (F_{q^m})^n \), we will denote by \([\alpha]\) the orbit \( \text{Gal}(F_{q^m} : F_q)\alpha \). It is clear that if \( F \in \text{MA}_n(F_q) \), then \( \phi \pi_q^m(F) = \pi_q^m \phi(F) \). With a little effort one can show that this is the only constraint:

**Proposition 2.2.1.**

\[
\pi_q^m(\text{MA}_n(F_q)) = \{ \sigma \in \text{Maps}(F_{q^m}^n, F_{q^m}^n) \mid \sigma \phi = \phi \sigma \forall \phi \in \text{Gal}(F_{q^m} : F_q) \}.
\]
Let \( \phi \in \text{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q) \) be the generator. We define the order of \( \alpha \in (\mathbb{F}_{q^m})^* \) under \( \phi \) to be the least positive integer \( a \) such that \( \phi^a(\alpha) = \alpha \).

The above proposition can be easily proved by the following lemma:

**Lemma 2.2.2.**

1. For every \( \alpha \in (\mathbb{F}_{q^m})^* \) there exists \( f_{\alpha,1} \in \mathbb{F}_q[Y_1, \ldots, Y_e] \) such that \( f_{\alpha,1}(\beta) = 0 \) if \([\beta] \neq [\alpha]\) and \( f_{\alpha,1}(\beta) = 1 \) if \([\beta] = [\alpha]\).

2. In case \( \mathbb{F}_q[\alpha] = \mathbb{F}_{q^m} \), then for every \( b \in \mathbb{F}_{q^m} \) there exists \( f_{\alpha,b} \in \mathbb{F}_q[Y_1, \ldots, Y_e] \) such that \( f_{\alpha,b}(\beta) = 0 \) if \([\beta] \neq [\alpha]\) and \( f_{\alpha,b}(\beta) = b \) if \( \beta = \alpha \).

**Proof.** It is trivial that there exists a polynomial \( g_{\alpha,1} \in \mathbb{F}_{q^m}[Y_1, \ldots, Y_e] \) such that \( g_{\alpha,1}(\beta) = 0 \) unless \( \beta = \alpha \), when it is 1. Defining

\[
    f_{\alpha,1} = \prod_{\sigma \in \text{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q)} \sigma(g_{\alpha,1})
\]

we see that \( f_{\alpha,1} \in \mathbb{F}_q[Y_1, \ldots, Y_e] \) as \( \sigma(f_{\alpha,1}(\beta)) = f_{\alpha,1}(\sigma(\beta)) \) for every \( \sigma \in \Delta, \beta \in (\mathbb{F}_{q^m})^* \). Now \( f_{\alpha,1}(\beta) = 0 \) if \([\beta] \neq [\alpha]\) and \( f_{\alpha,1}(\alpha) = 1 \), solving (1).

Assuming \( \mathbb{F}_q[\alpha] = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m} \), there exists some \( h \in \mathbb{F}_q[Y_1, \ldots, Y_e] \) such that \( h(\alpha) = b \). Now \( f_{\alpha,b} := hf_{\alpha,1} \) has the desired property yielding (2).

**Remark 2.2.3.** Let us write \( A \) for the right hand side of the equality. Let \( \sigma \in A \) such that \( \sigma(\alpha) = \beta \) for \( \alpha, \beta \in \mathbb{F}^{q^m}_{q^m} \). Define \( \sigma_{\alpha,\beta} \in A \) as the map which is zero outside of \([\alpha]\), and satisfies \( \sigma_{\alpha,\beta}(\alpha) = \beta \). (This fixes an element of \( A \).) Then we can write \( \sigma = \sum_{\alpha \in \mathbb{F}^{q^m}_{q^m}} \sigma_{\alpha,\beta} \) such that \( \phi \sigma = \sum_{\alpha \in \mathbb{F}^{q^m}_{q^m}} \phi \sigma_{\alpha,\beta} = \sum_{\alpha \in \mathbb{F}^{q^m}_{q^m}} \sigma_{\alpha,\beta} \phi = \sigma \phi \). Thus the maps \( \sigma_{\alpha,\beta} \) forms the generating set of \( A \).

**Proof.** (of proposition 2.2.1) Let us write \( A \) for the right hand side of the equality; we only need to show that \( A \subseteq \pi_{q^m}(\text{MA}_n(\mathbb{F}_q)) \). Note that \( A \) as well as \( \text{MA}_n(\mathbb{F}_q) \) are \( \mathbb{F}_q \)-vector spaces and \( \pi_{q^m} \) is \( \mathbb{F}_q \)-linear. If \( \alpha \in \mathbb{F}^{q^m}_{q^m} \) and \( \sigma \in A \), and \( \phi \) is a generator of the cyclic group \( \text{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q) \), then the order of \( \sigma(\alpha) \) under \( \phi \) must divide the order of \( \alpha \) under \( \phi \) (as \( \phi \sigma(\alpha) = \sigma(\phi(\alpha)) \)). Thus the degree of field extension \( [\mathbb{F}_q(\sigma(\alpha)) : \mathbb{F}_q] \) divides \( [\mathbb{F}_q(\alpha) : \mathbb{F}_q] \) meaning that \( \sigma(\alpha) \in \mathbb{F}_q(\mathbb{F}_q)^n \). If \( \alpha \in \mathbb{F}^{q^m}_{q^m}, \beta \in \mathbb{F}_q(\mathbb{F}_q)^n \) then define \( \sigma_{\alpha,\beta} \in A \) as the map which is zero outside of \([\alpha]\), and satisfies \( \sigma_{\alpha,\beta}(\alpha) = \beta \). (This fixes an element of \( A \).) The maps \( \sigma_{\alpha,\beta} \) form a generating set of \( A \). Now picking \( f_{\alpha,\beta} \) from lemma 2.2.2 and forming \( F = (f_{\alpha,\beta_1}, \ldots, f_{\alpha,\beta_n}) \) we have \( \pi_{q^m}(F) = \sigma_{\alpha,\beta} \) and we are done.

If \( d|m \), then there exists a natural restriction map \( \pi_{q^m}(\text{MA}_n(\mathbb{F}_q)) \rightarrow \pi_{q^d}(\text{MA}_n(\mathbb{F}_q)) \). In a diagram, we get
2.3. Automorphisms fixing a variable

\[
\lim_{m \in \mathbb{N}} \pi_{q^m}(\text{MA}_n(F_q))
\]

where above we have put the inverse limit \( \lim_{m \in \mathbb{N}} \pi_{q^m}(\text{MA}_n(F_q)) \) of this partially ordered diagram of monoids.

**Definition 2.2.4.** The inverse limit of the above partially ordered diagram of monoids is called the profinite polynomial endomorphism monoid over \( F_q \), and denoted as \( \hat{\text{MA}}_n(F_q) \). Similarly, we define \( \hat{\text{GA}}_n(F_q) \) and \( \hat{T\text{A}}_n(F_q) \), etc.

With \( \overline{F}_q \) denoting an algebraic closure of \( F_q \), note that \( \hat{\text{MA}}_n(F_q) \) can be seen as a subset of \( \text{Maps}(\overline{F}_q^{\mathbb{N}}, \overline{F}_q^{\mathbb{N}}) \), and in fact proposition 2.2.1 shows that \( \hat{\text{MA}}_n(F_q) = \{ \sigma \in \text{Maps}(\overline{F}_q^{\mathbb{N}}, \overline{F}_q^{\mathbb{N}}) \mid \sigma \phi = \phi \sigma, \forall \phi \in \text{Gal}(\overline{F}_q : F_q) \} \). We can also embed \( \text{MA}_n(F_q) \) into \( \hat{\text{MA}}_n(F_q) \) by the injective map \( \hat{\pi} : \text{MA}_n(F_q) \rightarrow \text{Maps}(\overline{F}_q^{\mathbb{N}}, \overline{F}_q^{\mathbb{N}}) \).

By definition, \( \hat{\text{MA}}_n(F_q) \) is the completion of \( \text{MA}_n(F_q) \) with respect to the topology with \( \{ \ker(\pi_{q^m}) \mid m \in \mathbb{N} \} \) as a basis of open sets. Note the analogy with the construction of the \( p \)-adics \( \mathbb{Z}_p \) in the introduction.

Another\(^1\) interpretation is that we put a topology on the set \( \text{MA}_n(F_q) \) where a basis of open sets is \( \{ \ker(\pi_{q^m}) \mid m \in \mathbb{N} \} \), and \( \hat{\text{MA}}_n(F_q) \) is the completion w.r.t. this topology. (There is similarity with the construction of the \( p \)-adic integers \( \mathbb{Z}_p \) out of the maps \( \mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z} \), or perhaps better, the construction of the profinite completion of \( \mathbb{Z}, \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \) out of \( \mathbb{Z}/n\mathbb{Z} \).)

2.3 Automorphisms fixing a variable

**Notations:** If \( F \in \text{GA}_n(k[Z]) \) and \( c \in k \), write \( F_c \in \text{GA}_n(k) \) for the restriction of \( F \) to \( Z = c \). In case we already have a subscript \( F = G_\sigma \), then \( G_{\sigma,c} = F_c \). If \( F \in \text{GA}_n(k) \), then by \( (F,Z) \in \text{GA}_{n+1}(k) \) (or any other appropriate variable in stead of \( Z \)) we denote the map obtained by \( F \) by adding one dimension, i.e. \( (F,Z) = (F_1(X_1, \ldots, X_n, Z), \ldots, F_n(X_1, \ldots, X_n, Z), Z) \).

---

\(^1\)Well, it's actually the definition.
If $F \in \text{GA}_n(k[Z])$ then we identify $F$ on $k[Z]^n$ with $(F, Z)$ on $k^{n+1}$ and denote both by $F$. (In fact, we think of $\text{GA}_n(k[Z])$ as a subset of $\text{GA}_{n+1}(k).$)

The main result of this section is the following theorem:

**Theorem 2.3.1.** If $F \in \text{TA}_n(\mathbb{F}_q(Z)) \cap \text{GA}_n(\mathbb{F}_q[Z])$, and $F_c \in \text{TA}_n(\mathbb{F}_q[c])$ for all $c \in \mathbb{F}_{q^m}$ and all $m \geq 1$, then $F \in \text{TA}_n(\mathbb{F}_q[Z])$.

This immediately yields the following important corollary:

**Corollary 2.3.2.**

$$\text{GA}_2(\mathbb{F}_q[Z]) \subseteq \text{TA}_2(\mathbb{F}_q[Z]) \subseteq \text{TA}_3(\mathbb{F}_q).$$

In particular, it shows that the famous (notorious?) Nagata automorphism $N = (X - 2Y\alpha - Z\alpha^2, Y + Z\alpha, Z)$ where $\alpha = XZ + Y^2$ is an element of $\text{TA}_3(\mathbb{F}_q)$. This shows that Nagata’s automorphism is the “limit” of tame maps, which calls up resemblance to [EP15], where a wild automorphism is shown to be a limit of tame maps in the “regular” topology over $\mathbb{C}$. Incidentally, the result of Smith [Smi89] shows that the Nagata automorphism is stably tame in the sense that $(N, Z) \in \text{TA}_n(\mathbb{C})$.

Before we state the proof of 2.3.1, we must derive some tools:

**Definition 2.3.3.** A map is called strictly Jonquières if it is Jonquières, and has affine part equal to the identity (i.e. the linear part identity and zero maps to zero).

**Lemma 2.3.4.** Let $F \in \text{TA}_n(k(Z))$ be such that the affine part of $F$ is the identity. Then $F$ can be written as a product of strictly Jonquières maps and permutations.

Proof. (rough sketch.) The whole proof works since one can “push” elements which are both Jonquières and affine to one side, since if $E$ is Jonquières (or affine), and $D$ is both, then there exists an $E'$ which is Jonquières (or affine), and $ED = DE'$. This argument is used to standardize many a decomposition. Here, we emphasize that the final decomposition is by no means of minimal length.

1. First, using the definition of tame maps, we decompose $F = E_1A_1E_2A_2 \cdots E_sA_s$ where each $E_i$ is Jonquières and each $A_i$ is affine.
2. We may assume that $E_i(0) = A_i(0) = 0$ for all $1 \leq i \leq s$. For any pure translation part can be pushed to the left, and then we use the fact that $F(0) = 0$, i.e. the $A_i$ are linear.
3. We may assume that $\det(A_i) = 1$ and the $E_i$ are strictly Jonquières. To realize this, one must notice that there exists a diagonal linear map $D_i$ satisfying $\det(D_i) = \det(A_i)$, and that we can do this by pushing diagonal linear maps to the left. The result follows since the determinant of the linear part of $F$ is 1, and hence the determinant of the Jacobian of $F$ is 1.
4. We may assume that each $A_i$ is either diagonal of determinant 1 or -1, or a permutation. Now we use Gaussian Elimination to write each $A_i = P_{i1}E_{i1} \cdots P_{il}E_{il}D_i$ as a composition of permutations $P_{ij}$, strictly Jonquières (elementary linear) maps $E_{ij}$, and one diagonal map $D_i$. We may assume that each
in the following way: replace each fraction

\[ \frac{g}{F} \]

\[ \tilde{g} \in F \]

elements \( F \) if that if \( G := \text{Gal} \) group only if \( g \) that this map acts as required. Since for \( X \) stands for \( X \) if all that all \( X \) is triangular. We can even write \( p \) be written as a composition of strictly Jonquières maps \( \alpha \) such that \( g \) is such that the affine part is the \( f \) of determinant 1 that have 1's on \( n-2 \) places, and at most two diagonal elements which are not 1, and \( D_1 \) has 1 on the diagonal except at one place, where it is 1 or -1. The following formulas explain how to write a diagonal map \( D_1 \) as product of (linear) strictly Jonquières maps and permutations, as well as \( D_1 \):

\[
P := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad E[a] := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}
\]

\[
\begin{pmatrix} f^{-1} & 0 \\ 0 & f \end{pmatrix} = E[f^{-1}] \cdot P \cdot E[1-f] \cdot P \cdot E[-1] \cdot P \cdot E[1-f] \cdot P
\]

\[
\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = E[1] \cdot P \cdot E[-1] \cdot P \cdot E[1] \cdot P.
\]

This finishes (the rough sketch of) the proof. \( \square \)

Lemma 2.3.5. Let \( \rho(Z) \in \mathbb{F}_q[Z] \).

Let \( F \in \text{TA}_n(\mathbb{F}_q[Z, g(Z)^{-1}]) \cap \text{GA}_n(\mathbb{F}_q[Z]) \) be such that the affine part is the identity. Assume that \( F_c \in \text{TA}_n(\mathbb{F}_q[c]) \) for all \( c \in \mathbb{F}_q \) and all \( m \). Then for any \( m \in \mathbb{N}^+ \) we find two maps \( G, \tilde{G} \in \text{TA}_n(\mathbb{F}_q[Z]) \) such that for \( c \in \mathbb{F}_q \):

1. \( G_c = I_n \) if \( g(c) \neq 0 \),
2. \( G_c = F_c \) if \( g(c) = 0 \),
3. \( \tilde{G}_c = F_c \) if \( g(c) \neq 0 \).

Proof. Since \( G, \tilde{G} \) are defined over \( \mathbb{F}_q \), without loss of generality, we may assume that \( m \) is such that \( g \) factors completely into linear factors over \( \mathbb{F}_q \).

Let \( \alpha \) be a root of \( g \). Consider \( F_\alpha \), which by assumption and lemma 2.3.4 can be written as a composition of strictly Jonquières maps \( e_i \) and permutations \( p_i : F_\alpha = e_1 p_1 e_2 \ldots e_s p_s \). Write the \( e_i \) as \( I_n + H_i \) where \( H_i \) is strictly upper triangular. We can even write \( H_i = f_i(\alpha, \mathcal{X}) \) where \( f_i(\mathcal{Z}, \mathcal{X}) \in \mathbb{F}_q[Z, \mathcal{X}]^n \) (and \( \mathcal{X} \) stands for \( \mathcal{X}_1, \ldots, \mathcal{X}_n \)).

Now we define \( \rho := 1 - g^{-\ell} \in \mathbb{F}_q[Z] \) and \( E_i := I_n + \rho f_i(\mathcal{Z}, \mathcal{X}) \). Note that all \( E_i \in \text{TA}_n(\mathbb{F}_q[Z]) \). We define \( G := E_1 p_1 E_2 p_2 \ldots E_s p_s \). Our claim is that this map acts as required. Since for \( c \in \mathbb{F}_q \) we have \( \rho(c) = 0 \) if and only if \( g(c) \neq 0 \), it follows that in that case \( G_c = I_n \). Since \( E_{i,\alpha} = e_i \) by construction, we have \( G_\alpha = F_\alpha \). Now let \( \Phi \) be an element of the Galois group \( \text{Gal}(\mathbb{F}_q^n[Z]) \). The remaining question is if \( G_{\Phi(\alpha)} = F_{\Phi(\alpha)} \). Note that if \( P(\mathcal{Z}, Z) \in \mathbb{F}_q[Z, \mathcal{X}] \) then \( \Phi(p(\mathcal{Z}, \mathcal{X})) = P(\Phi(\mathcal{Z}), \mathcal{X}) \). This implies that if \( F \in \text{GA}_n(\mathbb{F}_q[Z]) \), then \( F_{\Phi(\alpha)} = \Phi(F_\alpha) \). Thus \( G_{\Phi(\alpha)} = \Phi(G_\alpha) = \Phi(F_\alpha) = F_{\Phi(\alpha)} \) and we are done.

In order to construct \( \tilde{G} \), we again consider the decomposition \( F = e_1 p_1 e_2 p_2 \ldots e_s p_s \) where the \( e_i \). Now we modify \( H_i \) in \( e_i := I_n + H_i \) in the following way: replace each fraction \( g^{-t} \) by \( g^{t(q^{n-2})} \) making new elements \( \tilde{H}_j \) which are in \( \text{MA}_n(\mathbb{F}_q[Z]) \). Write \( e_i := I_n + \tilde{H}_j \) and define \( G := E_1 p_1 E_2 p_2 \ldots E_s p_s \). Note that if \( e \in \mathbb{F}_q^n \) and \( g(e) \neq 0 \), then \( g^{-t}(e) = \ldots \)
Thus, for every \( m \) using lemma 2.3.5 we find \( G \). We may assume that if

\[
(3)
\]

we can assume that \( g \) factors into linear parts over \( \mathbb{F}_{q^m} \).

(3) We may assume that if \( g(c) \neq 0 \) then \( F_c = I \); using lemma 2.3.5 we can find \( \tilde{g} \in \mathbb{F}_{q^n}[Z] \) such that \( \tilde{G}_c = F_c \) if \( g(c) \neq 0 \). We can replace \( F \) by \( \tilde{G}^{-1}F \).

(4) Using lemma 2.3.5 we find \( G \in \mathbb{F}_{q^n}[Z] \) such that \( F_c = G_c = I \) if \( g(c) \neq 0 \), \( F_c = G_c \) if \( g(c) = 0 \). Thus, \( G^{-1}F \) is the identity map on \( \mathbb{F}_{q^m}^n \).

Thus, for every \( m \in \mathbb{N} \) we can find a \( G_m \in \mathbb{F}_{q^n}[Z] \) such that \( \pi_{q^m}(G_m) = \pi_{q^m}(F) \) (as permutation on \( \mathbb{F}_{q^m}^n \)), meaning that \( F \in \mathbb{T}_{q^n}[F_q] \subset \mathbb{T}_{q^n}[F_q] \).

To finish this section, the below lemma clarifies exactly when a map in \( \mathbb{T}_{q^n}[F_q] \cap \operatorname{GA}_{n}(F_q) \) is in \( \mathbb{T}_{q^n}[F_q] \).

**Lemma 2.3.6.** Let \( F \in \mathbb{T}_{q^n}[F_q] \), and suppose that there exists a bound \( d \in \mathbb{N} \) such that for all \( m \in \mathbb{N} \) we have \( T_m \in \mathbb{T}_{q^n}[F_q] \) such that \( \pi_{q^m}(T_m) = \pi_{q^m}(F) \) and \( \deg(T_m) \leq d \). Then \( F \in \mathbb{T}_{q^n}[F_q] \).

**Proof.** There exists at most one \( T \in \mathbb{T}_{q^n}[F_q] \) of degree \( < q^m \) such that \( \pi_{q^m}(T) = \pi_{q^m}(F) \). This means that the sequence \( T_1, T_2, T_3, \ldots \) must stabilize. Thus \( F = T_m \) if \( q^m > d \).

Note that the converse of the above lemma is trivially true.

### 2.4 The profinite permutations induced by endomorphisms

**Definition 2.4.1.** Define \( \mathcal{M}_n(F_q) := \mathbb{T}_{q^n}[F_q] \cap \operatorname{Perm}(\mathbb{F}_q^n) \).

\( \mathcal{M}_n(F_q) \) is the set of permutations induced by endomorphisms. It is equal to the set of permutation of \( \mathbb{F}_q^n \) which commute with \( \operatorname{Gal}(\mathbb{F}_q : \mathbb{F}_q) \). We do have the following inclusions:

\[
\mathbb{T}_{q^n}[F_q] \subseteq \mathbb{GA}_n(F_q) \subseteq \mathcal{M}_n(F_q).
\]

This means that we have to briefly analyze \( \mathcal{M}_n(F_q) \) as this apparently is the “world” in which our more complicated objects \( \mathbb{T}_{q^n}[F_q] \) and \( \mathbb{GA}_n(F_q) \) live.

**Definition 2.4.2.** Define \( \mathcal{X}_d \) as the union of all orbits of size \( d \) of the action of \( \operatorname{Gal}(\mathbb{F}_q : \mathbb{F}_q) \) on \( \mathbb{F}_q^n \).

We denote by \( \mathcal{X}_d \) the quotient of \( \mathcal{X}_d \) under the action of \( \operatorname{Gal}(\mathbb{F}_q^d : \mathbb{F}_q) \), i.e. the set of orbits of size \( d \). This notation will be used in section 2.7.
Let $X$ be a set and $S$ a subgroup of the group of permutations of $X$. For $\sigma \in S$, we denote the action of $\sigma$ on $x \in X$ by $x^\sigma$, and thus $(x)^\sigma \rho = ((x)^\sigma)^\rho$ where $\sigma, \rho \in S$. This is for now more convenient than the notation $\sigma(x)$, as in the below corollary we do not need to talk about the opposite group action etc.

**Corollary 2.4.3.** (of 2.2.1)

(1) 
\[ \mathcal{M}_n(\mathbb{F}_q) = \bigoplus_{d \in \mathbb{N}} G_d \]

where $G_d$ is the set of permutations on $\mathcal{X}_d$ which commute with $\text{Gal}(\mathbb{F}_{q^d} : \mathbb{F}_q)$.

(2) This is means that 
\[ G_d \cong ((\mathbb{Z}/d\mathbb{Z})^{r_d} \rtimes \text{Perm}(r_d)) \]

where $r_d$ is the amount of orbits of size $d$ (i.e. $r_d = d^{-1} \# \mathcal{X}_d$) and $h : \text{Perm}(r_d) \to \text{Aut}((\mathbb{Z}/d\mathbb{Z})^{r_d})$ such that $h(\sigma)(a_1, a_2, \ldots, a_{r_d}) = (a_1)^\sigma, (a_2)^\sigma, \ldots, (a_{r_d})^\sigma$.

**Proof.** Part (1) is obvious using 2.2.1. Let $O_1, \ldots, O_{r_d}$ be the disjoint orbits in $\mathcal{X}_d$. Let $\alpha_i \in O_i$ be chosen from the orbits (at random). Write $\text{Gal}(\mathbb{F}_{q^d} : \mathbb{F}_q) = \langle \phi \rangle \cong \mathbb{Z}/d\mathbb{Z}$. Now if a permutation $P$ of $\mathcal{X}_d$ commutes with $\text{Gal}(\mathbb{F}_{q^d} : \mathbb{F}_q)$, then it permutes the orbits; say $\sigma \in \text{Perm}(r_d)$ is this permutation. It sends $[\alpha_i]$ to $[\alpha_{(i)^\sigma}]$ and thus $(\alpha_i)^P = \phi^{a_i \alpha_{(i)^\sigma}}$ where $a_i$ the integers are taken mod $d$, so can be thought of lying in $\mathbb{Z}/d\mathbb{Z}$. Thus, as a set we have equality. We only need to check how the multiplication acts:

We can construct a map
\[ \varphi : G_d \to (\mathbb{Z}/d\mathbb{Z})^{r_d} \rtimes \text{Perm}(r_d) \]
\[ P \to (a_1, a_2, \ldots, a_{r_d} ; \sigma_P) \].

Write $\varphi(P) = (a_1, \ldots, a_n; \sigma)$ and $\varphi(Q) = (b_1, \ldots, b_n; \rho)$ for some $P, Q \in G_d$.

Now $(\alpha_i)^{PQ} = (\phi^{a_i \alpha_{(i)^\sigma}})^Q = \phi^{a_i \alpha_{(i)^\sigma} b_{(i)^\sigma}}$, thus
\[ \varphi(PQ) = (a_1 + b_1, \ldots, a_n + b_n; \sigma \rho) \]

and since we want $\varphi(P) \cdot \varphi(Q) = \varphi(PQ)$ we get the multiplication rule for semidirect product
\[ (a_1, \ldots, a_n; \sigma) \cdot (b_1, \ldots, b_n; \rho) = (a_1 + b_1, \ldots, a_n + b_n; \sigma \rho) \]

Thus $\varphi$ is a group homomorphism. Since $\text{Ker}(\varphi) = \{ P \in G_d : \varphi(P) = (0, 0, \ldots, 0, id) \} = \{ id_{G_d} \}$, the map is injective. Since the orders of the groups are the same, we have an isomorphism. \( \square \)

### 2.5 The profinite tame automorphism group acting on orbits of a fixed size

Our goal is to understand “how far” $\widehat{\text{TAut}}_n(\mathbb{F}_q)$ can be from $\widehat{\text{GA}}_n(\mathbb{F}_q)$ if $n \geq 3$. Since $\text{GA}_n(\mathbb{F}_q)$ is too unwieldy if $n \geq 3$, we are in fact trying to understand “how far” $\widehat{\text{TAut}}_n(\mathbb{F}_q)$ is from $\mathcal{M}_n(\mathbb{F}_q)$, which squeezes $\widehat{\text{GA}}_n(\mathbb{F}_q)$ between them.
Chapter 2. The profinite polynomial automorphism group

In most of this section, we fix \( m \in \mathbb{N} \). We have to introduce several notations:

- set \( q = p^l \): \( p \) is a prime integer, \( l \geq 1 \),
- \( \Delta = \text{Gal}(\mathbb{F}_{q^m} : \mathbb{F}_q) \),
- \( \Xi = \text{Gal}(\overline{\mathbb{F}}_q : \mathbb{F}_q) \),
- \( \mathcal{X} \) is the union of the \( \Xi \) orbits of size \( m \) in \( \overline{\mathbb{F}}_q^n \),
- \( \Omega \) is the set of the \( \Xi \) orbits of size \( m \) in \( \mathbb{F}_q^{n-1} \),
- \( \bar{\mathcal{X}} \) is the quotient of \( \mathcal{X} \) under \( \Delta \), i.e. the set of orbits of size \( m \),
- we fix the dimension \( n \geq 3 \).

