Federal University of Minas Gerais
Department of Mathematics

The Jacobian Conjecture à la $\mathbb{Z}_p$

Wodson Mendson

Submitted in partial fulfillment of the requirements for the degree of Master of Science in Mathematics at Federal University of Minas Gerais

Advisor: Israel Vainsencher

Belo Horizonte

2018

Abstract

We survey some classical results about the Jacobian Conjecture and formulate the Invariance Conjecture. We show that this new conjecture is equivalent, in some sense, to the Jacobian Conjecture. We make a contribution to the Unimodular Conjecture, cf. [12, Essen-Lipton]. We define a new class of rings: unimodular rings and the invariant rings. The main objective is to show the close relationship between the Jacobian Conjecture and a related statement over the p-adic integers $\mathbb{Z}_p$.

Resumo

Estudamos alguns resultados clássicos na direção da Conjectura do Jacobiano e formulamos uma nova conjectura: a Conjectura da Invariância. Mostramos que tal conjectura é equivalente, em um certo sentido, à Conjectura do Jacobiano. Apresentamos algumas contribuições à Conjectura Unimodular, cf. [12, Essen-Lipton], e definimos uma nova classe de anéis: anéis invariantes e anéis unimodulares. Nosso objetivo principal consiste em mostrar a forte relação entre a Conjectura do Jacobiano e os inteiros p-ádicos $\mathbb{Z}_p$.

Acknowledgements

Gostaria de agradecer

ao Israel Vainsencher pela competente orientação, desde os tempos de IC, e por sempre estar disposto (e animado) a discutir matemática. Agradeço também pelas sugestões e correções feitas no texto.

aos meus pais pelo apoio e incentivo aos meus estudos.

ao Jeroen van de Graaf por me apresentar ao professor Israel.

à FAPEMIG pelo apoio financeiro.

Le juge: Accusé, vous tâcherez d'être bref.
L'accusé: Je tâcherai d'être clair.

Introduction

The following theorem is well known in the student world.

Inverse Function Theorem. *Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be an étale map*[1]*. Then f is a local homeomorphism.*

We remark that " local " can not be replaced by " global ". Indeed, if we consider

$$f = (e^X cos(Y), e^X sin(Y)) : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

then $\det Jf = e^{2X}$ and so f is an étale map. But note that $f(0,0) = f(0,2\pi)$.

In this dissertation we will study topics related to the **global inverse of polynomial maps**.

Let k be a field and $F : k^n \longrightarrow k^n$ a polynomial map i.e. $F_1, \ldots, F_n \in k[X_1, \ldots, X_n]$ where F_i is the i-th component of F. We say that F is an invertible polynomial map if there exists a polynomial map $G : k^n \longrightarrow k^n$, such that $F(G(X)) = X$ and $G(F(Y)) = Y$.

Linear maps are particular cases where each component is a homogeneous polynomial of degree 1. In this case it is easy to check that F is an invertible map if and only if F is injective. Furthermore, if $F_i = \sum_j A_{ij}X_j$ and $M = (A_{ij})$ is the associated matrix, we have that F is an invertible map if only if $M \in GL_n(k)$. Note that M is the jacobian matrix associated to F.

We can ask whether this is more general. More precisely, let $F : k^n \longrightarrow k^n$ be a polynomial map without restriction on $deg(F)$. Denote by $JF \in \mathcal{M}_n(k[X_1, \ldots, X_n])$ the associated jacobian matrix.

Question 1. *Is F invertible if and only if $JF \in GL_n(k[X_1, \ldots, X_n])$?*

Question 2. *Is F invertible if and only if F is injective?*

In this generality, we can find examples that answer negatively. Indeed, taking $k = \mathbb{F}_p$ and $F : k \longrightarrow k$ the polynomial map with $x \mapsto x^p + x$ we have $JF = 1$ but F is not invertible. If $k = \mathbb{Q}$, the map $F : k \longrightarrow k$ given by $x \mapsto x^3$ is injective but isn't invertible. Now if we consider k, an algebraically closed field with $char(k) = p > 0$,

[1] i.e. f is C^∞ and the map in tangent spaces $d_p f : T_p\mathbb{R}^n \longrightarrow T_{f(p)}\mathbb{R}^n$ are isomophism for all $p \in \mathbb{R}^n$.

and the map $f : k^n \longrightarrow k^n$ given by $(X_1, \ldots, X_n) \mapsto (X_1^p, \ldots, X_n^p)$ then f is injective but f is not an isomophism since the induced map of k-algebras $k[X_1^p, \ldots, X_n^p] \subset k[X_1, \ldots, X_n]$ isn't an isomophism. So, the questions above has relation with the structure of the field k.