The action of \( \text{TA}_n(\mathbb{F}_q) \) on \( \overline{\mathbb{F}}_q^n \) restricts naturally to \( \mathcal{X} \), and also induces an action on \( \bar{\mathcal{X}} \). This means that we have a natural group homomorphism \( \text{TA}_n(\mathbb{F}_q) \rightarrow \text{Perm}(\bar{\mathcal{X}}) \). We denote by \( \mathcal{G} \) the image of this group homomorphism.

Our first goal is to prove the below theorem.

**Theorem 2.5.1.** For \( n \geq 3 \), we have \( \text{Alt}(\bar{\mathcal{X}}) \subseteq \mathcal{G} \).

The rest of this section is devoted to proving this theorem.

**Definition 2.5.2.** A permutation group \( G \) acting on a set \( S \) is called primitive if \( G \) acts transitively on \( S \) and \( G \) preserves no nontrivial partition of \( S \).

The generic outline of the proof is as follows: It is enough to show that \( \mathcal{G} \) is primitive by a theorem of Jordan [Isa08, Corollary 8.19].

**Theorem 2.5.3.** (Jordan) Let \( G \) be a primitive subgroup of \( S_n \). Suppose \( G \) contains a 3-cycle. Then \( G \) contains the alternating subgroup \( A_n \).

**Overview of the proof of theorem 2.5.1.**
We will prove that the group \( \mathcal{G} \) contains a 3-cycle (lemma 2.5.6) and is 2-transitive (which implies primitive). The latter is the most complicated part, requiring some delicate induction arguments: lemmas 2.5.8-2.5.10 are preparations to prove proposition 2.5.11 (2-transitivity for a large class of points). Along with this, lemmas 2.5.14-2.5.17 are preparations to prove proposition 2.5.18 (2-transitivity in general). The difficulties in this proof are obviously its length and occasional technicality, but also in the rather complicated induction (the lemmas 2.5.14-2.5.17) which makes the proof quite nontrivial.

**Definition 2.5.4.** (i) Let \( a \in \Omega \). Then define

\[
\tau_{a,1} := (X_1 + f_{a,1}(X_2, \ldots, X_n), X_2, \ldots, X_n)
\]

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

\[
\tau_i := (X_i, X_2, \ldots, X_{i-1}, X_1, X_{i+1}, \ldots, X_n),
\]

the map interchanging \( X_i \) and \( X_1 \).
Definition 2.5.5. In this article we define the lexicographic ordering of two vectors $u := (u_1, \ldots, u_n), v := (v_1, \ldots, v_n)$, notation $u \geq_{\text{Lex}} v$, if there exists $m \in \mathbb{N}, 0 \leq m \leq n$ such that $u_m > v_m, (u_{m+1}, u_{m+2}, \ldots, u_n) = (v_{m+1}, v_{m+2}, \ldots, v_n)$. (i.e. the weight is at the “head” of a vector, not the tail).

Lemma 2.5.6. The group $\mathcal{G}$ contains 3-cycles

Proof. Consider $\mathbb{F}_q^m = \mathbb{F}_q(t)$. Let $a := (0, \ldots, 0, t) \in \Omega$ and let

$$s := \tau_{a,1} = (X_1 + g_{a,1}(X_2, \ldots, X_n), X_2, \ldots, X_n),$$
$$l := \tau_{2\tau_{a,1}^{-1}} = (X_1, X_2 + g_{a,1}(X_1, X_3, \ldots, X_n), X_3, \ldots, X_n).$$

Consider $L_1 = \{[(a_1, 0, 0, \ldots, 0, a_n)]|a_n \in \{t\} \text{ and } a_1 \in \mathbb{F}_q^m\}$ and $L_2 = \{[(0, a_2, 0, \ldots, 0, a_n)]|a_2 \in \mathbb{F}_q^m \text{ and } a_n \in \{t\}\}$, where $L_1, L_2$ are subsets of $\mathcal{X}$ and $[t] = \{\phi(t) : \phi \in \Delta\}$. Then $s$ permutes only the set $L_1$ and $l$ permutes only the set $L_2$. Both $s$ and $l$ are cyclic of order $p = \text{char}(\mathbb{F}_q^m)$ on $L_1$ and $L_2$ respectively. Let $w = s^{-1}l^{-1}sl$. Then $w$ acts trivially on $\mathcal{X} \setminus (L_1 \cup L_2)$ and nontrivially only on a subset of $L_1 \cup L_2$. Now if $b \notin L_2$ and $s(b) \notin L_2$, then since $l$ operates nontrivially only on elements of $L_2$ one can check easily that $w(b) = b$. Similarly if $b \notin L_1$ and $l(b) \notin L_1$ then $w(b) = b$. The other cases include:

1. $b \notin L_2$ and $s(b) \in L_2$ (e.g., the element $D := [(-1, 0, \ldots, 0, t)]$),
2. $b \notin L_1$ and $l(b) \in L_1$ (e.g., the element $E := [(0, -1, 0, \ldots, 0, t)]$),
3. $b \in L_1$ and $l(b) \in L_2$ (e.g., the element $F := [(0, 0, \ldots, 0, t)]$).

Since $s(D) = F, s(E) = E, l(E) = F, l(D) = D, s(F) \notin L_2, l(F) \notin L_1$. Using this observation we see that $w(D) = E, w(E) = F, w(F) = D$ and $w$ is the required 3-cycle. 

Here starts the technical proof of 2-transitivity (proposition 2.5.18). We slowly start by connecting more and more pairs $([r], [u])$ and $([s], [v])$ where $[r], [s], [v], [u] \in \mathcal{X}$. (For most lemmas, $[v] = [u]$.) We introduce the following definition:

Definition 2.5.7. We say that $u, v \in \mathbb{F}_q^m$ are weakly conjugate (or, $u$ is a weak conjugate of $v$) if $[u_i] = [v_i]$ for all $1 \leq i \leq n$. We denote this as $u \approx v$. We also denote $u \not\approx v$ for “not $u \approx v$”.

Note that $[u] = [v]$ implies $u \approx v$, but not the other way around. Similarly, $u \not\approx v$ implies $[u] \not= [v]$. In the below lemmas we will have to give special attention to cases where a pair among $r, s, u$ is weakly conjugate, as this complicates things.

Lemma 2.5.8. Let $r, u \in \mathcal{X}$ such that $[r] \neq [u]$. Assume $\mathbb{F}_q^m = \mathbb{F}_q(r_i)$ and $[r_j] \neq [u_i]$ for some $i, j \in \{1, 2, \ldots, n\}$. Then for any $k \in \{1, 2, \ldots, n\}$ with $k \neq i, j$ and $v \in \mathbb{F}_q^m$, there exist $P \in TA_n(\mathbb{F}_q)$ such that:

1. $P[u] = [u]$ and
2. $P[v] = [(r_1, \ldots, r_{k-1}, v, r_{k+1}, \ldots, r_n)]$.

Proof. Fix $a = (r_1, \ldots, r_k, \ldots, r_n)$. Define

$$P := (X_1, \ldots, X_k + f_{a, u-r_k}(X_1, \ldots, \hat{X}_k, \ldots, X_n), \ldots, X_n),$$
Lemma 2.5.9. Let \( s, r, u \in X \) s.t. \( s = (s_1, \ldots, s_n) \), \( r = (r_1, \ldots, r_n) \), and \( u = (u_1, \ldots, u_n) \) be in different orbits with \( F_{q^m} = F_q(r_1) = F_q(s_1) \) and suppose \( r \neq u, s \neq u \). Then there exist \( F \in TA_n(F_q) \) s.t. \( F(r) = [s] \) and \( F([u]) = [u] \).

Proof. We divide our lemma into the following four cases.

Case 1. \( [r_1] \neq [u_1] \) and \( [s_1] \neq [u_1] \).

Case 2. \( [r_1] \neq [u_1] \) and \( [s_1] \neq [u_1] \) for some \( 2 \leq i \leq n \).

Case 3. \( [s_1] \neq [u_1] \) and \( [r_1] \neq [u_1] \) for some \( 2 \leq i \leq n \).

Case 4. \( [r_1] \neq [u_1] \) and \( [s_1] \neq [u_1] \) for some \( i, j \in \{2, 3, \ldots, n\} \).

Case 1. \( [r_1] \neq [u_1] \) and \( [s_1] \neq [u_1] \).

As \( F_{q^m} = F_q(r_1) \) and \( [r_1] \neq [u_1] \) by applying the tame map as in lemma 2.5.8 several times we map the orbit \([r]\) to \([r_1, s_1, s_3, \ldots, s_n]\) and \([u]\) remains unchanged.

Sub-case 1.1. \( ([s_1, s_3, \ldots, s_n]) \neq ([u_2, \ldots, u_n]) \). Fix \( a := (s_1, s_3, \ldots, s_n) \). Define \( P_1 := (X_1 + f_{a,s_1-r_1}(X_2, \ldots, X_n), X_2, \ldots, X_n) \) where \( f_{a,s_1-r_1} \) is as in lemma 2.2.2. (Note that since \( s_1 \) generates \( F_{q^m} \), we can indeed apply this lemma as \( a = (s_1, \ldots) \).) Thus \( P_1([r_1, s_1, s_3, \ldots, s_n]) = ([s_1, s_1, \ldots, s_n]) \) and \( P_1([u]) = [u] \). Now as \( F_{q^m} = F_q(s_1) \) and \( [s_1] \neq [u_1] \) so by applying the tame map as in lemma 2.5.8 we map the orbit \([s_1, s_1, s_3, \ldots, s_n]\) to \([s_1, s_2, s_3, \ldots, s_n]\) and \([u]\) remains unchanged.

Sub-case 1.2. \( ([s_1, s_3, \ldots, s_n]) = ([u_2, \ldots, u_n]) \). In this case we have \( s_1 \in [u_2] \) and hence \( u_2 \) is also a generator of \( F_{q^m} \). Using lemma 2.5.8 and \( [r_1] \neq [u_1] \) we can send \([u]\) to \([u_1, u_2, u_1, u_4, \ldots, u_n]\) and \([r_1, s_1, s_3, \ldots, s_n]\) remains unchanged. Now with \( r_1 \) a generator of \( F_{q^m} \) and \([r_1] \neq [u_1] \), send \([r_1, s_1, s_3, \ldots, s_n]\) to \([r_1, s_1, s_3, \ldots, s_n]\) and \([u_1, u_2, u_1, u_4, \ldots, u_n]\) remains unchanged by lemma 2.5.8. With \( s_1 \) a generator of \( F_{q^m} \) and \([s_1] \neq [u_1] \), send \([s_1, s_1, s_3, \ldots, s_n]\) to \([s_1, s_2, s_3, \ldots, s_n]\) and \([u_1, u_2, u_1, u_4, \ldots, u_n]\) remains unchanged by applying lemma 2.5.8 two times. With \( s_1 \) a generator of \( F_{q^m} \) and \([s_1] \neq [u_1] \), send \([s_1, s_2, s_3, \ldots, s_n]\) to \([s_1, s_2, s_3, \ldots, s_n]\) and \([u_1, u_2, u_1, u_4, \ldots, u_n]\) remains unchanged by applying lemma 2.5.8. With \( u_2 \) a generator of \( F_{q^m} \) and \([s_1] \neq [u_1] \), send \([u_1, u_2, u_1, u_4, \ldots, u_n]\) to \([u]\) and \([s]\) remains unchanged by applying lemma 2.5.8.

Case 2. \( [r_1] \neq [u_1] \) and \([s_1] \neq [u_1] \) for \( 2 \leq i \leq n \).

Since \( n \geq 3 \) there exist \( k \in \{2, 3, \ldots, n\} \) such that \( k \neq i \). Without loss of generality we assume \( i = 2, k = 3 \). Since \( r_1 \) generates \( F_{q^m} \) and \([r_1] \neq [s_1] \), successive application of lemma 2.5.8 maps \([r]\) to \([r_1, s_2, s_1, s_4, \ldots, s_n]\) and \([u]\) to \([u]\). With \([s_2] \neq [u_2]\) and \( s_1 \) a generator of \( F_{q^m} \), map \([r_1, s_2, s_1, s_4, \ldots, s_n]\) to \([s_1, s_2, s_1, s_4, \ldots, s_n]\) and \([u]\) remains unchanged by lemma 2.5.8. With \([s_2] \neq [u_2]\) and \( s_1 \) a generator of \( F_{q^m} \), map \([s_1, s_2, s_1, s_4, \ldots, s_n]\) to \([s_1, s_2, s_3, s_4, \ldots, s_n]\) = \([s]\) and \([u]\) remains unchanged by lemma 2.5.8.

Case 3. \([s_1] \neq [u_1] \) and \([r_1] \neq [u_1] \) for \( 2 \leq i \leq n \).

By case 2 there exist a tame map \( F \in TA_n(F_q) \) s.t. \( F([s]) = [r] \) and \( F([u]) = [u] \), hence \( F^{-1}[r] = [s] \) and \( F^{-1}[u] = [u] \).
Case 4. \([r_i] \neq [u_i]\) and \([s_j] \neq [u_j]\) for some \(i, j \in \{2, 3, \ldots, n\}\).

Subcase 4.1. \([r_i] \neq [u_i]\) and \([s_j] \neq [u_j]\) for some \(i, j \in \{2, 3, \ldots, n\}\) with \(i \neq j\).

As above we assume \(i = 2, j = 3\). With \(\mathbb{F}_q^m = \mathbb{F}_q(r_1)\) and \([r_2] \neq [u_2]\), send the orbit \([r]\) to \([r_1, r_2, s_3, s_4, \ldots, s_n]\) and the orbit \([u]\) remains unchanged by applying the lemma 2.5.8 several times. With \(\mathbb{F}_q^m = \mathbb{F}_q(r_1)\) and \([s_3] \neq [u_3]\), map \([r_1, r_2, s_3, s_4, \ldots, s_n]\) to \([r_1, s_1, s_3, s_4, \ldots, s_n]\) and \([u]\) remains unchanged by lemma 2.5.8. With \(\mathbb{F}_q^m = \mathbb{F}_q(s_1)\) and \([s_3] \neq [u_3]\), map \([r_1, s_1, s_3, s_4, \ldots, s_n]\) to \([s_1, s_1, s_3, s_4, \ldots, s_n]\) and \([u]\) remains unchanged by lemma 2.5.8. With \(\mathbb{F}_q^m = \mathbb{F}_q(s_1)\) and \([s_3] \neq [u_3]\), map \([s_1, s_1, s_3, s_4, \ldots, s_n]\) to \([s_1, s_2, s_3, s_4, \ldots, s_n]\) and the orbit \([u]\) remains unchanged by lemma 2.5.8.

Subcase 4.2. \([r_i] \neq [u_i]\) and \([s_1] \neq [u_1]\) for some \(i \in \{2, 3, \ldots, n\}\).

Since \(n \geq 3\) there exist \(k \in \{2, 3, \ldots, n\}\) such that \(k \neq i\). Again we assume \(i = 2, k = 3\). As \(\mathbb{F}_q^m = \mathbb{F}_q(r_1)\) and \([r_2] \neq [u_2]\), so by applying the tame map as in lemma 2.5.8 several times we map the orbit \([r]\) to \([r_1, r_2, s_1, s_4, s_5, \ldots, s_n]\) and the orbit \([u]\) remains unchanged (Note that here we send \(r_3\) to \(s_1\), because \(s_1\) is a generator of \(\mathbb{F}_q^m\) and we need this to send \(r_1\) to \(s_1\)). With \(\mathbb{F}_q^m = \mathbb{F}_q(s_1)\) and \([r_2] \neq [u_2]\) we map the orbit \([r_1, r_2, s_1, s_4, s_5, \ldots, s_n]\) to \([s_1, r_2, s_1, s_4, s_5, \ldots, s_n]\) and the orbit \([u]\) remains unchanged by lemma 2.5.8. With \(\mathbb{F}_q^m = \mathbb{F}_q(s_1)\) and \([r_2] \neq [u_2]\) we map the orbit \([s_1, r_2, s_1, s_4, s_5, \ldots, s_n]\) to \([s_1, s_2, s_4, s_5, \ldots, s_n]\) and the orbit \([u]\) remains unchanged by lemma 2.5.8.

Subsubcase 4.2.1

\([s_1, r_2, s_3, s_4, \ldots, s_n]\) \(\neq [u_1, \hat{u}_2, u_3, u_4, \ldots, u_n]\). Fix \(a = (s_1, \hat{r}_2, s_3, s_4, \ldots, s_n)\). Define a tame map \(P = (X_1, X_2 + h_{a,s_2-s_2}) = (X_1, X_2, X_3, X_4, \ldots, X_n)\) where \(h_{a,s_2-s_2}\) is as in lemma 2.2.2. (Note that since \(s_1\) generates \(\mathbb{F}_q^m = \mathbb{F}_q(s_1)\), we can indeed apply lemma 2.2.2 as \(a = (s_1, \ldots, \ldots)\).

Thus \(P([s_1, r_2, s_3, s_4, \ldots, s_n]) = [s_1, s_2, \ldots, s_n] = [s]\) and \(P[u] = [u]\).

Subsubcase 4.2.2

\([s_1, r_2, s_3, s_4, \ldots, s_n]\) \(\neq [u_1, \hat{u}_2, u_3, u_4, \ldots, u_n]\). In this case \(u_1 \in [s_1]\), so \(\mathbb{F}_q(u_1) = \mathbb{F}_q^m\). Thus using \([r_2] \neq [u_2]\), send \([u]\) to \([u_1, u_2, u_3, u_4, \ldots, u_n]\) and \([s_1, r_2, s_3, s_4, \ldots, s_n]\) remains unchanged by lemma 2.5.8.

Now using \(\mathbb{F}_q(s_1) = \mathbb{F}_q^m\) and \([r_2] \neq [u_2]\), send \([s_1, r_2, s_3, s_4, \ldots, s_n]\) to \([s_1, r_2, s_3, s_4, \ldots, s_n]\) and \([u_1, u_2, u_3, u_4, \ldots, u_n]\) remains unchanged by lemma 2.5.8. With \(\mathbb{F}_q(s_1) = \mathbb{F}_q^m\) and \([r_2] \neq [u_2]\), send \([s_1, s_2, s_3, s_4, \ldots, s_n]\) to \([s_1, r_2, s_3, s_4, \ldots, s_n]\) and \([u_1, u_2, u_3, u_4, \ldots, u_n]\) remains unchanged by lemma 2.5.8. With \(\mathbb{F}_q(s_1) = \mathbb{F}_q^m\) and \([r_2] \neq [u_2]\), send \([s_1, s_2, s_3, s_4, \ldots, s_n]\) to \([s_1, s_2, s_3, s_4, \ldots, s_n]\) and \([u_1, u_2, u_3, u_4, \ldots, u_n]\) remains unchanged by lemma 2.5.8.

Thus in all cases we can find a tame map \(F \in TA_n(\mathbb{F}_q)\) such that \(F[r] = [s]\) and \(F[u] = [u]\).

\[
\text{Lemma 2.5.10. Let } r, u \in \mathcal{X} \text{ be in different orbits with } u = (u_1, \ldots, u_n) \text{ and } r = (r_1, \ldots, r_n), \mathbb{F}_q(r_1) = \mathbb{F}_q^m \text{ and } r \approx u. \text{ Then there exist } G \in TA_n(\mathbb{F}_q) \text{ such that } G(r) \neq G(u).
\]

\[
\text{Proof. Since } r_1 \in [u_i] \forall 1 \leq i \leq n, \text{ in particular } r_1 \in [u_1]. \text{ Thus } u_1 \text{ is a generator of } \mathbb{F}_q^m = \mathbb{F}_q(u_1). \text{ Define the tame map } G_k = (X_1, \ldots, X_k + f_k(X_1), \ldots, X_n) \text{ for } 2 \leq k \leq n \text{ where } f_k \in \mathbb{F}_q[X_k] \text{ is such that } f_k(u_1) = -u_k.
\]
and \( f_k([a_1]) = 0 \) if \([a_1] \neq [u_1]\). Define \( G = G_2G_3 \ldots G_n \). Thus \( G(u_1, \ldots, u_n) = (u_1, 0, 0, \ldots, 0), G(r_1, r_2, \ldots, r_n) = (r_1, \bar{r}_2, \bar{r}_3, \ldots, \bar{r}_n) \). Since \([r] \neq [u]\) it follows that \( G[r] \neq G[u] \). This shows at least one of \([\bar{r}_i] \neq [0]\) for \( i \geq 2 \) (as \([r_1] = [u_1] \) is given). Hence \( G(r) \neq G(u) \). \( \square \)

**Proposition 2.5.11.** Let \( s, r, u \in X \) s.t. \( s = (s_1, \ldots, s_n) \), \( r = (r_1, \ldots, r_n) \), and \( u = (u_1, \ldots, u_n) \) be in different orbits with \( \mathbb{F}_{q^n} = \mathbb{F}_q[r_1] = \mathbb{F}_q(s_1) \). Then there exist \( F \in TA_n(\mathbb{F}_q) \) s.t. \( F([r]) = [s] \) and \( F([u]) = [u] \).

**Proof.** Case \( r \approx u \) and \( s \not\approx u \): is done by lemma 2.5.9.

Case \( r \approx u \) and \( s \approx u \): In this case \( r_i \in [u] \) \( \forall \ 1 \leq i \leq n \), in particular \( r_1 \in [u_1] \). Thus \( u_1 \) is a generator of \( \mathbb{F}_{q^n} = \mathbb{F}_q(u_1) \). Define the tame map \( K = (X_1, \ldots, X_n) \) for \( 2 \leq k \leq n \) where \( F_k \in \mathbb{F}_q[X_k] \) is such that \( f_k(u_1) = -u_1 \) and \( f_k([a_1]) = 0 \) if \([a_1] \neq [u_1]\). Define \( F = F_2F_3 \ldots F_n \).

Thus \( F(u_1, \ldots, u_n) = (u_1, 0, 0, \ldots, 0), F(r_1, r_2, \ldots, r_n) = (r_1, \bar{r}_2, \bar{r}_3, \ldots, \bar{r}_n) \) and \( F(s_1, s_2, \ldots, s_n) = (s_1, \bar{s}_2, \bar{s}_3, \ldots, \bar{s}_n) \). Since \([r] \neq [u] \) and \([s] \neq [u] \), thus \( F[r] \neq F[u] \) and \( F[s] \neq F[u] \). This shows at least one of \([\bar{r}_i] \neq [0]\) for \( i \geq 2 \) (as \([r_1] = [u_1]\)). Similarly at least one of \([\bar{s}_i] \neq [0]\) for \( i \geq 2 \) or \([s_1] \neq [u_1]\). Thus we have reduced this case to the case \( r \not\approx u \) and \( s \neq u \).

Case both \( r \approx u \) and \( s \approx u \): Using lemma 2.5.10 we find a map \( G \) such that \( G[r] \neq G[u] \). By the previous case applied to the points \( G(r), G(s), G(u) \) we find an \( H \) such that \( H[G(r)] = [G(s)] \) and \( H[G(u)] = [G(u)] \). Now taking \( F = G^{-1}HG \) we see that \( F[r] = G^{-1}H[G(r)] = G^{-1}[G(s)] = [s], F[u] = G^{-1}H[G(u)] = G^{-1}[G(u)] = [u] \). \( \square \)

The above proposition proves the 2-transitivity of our group \( G \) under the assumption that both \( r_1 \) and \( s_1 \) are generators of \( \mathbb{F}_{q^n} \). The remaining part of this section is to prove the 2-transitivity of our group \( G \) without any assumption on generators. We will do this using induction steps to the type:

**Definition 2.5.12.** Let \( s = (s_1, \ldots, s_n) \in \mathbb{F}_{q^n}, m_i = [\mathbb{F}_q(s_i) : \mathbb{F}_q] \) and \( \text{lcm}(m_1, m_2, \ldots, m_n) = m \), so that \( s \in \mathbb{F}_{q^n} \). Then the type of \( s \) is a sequence \( m_s = (m_1, \ldots, m_n) \).

**Definition 2.5.13.** The type of \( s \) is said to be ordered type if the sequence \( m_s = (m_1, \ldots, m_n) \) is decreasing i.e., \( m_1 \geq m_2 \geq \cdots \geq m_n \).

Our induction step will involve assuming that we have proven 2-transitivity for all ordered types of a higher lexicographic order. The case that \( m_1 = m \) will then be solved by proposition 2.5.11.

The following lemma 2.5.14 will be helpful to prove the induction step, by making sure that some vector can be assumed to be in a different orbit from another vector without affecting the type of a vector.

**Lemma 2.5.14.** Let \( s, u \in X \) s.t. \( s = (s_1, \ldots, s_n) \), and \( u = (u_1, \ldots, u_n) \) are in different orbits, and suppose that \( s \) has ordered type \( m_s = (m_1, \ldots, m_n) \). If \( [s_1, \ldots, s_i, \ldots, s_n] = [(u_1, \ldots, u_i, \ldots, u_n)] \), then for all \( j \neq i \) with \( i, j \in \{1, 2, \ldots, n\} \) there exist a polynomial map \( f \in \mathbb{F}_q[X_1, \ldots, X_j, \ldots, X_n] \) such that \([s_1, \ldots, s_i, \ldots, s_j + f(s_1, \ldots, s_j, \ldots, s_n), \ldots, s_n] \neq [(u_1, \ldots, u_i, \ldots, u_j, \ldots, u_n)] \) and \([\mathbb{F}_q(s_j + f(s_1, \ldots, s_j, \ldots, s_n))] : \mathbb{F}_q = m_j \).

**Proof.** Since \([s_1, \ldots, s_i, \ldots, s_n] = [(u_1, \ldots, u_i, \ldots, u_n)] \) and \([s] \neq [u] \), there exist \( \phi \in \Delta \) such that \((s_1, \ldots, s_i, \ldots, s_n) = \phi(u_1, \ldots, u_i, \ldots, u_n) \) and \( s_i \neq \phi(s_i) \).
For any $j \neq i$ we have $[(s_1, \ldots, s_j, \ldots, s_n)] \neq [(u_1, \ldots, u_j, \ldots, u_n)]$. Fix $a = (s_1, \ldots, s_j, \ldots, s_n)$. Define a tame map

$$F = (X_1, \ldots, X_j + f_{a,1}(X_1, \ldots, \hat{X}_j, \ldots, X_n), \ldots, X_n)$$

where $f_{a,1}$ is as in lemma 2.2.2. Thus $F[s] = [(s_1, \ldots, s_{j-1}, s_j, s_{j+1}, \ldots, s_n)]$ and $F[u] = [u]$. We claim that $[(s_1, \ldots, s_i, \ldots, s_{j-1}, s_j, s_{j+1}, \ldots, s_n)] \neq [(u_1, \ldots, u_i, \ldots, u_{j-1}, u_j, u_{j+1}, \ldots, u_n)]$. For suppose that $[(s_1, \ldots, s_i, \ldots, s_{j-1}, s_j, s_{j+1}, \ldots, s_n)] = [(u_1, \ldots, u_i, \ldots, u_{j-1}, u_j, u_{j+1}, \ldots, u_n)]$. Combining it with $(s_1, \ldots, s_i, \ldots, s_n) = \phi(u_1, \ldots, u_i, \ldots, u_n)$ (in particular $s_k = \phi(u_k)$ for all $k \neq i$) we have $s_j = \phi(u_j)$ and $s_j + 1 = \phi(u_j)$, thus 1 = 0, a contradiction. Also $[F_q(s_j + f(s_1, \ldots, s_j, \ldots, s_n)) : F_q] = [F_q(s_j + 1) : F_q] = m_j$. □

**Lemma 2.5.15.** Let $r = (r_1, \ldots, r_n) \in X$ such that $m_i = [F_q(r_1) : F_q] \forall 1 \leq i \leq n$ with $m_1 \geq m_2 \geq \cdots \geq m_n$, with at least one strict inequality, then there exist $f(X_1, \ldots, X_{n-1}) \in F_q[X_1, \ldots, X_{n-1}]$ such that $[F_q(r_n + f(r_1, \ldots, r_{n-1})) : F_q] > m_n$.

**Proof.** For $f(X_1, \ldots, X_{n-1}) \in F_q[X_1, \ldots, X_{n-1}]$ set $\beta_f = r_n + f(r_1, \ldots, r_{n-1}) \in F_q^m$. Let

$$N = \{f(r_1, \ldots, r_{n-1}) : f(n) \in F_q[X_1, \ldots, X_{n-1}]\}$$

$$= \{f(r_1, \ldots, r_{n-1}) : f(n) \in F_q[X_1, \ldots, X_{n-1}]\}$$

$$= \#F_q[r_1, \ldots, r_{n-1}]$$

$$= \#F_q^{\text{lcm}(m_1, \ldots, m_{n-1})}.$$  

Since $m_1 \geq m_2 \geq \cdots \geq m_n$ has at least one strict inequality, if $w = \text{lcm}(m_1, \ldots, m_{n-1})$, then $m_n < w$. Thus

$$\#\{a \in F_q^m | [F_q(a) : F_q] \leq m_n\}$$

$$\leq 1 + q + \cdots + q^{m_n}$$

$$< q^w.$$  

Thus there exist some $f \in F_q[X_1, \ldots, X_{n-1}]$ such that $[F_q(\beta_f) : F_q] > m_n$. □

**Lemma 2.5.16.** Let $s, r, u \in X$ with $s = (s_1, \ldots, s_n), r = (r_1, \ldots, r_n)$ and $u = (u_1, \ldots, u_n)$ be in different orbits, suppose that $r$ has ordered type $m_r = (m_1, \ldots, m_n)$. Suppose $F_q(s_i) = F_q^m$ for some $i \in \{1, 2, \ldots, n\}$, then there exists $T \in \text{TA}_n(F_q)$ such that $T(s_1, \ldots, s_n) = (s_i, \ldots)$, and the ordered type of $r$ remains unchanged under the map $T$.

**Proof.** If $i = 1$, then $T = (X_1, X_2, \ldots, X_n)$ identity map. So we can suppose $i \in \{2, 3, \ldots, n\}$. We will give the prove of this lemma in two cases.

**Case 1.** $[(s_1, \ldots, s_n)] = [(s_2, \ldots, s_n)]$.

This implies that $s_i \in r_i$ which means that $F_q(r_i) = F_q^m$. Since $r$ has ordered type $m_r = [F_q(r_i) : F_q] = m$ and so the orderd type of $r$ becomes $m_1 = m_2 = \cdots = m_1 = m = m_{i+1} = \cdots \geq m_n$. Taking the map $T = (X_1, X_2, \ldots, X_{l-1}, X_1, X_{l+1}, \ldots, X_n)$ will not change the ordered type of $r$ and $T(s_1, \ldots, s_n) = (s_i, s_2, \ldots, s_{i-1}, s_1, s_{i+1}, \ldots, s_n)$.
Case 2. \( [(r_2, \ldots, r_n)] \neq [(s_2, \ldots, s_n)] \).

Fix \( a = (s_2, \ldots, s_n) \). Define \( T = (X_1 + f_{a,s_1 - s_1}(X_2, \ldots, X_n), X_2, \ldots, X_n) \)
where \( f_{a,s_1 - s_1} \) is as in lemma 2.2.2 (Notice that since \( s_i \) generates \( \mathbb{F}_q^m \), we can indeed apply this lemma.) Hence \( T(s) = (s_1, s_2, \ldots, s_i - 1, s_i, s_{i+1}, \ldots, s_n) \)
and \( T(r) = r \), which proves the lemma.

Lemma 2.5.17. Let \( r, s, u \in X \) with \( s = (s_1, \ldots, s_n) \), \( r = (r_1, \ldots, r_n) \) and \( u = (u_1, \ldots, u_n) \) be in different orbits with \( \mathbb{F}_q(s_1) = \mathbb{F}_q^{m_1} \), then there exists \( F \in \text{TA}_n(\mathbb{F}_q) \) such that \( F([r]) = [s] \) and \( F([u]) = [u] \).

Proof. We will prove this lemma using mathematical induction on the ordered type of \( r \). Our induction step will involve assuming that we have proven the lemma (2-transitivity) for all ordered types \( \tilde{m}_r = (\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_n) \) of a higher lexicographic order.

We may reorder and rename \( s_1, s_2, \ldots, s_n \) and \( r_1, r_2, \ldots, r_n \) such that \( r_1, r_2, \ldots, r_n \)
is of ordered type \( \tilde{m}_r = (m_1, m_2, \ldots, m_n) \) and \( s_i \) is generator of field \( \mathbb{F}_q^{m_i} \) (i.e. \( s_i \) is moved to the \( i \)-th position). Then by lemma 2.5.16 there exist a tame map \( T \in \text{TA}_n(\mathbb{F}_q) \) such that \( T(s_1, s_2, \ldots, s_n) = (s_i, \ldots) \) and the ordered type of \( r_1, r_2, \ldots, r_n \) remains unchanged under \( T \). Thus the case \( m_1 = m \) is done by proposition 2.5.11. This is the initial induction case.

We will now formulate the second step of induction involving the induction hypothesis. Define the tame map \( G := (X_1, X_2, \ldots, X_n + f(X_1, X_2, \ldots, X_{n-1})) \),
where \( f \in \mathbb{F}_q(X_1, X_2, \ldots, X_{n-1}) \) is s.t. \( m_n + k = [\mathbb{F}_q(\beta) : \mathbb{F}_q] \) by lemma 2.5.15 for some \( k \geq 1 \), where \( r_n + f(r_1, r_2, \ldots, r_{n-1}) = \beta \). Fix \( a = (u_1, \ldots, u_{n-1}) \).

Define a tame map \( H_f := (X_1, X_2, \ldots, X_n + h_{a, f(a)}(X_1, \ldots, X_{n-1})) \) where \( h_{a, f(a)} \) is as in lemma 2.2.2. Define \( G_1 = H_f \circ G \).

Case 1 Suppose \( [(r_1, \ldots, r_{n-1})] \neq [(u_1, \ldots, u_{n-1})] \). We compute \( G_1([r]) = G([r]) = [(r_1, r_2, \ldots, r_{n-1}, \beta)] \) and

\[
G_1([u]) = H_f \circ G((u_1, u_2, \ldots, u_n)) = H_f((u_1, u_2, \ldots, u_{n-1}, u_n + f(u_1, u_2, \ldots, u_{n-1})) = [(u_1, u_2, \ldots, u_{n-1}, u_n + f(u_1, u_2, \ldots, u_{n-1}) - f(u_1, u_2, \ldots, u_{n-1}))]
= [(u_1, u_2, \ldots, u_{n-1})].
\]

Rearrange \( r_1, r_2, \ldots, r_{n-1}, \beta \) by a swap map \( G_2 \) to get its ordered type \( \tilde{m}_r = (\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_n) \), where \( \tilde{m}_r \geq_{\text{lex}} \tilde{m}_r \). Then by the induction argument there exist a tame map \( G_3 \) s.t. \( G_3(G_2G_1([r])) = [s] \) and \( G_3G_2G_1([u]) = [u] \), hence \( F = G_3G_2G_1 \).

Case 2.

Now suppose that the elements \( r \) and \( u \) are such that \( [(r_1, \ldots, r_{n-1})] = [(u_1, \ldots, u_{n-1})] \). Then by lemma 2.5.14 we can find a tame map \( F_1 \) mapping \( [r] \) to \( [\tilde{r}_1, \ldots, \tilde{r}_n] \) and \( [u] \) to \( [\tilde{u}] \) such that \( [\tilde{r}_1, \ldots, \tilde{r}_{n-1}] \neq [(u_1, \ldots, u_{n-1})] \) and \( \mathbb{F}_q(\tilde{r}_i) : \mathbb{F}_q = m_i \) for all \( 1 \leq i \leq n \) (i.e., \( r \) and \( \tilde{r}_1, \ldots, \tilde{r}_n \) has same ordered type). Now by applying the case 1 of this lemma we can find a tame map \( F_2 \) such that \( F_2F_1([r]) = [s] \) and \( F_2F_1([u]) = [u] \), hence \( F = F_2F_1 \) is our required map.

Proposition 2.5.18. Let \( s, r, u \in X \) s.t. \( s = (s_1, \ldots, s_n) \), \( r = (r_1, \ldots, r_n) \),
and \( u = (u_1, \ldots, u_n) \) be in different orbits then there exist \( F \in \text{TA}_n(\mathbb{F}_q) \) s.t.
\( F([r]) = [s] \) and \( F([u]) = [u] \).
2.6. The case when \( m \) is a prime integer

Theorem 2.5.1 shows that \(
\Alt(\bar{\mathcal{X}}) \subseteq \mathcal{G}
\) for \( n \geq 3 \). In general it is difficult to describe the group \( \mathcal{G} \) exactly. But for some particular cases we are able to compute \( \mathcal{G} \) and show which of the two possibilities (alternating or symmetric) it is. In this section we assume that \( m \) is a prime integer. We will prove the following proposition:

**Theorem 2.6.1.** Let \( m, p \) be prime integers, \( q = p^l : l \geq 1 \) and \( n \geq 3 \), then \( \mathcal{G} = \Sym(\bar{\mathcal{X}}) \) if \( q \equiv 3, 7 \mod 8 \) with \( m = 2 \) and \( \mathcal{G} = \Alt(\bar{\mathcal{X}}) \) for all other \( q \) and \( m \).

We will postpone the proof of this proposition to the end of this section. We first prove some lemmas that we need.

**Lemma 2.6.2.** Let \( m, p \) be prime integers, \( q = p^l : l \geq 1 \). Let \( F_2 := (X_2, X_1, X_3, \ldots, X_n) \) then \( \pi_{qm}(F_2) \in \mathcal{G} \) is an odd permutation for \( q \equiv 3, 7 \mod 8 \) with \( m = 2 \) and is an even permutation for all other \( m \) and \( q \).

**Proof.** To determine the sign of the permutation \( \pi_{qm}(F_2) \) we need to count 2-cycles in the decomposition of \( \pi_{qm}(F_2) \) in transpositions. For this, first we will see how many orbits \( F_2 \) fixes and then subtract this number from total number of orbits. In this way we will get the total number of orbits moved by \( F_2 \). Dividing this number by 2 gives us the number of 2-cycles in \( \pi_{qm}(F_2) \).

To count the number of orbits fixed by \( F_2 \), consider \( [r] = [F_2(r)] \) for some \( r := (r_1, r_2, \ldots, r_n) \in \bar{\mathcal{X}} \). Then \( r = \phi(F_2(r)) \) and in particular \( r_1 = \phi(r_2) \), \( r_2 = \phi(r_1) \), \( r_3 = \phi(r_3) \), \ldots, \( r_n = \phi(r_n) \) for all \( \phi \in \Delta \). For \( \phi = \text{id} \), we have \( r_1 = r_2 \) and \( r_3, r_4, \ldots, r_n \) arbitrary. These are \( q^{m(n-1)} - q^{n-1} \) points. If \( \phi \neq \text{id} \), we have \( r_1 = \phi^2(r_1), r_2 = \phi^2(r_2), r_3 = \phi(r_3), \ldots, r_n = \phi(r_n) \) and so \( r_1, r_2, r_3, \ldots, r_n \in \mathbb{F}_q \) except for \( m = 2 \). When \( m = 2 \) we have \( r_1 = \phi(r_2) \) arbitrary and so \( r_1, r_2, r_3, \ldots, r_n \in \mathbb{F}_q \). Thus the case \( \phi \neq \text{id} \) gives no point for \( m \neq 2 \) and \((q^2 - q)q^{n-2} \) points satisfy \([r] = [F_2(r)] \) for \( m = 2 \).

When counting the number of points which satisfy \([r] = [F_2(r)] \), we get different results for the cases \( m \neq 2 \) and \( m = 2 \), so we distinguish these cases.

**Case 1** Let \( m \neq 2 \). In this case the number of points moved by \( F_2 = (X_2, X_1, X_3, \ldots, X_n) \) is \#\( \mathcal{X} \)\( - (q^{m(n-1)} - q^{n-1}) \). Thus the number of orbits moved by \( F_2 \) is \( (q^{mn} - q^n) - (q^{m(n-1)} - q^{n-1}) \). So the number of 2-cycles in this permutation is \( \frac{(q^{mn} - q^n) - (q^{m(n-1)} - q^{n-1})}{2m} \).
Let \( Q = (q^{mn} - q^n) - (q^{m(n-1)} - q^{n-1}) \). Since \( q^n \equiv q \mod m \), it follows that \( Q \equiv 0 \mod m \). Also it is trivial to check \( Q \equiv 0 \mod 4 \), hence \( Q \equiv 0 \mod 4m \). Thus \( \pi_{q^n}(F_2) \) is even.

**Case 2** Let \( m = 2 \). So the number of points moved by \( F_2 = (X_2, X_1, \ldots, X_n) \) is \( \#X - (q^{2(n-1)} - q^{n-1}) - (q^n - q)\). Thus \( \pi_{q^n}(aX_2, aX_1, \ldots, aX_n) \) is \( 2^{n-1} - 2q^{n-1} + 2q^n - 2q^{2(n-1)} \). The number of points moved by \( F \) is \( q^{2n} - q^{2(n-1)} - 2q^n + 2q^{n-1} \). This shows \( \pi_{q^n}(F_2) \) is odd for \( m = 2 \) and is an even permutation for all other \( m \).

**Lemma 2.6.3.** Let \( p, q \) be prime integers, \( q = p^l : l \geq 1 \) and \( \frac{q-1}{2} \not\equiv 2 \mod 8 \). Let \( F_1 := (aX_1, X_2, \ldots, X_n) : a \in (\mathbb{F}_q)^* \). Then \( \pi_{q^n}(F_1) \in \mathcal{G} \) is an odd permutation for \( q = 3, 7 \mod 8 \) and is an even permutation for all other \( m \) and \( q \).

**Proof.** **Case 1** Let \( q = 2l : l \geq 1 \). Then \( \text{sign}(F_1) = \text{sign}(F_1^{q-1}) = \text{sign}(a^{q-1}X_1, X_2, \ldots, X_n) = \text{sign}(X_1, X_2, \ldots, X_n) \). This shows \( \pi_{q^n}(F_1) \) is an even permutation in this case.

**Case 2** Let \( \frac{q-1}{2} \) be an odd integer. Then \( \text{sign}(F_1) = \text{sign}(F_1^{\frac{q-1}{2}}) \). Thus it is sufficient to consider \( F_1 := F_1^{\frac{q-1}{2}} = (-X_1, X_2, \ldots, X_n) \) instead of \( F_1 \) to check its sign.

To see the sign of permutation \( \pi_{q^n}(F_1) \) we will proceed similar to lemma 2.6.2. First we will see how many orbits \( F_1 \) fixes and then subtract this number from the total number of orbits. In this way we will get the total number of orbits moved by \( F_1 \). Dividing this number by 2 gives us the number of 2-cycles in \( \pi_{q^n}(F_2) \).

To count the number of orbits fixed by \( F_1 \), consider \([r] = [F_1(r)] \) for \( r := (r_1, r_2, \ldots, r_n) \in X \). Then \( F_1(r) = \phi(r) \) and in particular \( -r_1 = \phi(r_1) \), \( r_2 = \phi(r_2), \ldots, r_n = \phi(r_n) \) for all \( \phi \in \Delta \). For \( \phi = id \), we have \( r_1 = 0 \) and \( r_2, r_3, \ldots, r_n \in X \) arbitrary.

This gives \( q^{m(n-1)} - q^{n-1} \) points fixed by \( F_1 \). For \( \phi \neq id \), we have \( -r_1 = (r_1)^{q-1} \) for some integer \( i \) and \( r_2, r_3, \ldots, r_n \in \mathbb{F}_q \). For \( r_1^{q-1} = -1 \) and \( r_2, r_3, \ldots, r_n \in \mathbb{F}_q \). Now we check how many solutions do the equations \( r_1^{q-1} = -1 : 1 \leq i < m \) have in \((\mathbb{F}_q^m) \setminus (\mathbb{F}_q)\).

Let \( \alpha \) be the generator of \((\mathbb{F}_q^m)^*\) and let \( r_1 = \alpha^{\mu_k} \) satisfy \( r_1^{q-1} = -1 \) for some \( \mu_k \in \mathbb{Z} \). This gives \( \alpha^{\mu_k} = -1 \). Comparing powers we get \( \mu_k = \frac{q^{m-1} - 1}{(q^{m-1})} : k \in \mathbb{Z} \). We know \( i|m \) if and only if \( q^{m-1} | q^m - 1 \).

As \( k \) is prime, \( q^m - 1 \) does not divide \( q^m - 1 \). Hence we have no solution for \( r_1^{q-1} = -1 \) when \( 1 < i < m \). For \( i = 1 \), we can write \( \mu_k = \frac{q^{m-1} + q^{m-2} + \ldots + q}{2} + k(q^{m-1} + q^{m-2} + \ldots + 1) \). In this case \( \mu_k \not\in \mathbb{Z} \) if \( m \) is odd prime and \( \mu_k \in \mathbb{Z} \) if \( m = 2 \). The later case \( m = 2 \) gives us \((q - 1)\) solutions \( r_1 = \alpha^{qk} \), satisfying \( r_1^{q-1} = -1 \). Thus for \( \phi \neq id \), we have \( (q-1)q^{m-1} \) points fixed by \( F_1 \) when \( m = 2 \) and no point is fixed by \( F_1 \) when \( m \) is odd prime.

For \( m \) an odd prime, the total number of points in \( X \) moved by \( F_1 \) is \((q^{mn} - q^n) - (q^{m(n-1)} - q^{n-1}) := Q \). Thus the number of orbits moved by \( F \) is \( \frac{Q}{m} \).
2.7. A bound on the index of $\pi_{q^m}(TA_n(\mathbb{F}_q))$ in $\pi_{q^m}(GA_n(\mathbb{F}_q))$

So the number of 2-cycles in this permutation is $\frac{Q_1}{2m}$. In this case $Q \equiv 0 \mod m$ and $Q \equiv 0 \mod 4$, thus $Q \equiv 0 \mod 4m$. Hence $\pi_{q^m}(F_1)$ is an even permutation in this case.

For $m = 2$, the total number of points in $X$ moved by $F_1$ is $(q^m - q^n) - (q^{m-1} - q^{n-1}) - q^n + q^{n-1} = q^2 - q^{2n-1} - 2q^n + 2q^{n-1} := Q_1$. Thus the number of orbits moved by $F$ is $\frac{Q_1}{2^2}$. So the number of 2-cycles in this permutation is $\frac{Q_1}{2^2}$. In this case

$$Q_1 \mod 8 = \begin{cases} -4 & \text{if } q \equiv 3, 7 \mod 8 \\ 0 & \text{if } q \equiv 1, 5 \mod 8 \end{cases}.$$ 

Thus $F_1$ induces odd permutation for $q \equiv 3, 7 \mod 8$ with $m = 2$ and even permutation for all other values of $q$ and $m$.

\[\text{Lemma 2.6.4.}\] Let $F = (X_1 + f(X_2, X_3, \ldots, X_n), X_2, \ldots, X_n)$ then $\pi_{q^m}(F) \in G$ is an even permutation.

\[\text{Proof.}\] Define $f_{(a_2, a_3, \ldots, a_n)} \in \mathbb{F}_q[X_2, X_3, \ldots, X_n]$ such that for any $\beta \in (\mathbb{F}_q)^{n-1}\setminus(\mathbb{F}_q)^n$ $\{f_{(a_2, a_3, \ldots, a_n)}(\beta) = \begin{cases} 1 & \text{if } \beta = (a_2, \ldots, a_n) \\ 0 & \text{if } \beta \neq (a_2, \ldots, a_n) \end{cases}.$

Define $\eta = (X_1 + f_{(a_2, a_3, \ldots, a_n)}, X_2, \ldots, X_n).$ Then $\eta(a, a_2, a_3, \ldots, a_n) = (a + 1, a_2, a_3, \ldots, a_n) : \eta^p = id$, and $\eta(\beta_1, \beta) = 0$ for any $\beta \neq (a_2, a_3, \ldots, a_n), (\beta_1, \beta) \in X$. Thus the order of $\eta$ is $p$. Hence the permutation induced by $\eta$ is even. Since the maps of the type $\eta$ work as generators for shears, $\pi_{q^m}(F) \in G$ is even.

\[\text{Proof.}\] (of the main theorem 2.6.1) The group $G$ contains the group $Alt(\mathcal{X})$ by the theorem 2.5.1. Since $TA_n(\mathbb{F}_q)$ is generated by the maps of the form $F_1, F_2$ and $F$ as in lemmas 2.6.2, 2.6.3, 2.6.4 which are even except when $q \equiv 3, 7 \mod 8$ and $m = 2$ in which case $F_1, F_2$ are odd and $F$ is even, hence we have our desired result.

\[\text{2.7 A bound on the index of}\] $\pi_{q^m}(TA_n(\mathbb{F}_q))$ in $\pi_{q^m}(GA_n(\mathbb{F}_q))$

Theorem 2.5.1 tells us that the action of $TA_n(\mathbb{F}_q)$, if restricted to $\mathcal{X}$, contains the action of $Alt(\mathcal{X})$. However, our goal is to understand $\pi_{q^m}(TA_n(\mathbb{F}_q))$, and in particular compare it with $\pi_{q^m}(MA_n(\mathbb{F}_q)) \cap \text{Perm}(\mathbb{F}_q^n)$. Define

$$M_n^m[\mathbb{F}_q] := \pi_{q^m}(MA_n(\mathbb{F}_q)) \cap \text{Perm}(\mathbb{F}_q^n).$$

The following theorem estimates how far the group $\pi_{q^m}(TA_n(\mathbb{F}_q))$ is from $M_n^m[\mathbb{F}_q]$.

\[\text{Theorem 2.7.1.}\] We have the following bound on index

$$[M_n^m[\mathbb{F}_q] : \pi_{q^m}(TA_n(\mathbb{F}_q))] \leq 2^{\sigma_0(m)} \prod_{d | m} d,$$

where $\sigma_0(m)$ is the total number of divisors of $m$. 

We will postpone the proof of this theorem to the end of this section. The remaining part of this section is devoted towards the preparation of the proof of theorem 2.7.1.

**Definition 2.7.2.** If \( S \subseteq \mathbb{F}_q^n \), define \( TA_n(\mathbb{F}_q; S) \) as the set of elements in \( TA_n(\mathbb{F}_q) \) which are the identity on \( S \). Similarly, if \( S = \Delta S \) (i.e. it is a union of orbits) then define \( \pi_S : MA_n(\mathbb{F}_q) \rightarrow \text{Maps}(S, S) \) and thus also \( \pi_S(TA_n(\mathbb{F}_q)) \). We define \( \pi_S : TA_n(\mathbb{F}_q; T) \rightarrow \text{Maps}(S, S) \) as a permutation on \( S \) which fix \( L \) where \( L \subset S \). \( \pi_S(TA_n(\mathbb{F}_q; T)) \) etc.

Let \( L \) be the union of all orbits of \( \Delta \) acting on \( \mathbb{F}_q^n \) of order a strict divisor of \( m \); i.e. \( L \) contains all orbits of size \( d \) where \( d \mid m \) but not the ones of size \( m \). Then we have \( \pi_L(TA_n(\mathbb{F}_q)) \) as well as \( \pi_q^m(TA_n(\mathbb{F}_q; L)) \). The first group restricts to permutations of \( L \), the second consist permutations on \( \mathbb{F}_q^n \) which fix \( L \). Is there some way to glue these to get \( \pi_q^m(TA_n(\mathbb{F}_q)) \)? Well, only in part: \( \pi_q^m(TA_n(\mathbb{F}_q)) \) is not a semidirect product of the other two, but their sizes compare:

Recalling \( \chi_d \) from the definition 2.4.2 we have

**Lemma 2.7.3.**

\[
\#\pi_q^m(TA_n(\mathbb{F}_q)) = \#\pi_{\chi_1}(TA_n(\mathbb{F}_q)) \cdot \#\pi_{\chi_1}(TA_n(\mathbb{F}_q; \chi_1)),
\]

where \( \chi_1 \) is defined in def. 2.4.2.

**Proof.** Pick a representant system \( R \) in \( TA_n(\mathbb{F}_q) \) of \( \pi_{\chi_1}(TA_n(\mathbb{F}_q)) \). Then for each \( \pi_q^m(F) \in \pi_q^m(TA_n(\mathbb{F}_q)) \) there exists a unique \( G \in R \) such that \( \pi_q^m(GF) \in \pi_q^m(TA_n(\mathbb{F}_q; \chi_1)) \). Thus, \( \#R \cdot \#\pi_q^m(TA_n(\mathbb{F}_q; \chi_1)) = \#\pi_q^m(TA_n(\mathbb{F}_q)) \).

The same proof works too to show

\[
\#\pi_q^m(TA_n(\mathbb{F}_q; \chi_1)) = \#\pi_{\chi_2}(TA_n(\mathbb{F}_q; \chi_1)) \cdot \#\pi_q^m(TA_n(\mathbb{F}_q; \chi_1 \cup \chi_2)).
\]

Meaning, we can decompose \( \#\pi_q^m(TA_n(\mathbb{F}_q)) \) into smaller parts: let \( d_0 := 1, d_1, d_2, \ldots, d_{m-1}, d_m := m \) be the increasing list of divisors of \( m \). Let \( Q_{d_j} = \pi_{\chi_{d_j}}(TA_n(\mathbb{F}_q; \bigcup_{d < d_j, d \mid m} \chi_{d})) \) for all \( 0 \leq j \leq m - 1 \) and \( Q_{d_m} = \pi_q^m(TA_n(\mathbb{F}_q; L)) \) where \( L \) be the union of orbits of size \( d \mid m, d \neq m \), then

\[
\#\pi_q^m(TA_n(\mathbb{F}_q)) = \#Q_{d_0} \cdot \#Q_{d_1} \cdot \ldots \cdot \#Q_{d_m}.
\]

The same construction will work for the group \( \mathcal{M}_n^m(\mathbb{F}_q) \). Meaning, we can decompose \( \#\mathcal{M}_n^m(\mathbb{F}_q) \) into smaller parts:

\[
\#\mathcal{M}_n^m(\mathbb{F}_q) = \#G_{d_0} \cdot \#G_{d_1} \cdot \ldots \cdot \#G_{d_m},
\]

where \( G_{d_i} \) are defined in corollary 2.4.3.

For each divisor \( d \) of \( m \), let \( \{O_i | 1 \leq i \leq r_d \} \) be the set of orbits of size \( d \) and choose \( \alpha_i \in O_i \). Define two subgroups of \( Q_d \) by \( N_d := \{m \in Q_d | m(O_i) = O_i \} \) and \( R_d := \{m \in Q_d | m(\alpha_1, \ldots, \alpha_{r_d}) \subseteq \{\alpha_1, \ldots, \alpha_{r_d}\} \} \), where \( d \) is any divisor of \( m \) and \( \alpha_i \in O_i \) be the fixed representatives of orbits \( O_i \) of size \( d \). The group \( N_d \) moves elements inside the orbits \( O_i \) by keeping orbits \( O_i \) fixed for all \( i \) and the group \( R_d \) moves only orbits to orbits.
2.7. A bound on the index of $\pi_{q^m}(TA_n(F_q))$ in $\pi_{q^m}(GA_n(F_q))$

By definition $N_d = \text{Ker}\{Q_d \to \pi_{\tilde{X}_d}(TA_n(F_q; \bigcup_{i<d,i|m} X_i)\}$ and by theorem 2.5.1 $\text{Alt}(\alpha_1, \ldots, \alpha_{r_d}) \subseteq R_d \subseteq \text{Perm}\{\alpha_1, \ldots, \alpha_{r_d}\}$. Hence the group $N_d$ is normal in group $Q_d$.

**Proposition 2.7.4.** The group $Q_d$ can be represented as a semidirect product of groups $N_d$ and $R_d$.

**Proof.** Since $Q_d = \pi_{\tilde{X}_d}(TA_n(F_q; \bigcup_{i<d,i|m} X_i))$, if $\tau \in Q_d$ then $\tau(\alpha_i) = \phi^\mu_i(\alpha_{\sigma(i)}$) where $\sigma \in \text{Perm}(r_d)$, $\phi$ is generator for $\text{Gal}(F_{q^m} : F_q)$ and $\mu_i$ is an integer. Then we can find $m_0 \in N_d$ and $m_1 \in R_d$ such that $m_0(\alpha_i) = \phi^\mu_i(\alpha_i)$ and $m_1(\alpha_i) = \alpha_{\sigma(i)}$ and $m_1 m_0(\alpha_i) = m_1(\phi^\mu_i(\alpha_i) = \phi^\mu_i(m_1(\alpha_i)) = \phi^\mu_i(\alpha_{\sigma(i)}).$ Thus $R_d N_d = Q_d$. That $N_d \cap R_d = \{id\}$ is clear by definition of $N_d$ and $R_d$. Since $N_d$ is normal in $Q_d$, all conditions semidirect product are satisfied. \[ \square \]

**Corollary 2.7.5.** (of the lemma 2.5.6) Let $\{\alpha_i \in O_i\}$ be representants of the orbits of size $d$. For each $i \neq j$, there exist a map $\zeta \in N_d$ such that $\zeta(\alpha_i) = \phi^{-1}(\alpha_i)$, $\zeta(\alpha_j) = \phi(\alpha_j)$ for all $\phi \in \Delta$, and $\zeta(\alpha_k) = \alpha_k$ for all $k \neq i, j$.

**Proof.** Define $A := (-1,0,\ldots,0,t)$, $B := (0,-1,0,\ldots,0,t)$, $C := (0,0,\ldots,0,t)$, where $t$ is a generator of the multiplicative group $(F_{q^d})^*$. Let

$$s_3 = (X_1, X_2, X_3 + f_3(X_2, X_n), X_4, \ldots, X_n),$$

$$s_2 = (X_1, X_2, \ldots, X_{n-1}, X_n + f_2(X_2, X_3),$$

$$s_1 = (X_1, X_2, X_3 + f_1(X_2, X_n), X_4, \ldots, X_n),$$

$$f_3(a_2, a_n) = \begin{cases} t & \text{if } (a_2, a_n) = (0,t) \\ 0 & \text{elsewhere if } [(a_2, a_n)] \neq [(0,t)] \end{cases},$$

$$f_2(a_2, a_3) = \begin{cases} \phi(t) - t & \text{if } (a_2, a_3) = (0,t) \\ 0 & \text{elsewhere if } [(a_2, a_3)] \neq [(0,t)] \end{cases},$$

$$f_1(a_2, a_n) = \begin{cases} -t & \text{if } (a_2, a_n) = (0, \phi(t)) \\ 0 & \text{elsewhere if } [(a_2, a_n)] \neq [(0, \phi(t))] \end{cases},$$

and set $s = s_1 s_2 s_3$. Define $\tilde{w} = \bar{s}^{-1} s^{-1} l^{-1} \bar{s} s l$ where $s, l$ are maps as defined in lemma 2.5.6.

Note that

$$s_3^{-1} = (X_1, X_2, X_3 - f_3(X_2, X_n), X_4, \ldots, X_n),$$

$$s_2^{-1} = (X_1, X_2, \ldots, X_{n-1}, X_n - f_2(X_2, X_3),$$

$$s_1^{-1} = (X_1, X_2, X_3 - f_1(X_2, X_n), X_4, \ldots, X_n).$$

Thus $\tilde{w}(A) = \phi(B)$, $\tilde{w}(B) = C$ and $\tilde{w}(C) = \phi^{-1}(A)$. Define $\eta := \tilde{w}^{-1}w$, where $w$ is as defined in lemma 2.5.6. Thus $\eta(A) = \tilde{w}^{-1}w(A) = \tilde{w}^{-1}(B) = \phi^{-1}(A), \eta(B) = \tilde{w}^{-1}w(B) = \tilde{w}^{-1}(C) = B$ and $\eta(C) = \tilde{w}^{-1}w(C) = \tilde{w}^{-1}(A) = \phi(C)$.

Consider $L_1 = \{[(a_1, 0,0,\ldots,0,a_n)]|a_n \in [t] \text{ and } a_1 \in F_{q^d}\}$ and $L_2 = \{[(0,a_2,0,\ldots,0,a_n)]|a_2 \in F_{q^d}$ and $a_n \in [t]\}$, where $L_1, L_2$ are subsets of $\tilde{X}_d$ and $[t] = \{\phi(t) : \phi \in \text{Gal}(F_{q^d} : F_q)\}$. Similar to lemma 2.5.6, $s$ permutes only the set $L_1$ and $l$ permutes only the set $L_2$. Then $sl$ (and hence $s^{-1}l^{-1}$) acts trivially on $\tilde{X}_d \setminus (L_1 \cup L_2)$ and nontrivially only on a subset of $L_1 \cup L_2$.\[ \square \]
Thus the map \( \hat{w} \) acts trivially on \( \hat{X}_d \setminus (L_1 \cup L_2) \) and nontrivially only on a subset of \( L_1 \cup L_2 \). Since the map \( w \) fixes all orbits except \([A], [B]\) and \([C]\), hence the map \( \hat{w} \) can only acts nontrivially on orbits \([A], [B]\) and \([C]\) due to definition of \( \hat{s} \).

Since the group \( Q_d \) contains the alternating permutation group on \( \{\alpha_1, \ldots, \alpha_{r_d}\} \) by theorem 2.5.1, it is 2-transitive. Thus there exist a map \( \xi \) such that \( \xi(A) = \alpha_i \) and \( \xi(C) = \alpha_j \). Hence \( \xi = \xi \eta \xi^{-1} \) is our required map. \( \square \)

**Corollary 2.7.6.** The group \( N_d \) contains a group isomorphic to \( \{(a_1, a_2, \ldots, a_{r_d}) \in (\mathbb{Z}/\mathbb{Z})^{r_d} | a_1 + a_2 + \cdots + a_{r_d} = 0\} \).

**Proof.** Let \( \{\alpha_i\} \) be representatives for the orbits \( \{O_i\} \) of order \( d \) and \( \phi \) a generator for \( \Delta \). Then for any \( \sigma \in N_d \) we have \( \sigma(\alpha_i) = \phi^{n_i}(\alpha_i) \) where \( a_1 + a_2 + \cdots + a_{r_d} = 0 \) (corollary 2.7.5). Since \( \text{Gal}(\mathbb{F}_{q^d} : \mathbb{F}_q) \cong (\mathbb{Z}/d\mathbb{Z}) \), hence \( \{(a_1, a_2, \ldots, a_{r_d}) \in (\mathbb{Z}/\mathbb{Z})^{r_d} | a_1 + a_2 + \cdots + a_{r_d} = 0\} \subseteq N_d \) as an isomorphic subgroup. \( \square \)

**Lemma 2.7.7.** We have the following bound on the index

\[ [G_d : Q_d] \leq 2d. \]

**Proof.** We know by corollary 2.4.3

\[ G_d \cong (\mathbb{Z}/d\mathbb{Z})^{r_d} \times (\text{Perm}(r_d)) \]

and by proposition 2.7.4

\[ Q_d \cong N_d \rtimes R_d. \]

Also by corollary 2.7.5

\[ \{(a_1, a_2, \ldots, a_{r_d}) \in (\mathbb{Z}/\mathbb{Z})^{r_d} | a_1 + a_2 + \cdots + a_{r_d} = 0\} \subseteq N_d \]

and by theorem 2.5.1

\[ \text{Alt}\{\alpha_1, \ldots, \alpha_{r_d}\} \subseteq R_d \subseteq \text{Perm}\{\alpha_1, \ldots, \alpha_{r_d}\}. \]

This gives \([ (\mathbb{Z}/d\mathbb{Z})^{r_d} : N_d ] \leq d, [\text{Perm}(r_d) : R_d] \leq 2, \text{ and hence we have } [G_d : Q_d] \leq 2d. \]

**Proof.** (of main theorem 2.7.1) Since

\[ \#\pi_{q^m}(\text{TA}_n(\mathbb{F}_q)) = \#Q_{d_0} \cdot \#Q_{d_1} \cdots \#Q_{d_m}, \]

\[ \#\mathcal{M}_n^\text{m}(\mathbb{F}_q) = \#G_{d_0} \cdot \#G_{d_1} \cdots \#G_{d_m}. \]

By lemma 2.7.7 we have the result. \( \square \)

**Corollary 2.7.8.** (of theorem 2.6.1, and lemma 2.7.7)

For \( m = 2, q \equiv 3, 7 \mod 8 \) we have

\[ [\mathcal{M}_n^2(\mathbb{F}_q) : \pi_{q^2}(\text{TA}_n(\mathbb{F}_q))] \leq 2. \]

**Proof.** By theorem 2.6.1 we have \( R_d = \text{Perm}(r_d) \) and by using it in the proof of lemma 2.7.7 we can deduce that \([G_d : Q_d] \leq d, \text{ where } d = 1, 2 \) are the divisors of \( m = 2 \). Since \( \#\mathcal{M}_n^2(\mathbb{F}_q) = \#G_1 \cdot \#G_2 \) and \( \#\pi_{q^2}(\text{TA}_n(\mathbb{F}_q)) = \#Q_1 \cdot \#Q_2 \) we get the desired result. \( \square \)
Chapter 3

A new formulation of the Jacobian Conjecture in characteristic $p$

3.1 Introduction

The Jacobian Conjecture involve the condition $\det(Jac(F)) \in k^*$ on a polynomial map $F$, which itself implies many conditions on the coefficients of $F$. In characteristic $p$ examples shows that these conditions do not suffice to force a polynomial map to be invertible. In this chapter, we describe how to construct conjecturally sufficient conditions in characteristic $p$ for a polynomial map to be invertible. This provides an alternative to Adjamagbo’s formulation of the Jacobian Conjecture in characteristic $p$. We strengthen this formulation by investigating some special cases and by linking it to the regular Jacobian Conjecture in characteristic zero.

We define $\text{SA}_n(R) = \{ F \in \text{GA}_n(R) \mid \det(Jac(F)) = 1 \}$. Similarly, we define $\text{STA}_n(R) = \text{SA}_n(R) \cap \text{TA}_n(R)$ etc.

For each of these sets, we define $\text{MA}_d^n(R) = \{ F \in \text{MA}_n(R) \mid \text{deg}(F) \leq d \}$, $\text{GA}_d^n(R) = \text{GA}_n(R) \cap \text{MA}_d^n(R)$ etc.

We use the notation $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ if $\alpha \in \mathbb{N}^n$.

3.2 Initial considerations

Consider a generic polynomial automorphism of $k^2$ of degree 2, having as affine part the identity:

$$F = (x + a_1x^2 + a_2xy + a_3y^2, y + b_1x^2 + b_2xy + b_3y^2)$$

Then, in characteristic zero, the equation $1 = \det(Jac(F))$ yields several equations on the coefficients:

$$1 = \det(Jac(F))$$
$$= 1 + (2a_1 + b_2)x + (a_2 + 2b_3)y + (2a_1b_2 + 2a_2b_1)x^2 + (2b_2a_2 + 4a_1b_3 + 4a_3b_1)xy + (2a_2b_3 + 2a_3b_2)y^2$$
One of the equations is \(2a_1b_2 + 2a_2b_2 = 0\). In characteristic zero, this implies the equation \(a_1b_2 + a_2b_1 = 0\). Looking at it like this, it seems strange to exclude this latter equation in characteristic 2. Also, if we define the ideal 

\[ I = (2a_1 + b_2, a_2 + 2b_3, 2a_1b_2 + 2a_2b_1, 2b_2a_2 + 4a_1b_3 + 4a_3b_1, 2a_2b_3 + 2a_3b_2) \]

in the ring \(\mathbb{Q}[a_1, a_2, a_3, b_1, b_2, b_3]\), then any invertible polynomial map of degree 2 over \(\mathbb{Q}\) will have coefficients which satisfy every polynomial in \(I\). Even more, they satisfy every polynomial appearing in \(\text{rad}(I)\). Again, in the same vein as before, we can argue that every polynomial appearing in \(\text{rad}(I)\), should appear as polynomial in characteristic \(p\), also. Hence, in this way we can give some universal conditions which should be the equations which work in any characteristic.

This is essentially the formulation of the Jacobian Conjecture in characteristic \(p\) we introduce in the next section, but we have to use more formal language.

### 3.3 A new formulation of the Jacobian Conjecture in characteristic \(p\)

Given \(F = (F_1, \ldots, F_n) \in \text{MA}_n(R)\) where \(R\) is some ring, we can write \(F = \sum_{a \in \mathbb{N}^n} c_{i,a} x^a\). We can also make the infinitely generated ring \(C_R := \mathbb{R}[c_{i,a} \mid 1 \leq i \leq n, \alpha \in \mathbb{N}^n]\) where the \(c_{i,a}\) are variables and with \(\alpha = (\alpha_1, \ldots, \alpha_n)\) we set \(\max\{\alpha_j | c_{i,a} \neq 0\} = d\). One can now make the universal polynomial map of degree \(d \in \mathbb{N}\) by taking the polynomial map in \(\text{MA}_n(C_R)\) which has as coefficients the variables \(c_{i,a}\). Lets say that \(C_{R,d}\) is the finitely generated ring generated by the coefficients up to and including degree \(d\). (I.e. \(C_R\) is the union, or direct limit, of the rings \(\ldots \subset C_{R,d} \subset C_{R,d+1} \subset \ldots\))

**Definition 3.3.1.** Let \(F[d] \in \text{MA}_n(C_{Q,d})\) be the universal polynomial endomorphism of degree \(d\) having affine part equal to the identity. Computing \(\det \text{Jac}(F[d]) = 1\) yields a polynomial in \(x_1, \ldots, x_n\) having coefficients \(E_\alpha \in C_{Q,d}\). Define the ideal \(I_{Q,d} = (E_\alpha \mid \alpha \in \mathbb{N}^n)\) in \(C_{Q,d}\) generated by the conditions determined by the coefficients of the monomials in \(x_1, \ldots, x_n\) found in the formula \(\det \text{Jac}(F[d]) = 1\). We define the ideal \(I_{Q}\) in \(C_Q\) as the inverse limit of the canonical chain \(\ldots \rightarrow I_{Q,d+1} \rightarrow I_{Q,d} \rightarrow \ldots\), where we define the canonical map \(I_{d+1} \rightarrow I_d\) by setting to 0 the coefficients of monomials of degree \(d + 1\). It coincides with the conditions found in the coefficients of \(\det \text{Jac}(F[\infty])\) = 1, where \(F[\infty]\) has as components power series with universal coefficients.

**Definition 3.3.2.** We define \(J_{Z} := \text{rad}(I_{Q}) \cap C_Z\) as the “ideal of integer Keller conditions”. This ideal captures the universal conditions described in the previous section. If \(R\) is a ring, we define \(J_R := J_{Z} \otimes R\) as an ideal in the ring \(C_R\). It is the ideal in \(C_R\) generated by those same conditions (in characteristic zero) or by those conditions modulo \(p\) (in characteristic \(p\)). In particular, we define \(J_p := J_{Z} \otimes R\) as an ideal in \(C_{Z,p}\). Similarly we define \(J_{Z}^d := \text{rad}(I_{Q}) \cap C_{Z,d}\), \(J_R^d := J_{Z}^d \otimes R\) and \(J_p^d := J_{Z}^d \mod p\) where \(d = \deg(F)\).
Let $M_d$ be the number of variables in $F[d]$ (i.e. the dimension of the ring $\mathbb{C}_{R,d}$). We say that $v \in R^{M_d}$ satisfies $J_R^d$ if $f(v) = 0$ for all $f \in J^d_R$. We say that “$v \in R^{M_d}$ satisfies $J_R$” if $v \in R^{M_d}$ satisfies $J^d_R$.

We can identify $F \in \text{MA}_n(R)$ by the vector of coefficients $v(F)$ of $F$; in particular, if $F \in \text{MA}_n(R)$ we say that “$F$ satisfies $J_R (J^d_R)$” if $v(F)$ satisfies $J_R (J^d_R)$.

Throughout, we will write the elements of $J_R = J_{\mathbb{Z}} \otimes R$ by $\sum_i e_i h_i$ instead of $\sum_i e_i \otimes h_i$, where $e_i \in J_{\mathbb{Z}}$ and $h_i \in R$ for all $i$ (for simplicity, we will omit the tensor notation in this manuscript).

**Definition 3.3.3.** A polynomial map $F \in \text{MA}_n(R)$ is Keller map if $\det \text{Jac}(F) \in R^*$. We say that $F \in \text{MA}_n(R)$ is a strong Keller map if $F$ satisfies $J_R$ (or equivalently $F \in \text{MA}_n(R)$ is a strong Keller map if $F$ satisfies $J^d_R$ where $\deg(F) = d$). We denote the set of strong Keller maps by $\text{SKE}_n(R)$ and the set of Keller maps by $\text{KE}_n(R)$.

**Conjecture 3.3.4.** Jacobian conjecture over any field (in particular, in positive characteristic) $(JC(k, n))$ Let $k$ be a field (of characteristic $p$) and $F \in \text{MA}_n(k)$ be a strong Keller map. Then $F \in \text{GA}_n(k)$.

So, an alternative definition of $JC(k, n)$ is “$\text{SKE}_n(k) = \text{GA}_n(k)$”. We will use curly letter notation $\mathcal{JC}$ to represent Jacobian conjecture in characteristic $p$.

Of course, we still need to show that the above formulation coincides with the regular formulation in case the field is of characteristic zero. However, this will follow directly from lemma 3.4.3.

Note that we only defined the conjecture for fields of any characteristic, but with a slight modification one can define it for all domains (of any characteristic). However, we will stick with this formulation in this first encounter.

Before we will study the validity of this conjecture, we will introduce some facts and concepts we will use afterwards.

### 3.4 Basic facts

Some basic facts are mentioned in the following remark about the map $F \mod p$ for $F \in \text{MA}_n(\mathbb{Z})$. They are used in various places without mentioning.

**Remark 3.4.1.** Let $F \in \text{MA}_n(\mathbb{Z})$. Then

$$(\det \text{Jac}(F)) \mod p = \det(\text{Jac}(F) \mod p) = \det \text{Jac}(F \mod p)$$

In particular:

- $\det \text{Jac}(F) = 1 \mod p \iff \det \text{Jac}(F \mod p) = 1 \mod p$.

- If $F \in \text{MA}_n(\mathbb{Z})$ such that $F \mod p \in \text{SKE}_n(\mathbb{F}_p)$, then $\det \text{Jac}(F) = 1 + pH$ for some $H \in \text{MA}_n(\mathbb{Z})$.

- $(F \circ G) \mod p = (F \mod p) \circ (G \mod p)$, and $\det \text{Jac}(F \circ G) \mod p = \det \text{Jac}(F \mod p \circ G \mod p)$.
Remark 3.5.1. Let $F$ be an affine or triangular map having determinant Jacobian 1. If $c_\alpha x^\alpha$ is a generic monomial where $\alpha \in \mathbb{N}^n$ and $c_\alpha \in \mathbb{Z}$, then
\[
\frac{\partial c_\alpha x^\alpha}{\partial x_i} \mod p = \frac{\partial c_\alpha x^\alpha}{\partial x_i} \mod p
\]
which is true (just check the case where $p$ divides $c_\alpha$ or $p$ divides $\alpha_i$ separately).

\[\square\]

Lemma 3.4.2. Let $F \in \text{ME}_n(R)$. If $F$ satisfies the ideal $I_Q$ then it satisfies the ideal $J_Z$.

Proof. Consider $Q \in J_Z$. Note that $J_Z = \text{rad}(I_Q) \cap C_Z = \text{rad}(I_Q \cap C_Z)$ thus there exists $n \in \mathbb{Z}$ such that $Q^n \subseteq I_Q \cap C_Z \subseteq C_Z$. Assume $I_Q$ is generated by $\{e_i\}_{i \in \Omega}$, then $Q^n = \sum_i h_i e_i$ for $h_i \in C_Z$ for all $i$. Thus $Q^n(\nu(F)) = \sum_i h_i(\nu(F)) e_i(\nu(F)) = 0$ since $F$ satisfies $e_i \in I_Q$. Hence $Q(\nu(F)) = 0$ as $C_Z$ is integral domain.

\[\square\]

Lemma 3.4.3. Let $R$ be a ring with $\text{char}(R) = 0$, then $F \in \text{SKE}_n(R)$ if and only if $F \in \text{KE}_n(R)$.

Proof. Let $F \in \text{SK}E_n(R)$, then $\forall Q \in J_R$ we have $Q(\nu(F)) = 0$. Since $f \otimes 1 \in J_R$ for $f \in J_Z$ and $1 \in R$ it follows that $f(\nu(F)) = 0$ for all $f \in J_Z$. As $I_Q \cap C_Z \subseteq J_Z$, it follows that $f(\nu(F)) = 0$ for all $f \in I_Q \cap C_Z$. For any $e \in I_Q$ we can find $f \in I_Q \cap C_Z$ such that $e = \frac{f}{m}$ for some $m \in \mathbb{Z}$. Thus $e(\nu(F)) = 0$ for all $e \in I_Q$. Hence $F \in \text{KE}_n(R)$. Conversely suppose that $F$ is a Keller map, then $F$ satisfies $I_Q$. Thus by lemma 3.4.2 we have $e(\nu(F)) = 0$ for all $e \in J_Z$. Now for any $\sum_i e_i r_i \in J_R$ we have $\sum_i e_i r_i(\nu(F)) = \sum_i e_i(\nu(F)) r_i(\nu(F)) = 0$, where $r_i \in R$ and $e_i \in J_Z$ for all $i$. Thus $F$ is strong Keller map.

\[\square\]

Lemma 3.4.4. $\text{SKE}_n(k) \subset \text{SKE}_n(\hat{k})$ for any fields $k \subset \hat{k}$ of positive characteristic.

Proof. Let $F \in \text{SKE}_n(k)$. Consider $k_0$, the subfield of $k$ generated by the coefficients of $F$. Then $F \in \text{SKE}_n(k_0)$ and so $F$ satisfies the ideal $J_{k_0}$. Since $J_{k_0} \subset J_{\hat{k}}$, it is obvious that $q(\nu(F)) = 0$ for any $q \in J_{\hat{k}} \setminus J_{k_0}$. Thus $F$ satisfies the ideal $J_{\hat{k}}$ and so $F \in \text{SKE}_n(\hat{k})$.

\[\square\]

3.5 Two surjectivity conjectures

Given $F \in \text{GA}_n(\mathbb{Z})$ we can define $F \mod p$ for any prime $p$, yielding an element of $\text{MA}_n(\mathbb{F}_p)$. If we additionally assume that $p \not| \det(\text{Jac}(F))$ then $F \mod p \in \text{GA}_n(\mathbb{F}_p)$, even. This yields the natural map $\pi : \text{SA}_n(\mathbb{Z}) \rightarrow \text{SA}_n(\mathbb{F}_p)$. The following fact is not that difficult to prove:

Remark 3.5.1. $\pi(\text{STA}_n(\mathbb{Z})) = \text{STA}_n(\mathbb{F}_p)$.

The reason for this is that (1) any affine or triangular map having determinant Jacobian 1 has a preimage under $\pi$, (2) any tame automorphism of determinant Jacobian 1 can indeed be written as a composition of affine and triangular automorphisms of determinant Jacobian 1. (See [MR15b] lemma 3.4.)
Now an obvious question is whether the map \( \pi : \text{SA}_n(\mathbb{Z}) \rightarrow \text{SA}_n(\mathbb{F}_p) \) is surjective or not; this question is interesting as nonsurjectivity would yield non-tame maps due to the above remark. This is part of the topic of the papers [MR15b]; [Mau01]; [MW11].

**Definition 3.5.2.** Let \( R \) be a \( \mathbb{Z} \) algebra and \( k \) be a field such that we have a surjective ring homomorphism \( R \rightarrow k \). We can extend it naturally \( \text{ME}_n(R) \rightarrow \text{ME}_n(k) \). We denote this extended map by \( \pi \).

We notice that corresponding to each automorphism \( F \in \text{SA}_n(\mathbb{Z}) \) we have \( F \mod p \in \text{SA}_n(\mathbb{F}_p) \), but there may exist some automorphisms \( f \in \text{SA}_n(\mathbb{F}_p) \) such that \( \pi^{-1}(f) \not\subset \text{SA}_n(\mathbb{Z}) \). We conjecture the following for a \( \mathbb{Z} \) algebra \( R \) and a field \( k \):

**Conjecture 3.5.3.** Let \( R \) be a \( \mathbb{Z} \) algebra and \( k \) be any field. If we have a surjective ring homomorphism \( R \rightarrow k \), then we have

1. \( \pi(\text{SA}_n(R)) = \text{SA}_n(k) \).
2. \( \pi^{-1}(\text{SA}_n(k)) \cap \text{KE}_n(R) = \text{SA}_n(R) \).

A similar conjecture is the following (see also lemma 3.7.8 and corollary 3.7.9):

**Conjecture 3.5.4.** Let \( R \) be a \( \mathbb{Z} \) algebra and \( k \) be any field of characteristic \( p \). If we have a surjective ring homomorphism \( R \rightarrow k \), then the map \( \pi : \text{KE}_n(R) \rightarrow \text{MA}_n(k) \) has \( \text{SK}_n(k) \) in its image.

If the above conjecture is not true, then it can mean various things: it could mean that \( \mathcal{J}\mathcal{C}(k,n) \) is not true (or should be reformulated), or that there exist non-tame automorphisms over \( k \).

Assuming \( \mathcal{J}\mathcal{C}(k,n) \) to be true, then conjecture 3.5.3 imples 3.5.4, but no other implications can be made, nor does \( \mathcal{J}\mathcal{C}(k,n) \) imply any of the above conjectures.

**Justification of the above conjectures:** The above conjectures are not made to “match exactly what we need in our proofs”. They capture the essence of whether characteristic \( p \) is truly different from characteristic zero. If one or more of these conjectures is wrong, then characteristic \( p \) is in its core different from characteristic zero (for example, there might exist \( \mathbb{F}_p \)-automorphisms of \( \mathbb{F}_p^{[n]} \) which are of a completely different nature than one can find in characteristic zero), while if both of them are correct, then characteristic \( p \) is not too unsimilar from characteristic zero and both are intricately linked.

The tendency is to believe the conjectures (hence the name “conjecture” and not “problem” or “question”): it would be really surprising if any counterexamples would not be easily constructable in low degree and dimension (and known), whereas it can be easily imagined that the conjectures are true but hard to prove. For example, due to the the fact that we do not even have a (parametrized) list of generators for the automorphism group \( \text{GA}_n(k) \) (unlike for \( \text{GL}_n(k) \), \( \text{TA}_n(k) \)), we can understand that conjecture 3.5.4, if true, is very hard to prove.\(^1\)

\(^1\)Note, that with a little change, _some people_ would agree on the same text for the Jacobian Conjecture.
3.6 Some computations indicating the correctness of conjecture $JC(k,n)$

We should check this conjecture for some nontrivial cases, in order to point out that it might do what it claims. Therefore, in this subsection we considered polynomial endomorphisms of degree $\leq 3$ with coefficients in field of characteristic $p$, and having affine part identity. We will check if $JC(k,2)$ is true for these maps for fields $k$ of characteristic $p$. Let us write down such a polynomial map with generic coefficients:

$$T = (x, y) + (Ax^2 + By^2 + Cxy + Dx^3 + Ey^3 + Fx^2y + Gxy^2, A_1x^2 + B_1y^2 + C_1xy + D_1x^3 + E_1y^3 + F_1x^2y + G_1xy^2).$$

Let us take the determinant of the Jacobian and equal it to 1:

$$1 = \det(Jac(T)) = 1 + (C_1 + 2A)x + (2B_1 + C)y$$

$$+ (F_1 + 3D + 2AC_1 - 2A_1C)x^2 + (2G_1 + 2F + 4AB_1 - 4A_1B)xy$$

$$+ (3E_1 + G + 2CB_1 - 2BC_1)y^2$$

$$(6AE_1 - 6A_1E + 4B_1F - 4BF_1 + CG_1 - C_1G)xy^2$$

$$(6DB_1 - 6D_1B + 4AG_1 - 4A_1G + FC_1 - F_1C)x^2y$$

This gives us generators of the ideal $I_Q = \langle C_1 + 2A, 2B_1 + C, \ldots \rangle$ in the ring $Q[A, B, \ldots, E_1]$. It is clear that the following conditions are in $I_Q$ also, by doing some elementary manipulations:

$$F_1 + 3D, AC_1 - A_1C, G_1 + F, AB_1 - A_1B, 3E_1 + G, CB_1 - BC_1, AE_1 - A_1E, B_1F - BF_1, \quad CG_1 - C_1G, DB_1 - D_1B, AG_1 - A_1G, FC_1 - F_1C, DE_1 - D_1E, FG_1 - F_1G, FA_1 - F_1A, \quad DC_1 - D_1C, CE_1 - C_1E, B_1G - BG_1, DG_1 - GD_1, FE_1 - EF_1, DF_1 - D_1F$$

$$C_1 + 2A, C + 2B_1, GE_1 - EG_1 \in I_Q. \quad (3.1)$$

Moreover it can be checked by any computer algebra package (we used singular) that

$$A^3E_1^2 - B^3D_1^2, A^3E^2 - B^3D^2 \in \text{rad}(I_Q), \quad (3.2)$$

where these conditions do not belong to $I_Q$.

As before, we define $J_Z := \text{rad}(I_Q) \cap Z[A, B, \ldots, E_1]$, and $J_p := J_Z \mod p$. It is possible to now use a computer algebra system to show that 3.1 and 3.2 generate $J_p$, but this can be quite a strain on the computer system, which we can avoid in this case: We will show that (Part 1) assuming these conditions forces $T$ to be invertible for any $p$, and (Part 2) if $T$ is assumed to be invertible, then it satisfies the conditions 3.1 and 3.2 (meaning we show that these conditions might not generate $J_p$, but $J_p$ is the radical of the ideal generated by them).
3.6. Some computations indicating the correctness of conjecture

\( \mathcal{J} \mathcal{C}(k,n) \)

**Part 1: Assuming the conditions yields invertibility.**
We first assume that \( A, A_1, E \) are all nonzero. Then solving (1) and (2) yields

\[
C_1 = -2A, C = \frac{2A^2}{A_1}, B_1 = \frac{A^2}{A_1}, B = \frac{A^3}{A_1^2},
\]

\[
G = -\frac{3A_1E}{A^4}, G_1 = -\frac{3A_1^2E}{A^2},
\]

\[
D = -\frac{A_1^3E}{A^3}, D_1 = \frac{A_1^4E}{A^4}
\]

\[
F_1 = -3D, G = -3E_1, F = -G_1.
\]

Thus

\[
T = (x,y) + (A x^2 + \frac{A^3}{A_1^2} y^2 - \frac{2A^2}{A_1} x y - \frac{A_1^3E}{A^3} x^3 + \frac{3A_1^2E}{A^2} x^2 y - \frac{3A_1E}{A} x y^2,\]

\[
A_1 x^2 + \frac{A^2}{A_1} y^2 - 2A x y - \frac{A_1^4E}{A^4} x^3 + \frac{A_1 E}{A} y^3 + \frac{3A_1^3E}{A^3} x^2 y - \frac{3A_1^2E}{A^2} x y^2).
\]

This can be rewritten as

\[
T = \left( x + A(x - \frac{A}{A_1} y)^2 - \frac{A_1^3E}{A^3}(x - \frac{A}{A_1} y)^3 \right)
\]

\[
(y + A_1(x^2 - \frac{A}{A_1} y)^2 - \frac{A_1 E}{A^3}(x - \frac{A}{A_1} y)^3)
\]

Regardless of characteristic, \( T \) is a tame map of the form

\[
T = (x + A \frac{A}{A_1} y, y)(x + A_1 x^2 - \frac{EA_1^3}{A^3} x^3)(x - \frac{A}{A_1} y, y)
\]

meaning that \( T \) is invertible.

In case one or more of \( A, A_1, E \) is zero is easier than the above case (many coefficients are forced to be zero in these cases) and we leave it to the reader.

**Part 2: Invertibility implies that the conditions are satisfied.** Since we have a map in dimension 2, it is tame, and we can use the Jung-van der Kulk theorem. Since the degree is three or less, it is a map of the form \( \alpha \circ (x, y + f(x)) \circ \beta \) where \( \alpha, \beta \) are affine invertible maps, and \( \deg(f) \leq 3 \).

(There can only be one triangular map involved, as the degree is prime.) We can assume that \( \beta = (ax + by + c, y) \) as we can put anything occurring in the second component in \( f \). Also, we can assume \( f \) is of degree 2 or 3, and also we can assume that \( f(0) = 0 \) as we can put any constant added in \( \alpha \). Adding in the requirement that the affine part of \( \alpha \circ (x, y + f(x)) \circ \beta \) must be the identity yields requirements on \( \alpha \) given \( \beta \) and \( f(x) \). Working this out yields a generic map that is actually very similar to the formula of \( T \) above; it can be easily checked that it satisfies the conditions.

**Remark:** It is very hard to check this conjecture for specific degrees, even in \( n = 2 \), as there is no shortcut other than doing hard-core computations. In fact, en passant, one is proving the conjecture, and the computations are very similar to proving the Jacobian Conjecture in characteristic zero - which is (we hope the reader agrees) a difficult task...

Of course, we also checked the conjecture for many specific examples (which we do not list here, though we specifically mention that we could...
3.7 Implications of the Jacobian Conjecture among various fields

In this section we will see if \( k, \bar{k} \) are two arbitrary fields of characteristic \( p \) then what is the connection between \( \mathcal{JC}(k, n) \) and \( \mathcal{JC}(\bar{k}, n) \). We denote the Jacobian conjecture over all domains having characteristic zero by \( \mathcal{JC}(n, 0) \) and the Jacobian conjecture over all fields with characteristic \( p \) by \( \mathcal{JC}(n, p) \). In characteristic zero we have the following theorem (theorem 1.1.18 in \([\text{Ess00}]\)).

**Theorem 3.7.1.** Let \( R, \hat{R} \) be commutative rings contained in a \( \mathbb{Q} \)-algebra. If \( \mathcal{JC}(R, n) \) is true for all \( n \geq 1 \), then \( \mathcal{JC}(\hat{R}, n) \) is true for all \( n \geq 1 \).

For the characteristic \( p \) equivalent we have to assume part of our conjectures:

**Theorem 3.7.2.** Assume the conjectures 3.5.3(2), 3.5.4 are true. Let \( k, \bar{k} \) be two fields contained in an \( \mathbb{F}_p \)-algebra such that \( \mathcal{JC}(k, n) \) is true for all \( n \geq 1 \), then \( \mathcal{JC}(\bar{k}, n) \) is true for all \( n \geq 1 \). In particular, it is enough to verify \( \mathcal{JC}(\mathbb{F}_p, n) \).

It is very hard to prove the statement 3.7.2 without making any assumption. To mention the main hurdle: consider an infinite field \( k \) and \( k_1 \subset k \) a finite Galois extension, \( a_1, a_2, \ldots, a_n \) a basis of \( k_1 \), and denote by \( \alpha : k_1^m \to k \) the map defined by \( \alpha(y_1, \ldots, y_m) = y_1a_1 + \cdots + y_ma_m \). The obvious extension \( (k_1^m)^n \to k^n \) which we also denote by \( \alpha \), is clearly injective. Let \( F = (F_1, \ldots, F_n) : k^n \to k^n \) be a polynomial map. Conjugating \( F \) with \( \alpha \) we get the map \( F^\alpha := \alpha^{-1}F\alpha : k_1^mn \to k_1^mn \). Comparing to the characteristic zero proof of theorem 3.7.1 there we know that \( \det\text{Jac}(F) \in k^* \) if and only if \( \det\text{Jac}(F^\alpha) \in k_1^* \) (equation 1.1.26 in \([\text{Ess00}]\)). In characteristic \( p \) we should have a similar statement that \( F \) satisfies \( J_k \) if and only if \( F^\alpha \) satisfies \( J_{k_1} \), but the proof of this is not clear. This property that \( F \) satisfies \( J_k \) if and only if \( F^\alpha \) satisfies \( J_{k_1} \) is needed to prove the theorem 3.7.2 if we don’t assume that conjectures 3.5.3(2) and 3.5.4 are true. The remaining part of this section is devoted towards the proof of theorem 3.7.2. We begin with some definitions and lemmas.

Let \( \Omega \) be an algebraic closure of \( \mathbb{F}_p(\{x_i | i \in \mathbb{N}\}) \). Note that \( \Omega \) is a field with infinite transcendence degree over \( \mathbb{F}_p \).

**Definition 3.7.3.** Let \( R, S \) be commutative rings. Let \( \phi : R \to S \) a ring homomorphism. If \( F \in R[X]^n \), then \( F^\phi \) denotes the element of \( S[X]^n \) obtained by applying \( \phi \) to the coefficients of the \( F_i \).

We use the notation \( X = (x_1, x_2, \ldots, x_n) \). The following proposition is taken from \([\text{Ess00}]\) (proposition 1.1.7). Let \( \eta \) be the nilradical of \( R \).

**Proposition 3.7.4.** (Invertibility under base change) Let \( \phi : R \to S \) be a ring homomorphism with \( \ker \phi \subset \eta \). Let \( F \in R[X]^n \) with \( \det JF(0) \in R^* \). Then \( F \) is invertible if and only if \( F^\phi \) is invertible over \( S \).

We use this to show that proving the \( \mathcal{JC} \) for \( \Omega \) is universal in the sense that it proves the Jacobian Conjecture for all fields of the same characteristic.
Proposition 3.7.5. Let \( n \geq 1 \). If \( JC(\Omega, n) \) is true then \( JC(k, n) \) is true for every field \( k \) of characteristic \( p \).

Proof. Let \( F \in k[X]^n \) satisfy \( J_Z \otimes k \). Let \( k_0 \) be the subfield of \( k \) generated over \( \mathbb{F}_p \) by the coefficients of \( F \) (i.e. \( k_0 = \mathbb{F}_p(x_1, \ldots, x_m) \) for some \( x_1, \ldots, x_m \in k \)). Then \( F \) satisfies \( J_Z \otimes k_0 \). As \( \Omega \) is an algebraic closure of \( \mathbb{F}_p(\{x_i \mid i \in \mathbb{N}\}) \), it is trivial that we get an embedding \( \phi : k_0 \to \Omega \). Since \( F \) satisfies \( J_Z \otimes k_0 \) we get that \( F^\phi \) satisfies \( J_Z \otimes \phi(k_0) \) and by lemma 3.4.4 we have \( F^\phi \) satisfies \( J_Z \otimes \Omega \). This gives \( F^\phi \) is invertible over \( \Omega \) since we assume that \( JC(\Omega, n) \) is true. Thus \( F \) is invertible over \( k_0 \) by proposition 3.7.4 and hence over \( k \). \( \Box \)

Corollary 3.7.6. of lemma 3.4.4
Let \( n \geq 1 \) and \( k_0 \subset k \) be fields of characteristic \( p \). If \( JC(k, n) \) is true then \( JC(k_0, n) \) is true for any subfield \( k_0 \) of \( k \).

Proof. Let \( F \in SKE_n(k_0) \) then by lemma 3.4.4 we have \( F \in SKE_n(k) \). Since we assume that \( JC(k, n) \) is true, \( F \) is invertible over \( k \). Hence \( F \) is invertible over \( k_0 \) by proposition 3.7.4. \( \Box \)

Let \( k \) be any countable field of characteristic \( p \). We can write \( k = \{a_1, a_2, \ldots\} \) where \( a_i \neq a_j \) for \( i \neq j \). We can also assume that \( k \) is ordered set. Corresponding to each element \( a_i \) in \( k \) consider the indeterminate \( x_i \) Define a polynomial ring over \( \mathbb{Z} \) by \( \Lambda_k := \mathbb{Z}[x_1, x_2, \ldots] \). Define a map by \( \tau : \Lambda_k \to k \) by \( x_i \mapsto a_i \) and \( m \mapsto m \mod p \) for any \( m \in \mathbb{Z} \). Then it is clearly well defined surjective ring homomorphism. Thus we have the following definition

Definition 3.7.7. For each countable field \( k \) of characteristic \( p \), define a polynomial ring \( \Lambda_k \) over \( \mathbb{Z} \) such that \( \tau : \Lambda_k \to k \) is a surjective ring homomorphism. This define the pair \((\Lambda_k, \tau)\).

Notice that we can naturally extend \( \tau \) to a map \( ME_n(\Lambda_k) \to ME_n(k) \). We denote this extended map by \( \pi \) as in definition 3.5.2. This gives the pair \((\Lambda_k, \pi)\).

Thus we have the following lemma.

Lemma 3.7.8. Let \( k \) be a countable field of characteristic \( p \). We have \( \pi(KE_n(\Lambda_k)) \subseteq SKE_n(k) \) for every \( n \geq 1 \).

Proof. Let \( F \in KE_n(\Lambda_k) \), then \( \text{det}(\text{Jac}(F)) = 1 \) and so \( F \) satisfies \( I_Q \). We want to show \( \pi(F) \in SKE_n(k) \). Let \( J_Z \) be the ideal of integer Keller conditions for the polynomial \( \pi(F) \) and \( J_k := J_Z \otimes k \) (see definition 3.3.2). Let \( q \in J_k \) then \( q = \sum_i e_i h_i \) for \( e_i \in J_Z \) and \( h_i \in k \) for all \( i \) (here \( e_i h_i = e_i \otimes h_i \), but we omit the tensor notation). Since \( h_i \in k \) there exist \( H_i \in \Lambda_k \) such that \( \tau(H_i) = h_i \). We can define a surjective homomorphism \( J_{\Lambda_k} := J_Z \otimes \Lambda_k \to J_Z \otimes k \) by \( a \otimes b \mapsto \tau(a) \otimes \tau(b) \) where \( a \in J_Z \) and \( b \in \Lambda_k \). Thus there exists \( Q \in J_{\Lambda_k} \) defined by \( Q = \sum e_i H_i \) such that \( \tau(Q) = q \), i.e. \( \sum_i \tau(e_i) \tau(H_i) = \sum_i e_i h_i \) where \( e_i \in J_Z \) such that \( \tau(e_i) = e_i \) for all \( i \). By lemma 3.4.2 we have \( e_i(\nu(F)) = 0 \) for all \( i \) (since \( F \) satisfying \( I_Q \)). If we identify \( x_i \) with \( a_i \) as in definition of \( \tau, e_i(\nu(\pi(F))) = e_i(\nu(F)) \mod p = 0 \mod p \) for all \( i \). Thus \( q(\nu(\pi(F))) = \sum e_i(\nu(\pi(F))) h_i(\nu(\pi(F))) = 0 \mod p \). This shows that \( \pi(F) \) satisfies \( J_k \). Hence \( \pi(F) \in SKE_n(k) \) which proves the lemma. \( \Box \)

Of course, the above lemma slightly reformulates conjecture 3.5.4:
Corollary 3.7.9. Assume conjecture 3.5.4 is true and that $k$ is a countable field of characteristic $p$. Then $\pi(KE_n(\Lambda_k)) = SKE_n(k)$.

We are now ready to link $JC(n, 0)$ to $JC(n, p)$.

Proposition 3.7.10.
(1) Assume conjecture 3.5.4 is true. Then
$$JC(n, 0) \forall n \in \mathbb{N}^* \implies JC(n, p) \forall n \in \mathbb{N}^*.$$  
(2) Assume conjectures 3.5.3(2), 3.5.4 are true. Then
$$JC(n, 0) \forall n \in \mathbb{N}^* \iff JC(n, p) \forall n \in \mathbb{N}^*.$$  

In fact, it is enough to prove or disprove $JC(n,Z)$ for all $n$ to prove or disprove $JC(k,n)$ for all $n$ and for any field $k$.

Proof. (1) Consider $K$, an arbitrary field of characteristic $p$, and $f \in SK_n(K)$. Let $k$ be the subfield of $K$ generated over $\mathbb{F}_p$ by the coefficients of $f$. Since $k$ is countable, we have a surjective ring homomorphism $\tau : \Lambda_k \rightarrow k$ (definition 3.7.7). By corollary 3.7.9 there exists $F \in KE_n(\Lambda_k)$ such that $\pi(F) = f$. Thus $F$ is invertible since we assume that $JC(n, 0)$ is true, so there exists $G \in ME_n(\Lambda_k)$ such that $F \circ G = I$. Applying $\pi$ we have $\pi(F) \circ \pi(G) = \pi(I) = I$ mod $p$. Thus $\pi(G)$ is an inverse of $f = \pi(F)$. This shows that $f$ is invertible over $k$ and hence over $K$.

(2) Let $K$ be an arbitrary field of characteristic $p$ and consider $k \subseteq K$ a countable field (if $K$ is itself countable then take $k = K$). By corollary 3.7.9 we have $\pi(KE_n(\Lambda_k)) = SKE_n(k)$ (where $\Lambda_k$ is defined in 3.7.7). Let $F \in KE_n(\Lambda_k)$ then $\pi(F)$ satisfies $J_k$. Suppose $JC(K,n)$ is true then $JC(k,n)$ is true by corollary 3.7.6. Thus $\pi(F) \in SA_n(k)$ and so $F \in \pi^{-1}(SA_n(k))$. By conjecture 3.5.3(2) we have $F \in SA_n(\Lambda_k)$. By theorem 3.7.1 we have that $JC(n,0)$ is true.

Proof. (of theorem 3.7.2)
This is direct consequence of proposition 3.7.10

3.8 Some results related to $JC(k,n)$

In this section we present some basic results related to our formulation of the Jacobian conjecture in characteristic $p$.

Invertible polynomial maps and $JC(k,n)$

In this subsection we will discuss a natural question which can come to mind when studying the previous results. If the characteristic of $k$ is zero then we know that if $F \in SA_n(k)$ then $F$ satisfies the Keller condition $\det \Jac(F) = 1$ (the only condition for Jacobian conjecture $JC(k, n)$). This is due to the fact that the determinant of the Jacobian has the property $\det \Jac(G \circ F) = \det \Jac(F) \cdot (\det \Jac(G) \circ F)$. If characteristic of $k$ is $p$, it is not easy to prove that if $F \in SA_n(k)$ then $F$ satisfies $J_k$ (the universal conditions).

Nevertheless, assuming conjectures 3.5.3(1) and 3.5.4 we can prove that if $F \in SA_n(k)$ then $F \in SKE_n(k)$. 


Proposition 3.8.1. Assume conjectures 3.5.3(1) and 3.5.4 are true and $k$ be a field of characteristic $p$. If $f \in \text{SA}_n(k)$ then $f \in \text{SKE}_n(k)$.

Proof. Let $f \in \text{SA}_n(k)$. Consider $k_0 \subset k$ generated over $\mathbb{F}_p$ by the coefficients of $f$. By conjecture 3.5.3(1) there exists some $F \in \text{SA}_n(\Lambda_{k_0})$ such that $\pi(F) = f$ and thus $F$ satisfies $\text{KE}_n(\Lambda_{k_0})$. Assuming conjecture 3.5.4 we have $\pi(\text{KE}_n(\Lambda_{k_0})) = \text{SKE}_n(k_0)$ by corollary 3.7.9. Thus $f \in \text{SKE}_n(k_0)$ and hence $f \in \text{SKE}_n(k)$ by lemma 3.4.4.

Closure property of $\text{SKE}_n(k)$

The set $\text{KE}_n(R)$ is closed under composition for any ring $R$, and also for $R = k$ a field of characteristic $p$, even though it does not only consist of automorphisms. One would expect that $\text{SKE}_n(\mathbb{F}_p)$ is also closed under composition. However, trying to prove this turns out to be an incredibly difficult task: if $F \in \text{SKE}_n(\mathbb{F}_p)$ then the coefficients of $F$ satisfy certain conditions that can be found in $J_p$. If we compose two such maps $F, G \in \text{SKE}_n(\mathbb{F}_p)$, then the coefficients of the resulting map $F \circ G$ (denoted $v(F \circ G)$) are polynomials in the coefficients of $F$ and $G$, i.e. $v(F \circ G) = P(v(F), v(G))$ for some polynomial map $P$. To check if $F \circ G$ is in $\text{SKE}_n(\mathbb{F}_p)$ we need to see if $v(F \circ G)$ satisfy the conditions in $J_p$; however, this turned out to be extremely difficult.

Comparing to characteristic zero, there we know a priori due to the “magical” equation $\det \text{Jac}(F \circ G) = \det \text{Jac}(G) \cdot (\det \text{Jac}(F) \circ G)$ that $\text{KE}_n(\mathbb{Z})$ is closed under composition. As a corollary, it gives that “$v(F)$ satisfies $J_{\mathbb{Z}}$ and $v(G)$ satisfies $J_{\mathbb{Z}}$” implies “$v(F \circ G)$ satisfies $J_{\mathbb{Z}}$”, but exactly how is very complicated.

Nevertheless, making an assumption we can prove that $\text{SKE}_n(\mathbb{F}_p)$ is closed under composition.

Proposition 3.8.2. Assume conjecture 3.5.4 is true. Then $\text{SKE}_n(k)$ is closed under composition, where $k$ is any field of characteristic $p$.

Proof. Let $f, g \in \text{SKE}_n(k)$. Let $k_1$ be the subfield of $k$ generated over $\mathbb{F}_p$ by the coefficients of $f$ and $g$. Field $k_1$ is countable, thus by corollary 3.7.9 there exist $F, G \in \text{KE}_n(\Lambda_{k_1})$ such that $\pi(F) = f$ and $\pi(G) = g$. Now $F \circ G \in \text{KE}_n(\Lambda_{k_1})$ as $\text{KE}_n(\Lambda_{k_1})$ is closed under composition. Thus $f \circ g = \pi(F) \circ \pi(G) = \pi(F \circ G) \in \text{SKE}_n(k_1)$ by corollary 3.7.9. Hence $f \circ g \in \text{SKE}_n(k)$ (lemma 3.4.4).

Connections between $\mathcal{JC}(\mathbb{F}_p, n)$ and $\mathcal{JC}(\mathbb{Z}, n)$.

In this subsection we will see how we can move back and forth between $\mathcal{JC}(\mathbb{F}_p, n)$ and $\mathcal{JC}(\mathbb{Z}, n)$. We quote theorem 10.3.13 from [Ess00]. We will need this theorem to build the connection between $\mathcal{JC}(\mathbb{F}_p, n)$ and $\mathcal{JC}(\mathbb{Z}, n)$.

Theorem 3.8.3. Let $F \in \mathbb{Z}[x_1, x_2, \ldots, x_n]^n$. If $F \mod p : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ is injective for all but finitely many primes $p$ and $\det \text{Jac}(F) \in \mathbb{Z} \setminus \{0\}$, then $F$ is invertible over $\mathbb{Z}$.

Lemma 3.8.4. If $\mathcal{JC}(\mathbb{F}_p, n)$ is true for all but finitely many primes $p$, then $\mathcal{JC}(\mathbb{Z}, n)$ is true.
This is a slight variation on proposition 3.7.10 but without any requirements.

Proof. Let \( F \in \operatorname{MA}_n(\mathbb{Z}) \), such that \( \det(\operatorname{Jac}(F)) = 1 \). Then \( F \mod p \) satisfies \( J_p \) by lemma 3.7.8. Thus \( F \mod p \) is invertible for almost all \( p \) by given assumptions. By theorem 3.8.3 we conclude that \( F \) is invertible. \( \square \)

For the converse of this lemma we need to assume conjecture 3.5.4 to be true. This in turn resembles proposition 3.7.10.

**Lemma 3.8.5.** Suppose conjecture 3.5.4 and \( JC(\mathbb{Z}, n) \) are true, then \( JC(\mathbb{F}_p, n) \) is true.

**Proof.** Let \( f \in \operatorname{ME}_n(\mathbb{F}_p) \) such that \( f \) satisfies \( J_p \). By corollary 3.7.9 there exists \( F \in \operatorname{KE}_n(\mathbb{Z}) \) such that \( F \mod p = f \). By assumption, \( F \) is invertible, so there exists \( G \in \operatorname{ME}_n(\mathbb{Z}) \) such that \( F \circ G = I \). Thus \( (F \mod p) \circ (G \mod p) = I \mod p \) and hence \( G \mod p := g \) is the inverse of \( f \). \( \square \)

**Boundedness**

In this subsection we see that if \( p \) is “large enough” with respect to some formula depending on \( d \) and \( n \) and the coefficients, of a polynomial map, then the situation is exactly the same as in characteristic zero. We fix \( n \) in this section, but note that the constant \( N_d \) below depends also on \( n \). Let \( \operatorname{ME}_n(\mathbb{F}_p)^d \) be the set of polynomial endomorphisms of degree at most \( d \). Similarly we can define \( \operatorname{KE}_n(\mathbb{Z})^d \), \( \operatorname{SKE}_n(\mathbb{F}_p)^d \) etc.

**Lemma 3.8.6.** Let \( F \in \operatorname{ME}_n(\mathbb{F}_p)^d \) and \( I^d_Q = (E_1, \ldots, E_m) \) then there exists a positive integer \( N_d \) such that for \( p > N_d \) we have \( J^d_R = \operatorname{rad}(E_1, \ldots, E_m) \) for \( R := \mathbb{Z}[\frac{1}{N_d}] \).

**Proof.** Consider the ideals \( I^d_Q = (E_1, \ldots, E_m) \) and \( I^d_Q \cap C_{R,d} = (E_1, \ldots, E_m, Q_1, \ldots, Q_r) \), where \( Q_i = \frac{P_i(E_1, \ldots, E_m)}{n_i} \), and \( P_i(X) \) are polynomials with integer coefficients. Let \( N_d = \operatorname{lcm}(n_1, n_2, \ldots, n_r) \). Then for \( p > N_d \) we have \( I^d_Q \cap C_{R,d} = (E_1, \ldots, E_m) \) where \( R := \mathbb{Z}[\frac{1}{N_d}] \). Hence \( J^d_R := \operatorname{rad}(I^d_Q \cap C_{R,d}) = \operatorname{rad}(E_1, \ldots, E_m) \). \( \square \)

In the rest of this section we will use the same definition of constant \( N_d \) as given in the proof of the lemma 3.8.6.

**Corollary 3.8.7.** Let \( F \in \operatorname{ME}_n(\mathbb{F}_p)^d \) and \( I^d_Q = (E_1, \ldots, E_m) \) then there exists a positive integer \( N_d \) such that for \( p > N_d \) we have \( J^d_p = \operatorname{rad}(E_1 \mod p, \ldots, E_m \mod p) = J^d_R \mod p \) for \( R := \mathbb{Z}[\frac{1}{N_d}] \).

**Proof.** Since by definition

\[
J^d_p = J^d_Z \mod p = J^d_Z \otimes_{\mathbb{Z}} \mathbb{F}_p
\]

Since for \( p > N_d \) we have \( R \otimes_R \mathbb{F}_p = \mathbb{F}_p \), thus

\[
J^d_p = J^d_Z \otimes_{\mathbb{Z}} (R \otimes_R \mathbb{F}_p) = (J^d_Z \otimes_{\mathbb{Z}} R) \otimes_R \mathbb{F}_p
\]
3.8. Some results related to $JC(k,n)$

$$= J_R^d \otimes_R \mathbb{F}_p$$
$$= J_R^d \mod p.$$  

By lemma 3.8.6 we get $J_R^d = J_R^d \mod p = \text{rad}(E_1 \mod p, \ldots, E_m \mod p)$ for $R := \mathbb{Z}[\frac{1}{N_d}]$ and $p > N_d$.  

**Corollary 3.8.8.** There exists a positive integer $N_d$ such that $\text{KE}_n(\mathbb{Z})^d \mod p \subset \text{SKE}_n(\mathbb{F}_p)^d$ for $p > N_d$.  

**Proof.** Direct consequence of corollary 3.8.7.  

Let $\text{ME}_n(\mathbb{Z})^{d,C}$ be the set of polynomial endomorphisms of degree at most $d$ with coefficients bounded by $C$. Similarly we define $\text{KE}_n(\mathbb{Z})^{d,C}$ be the set of Keller maps of degree at most $d$ with coefficients bounded by $C$ and $\text{SKE}_n(\mathbb{F}_p)^{d,C}$ be the set of strong Keller maps of degree at most $d$ with coefficients bounded by $C$.

**Lemma 3.8.9.** Let $F \in \text{ME}_n(\mathbb{Z})^{d,C}$ and $I_Q^d = (E_1, \ldots, E_m)$. There exists a positive integer $N_d(C)$ such that for $p > N_d(C)$ we have $|E_i(\nu(F))| < p$ for all $1 \leq i \leq m$.  

**Proof.** Let $N_i := \max\{|E_i(\eta)| : \eta \in [-C, C]^l, l = \text{the number of coefficients of the generic polynomial } F\}$ and $N_d(C) := \max\{N_d, N_1, N_2, \ldots, N_m\}$. Then for $p > N_d(C)$ we have $|E_i(\nu(F))| < p$ for all $1 \leq i \leq m$.  

The following lemma is intuitively clear: if you have a polynomial map having coefficients which are (in $\mathbb{Z}$) small, then knowing that the map modulo $p$ is a (special) Keller map yields that it was a Keller map to start with.

**Lemma 3.8.10.** Let $F \in \text{ME}_n(\mathbb{Z})^{d,C}$ and fix $p > N_d(C)$ such that $f := F \mod p \in \text{SKE}_n(\mathbb{F}_p)^{d,C}$, where $N_d(C)$ is as in lemma 3.8.9. Then $F \in \text{KE}_n(\mathbb{Z})^d$.  

**Proof.** By definition for $f \in \text{SKE}_n(\mathbb{F}_p)^d$ we have $s(\nu(f)) = 0 \mod p$ for all $s \in J_p^d$. By corollary 3.8.7 there exists a positive integer $N_d$ such that for $p > N_d(C) > N_d$ we have $J_R^d = \text{rad}(E_1 \mod p, \ldots, E_m \mod p) = J_R^d \mod p$ for $R := \mathbb{Z}[\frac{1}{N_d}]$. Thus for given $F \in \text{ME}_n(\mathbb{Z})^d$ such that $F \mod p = f$ we have $S(\nu(F)) \mod p = 0 \mod p$ for all $S \in J_R^d$ with $p > N_d(C)$. In particular for $p > N_d(C)$ we have $E_i(\nu(F)) \mod p = 0 \mod p$ for all $1 \leq i \leq m$. By lemma 3.8.9 for $p > N_d(C)$ we have $|E_i(\nu(F))| < p$ for all $1 \leq i \leq m$. Thus $E_i(\nu(F)) = 0$ for all $1 \leq i \leq m$. Hence $F \in \text{KE}_n(\mathbb{Z})^d$.  

Under some very stringent conditions we can now show closedness under composition of some elements in $\text{SKE}_n(\mathbb{F}_p)$.  

**Corollary 3.8.11.** There exists a positive integer $N_{d^2}(C)$ such that if $f, g \in \text{SKE}_n(\mathbb{F}_p)^{d,C}$ with $p > N_{d^2}(C)$ then $f \circ g \in \text{SKE}_n(\mathbb{F}_p)^{d^2,C}$.  

**Proof.** Let $F, G \in \text{ME}_n(\mathbb{Z})^{d,C}$ such that $F \mod p = f$ and $G \mod p = g$. By lemma 3.8.10 there exists a positive integer $N_d(C)$ such that for $p > N_d(C)$ we have $F, G \in \text{KE}_n(\mathbb{Z})^{d,C}$. Since $\text{KE}_n(\mathbb{Z})$ is closed under composition.
Thus $F \circ G \in \text{KE}_n(\mathbb{Z})^{d^2, C}$. Hence by corollary 3.8.8 there exists a positive integer $N_{d^2}$ such that for $p > N_{d^2}(C) := \max\{N_{d^2}, N_d(C)\}$ we have $f \circ g \in \text{SKE}_n(\mathbb{F}_p)^{d^2, C}$.

The generic case eludes us:

**Conjecture 3.8.12.** Let $k$ be a field of characteristic $p$. Then $\text{SKE}_n(k)$ is closed under composition.
Chapter 4

Counter example to the cancellation problem in characteristic $p$

4.1 Introduction

Let $A$ be an affine algebra and $k$ be the field of characteristic $p > 0$. In [Asa87], Asanuma provides an example of a threefold $A$ which satisfies $A^{[1]} \cong k^{[4]}$. Later in 1994 he asks the question does $A \cong k^{[3]}$ [Asa94]. In [Gup14a] Gupta gives a negative answer to this question by using techniques developed by L. Makar-Limanov and A. Crachiola. This results in a counter example to the cancellation problem in characteristic $p > 0$. Asanuma’s proof is actually more general and is not easy to follow. In this chapter we choose some simple parameters and are able to provide an elementary proof of $A^{[1]} \cong k^{[3]}$ in this case. Moreover we give a proof of Gupta’s result $A \neq k^{[3]}$ for a less general situation. In this way we provide the counter example to cancellation problem in one place so that the reader can easily access it.

4.2 Preliminaries

Degree functions and related lemmas. Given an exponential map $\phi : A \rightarrow A[U]$ on a domain $A$ over $k$, we can define the $\phi$-degree of an element $a \in A$ by $\deg_\phi(a) = \deg_U(\phi(a))$ (where $\deg_U(0) = -\infty$). Note that $A^\phi$ consists of all elements of $A$ with non-positive $\phi$ degree. The function $\deg_\phi$ is a degree function on $A$, i.e. it satisfies these two properties for all $a, b \in A$:

1. $\deg_\phi(ab) = \deg_\phi(a) + \deg_\phi(b)$.
2. $\deg_\phi(a + b) \leq \max\{\deg_\phi(a), \deg_\phi(b)\}$

We first see some of the useful properties of exponential maps. The following two lemmas 4.2.1, 4.2.2 are present in [Cra06].

Lemma 4.2.1. Let $A$ be an affine domain over a field $k$. Suppose that there exists a non-trivial exponential map $\phi$ on $A$. Let $D = \{D^i\}$ be the locally finite iterative higher derivation associated to $\phi$. Then the following statements hold:

1. $A^\phi$ is factorially closed in $A$, i.e., if $a, b \in A$ such that $ab \in A^\phi \setminus \{0\}$, then $a, b \in A^\phi \setminus \{0\}$.
2. $A^\phi$ is algebraically closed in $A$. 

3. Let \( 0 \neq c = D^n(x) \) for some \( x \in A \). Then \( A \) is a sub-algebra of \( A^\phi [c^{-1}][x] \), where \( A^\phi [c^{-1}] \subset \text{Frac}(A^\phi) \) is the localization of \( A^\phi \) at \( c \).

4. Let \( \text{tr.deg}_k \) denote transcendence degree over \( k \). If \( \text{tr.deg}_k(A) \) is finite, then \( \text{tr. deg}_k(A^\phi) = \text{tr. deg}_k(A) - 1 \).

**Lemma 4.2.2.** Let \( k \) be a field and \( A \) a \( k \) domain satisfying

1. \( \text{tr.deg}_k(A) = 1 \) and

2. \( k \) is algebraically closed in \( A \).

Then \( \text{AK}(A) = k \) if and only if \( A = k^{[1]} \). Otherwise, \( \text{AK}(A) = A \).

Thus \( k^{[1]} \) is the only transcendence degree 1 domain over \( k \) which admits nontrivial exponential maps.

**Lemma 4.2.3.** Let \( \phi \) be an exponential map on a domain \( A \) over \( k \). Extend \( \phi \) to a homomorphism \( \phi : \text{Frac}(A) \to \text{Frac}(A)(U) \) by \( \phi(ab^{-1}) = \phi(a)\phi(b)^{-1} \), and let \( \text{Frac}(A)^\phi = \{ f \in \text{Frac}(A) | \phi(f) = f \} \). Then \( \text{Frac}(A)^\phi = \text{Frac}(A^\phi) \).

**Proof.** The inclusion \( \text{Frac}(A^\phi) \subset \text{Frac}(A)^\phi \) follows because for any \( ab^{-1} \in \text{Frac}(A^\phi) \) we have \( \phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = ab^{-1} \). For the reverse inclusion, let \( a, b \in A \setminus \{ 0 \} \) satisfy \( ab^{-1} \in \text{Frac}(A)^\phi \). Then

\[
ab^{-1} = \phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = \left( \sum_i D^i(a)U^i \right) \left( \sum_i D^i(b)U^i \right)^{-1},
\]

and thus

\[
\left( \sum_i aD^i(b)U^i \right) = \left( \sum_i bD^i(a)U^i \right).
\]

By comparing leading coefficients we see that \( a \) and \( b \) have the same \( \phi \)-degree, say \( n \), and \( ab^{-1} = D^n(a)D^n(b)^{-1} \). Since \( D^n(a), D^n(b) \in A^\phi \), we obtain \( ab^{-1} \in \text{Frac}(A^\phi) \).

**Remark 4.2.4.** Let \( A \) be a domain over \( k \), and let \( \phi \in \text{EXP}(A) \). Let \( B \) be the domain over \( \text{Frac}(A^\phi) \) obtained by localizing \( A \) at the multiplicative set \( A^\phi \setminus 0 \). By Lemma 4.2.3, \( \phi \) extends to a \( \text{Frac}(A^\phi) \)-homomorphism \( \bar{\phi} : B \to B[U] \) which is an exponential map on \( B \) with ring of invariants \( \text{Frac}(A^\phi) \).

The proof of the following lemma can be found in [Cra04].

**Lemma 4.2.5.** Let \( A \) be a domain of characteristic \( p \). Let \( m, n \in \mathbb{N} \) such that \( m \geq 2 \), \( n \geq 2 \), and neither \( m \) nor \( n \) are the power of \( p \). Let \( \phi \) be an exponential map on \( A \) and \( c_1, c_2 \in A^\phi \setminus 0 \). Suppose \( a, b \in A \). If \( c_1a^m + c_2b^n \in A^\phi \setminus 0 \) then \( a, b \in A^\phi \).

The following version of a result of H. Derksen, O. Hadas and L. Makar-Limanov is presented in [[Gup14a], Theorem 2.3].

**Theorem 4.2.6.** Let \( A \) be an affine domain over a field \( k \) with a proper \( \mathbb{Z} \)-filtration which is admissible. Let \( \phi \) be a non-trivial exponential map on \( A \). Then \( \phi \) induces a non-trivial exponential map \( \bar{\phi} \) on \( \text{gr}(A) \) such that \( \rho(A^\phi) \subset \text{gr}(A)^{\bar{\phi}} \).
4.3. Main theorem of Gupta

Lemma 4.2.7. (Lemma 3.3 in [Gup14a]) Let $A$ be an affine domain over an infinite field $k$. Let $f \in A$ be such that $f - \mu$ is a prime element of $A$ for infinitely many $\mu \in k$. Let $\phi$ be a non-trivial exponential map on $A$ such that $f \in A^\circ$. Then there exists $\gamma \in k$ such that $f - \gamma$ is a prime element of $A$ and $\phi$ induces a non-trivial exponential map on $A/(f-\gamma)$.

Lemma 4.2.8. (Lemma 3.4 in [Gup14a])

1. Let $A = k[X, Y, Z, T]/(X^nY - g)$ where $m > 1$ and $g \in k[Z, T]$. Let $f$ be a prime element of $k[Z, T]$ such that $g \notin f k[Z, T]$ and $B = A/fA$. Then $B$ is an integral domain.

2. Suppose that there exists a maximal ideal $M$ of $k[Z, T]$ such that $f \in M$ and $g \in f k[Z, T] + M^2$. Then there does not any non-trivial exponential map $\phi$ on $B$ such that the image of $Y$ in $B$ belongs to $B^\circ$.

The following lemma is useful in the next section.

Lemma 4.2.9. Let $a, b$ be positive integers such that $\gcd(a, b) = 1$ and $p | a$. Then the polynomial $X^a + Y^b + \lambda \in k[X, Y]$ is irreducible, where $k$ is field of characteristic $p$ and $\lambda \in k \setminus 0$.

Proof. We will use Eisenstein criterion to prove this lemma. We make the identification $k[X, Y] = k[X][Y]$ via natural isomorphism. We want to show that $Y^b + \lambda \in k[Y]$ is divisible by some prime $q(Y) \in k[Y]$ but not by $q^2$. For this it is sufficient to see that $f(Y) = Y^b + \lambda$ is not unit and has no repeated root in $k[Y]$. As $b > 0$, $f(Y)$ is not unit in $k[Y]$. Since $\gcd(a, b) = 1$ and $p | a$ we have $p | b$. Thus $f = bY^{b-1}$ is a nonzero constant or has 0 as its multiple roots which is not a root of $f$ as $\lambda \neq 0$. Thus $f(Y)$ is non unit square free in $k[Y]$. Let $q$ be the prime factor of $f(Y)$ then $q^2 \nmid f(Y)$. Thus Eisenstein criterion applies to $X^a + Y^b + \lambda$ and $q$.

4.3 Main theorem of Gupta

In this section we shall use the techniques developed by L. Makar-Limanov and A. Crachiola to prove theorem 4.3.1. We shall prove that $\text{AK}(A) = k[x]$. From this we conclude that $A \not\cong k^{[3]}$. The purpose of this chapter is to make the counterexample to cancellation problem in characteristic $p$ easily readable and to put the whole proof present in one place.

Let $k$ be a field with $\text{char}(k) = p > 0$ and

$$A = k[X, Y, Z, T]/(X^mY + C(X, Z, T) + (\alpha_1Z^c + \alpha_2T^d)c),$$

where $\alpha_1, \alpha_2 \in k^*$ and $m, c, d, e$ are positive integers such that $e \geq 1$, $m > 1$, $c = \gcd(c, d)\hat{c}$, $d = \gcd(c, d)d$ with $\hat{c} > 1$ and $\hat{d} > 1$. Moreover we place the condition that if either $\hat{c}$ or $\hat{d}$ is a power of $p$, then $\gcd(c, d)$ is a power of $p$. In addition we write $C(X, Z, T) = \sum_{1 \leq i} C_i(Z, T)X^i$ with $C_i(Z, T) \in k[Z, T]$ for all $i \geq 0$ and suppose that the polynomial $C_0(Z, T)$ is the sum of monomials $c_{i, \eta}Z^\eta T^n$ such that $d\zeta + c\eta < cde$ for all $(\zeta, \eta) \in Z_{\geq 0}^2$. Let $x, y, z, t \in A$ denote the cosets of $X, Y, Z, T$, respectively. If we wish to emphasize a choice of $k$, we write $A = A_k$. We shall prove

Theorem 4.3.1. $\text{AK}(A) = k[x]$ for any field $k$ with $\text{char}(k) = p > 0$. 
Since $\operatorname{AK}(k^{[3]}) = k$, we have

**Corollary 4.3.2.** \( A \not\cong k^{[3]} \) for any field \( k \) with \( \operatorname{char}(k) = p > 0 \).

To prove theorem 4.3.1, we begin with the following lemma.

**Lemma 4.3.3.** \( x \in \operatorname{AK}(A) \).

**Proof.** If we prove the lemma under the assumption that \( k \) is algebraically closed, then the result will follow for any field. For suppose that \( K \) is a field with algebraic closure \( k \). Then \( A_K \otimes_K k = A_k \). Let \( \phi \in \operatorname{EXP}(A_K) \) and \( \phi \in \operatorname{EXP}(A_k) \). Since \( A_k^\phi \) is algebraically closed in \( A_K \), \( x \in A_K \cap A_k^\phi \) implies \( x \in A_k^\phi \). If we know that \( x \in A_K \) is an invariant of \( \phi \), then \( x \) must also be an invariant of \( \phi \). So let us now assume that \( k \) is algebraically closed.

Since \( k \) is algebraically closed we can replace in \( A, \alpha_1 Z^c \) by \( \bar{Z}^c \) and \( \alpha_2 T^d \) by \( T^d \) where \( \bar{Z} = \beta_1 Z \) with \( \beta_1^c = \alpha_1 \) and \( \bar{Z} = \beta_2 Z \) with \( \beta_2^c = \alpha_2 \). By omitting the bar notation we can rewrite

\[
A = k[X, Y, Z, T]/(X^m Y + C(X, Z, T) + (Z^c + T^d)^e).
\]

Let \( \phi : A \rightarrow A[U] \) be a nontrivial exponential map on \( A \). We have to show that \( x \in A^\phi \). Consider \( A \) as a subalgebra of \( k[x, x^{-1}, z, t] \) with \( y = -x^{-m}(C(x, z, t) + (z^c + t^d)^e) \). Ring \( A \) has the structure of a \( \mathbb{Z} \)-graded algebra over \( k \) with the following weights on the generators: \( w_1(x) = -1, w_1(y) = m, w_1(z) = 0, w_1(t) = 0 \). This grading induces a proper \( \mathbb{Z} \)-filtration \( \{A_i\} \) on \( A \), where \( A_i \) consist of all \( a \in A \) with \( w(a) \leq i \). For any \( f \in A \) let \( \tilde{f} \) denote the \( w_1 \)-homogeneous part of \( f \) in \( \operatorname{gr}(A)(\cong A) \) of highest degree. With \( \bar{y} \) denoting the homogeneous summand of highest degree of \( y \), we have \( \bar{y} = -\bar{x}^{-m}(C_0(z, t) + (z^c + t^d)^e) \). So the corresponding graded domain \( \operatorname{gr}(A) \) is generated by \( \bar{x}, \bar{y}, \bar{z}, \bar{t} \) and is subject to the relation \( \bar{x}^{-m}\bar{y} = -(C_0(z, t) + (z^c + t^d)^e) \). (There cannot be any other relations because \( \bar{x}, \bar{z} \) and \( \bar{t} \) are algebraically independent.) We continue to write \( x, y, z, t \) in place of \( \bar{x}, \bar{y}, \bar{z}, \bar{t} \), respectively. Then

\[
\operatorname{gr}(A) = k[X, Y, Z, T]/(X^m Y + C_0(Z, T) + (Z^c + T^d)^e).
\]

For a first step we show the following sublemma

**Sublemma 4.3.4.** \( A^\phi \subset k[x, z, t] \).

**Proof.** On the contrary suppose that there exist \( g \in A^\phi \) such that \( g \notin k[x, z, t] \). By theorem 4.2.6, \( \phi \) induces a nontrivial exponential map \( \phi \) on \( \operatorname{gr}(A) \) such that \( \bar{g} \in \operatorname{gr}(A)^\phi \). Using the relation \( x^m y = -(C_0(z, t) + (z^c + t^d)^e) \), we can write \( \bar{g} = x^i y^j h(z, t) \) for some natural numbers \( i \) and \( j \) and some polynomial \( h(z, t) \in k[z, t] \). Since \( g \notin k[x, z, t] \), \( j \) must be positive. Also since a factor \( x^m y \) of \( \bar{g} \) can be absorbed into \( h(z, t) \) by the relation \( x^m y = -(C_0(z, t) + (z^c + t^d)^e) \), we have \( 0 \leq i < m \). We may assume \( i = 0 \): for if \( 0 < i < m \), then we can replace \( g \) by \( y^m \) in our arguments. Thus we have \( \bar{g} = y^i h(z, t) \) in \( \operatorname{gr}(A)^\phi \). Also, \( \operatorname{trdeg}_{k}(A^\phi) = 2 \) by lemma 4.2.1(4). So we can assume that \( h(z, t) \) is not a constant polynomial by replacing \( g \) if necessary with another element of \( A^\phi \). By lemma 4.2.1(1), \( \operatorname{gr}(A)^\phi \) is factorially closed. So both \( y \) and \( h(z, t) \) belong to \( \operatorname{gr}(A)^\phi \).
Consider \( \text{gr}(A) \) as a subalgebra of \( k[x, x^{-1}, z, t] \) with \( y = -x^{-m}(C_0(z, t) + (z^e + t^d)e) \). We note that \( k[x, x^{-1}, z, t] \) has the structure of a \( \mathbb{Z} \)-graded algebra over \( k \), say \( k[x, x^{-1}, z, t] = \bigoplus_{n \in \mathbb{Z}} K_i \), with the following weights on the generators \( w(x) = 0, w(z) = d, w(t) = c \). Consider a proper \( \mathbb{Z} \)-filtration \( \{B_n\}_{n \in \mathbb{Z}} \) on \( \text{gr}(A) \) defined by \( B_n := \text{gr}(A) \cap \bigoplus_{i \leq n} K_i \). Notice that under the relation \( x^m y = -(C_0(z, t) + (z^e + t^d)e) \) any \( f \in \text{gr}(A) \) can be uniquely expressed as

\[
 f = \sum_{r \geq 0} f_r(z, t)x^r + \sum_{0 \leq i < m, j > 0} f_{ij}(z, t)x^iy^j
\]

where \( f_r(z, t), f_{ij}(z, t) \in k[z, t] \). From the unique expression of any element \( f \in \text{gr}(A) \), it is easy to see that the filtration defined on \( \text{gr}(A) \) is admissible with the generating set \( \{x, y, z, t\} \). For each \( f \in \text{gr}(A) \), let \( \tilde{f} \in \text{gr}(\text{gr}(A)) \) denote the top part of \( f \). Thus by remark 1.1.4(2) \( \text{gr}(\text{gr}(A)) \) is generated by \( \tilde{x}, \tilde{y}, \tilde{z}, \tilde{t} \). Since we can see \( \text{gr}(\text{gr}(A)) \) as a subalgebra of \( \text{gr}(k[x, x^{-1}, z, t]) \cong k[x, x^{-1}, z, t] \), the elements \( \tilde{x}, \tilde{z}, \tilde{t} \in \text{gr}(A) \) are algebraically independent over \( k \). Since \( w(x^m y) = w((z^e + t^d)e) = cde \) and by our assumption each monomial in polynomial \( C_0(z, t) \) has weight strictly less than \( cde \), we have the top part \( \tilde{x}^m \tilde{y} + (\tilde{z}^e + \tilde{t}^d)e = 0 \) in \( \text{gr}(\text{gr}(A)) \). The polynomial \( X^m Y + (Z^e + T^d)e \) being linear in \( Y \) is irreducible in \( k[X, Z, T, Y] \cong k[X, Y, Z, T] \). Thus \( k[X, Y, Z, T]/(X^m Y + (Z^e + T^d)e) \) is integral domain. This gives

\[
 \text{gr}(\text{gr}(A)) \cong k[X, Y, Z, T]/(X^m Y + (Z^e + T^d)e).
\]

We continue to write \( x, y, z, t \) in place of \( \tilde{x}, \tilde{y}, \tilde{z}, \tilde{t} \) for the elements of \( \text{gr}(\text{gr}(A)) \). Denote \( \text{gr}(\text{gr}(A)) \) by \( D \). The effect of imposing \( w \) on \( A \) is to refine the top part that were obtained via \( w_1 \), so that on the elements \( x, y, z, t \) there are two weights: the primary weights given by \( w_1 \) and the secondary weights given by \( w \). By theorem 4.2.6, \( \tilde{\phi} \) induces a nontrivial exponential map \( \phi \) on \( D \), a refinement of \( \tilde{\phi} \) such that \( k[y, \tilde{h}(z, t)] \subset D^\phi \). Since \( k \) is an algebraically closed field, we can decompose \( \tilde{h}(z, t) \) as

\[
 \tilde{h}(z, t) = \nu z^\alpha t^\beta \prod_i (z^{e_i} + \lambda_i t^d)
\]

for \( \nu, \lambda_i \in k^*, \alpha, \beta \in \mathbb{N} \). Since \( D^\phi \) is factorially closed we have \( z, t, z^e + \lambda_i t^d \in D^\phi \) for each \( \lambda_i \). In the rest of the proof we shall exhaust all these possibilities. Our final contradiction will occur when we cannot reconcile this observation with the above factorization of \( \tilde{h}(z, t) \).

Suppose \( t \in D^\phi \). Then \( k[y, t] \subset D^\phi \). Thus \( D^\phi \) contains two algebraically independent elements \( y, t \in D \) over \( k \). In fact, since \( D^\phi \) is algebraically closed in \( D \) (lemma 4.2.1(2)) and \( \text{tr.deg}_k(D^\phi) = 2 \), we have \( D^\phi = k[y, t] \). By remark 4.2.4 \( \tilde{\phi} \) induces a nontrivial exponential map \( \phi \) on the domain

\[
 S^{-1}D = k(y, t)[x, z]/(x^m y + (z^e + t^d)e)
\]

such that \( (S^{-1}D)^\phi = k(y, t) \), where \( S = D^\phi \setminus \{0\} = k[y, t] \setminus \{0\} \). By lemma 4.2.1(2), \( (S^{-1}D)^\phi = k(y, t) \) is algebraically closed in \( S^{-1}D \). But \( \text{tr.deg}_k(y, t)(S^{-1}D) = 1 \) and \( S^{-1}D \not\cong k(y, t)[t] \), a contradiction to lemma 4.2.2.
Thus $t \notin D^\phi$.

Now suppose that $z \in D^\phi$. This gives $D^\phi = k[y, z]$ and similar to the previous case we get a nontrivial exponential map $\tilde{\phi}_1$ on the domain

$$S_1^{-1}D = k(y, z)[x, t]/(x^m y + (z^c + t^d)^\gamma)$$

such that $(S_1^{-1}D)^{\tilde{\phi}_1} = k(y, z)$, where $S_1 = D^\phi \setminus \{0\} = k[y, z] \setminus \{0\}$. By lemma 4.2.1(2), $(S_1^{-1}D)^{\tilde{\phi}_1} = k(y, z)$ is algebraically closed in $S_1^{-1}D$. Again $tr.\text{deg}_{k(y, z)}(S_1^{-1}D) = 1$ and $S_1^{-1}D \not\cong k(y, z)^{[1]}$, a contradiction to lemma 4.2.2. Thus $z \notin D^\phi$. As $D^\phi$ is factorially closed, $\alpha = 0$ and $\beta = 0$ in the above factorization of $\tilde{h}(z, t)$.

Suppose now that $z^c + \lambda_t t^d \in D^\phi$ then $k[y, z^c + \lambda_t t^d] \subset D^\phi$. If neither $c$ nor $d$ are powers of $p$ then by lemma 4.2.5 we have $z, t \in D^\phi$, which we just have shown impossible. Thus we can suppose $c$ or $d$ is power of $p$ (both cannot be power of $p$ as $\text{gcd}(c, d) = 1$). In this case by our assumption $\text{gcd}(c, d) = p^s$ for some $s \geq 1$.

Ignoring multiplicity we can see that there is only one factor of the form $z^c + \lambda_t t^d \in D^\phi$. Indeed, given two such factors of this type there difference belongs to $D^\phi$ from which we conclude that $z^c + \lambda_t t^d \in D^\phi$. Since $D^\phi$ is factorially closed we have $z, t \in D^\phi$, which we just have shown to be impossible. Also $z^c + t^d$ cannot be a factor of $\tilde{h}(z, t)$, since otherwise we would have $x^m y = -(z^c + t^d)^\nu \in D^\phi$. This gives three algebraically independent elements $x, y, z^c + t^d \in D^\phi$. Thus $D^\phi = D$, contradicting the nontriviality of $\tilde{\phi}$ (by definition of exponential map). Thus

$$\tilde{h}(z, t) = \nu(z^c + \lambda t^d)^\gamma$$

for some $\gamma \in \mathbb{N}$ and $\nu, \lambda \in k^*$ with $\lambda \neq 1$.

Now to exclude the possibility that $z^c + \lambda t d \in D^\phi$, we note that for every $\mu \in k^*$, $z^c + \lambda t d - \mu$ is a prime element of $k[z, t]$ by lemma 4.2.9 and $(z^c + t d) \notin (z^c + \lambda t d - \mu)k[z, t]$. Thus $(z^c + \lambda t d - \mu)$ is a prime element of $D$ by lemma 4.2.8(1). Thus by lemma 4.2.7 there exist $\gamma \in k^*$ such that $\phi$ induces a non-trivial exponential map $\tilde{\phi}_2$ on $D/(z^c + \lambda t d - \gamma)$ with the image of $y$ in $E := D/(z^c + \lambda t d - \gamma)$ lying in the ring of invariants of $\tilde{\phi}_2$. Set $g_0 = z^c + t^d$, $g_1 = g_0^\nu = (z^c + t^d)^\nu$ and $g_2 = z^c + \lambda t d - \gamma$. Since $\lambda \neq 1$, $g_2$ and $g_0$ are not conomaxial in $k[z, t]$. Let $M$ be a maximal ideal of $k[z, t]$ containing $g_2$ and $g_0$. Then $g_1 = g_0^\nu \in M^2$ since $s \geq 1$. Thus by lemma 4.2.8(2) there does not exist any nontrivial exponential map $\xi$ on $E$ such that the image of $y$ belongs to $D^\xi$. This contradiction proves the sublemma.

We are now in the position to prove that $x \in A^\phi$. On the contrary suppose $x \notin A^\phi$. If $g \in A^\phi \subset k[x, z, t]$, write $g = x g_1(x, z, t) + g_2(z, t)$ with $g_2 \neq 0$ as $x \notin A^\phi$. Consider $\text{gr}(A) \cong A$ given by $w_1$. As $w_1(x g_1(x, z, t))$ is negative and $w_1(g_2(z, t)) = 0$, we have $g = g_2(z, t) \in \text{gr}(A)^\phi$. As $tr.\text{deg}_k(A^\phi) = 2$ by part (4) of lemma 4.2.1, there exist some $f \in A^\phi$ algebraically independent with $g$ over $k$. We write $f = x f_1(x, z, t) + f_2(z, t)$, where $f = f_2(z, t) \neq 0$. Suppose $f_2, g_2$ are algebraically dependent over $k$, then $P(f_2, g_2) = 0$ for some $P \in k^{[2]}$. Since $f, g$ are algebraically independent in $A^\phi$ we have
Theorem 4.4.2. Given \( k \) \( p \)-localization of ring of integer, \( G \) we consider two classes of maps \( \phi \). Let \( \phi \) be actually more general, but the simple parameters chosen serve our purposes.

In [Asa87], Asanuma gave the following example: (Asanuma’s example of Asanuma 4.4 An important example of Asanuma 55)

Proof. of theorem 4.3.1
We know by lemma 4.3.3 that \( k \) \( P \) is algebraically closed in \( \text{gr} \) (part (1) of lemma 4.2.1), we deduce \( \text{gr} \) is algebraically closed in \( \text{gr} \). Now \( x^m = - (C_0(z, t) + (z^c + m^d) \gamma) \in \text{gr} \), and this implies that \( x, y \in \text{gr} \). Thus \( \text{gr} \) is trivial, contradicting our assumption that \( x \notin \text{gr} \). Hence \( x \in \text{gr} \) for every \( \phi \in \text{EXP} \).

\[
\phi_1(x) = x, \\
\phi_1(y) = C(x, z + x^m f(x, t) U, t) + (\alpha_1(z + x^m f(x, t) U)^\gamma + \alpha_2 t d)^e, \\
\phi_1(z) = z + x^m U, \\
\phi_1(t) = t.
\]

Since \( k \) \( k \) is algebraically closed in \( A \) and of transcendence degree 2, the ring of \( \phi_1 \)-invariants is \( k \). Define \( \phi_2 : A \to A[U] \) by

\[
\phi_2(x) = x, \\
\phi_2(y) = C(x, z, t + x^m f(x, z) U) + (\alpha_1 z^e + \alpha_2 t + x^m f(x, z) U)^d)^e, \\
\phi_2(z) = z, \\
\phi_2(t) = t + x^m U.
\]

Again, the ring of \( \phi_2 \)-invariants is \( k \). Thus \( AK(A) \subset k[t] \cap k[x, z] = k[x] \) and hence \( AK(A) = k[x] \).

4.4 An important example of Asanuma

In [Asa87], Asanuma gave the following example: (Asanuma’s example is actually more general, but the simple parameters chosen serve our purposes).

Definition 4.4.1. Let \( A := k[w][x, y, z]/(G + w^m z) \) where \( m \) is a positive integer, \( G = -x^p + y + y^p \), \( k \) is field of characteristic \( p \), \( k[w][w] \) is the localization of ring \( k[w] \) by its prime ideal \( (w) \) and \( s \) is a positive integer such that \( p \nmid s \).

Notice that we have quotient field \( k(w) = k[w][w^{-1}] \) and residue field \( k = k[w]/w k[w][w] \).

Theorem 4.4.2. Given \( A \) as above, then
1. \( A \otimes k(w) = A[w^{-1}] \cong k(w)[w] \)

2. \( A \otimes k[w] k[w]/wk[w] = A/(w) \cong k^{[2]} \)

3. \( A^{[1]} \cong k[w]^{[3]}(w) \).

We first prove the following lemma.

**Lemma 4.4.3.** Let \( k \) be field of characteristic \( p > 2 \), \( s \) any fixed integer greater than or equal to 2, and \( G = -x^{p^2} + y + y^{sp} \in k[x, y] \). Then \( k[x, y]/(G) \cong k^{[1]} \).

**Proof.** Let \( k^{[1]} = k[z] \). Define a ring homomorphism \( \phi : k[x, y] \longrightarrow k[z] \) by \( x \mapsto z^{sp} + z, y \mapsto z^{p^2} \). Since \( \phi(x - (x^p - y^s)^s) = z^{sp} + z - (z^{sp} + z^{p^2} - z^{sp})^s = z \), \( \phi \) is surjective. Notice that \( \text{Ker}(\phi) \) must be a height 1 prime ideal, since the Krull dimensions of \( k[x, y] \) and \( k[z] \) are equal to 2 and 1 respectively. Since \( k[x, y] \) is Noetherian and an UFD, \( \text{Ker}(\phi) \) is a principal ideal (a Noetherian integral domain is a unique factorization domain if and only if every height 1 prime ideal is principal). As \( \phi(G) = \phi(-x^{p^2} + y + y^{sp}) = -z^{sp} - z^{p^2} + z^{p^2} + z^{sp} = 0 \), we have \( (G) \subseteq \text{Ker}(\phi) \). Now to show that \( \text{Ker}(\phi) = (G) \) it is sufficient to show that \( G \) is irreducible over the field \( k \). Let \( \beta \) be an element of an extension field of \( k = k(y) \) such that \( \beta^{p^2} = \alpha := y^{sp} + y \). Then \( G = -\beta^{p^2} + \alpha = (-x + \beta)^{p^2} \) over \( K(\beta) \). Let \( 1 \leq i \leq p^2 \) be minimal such that \( (-x + \beta)^i \in K[x] \). Then \( (-x + \beta)^i \) is irreducible over \( K \), and in fact the only irreducible factor of \( G \) (since two positive powers of \(-x + \beta \) cannot be coprime). Hence \( G \) is a power of \((-x + \beta)^i \), and \( i \mid p^2 \). Now suppose \( i = 1 \) or \( i = p \). Then \(-x^{p^2} + \beta^p = (-x + \beta)^p \in K[x] \), so \( \alpha = (\beta^p)^p \in K^p = k(y^p) \), a contradiction. As a result, \( m = p^2 \), and the conclusion is that \( G \) is irreducible over \( K \). Thus by first isomorphism theorem \( \phi \) is required isomorphism. \( \square \)

**Proof.** of theorem 4.4.2

(1) Note that \( A \) can be seen as a subring of \( k(w)[x, y] \) where \( z = w^{-m} G \), i.e. \( A = k[w][w][x, y, w^{-m} G] \). Now \( A[w^{-1}] = k[w][x, y, w^{-m} G] \cong k(w)[x, y] \).

(2) \( A/(w) = k[w][w], y, z]/(G + w^m z, w) = k[w][w][x, y, z]/(G, w) = k[x, y, z]/(G) \) but by lemma 4.4.3 \( k[x, y]/(-x^{p^2} + y + y^{sp}) \cong k^{[1]} \), so \( A/(w) \cong k^{[2]} \).

(3) Let \( A^{[1]} = A[T] \). We will give explicit generators. First, define \( B = x^p - y^s \) and \( f(x, y) = x - B^p \). Note that

\[
B(t + t^{sp}, t^p) = (t + t^{sp})^p - (t^p)^s = t^p
\]

and

\[
f(t + t^{sp}, t^p) = (t + (t^{sp})^p - (t^p)^s)^s
= t + t^{sp} + (t^p + t^{sp^2} - t^{sp^2})^s
= t + t^{sp} - t^{sp}
= t
\]

We define the following elements of \( k(w)[x, y, T] \):

\[
H = w^m T + f,
F = \frac{1}{w^m} (x - H - H^{sp}),
E = \frac{1}{w^m} (y - H^{p^2}),
\]

and claim that \( H, F, E \) generate \( A[T] \). Define \( S := k[w](H, F, E) \). \( S \subseteq A[T] \):
We need to show $F, E \in A[T]$. Note that $G, w^m \in w^m A[T]$ so if we show that $w^m F \mod (w^m, G) = 0$ then $w^m F \in w^m A[T]$ and $F \in A[T]$. Note that we are computing modulo $w^m$, but we explicitly state that $G$ in $w^m A$ thus that we can compute modulo $G$ as well. Now,

$$B^p \equiv x^{p^2} - y^{sp} \equiv y \mod (w^m, G)$$

so

$$f^p \equiv (x - B^s)^p \equiv x^p - (B^s)^p \equiv x^p - y^s \equiv y \mod (w^m, G)$$

meaning that

$$w^m F \equiv x - H - H^{sp} \equiv x - f - f^{sp} \equiv x - (x - B^s) - B^s \equiv 0 \mod (w^m, G),$$

so that $w^m F \in w^m A[T], \text{ and } F \in A[T]$. Now,

$$w^m E \equiv y - H^{sp^2} \equiv y - (f^p)^p \equiv y - B^p \equiv y - y \equiv 0 \mod (w^m, G).$$

Thus $E \in A[T], \ A[T] \subseteq S$:

It is easy to show $x, y \in S$ as

$$x = w^m F + H + H^{sp},$$

$$y = w^m E + H^{p^3}$$

We need to show $T, \frac{1}{w^m} G \in S$. We will now show that $G \in w^m S$, meaning $\frac{1}{w^m} G \in S$:

$$G = -x^{p^2} + y + y^{sp}$$

$$\equiv - (w^m F + H + H^{sp})^{p^2} + (w^m E + H^{p^3}) + (w^m E + H^{p^2})^{sp} \mod w^m S$$

$$\equiv - H^{p^2} - H^{sp^3} + H^{p^2} + H^{sp^3} \mod w^m S$$

$$= 0 \mod w^m S.$$

For $T$ we do the following computations:

$$f = f(w^m F + H + H^{sp}, w^m E + H^{p^2})$$

$$\equiv f(H + H^{sp}, H^{p^3}) \mod w^m S$$

$$\equiv H \mod w^m S$$

thus

$$w^m T = H - f \equiv 0 \mod w^m S$$

thus $w^m T \in w^m S$, and hence $T \in S$.

In conclusion, $A[T] = S = k[w]_{(w)}[H, F, E] \cong k[w]_{(w)}^{[3]}$.

\[\square\]

**Corollary 4.4.4.** Let $k$ be a field of characteristic $p$. Let $A = k[w][x, y, z]/(G + w^m z)$ where $m \geq 1, G = -x^{p^2} + y + y^{sp},$ and $s$ is a positive integer such that $p \nmid s$. Then $A$ satisfies
1. \( A \otimes k(p) \cong k(p)[2] \) for each prime ideal \( p \subset k[w] \), i.e.,

\[ A^{[1]} \cong k[w][3], \text{ i.e., } A \text{ is an } \mathbb{A}^2_k \text{ fibration over } \mathbb{A}^1_k = \text{Spec}(k[w]). \]

Proof. (1) Note that \( A \) can be seen as a subring of \( k(w)[x, y] \) where \( z = w^{-m}G \), i.e. \( A = k[w][x, y, w^{-m}G] \). Thus \( A \otimes k(w) = k(w)[x, y] \). Let \( k[w]_p \) be the localization at the prime ideal \( p \subset k[w] \). Then \( A \otimes k[w]_p = k[w][x, y, w^{-m}(x^p - y - y^p)] \). If \( p = (w) \), then by theorem 4.4.2(2) \( A \otimes k[w](w)/wk[w](w) = k[2] \). If \( p \neq (w) \) then \( A \otimes k[w]_p = k[w]_p[x, y] \) and hence \( A \otimes k[w]_p/k[w]_p = k[w]_p[x, y] = k(p)[2] \).

(2) If \( p = (w) \) then \( A \otimes k[w](w) = k[w](w)[x, y, z]/(G + w^mz) \) and so we have \( (A \otimes k[w](w))[1] \cong k[w][3] \) by theorem 4.4.2(3). Now if \( p \neq (w) \), then
\[ A \otimes k[w]_p = k[w]_p[x, y, z]/(G + w^mz) = k[w]_p[x, y, w^{-m}(x^p - y - y^p)] = k[w]_p[x, y]. \]
Thus for the case \( p \neq (w) \) then
\[ (A \otimes k[w]_p)^[1] = k[w]_p[x, y][1] = k[w][3]. \]

Hence for any prime ideal \( p \) of \( k[w] \) we have \( A^{[1]} \otimes k[w]_p = k[w][3] \). This shows that \( A^{[1]} \) is locally a polynomial \( k[w] \)-algebra, and by a result of Bass-Connell-Wright [BCW76] (“locally polynomial algebras are symmetric algebras”) we get that \( A^{[1]} \cong k[w][3] \). \( \square \)

It is worth pointing out a distinction between characteristic 0 and characteristic \( p \). Assertion 1 of Corollary 4.4.4 says that \( \text{Spec}(A) \to \text{Spec}(k[w]) \) is an \( \mathbb{A}^2_k \) fibration. Sathaye’s theorem in [Sat83] says in characteristic 0 that an affine \( \mathbb{A}^2_k \) fibration over a smooth curve is an \( \mathbb{A}^2_k \) bundle. But, because the base is affine, the Bass Connell Wright theorem says that it is a vector bundle hence trivial because the base is the affine line.

So in characteristic 0, an algebra \( A \) satisfying the conditions of Assertion 1 has to be a polynomial ring in three variables.

### 4.5 Cancellation counterexamples

Reshuffling some variables, we can rewrite the example from corollary 4.4.4 as
\[ A = k[x, y, z, t]/(x^m y + z^2 + t^p). \]

Joining corollary 4.3.2 for \( m = 2 \) with corollary 4.4.4 part (2) we get that \( A \) is a counterexample to cancellation in characteristic \( p \).
Chapter 5

On surjectivity of quotient maps

5.1 Introduction

Let \( R \) be a ring containing \( \mathbb{Q} \). In [VDEMV07], Van den Essen, Maubach and Vénéreau prove that the map \( \text{SA}_n([R[x]]) \to \text{SA}_n(R[x]/(x^m)) \) is surjective. This result has strong consequences in [VDEMV07; DMJP14; BVDEW12]. In this chapter we extend this result. Moreover we give a partial answer to the question when the natural map \( \text{Aut}_k(k[[n]]) \to \text{Aut}_k(k[[n]]/a) \) is surjective, where \( k \) is a field of characteristic 0 and \( a \) is ideal in \( k[[n]] \).

5.2 Surjectivity theorem

Let \( A \) be a commutative ring. We define the group

\[ \text{SA}_n(A) = \{ F \in \text{GA}_n(A) \mid \det \text{Jac}(F) = 1 \} \]

Definition 5.2.1. If \( A \) is a commutative ring, and \( a \) an ideal of \( A \), then we define

\[ \pi : \text{GA}_n(A) \to \text{GA}_n(A/a) \]

and

\[ \sqrt{\pi} : \text{GA}_n(A) \to \text{GA}_n(A/\sqrt{a}) \]

where \( \sqrt{a} \) is the radical of \( a \). For any element \( f \) having coefficients in \( A/a \) or \( A \) we write “\( \bar{f} \)” for its image in \( A/\sqrt{a} \).

We want to prove the following:

Theorem 5.2.2. Let \( A \) be a Noetherian commutative ring containing \( \mathbb{Q} \) and \( a \) an ideal of \( A \). Suppose \( f \in \text{SA}_n(A/a) \). Then there is equivalence between

1. \( \bar{f} \in \sqrt{\pi}(\text{SA}_n(A)) \),
2. \( f \in \pi(\text{SA}_n(A)) \).

We will prove this theorem in several steps. We begin with the following lemma.

Lemma 5.2.3. Let \( G, H \in \text{MA}_n(A) \), \( a \) an ideal of \( A \). Suppose that \( a \in A \) satisfies \( a^2 \in a \), and write \( g := I + aG, h := I + aH \). Write \( \bar{h} := h \mod a \) etc. Then

1. \( \bar{h} \circ \bar{g} = I + a(H + G) \mod a \)
2. $\tilde{h} \in GA_n(A/a)$ (having inverse $I - aH \mod a$)

3. $\tilde{h} \in SA_n(A/a)$ if and only if \( \text{Div}(H) := \frac{\partial}{\partial x_1} H_1 + \ldots + \frac{\partial}{\partial x_n} H_n = 0 \mod a \).

Proof. (1) and (2) are immediate. To see (3), just observe that $\det(\text{Jac}(h)) = 1 + \tilde{a} \text{Div}(H)$.

The following remark is useful in the proof of lemma 5.2.6.

**Remark 5.2.4.** Let $f = (x + aF, y + aG) \in MA_2(A)$ where $a^2 = 0$. Suppose $F = \sum_{i=0}^t M_i, G = \sum_{i=0}^t N_i$ where $M_i, N_i$ are monomials in $x, y$. Then by using 5.2.3(1) we can split $f$ into $(x + aM_1, y)(x + aM_2, y)...(x + aM_s, y)(x, y + aN_1)...(x, y + aN_t)$. If we want to incorporate $\det(\text{Jac}(f)) = 1$ and still write it as product of monomials (which is what happens in the middle of the proof of 5.2.6) then we can link each $M_i$ with one $N_i$, where $\frac{\partial M_i}{\partial x} = -\frac{\partial N_i}{\partial y}$ gives that $a \frac{\partial M_i}{\partial x} + a \frac{\partial N_i}{\partial y} = 0$. In this case, $f = (x + aM_1, y - aN_1)(x + aM_2, y - aN_1)...(x + aM_s, y - aN_t)$.

**Lemma 5.2.5.** Given $M = x^i y^j$ where $d = i + j$, then $M$ is a $\mathbb{Q}$-linear combination of $(x + qy)^d$ where $0 \leq q \leq d$.

Proof. $(x + qy)^d = \sum_{i=0}^d \binom{d}{i} q^i x^{d-i} = \left( \binom{d}{0} q^0 \binom{d}{1} q^1 \ldots \binom{d}{d} q^d \right) \left( \begin{array}{c} y^d \\ xy^{d-1} \\ \vdots \\ x^d \end{array} \right) = DA \left( \begin{array}{c} y^d \\ xy^{d-1} \\ \vdots \\ x^d \end{array} \right)$

where

$$D = \text{Diag} \left( \binom{d}{0}, \binom{d}{1}, \binom{d}{2}, \ldots, \binom{d}{d} \right), \ A = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ 0 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & d \end{pmatrix}.$$
5.2. Surjectivity theorem

$D$ and $A$ are both invertible, so we can find a matrix $M = (DA)^{-1}$ such that

$$
M \begin{pmatrix} x^d \\ (x + y)^d \\ (x + 2y)^d \\ \vdots \\ (x + dy)^d \end{pmatrix} = \begin{pmatrix} y^d \\ xy^{d-1} \\ \vdots \\ x^d \end{pmatrix}
$$

which proves the lemma.

\[\square\]

**Lemma 5.2.6.** Theorem 5.2.2 holds for the case $n = 2$ and $\sqrt{a} = (a, a)$ where $a^2 \in a$.

**Proof.** (2) implies (1), so let us assume (1). The below proof is essentially corollary 3.3 in [VDEMV07], we refer to that paper for a slightly more detailed proof. If $F$ is the preimage of $\overline{f}$ in $\text{SA}_n(A)$, then we can consider $(F^{-1} \mod \text{rad } a)f$ in stead of $f$, so we can assume that $f$ is the identity. So we can write $f = (x_1, x_2) + a(H_1, H_2)$. Since $\det(\text{Jac}(f)) = 1$ we get that $\frac{\partial}{\partial x_1} H_1 + \frac{\partial}{\partial x_2} H_2 = 0$ by 5.2.3 part (3). So there exists $P \in A[x_1, x_2]$ such that $H_1 = P_{x_2}$ and $H_2 = -P_{x_1}$. (see [Ess00], 1.3.53). So $f = (x_1, x_2) + a(P_{x_2} - P_{x_1})$. Since $P$ is a sum of monomials, it follows from lemma 5.2.3 part (1) that we may assume that $P = r x_1^i x_2^j$ for some $r \in A$ and $i, j \geq 0$. By lemma 5.2.5 each monomial $x_1^i x_2^j$ is a $\mathbb{Q}$-linear combination of the $d := i + j$ polynomials of the form $(x_1 + q x_2)^d$ where $q$ runs from 0 to $d$. Therefore, again by lemma 5.2.3 part (1), we may assume that $P = r L^d$ for some $r \in A$ and $d \in \mathbb{N}$ where $L = x_1 + q x_2$ and $q \in A, 0 \leq q \leq d$.

Finally, consider the derivation $D := a((r L^d) x_1 \partial x_1 - (r L^d) x_2 \partial x_2) = ar L^{d-1}(q \partial x_1 - \partial x_2)$. It is easy to check that $D$ is a locally nilpotent derivation on $A[x_1, x_2]$, hence $G = \exp(D) = (x_1, x_2) + a(P_{x_2} - P_{x_1}) \in GA_2(A)$. From the special form of $P$ it follows that $\det(\text{Jac}(G)) = 1$. So $G \in SA_2(A)$. Since $H_1 = P_{x_2}, H_2 = -P_{x_1}$ it follows that $G \mod a = f$, as desired.

\[\square\]

**Lemma 5.2.7.** Theorem 5.2.2 holds for the case that $\sqrt{a} = (a, a)$ where $a^2 \in a$.

**Proof.** The proof is essentially corollary 3.3 in [VDEMV07]. We give merely a proof-sketch here. Again (2) implies (1), so we assume (1). We can assume $f = (x_1, \ldots, x_n) + a(H_1, \ldots, H_n)$. Lemma 5.2.6 applied to the case $SA_2(A[x_1, \ldots, x_{n-2}])$ we find an element $F \in SA_2(A[x_1, \ldots, x_{n-2}])$ such that $F \mod a = (x_1, \ldots, x_{n-2}, x_{n-1} + a K, x_n - a H_n)$. Thus replacing $f$ by $(F \mod a)f$ we can assume that $H_n = 0$; applying an induction argument we can assume that $f = (x_1 + a H_1, x_2 + a H_2, x_3, \ldots, x_n)$. Now we apply lemma 5.2.6 for the case $SA_2(A[x_3, \ldots, x_n])$ and we are done.

\[\square\]

**Lemma 5.2.8.** Let $a$ be an ideal in a Noetherian commutative ring $A$ containing $\mathbb{Q}$. Then there exists a finite chain $\sqrt{a} = a_0 \supseteq a_1 \supseteq a_2 \supseteq \ldots \supseteq a_n = a$ and elements $a_1, a_2, \ldots, a_n \in \sqrt{a}$ such that for each $0 \leq i \leq n - 1$, $a_i^2 \in a_i$ and $a_{i-1} = (a_i, a_i)$.

**Proof.** Since $A$ is Noetherian, all ideals are finitely generated. Let $\sqrt{a} = (r_1, \ldots, r_m)$. Then there exists some $n \in \mathbb{N}$ such that $r_i^2 \in a$ all $1 \leq i \leq n$, so $(\sqrt{a})^n \subseteq a$. 

We claim that it is enough to show the lemma for the case \( a_n = (\sqrt{a})^n \), i.e. we can find a chain \( \sqrt{a} = a_0 \supseteq a_1 \supseteq a_2 \supseteq \ldots \supseteq a_n = (\sqrt{a})^n \) and corresponding elements \( a_i \in \sqrt{a} \) such that \( a_i^2 \in a_i \), \((a_i, a_i) = a_i \). For then we can pick the same elements \( a_i \) and expand the chain by \( a \) to get the chain \( \sqrt{a} = a_0 \supseteq (a_1 + a) \supseteq (a_2 + a) \supseteq \ldots \supseteq (a_n + a) = (\sqrt{a})^n + a = a \).

We will prove the existence of such an ideal chain by induction to \( n \), i.e. we assume there exists a chain as said in the lemma from \( \sqrt{a} \) to \( (\sqrt{a})^{n-1} \). (For the case \( n = 1 \) is trivial.) We thus need to lengthen this chain from \( (\sqrt{a})^{n-1} \) to \( (\sqrt{a})^n \). Assume \( (\sqrt{a})^{n-1} = (s_1, \ldots, s_{m}) \). We have \( s_i^2 \in (\sqrt{a})^n \), and now we define a chain of ideals \( b_m := (\sqrt{a})^n, b_i := (b_{i+1}, s_{i+1}) \) for \( 0 \leq i \leq m - 1 \). It is clear that this chain \( (\sqrt{a})^{n-1} = b_0 \supseteq b_1 \supseteq \ldots \supseteq b_{m-1} \) and corresponding elements \( s_1, \ldots, s_m \) extends the chain.

**Proof.** (of theorem 5.2.2) The implication \( (2) \implies (1) \) is immediate. So assume \( f \in \sqrt{\pi}(A) \). Lemma 5.2.8 now yields a chain of ideals \( \sqrt{a} = a_0 \supseteq a_1 \supseteq a_2 \supseteq \ldots \supseteq a_m = a \) and elements \( a_1, \ldots, a_m \) such that \( a_i = (a_{i+1}, a_{i+1}) \) for \( 1 \leq i \leq m \). Now \( f \in \sqrt{\pi}(A) \) means \( f \) mod \( a_0 \) in \( A/\sqrt{a} \) mod \( a_0 \). Applying lemma 5.2.7 to “\( f \) mod \( a_1 \in A/\sqrt{a} \) mod \( a_1 \)” implies “\( f \) mod \( a_1+1 \in A/\sqrt{a} \) mod \( a_1+1 \)” By induction we thus get \( f \) mod \( a_n \in A/\sqrt{a} \) mod \( a_n \), i.e. \( f \in \pi(A) \).

**Obstructions for being a group homomorphism**

If we assume that the map \( \sqrt{\pi} : A/\sqrt{a} \to A/\sqrt{a} \) has a section then theorem 5.2.2 gives a way to construct a section

\[
s : \text{SA}_n(A/\sqrt{a}) \to \text{SA}_n(A).
\]

which is a one-sided inverse \( \pi s(f) = f \). The construction does not fix this map \( s \) - one can define it in many ways. However, we need to point out that \( s \) is not made into a group homomorphism, and in fact, we think it is never possible except if \( n = 1 \) or \( a = \sqrt{a} \). (It is possible that \( \text{SA}_n(A/\sqrt{a}) \to \text{SA}_n(A) \) is a group homomorphism, for example if \( A/\sqrt{a} \) is isomorphic to a subring of \( A \).

For simplicity, let us assume that \( A \) is a \( K \)-algebra where \( K \) is a field of characteristic zero. The following lemma is obvious, but we state it here explicitly as the key point:

**Lemma 5.2.9.** Suppose \( A, B \) are \( K \)-algebras where \( K \) is a field of characteristic zero, and \( S_1 = \text{spec}(A), S_2 = \text{spec}(B) \). If \( s : \text{SA}_n(B) \to \text{SA}_n(A) \) is a group homomorphism, then \( s \) sends additive group actions on \( S_2 \) to additive group actions on \( S_1 \), which means:

Assume that given is an algebraic \((K, +)\)-action \( K \times S_2 \to S_2 \) by \((\lambda, y) \to f_\lambda(y) \) where \( f_\lambda \in \text{SA}_n(B) \). Then defining \( g_\lambda := s(f_\lambda) \), we get a \((K, +)\)-action \( K \times S_1 \to S_1 \) given by \((\lambda, x) \to g_\lambda(x) \).

**Proof.** \( s \) is a group homomorphism so \( g_\lambda g_\mu = g_{\lambda+\mu} \).

**Corollary 5.2.10.** If \( A \) is a \( K \)-algebra, \( n \geq 2 \), and \( a \neq \sqrt{a} \), then any section

\[
s : \text{SA}_n(A/\sqrt{a}) \to \text{SA}_n(A)
\]

is not a group homomorphism, where the map \( \text{SA}_n(A/\sqrt{a}) \to \text{SA}_n(A) \) is not a group homomorphism.
5.2. Surjectivity theorem

The idea of the proof of the above corollary is clear if one takes lemma 5.2.9 in mind: pick two additive group action in $SA_n(A)$ which do not commute, and pick them such that they commute in $SA_n(A/a)$. Indeed, in $SA_n(A/a)$ you find a huge commutative subgroup, namely if $a \in \sqrt{\alpha}, a \notin a$ such that $a^2 \in a$ then the maps of the form $I + aH$ all commute. Now the only issue is finding noncommuting additive group actions that, after taking quotients, end in this group, and then show that any additive group action mapping to these quotients does not commute:

Proof. Let $a \in \sqrt{\alpha}, a \notin a$ such that $a^2 \in a$. Write $a = a \mod a$. Define the following locally nilpotent derivations: $D = ax_1^2 \frac{\partial}{\partial x_1}, E = ax_1^2 \frac{\partial}{\partial x_2}$. They define additive group actions by defining $d_\lambda := \exp(\lambda D), e_\lambda := \exp(\lambda E)$ (which are both elements of $SA_n(A/a)$) when $\lambda \in K$. Note that $[D, E] = 0$ and thus $d_\lambda$ and $e_\mu$ commute.

Assume $s$ is a group homomorphism, then $s(d_\lambda), s(e_\mu)$ commute. Lemma 5.2.9 shows that there exist $D, E$ locally nilpotent derivations of $A[a]$ such that $s(d_\lambda) = \exp(\lambda D), s(e_\mu) = \exp(\mu E)$. Since $\pi s(d_\lambda) = d_\lambda \mod a = D$, and similarly $E \mod a = E$. Now $E \bar{D}(x_1) = a^2(2x_1^2x_2)$ thus $\bar{E} \bar{D}(x_1) \neq 0$, but $\bar{D} \bar{E}(x_1) = 0$. This means that $E, \bar{D}$ do not commute, and hence $s(d_1) = \exp(\bar{D})$ and $s(e_1) = \exp(\bar{E})$ do not commute, contradiction to proposition 1.1.9(2). Thus $s$ is not a group homomorphism.

The above might make the reader think that, even though $s$ is not a group homomorphism, one can make sure that subgroups isomorphic to $(K, +)$ are mapped to subgroups isomorphic to $(K, +)$. However:

Example 5.2.11. Let $A = \mathbb{C}[t]$ and $a = (t^2)$. Then $\delta = \bar{t}x_1^2 \frac{\partial}{\partial x_1}$ is a locally nilpotent derivation of $A/a[x_1, x_2, \ldots, x_n]$, but there does not exist a $\mathbb{C}[t]$-linear locally nilpotent derivation $D$ of $\mathbb{C}[t][x_1, x_2, \ldots, x_n]$ such that $D \mod a = \delta$.

Proof. Suppose $D$ is such a locally nilpotent derivation. We can make a grading on $\mathbb{C}[t][x_1, \ldots, x_n]$ by giving $t$ weight 1 and the other variables zero. Then by proposition 1.1.5, $D = D_1 + D_2 + \ldots + D_d$ where the $D_i$ are the homogeneous components. If $D$ is locally nilpotent, then $D_1$ and $D_d$ are locally nilpotent by lemma 1.1.6. Now $D_1 = t x_1^2 \frac{\partial}{\partial x_1}$ by assumption, which is not locally nilpotent, contradiction.

Concluding, one can state that the map $s : SA_n(A/a) \rightarrow SA_n(A)$ is a very nontrivial map (while the map $SA_n(A/\sqrt{\alpha}) \rightarrow SA_n(A)$ might be trivial). Perhaps this “unnaturality” explains its usefulness - it is quite non-trivial to construct such a map.

Special case

We can see the main theorem in [VDEM07] as a special case of theorem 5.2.2. Take $A = R[t]$ and $a = (t^m)$ in theorem 5.2.2. Consider $f \in SA_n(R[t]/(t^m))$ and take $\bar{f} = f \mod t \in SA_n(R[t]/(t)) \cong SA_n(R)$. This map $\bar{f}$ has preimage in $SA_n(R[t])$, that is $\bar{f} \in \sqrt{\pi}(SA_n(R[t]))$. Thus by theorem 5.2.2, $f \in \pi(SA_n(R[t]))$. This show $SA_n(R[t]/(t^m)) \subset \pi(SA_n(R[t]))$. The other direction is trivial and hence $\pi : SA_n(R[t]) \rightarrow SA_n(R[t]/(t^m))$ is surjective.
This result is used in three articles [VDEMV07]; [BVDEW12]; [DMJP14]. In [BVDEW12], Berson, van den Essen, and Wright use it to prove an impressive stably tameness result, and in [DMJP14], Dubouloz, Moser-Jauslin and Poloni use it to determine the automorphism group of the Koras-Russel threefold.

5.3 More general situations

If one defines the group $Aut_C(B; a)$ where $B$ is a finitely generated $C$-algebra and $a$ is an ideal of $B$ (as opposed to being an ideal of $A$, the coefficient ring, in the previous section) as

$$Aut_C(B; a) = \{ \varphi \in Aut_C(B) \mid \varphi(a) \subseteq a \}$$

then one can define the map

$$\pi : Aut_C(B; a) \rightarrow Aut_C(B/a).$$

It is an important question when an element is in the image of $\pi$, and when not. (For example, if one can answer this, then one can understand automorphisms of any finitely generated $C$-algebra much better.) In the case of section 1, we only consider $B = A^n$ and ideals of the form $rB$ where $r$ is an ideal of $A$. In this case, $Aut_C(B; a) = Aut_C(B)$ making life easier.

The equivalent question here is the following:

**Question 5.3.1.** Let

$$\sqrt{\pi} : Aut_C(B; \sqrt{a}) \rightarrow Aut_C(B/\sqrt{a}).$$

Suppose that $\varphi \in Aut_C(B/\sqrt{a})$ such that $\varphi \mod \sqrt{a} \in \sqrt{\pi(Aut_C(B; \sqrt{a}))}.  \footnote{Note that if $\varphi \in Aut_C(B; a)$, then $\varphi \mod a$ sends the nilradical $\sqrt{a}/a$ to itself, and thus $\varphi \mod \sqrt{a}$ is well-defined.}$

Under what conditions is $\varphi \in \pi(Aut_C(B; a))$?

In the case $B = A^n$ described above, it turns out that it is natural to require elements in $Aut_C(B/a)$ to be special, i.e. they come from polynomial maps of determinant Jacobian 1. In the general case, it is very unclear what type of requirement one should put on elements $\varphi \in Aut_C(B/a)$, or on the ideal $a$. For one, there’s no natural way to define the concept of special when talking about $Aut_C(B)$, as there’s no natural way to define the Jacobian. However, we can give an answer in the following special case:

**Proposition 5.3.2.** Let $B = k[x_1, \ldots, x_n]$ and $a \subset k[x_1, \ldots, x_n]$ such that $\sqrt{a}$ is a maximal ideal. Assume

1. $\varphi \in Aut_k(B/a)$ such that $\varphi \mod \sqrt{a} \in \sqrt{\pi(Aut_C(B; \sqrt{a}))}$, and
2. if $E \in MA_n(k)$ such that $\pi(E) = \varphi$, then $det(Jac(E)) = 1 \mod a$.

Then there exists $E \in GA_n(k)$ such that $\pi(E) = \varphi$.

**Proof.** Of course we assume $\text{rad } a = (x_1, \ldots, x_n)$. We may also assume $a = (x_1, \ldots, x_n)^m$ as $(\text{rad } a)^m$ is contained in $a$ for some $m$. We will proceed by induction to $m$; the case that $m = 1$ is trivial as then $a = \text{rad } a$. So assume the theorem has been proven for $m - 1$. So we can find $E_{m-1}^\varphi \in G\alpha_n(k)$ such that $E_{m-1}^\varphi = \varphi \mod (x_1, \ldots, x_n)^{m-1}$. Replacing $\varphi$ by $E_{m-1}^\varphi \varphi$
we may assume that \( \varphi \mod (x_1, \ldots, x_n)^{m-1} \) is the identity, i.e. \( \varphi = I + H \) where \( H = (H_1, \ldots, H_n) \) is homogeneous of degree \( m \). The proof is now very similar to the proof of lemma 5.2.6 and lemma 5.2.7: the assumption \( \det(\text{Jac}(I + H)) = 1 \mod (x_1, \ldots, x_n)^{m-1} \) yields that

\[
\text{Div}(H) = \frac{\partial H_1}{\partial x_1} + \ldots + \frac{\partial H_n}{\partial x_n} = 0.
\]

It is enough proving the \( n = 2 \) case, as an argument as in lemma 5.2.7 will yield the general result. For the case \( n = 2 \) we notice that there thus exists \( P \) homogeneous of degree \( m \) such that \( H_1 = P_y, H_2 = -P_x \). We then write \( P \) as a linear combination of \( \lambda L^m = \lambda(x + qy)^m \), each of which can be realized as an automorphism \( \exp(D) \) where \( D = \lambda L_y^p \partial_x - \lambda L_x^p \partial_y \). Composing these automorphisms yields an automorphism \( E \) such that \( \pi(E) = \varphi \).

However, the case when \( \text{rad } a \) is not a maximal ideal, are not clear. The following example is quite insightful:

**Example 5.3.3.** Let \( a := ((xy - z^2)^2), \sqrt{a} = (xy - z^2), B = \mathbb{C}[x, y, z] \). Then a corollary of a result by [ML90] is that the map

\[
\text{Aut}_\mathbb{C}(B; \sqrt{a}) \rightarrow \text{Aut}_\mathbb{C}(B/\sqrt{a})
\]

is surjective.

**Question 5.3.4.** is

\[
\text{Aut}_\mathbb{C}(B; a) \rightarrow \text{Aut}_\mathbb{C}(B/a)
\]

surjective, under some mild “Jacobian is 1” or perhaps “étale” conditions? Which elements are in the image of this map?

When naively and computationally trying to solve this example we just pick some \( F = (F_1, F_2, F_3) \in MA_3(\mathbb{C}) \), and make sure that \( F(xy - z^2) \in (xy - z^2)B \), while at the same time requiring \( F \mod a \) is an automorphism of \( B/a \). We arrive at a situation as \( F \) being of the form

\[
\begin{align*}
    x + (xy - z^2)p + P(xy - z^2)^2 \\
    y + (xy - z^2)q + Q(xy - z^2)^2 \\
    z + (xy - z^2)r + R(xy - z^2)^2
\end{align*}
\]

where \( p, q, r, P, Q, R \in \mathbb{C}[x, y, z] \). For which \( p, q, r \) do there exist \( P, Q, R \) such that the above formula forms an invertible polynomial map? This approach ends up in ridiculously hard computations which lack the elegance which was so nice in for example the case \( \text{SA}_n(\mathbb{C}[t]) \rightarrow \text{SA}_n(\mathbb{C}[t]/(t^m)) \).

### 5.4 Non-surjectivity

First notice that in theorem 5.2.2 is not true if one replaces \( \text{SA} \) by \( \text{GA} \), even if \( n = 1 \). Pick \( A = \mathbb{C}[t], a = (t^2), a = t, f := X + aX^2 \mod a \). Then \( \bar{f} = X \in \sqrt{\pi}(\text{GA}_n(A)), \) but \( f \not\in \pi(\text{GA}_n(A)) \) (as \( f \) is not linear).

However, it is an interesting question for which rings \( A \) and ideals \( a \) we have surjectivity of \( \text{SA}_n(A) \rightarrow \text{SA}_n(A/a) \). The theorem 5.2.2 shows that one can assume \( a \) to be reduced, but how does this work in general?
Question 5.4.1. Let \( A \) be a Noetherian commutative ring containing \( \mathbb{Q} \) and \( a \) an ideal of \( A \). What is the image of \( \text{SA}_n(A) \rightarrow \text{SA}_n(A/a) \)?

We define \( \mathcal{E}_n(A) \) as the subgroup of \( \text{SA}_n(A) \) generated by shears, and \( \mathcal{E}_n(A) \) as the subgroup of \( \text{SL}_n(A) \) generated by shears. We define \( \text{STA}_n(A) \) as the set of tame automorphisms having determinant Jacobian 1. Of course we have \( \text{SA}_n(A) \supseteq \text{STA}_n(A) \supseteq \mathcal{E}_n(A) \).

Lemma 5.4.2. \( \pi(\mathcal{E}_n(A)) = \mathcal{E}_n(A/a) \) and \( \pi(\mathcal{E}_n(A)) = \mathcal{E}_n(A/a) \), and thus the restrictions
\[
\pi : \mathcal{E}_n(A) \rightarrow \mathcal{E}_n(A/a)
\]
and
\[
\pi : \mathcal{E}_n(A) \rightarrow \mathcal{E}_n(A/a)
\]
are surjective.

The proof is trivial as any shear has a preimage under \( \pi \).

Lemma 5.4.3. \( \mathcal{E}_n(A) \cap \text{SL}_n(A) = \mathcal{E}_n(A) \).

Proof. Actually, is this easy to prove? I put it here, but don’t need it. \( \square \)

Example 5.4.4. Let \( A = \mathbb{R}[x, y] \) and \( a = (x^2 + y^2 - 1) \). Assume \( n \geq 3 \). Then
\[
\pi : \text{SL}_n(A) \rightarrow \text{SL}_n(A/a)
\]
and
\[
\pi : \text{SA}_n(A) \rightarrow \text{SA}_n(A/a)
\]
are both not surjective.

Proof. It is in [Wei96] that the matrix
\[
M_2 := \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mod a
\]
cannot be written as a product of elementary matrices over \( A/a \). Moreover the trivially extended matrix
\[
M_n := \begin{pmatrix} x & -y & 0 & \ldots & 0 \\ y & x & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \mod a
\]
is not in \( E_n(A/a) \) for \( n > 2 \). Suppose there exists \( L \in \text{SL}_n(A) \) such that \( \pi(L) = M_n \) where \( n > 2 \). Now a theorem of [Sus77] shows that \( \text{SL}_n(A) = E_n(A) \) if \( n > 2 \). But then \( \pi(L) \in E_n(A/a) \), contradiction.

Now consider the same linear map \( M_n, n > 2 \). Assume \( F \in \text{SA}_n(A) \) such that \( \pi(F) = M_n \). Write \( F = L + H \) where \( L \) is the linear part of \( F \), and \( H \) has coefficients in \( a \). Then \( L \in \text{SL}_n(A) = E_n(A) \) and thus \( \pi(F) = \pi(L) = M_n \in E_n(A/a) \), giving the same contradiction. \( \square \)

In some sense, the map \( \pi \) tells us if \( \text{SA}_n(A/a) \) is “farther away” from \( \mathcal{E}_n(A/a) \) than \( \mathcal{E}_n(A) \) from \( \mathcal{E}_n(A) \).
Bibliography


[Gup14b] Neena Gupta. “On the family of affine threefolds $x^m y = F(x, z, t)$”. In: Compos. Math. 150.6 (2014), pp. 979–998.


[VDEMV07] Arno Van Den Essen, Stefan Maubach, and Stéphane Vénéreau. “The special automorphism group of $R[t]/(t^n)[x_1, \ldots, x_n]$ and coordinates of a subring of $R[t][x_1, \ldots, x_n]$”. In: *J. Pure Appl. Algebra* 210.1 (2007), pp. 141–146.