We can suspect that something interesting occurs when k is algebraically closed field and $char(k) = 0$. Indeed, formulated initially by Keller in 1939, the first question is an open problem [1] known as **Jacobian Conjecture** or **Keller Problem**. It is a problem well known for its easy formulation in spite of being very difficult. Many results in positive direction make use of deep theorems of algebraic geometry. For example, in case k is an algebraically closed field and $char(k) = 0$, the answer for the 2nd question above is YES. The proof involves Zariski's Main Theorem (cf.[8, Theorem 8.45]).

The Keller Problem also is known by the many wrong proofs that can be found on Internet. We quote the paper "Proof Of Two Dimensional Jacobian Conjecture" by Yucai Su (2005). In 2006, Moh[2] published a paper with the objective of indicating the mistakes in Su's paper. Most interesting is his remark made at the end:

" **A few words for Mr. Su**

The problem of Jacobian Conjecture is very hard. Perhaps it will take human being another 100 years to solve it. Your attempt is noble, Maybe the Gods of Olympus will smile on you one day. Do not be too disappointed. B. Sagre has the honor of publishing three wrong proofs and C. Chevalley mistakes a wrong proof for a correct one in the 1950's in his Math Review comments, and I.R. Shafarevich uses Jacobian Conjecture (to him it is a theorem) as a fact. You are in a good company. One only remembers the correct statements from Scientists and Mathematicians, nobody remembers the wrong ones."

In the present text, we survey a few aspects of the questions above.

In the first part (chapter 1,2), we are interested in results about reductions. The main point in this part is to show that for the Jacobian Conjecture is sufficient to consider polynomial maps of type $F = X + H$ where $H = (H_1, \ldots, H_n)$ is homogeneous of degree 3 with jacobian matrix JH nilpotent.

Also, we discuss the 2nd question for the case $char(k) = 0$ and algebraically closed.

In the second part (chapter 3), we present some reformulations of the Jacobian Conjecture. We show, following [12, Essen-Lipton], that the Jacobian Conjecture is equivalent to the **Unimodular Conjecture**. We make some contribution to the Unimodular Conjecture, and we define two new classes of rings: *unimodular rings* and *invariant rings*. The main objective is to show the close relationship between the Jacobian Conjecture and p-adic integers $\mathbb{Z}_p$. This part contains new results that are denoted by **WM**. For example, **Theorem 3.15 (WM)** means that Theorem 3.15 is a new result.

[1] This is the 16º problem in Steve Smale list: "Mathematical problems for the next century."
[2] https://arxiv.org/pdf/math/0604049.pdf

Contents

Chapter 1

Polynomial Maps and the Keller Problem

Let R be a domain and $F : R^n \longrightarrow R^n$ a polynomial map. In this chapter we will study the following questions:

Question 1. *Is F invertible if and only if F is injective?*

Question 2. *Is F invertible if and only if the jacobian matrix JF is in $GL_n(R[X_1, \ldots, X_n])$?*

We will show that if $R = k$, an algebraically closed field with $char(k) = 0$, the answer to first questions is YES. The second question is false for $char(R) \neq 0$. In case $char(R) = 0$ it is an open problem (for $n \geq 2$):

Jacobian Conjecture. *(or Keller Problem) Let R be a domain with $char(R) = 0$ and $F : R^n \longrightarrow R^n$ a polynomial map with $JF \in GL_n(R[X_1, \ldots, X_n])$. Then, F is invertible.*

1.1 Polynomial maps

In this section R will denote a domain.

We will denote by $\mathcal{MP}_n(R)$ the collection of polynomial maps $F : R^n \longrightarrow R^n$. Note that we can equip $\mathcal{MP}_n(R)$ with a graded structure, via the graded structure of the ring $R[X_1, \ldots, X_n]$. More precisely, $\mathcal{MP}_n(R) = \bigoplus_{d \in \mathbb{N}} \mathcal{MP}_n(R)_d$ where $\mathcal{MP}_n(R)_d = \{F = (F_1, \ldots, F_n) \in \mathcal{MP}_n(R) \mid F_1, \ldots, F_n \text{ are homogeneous of degree } d\}$. Given $F \in \mathcal{MP}_n(R)$ we define $deg(F) := \mathbf{Max}\{deg(F_1), \ldots, deg(F_n)\}$ where $deg(F_k)$ is the degree of F_k.

Given $F \in \mathcal{MP}_n(R)$ we will denote by JF the jacobian matrix associated to F and we say that F is a **Keller map** if $\det JF = 1$. We say that F is invertible if there exists a polynomial map $G : R^n \longrightarrow R^n$ such that $G(F(X)) = X$ and $F(G(Y)) = Y$.

Some notations:

- $\mathcal{MP}_n(R)^{(0)} := \{F \in \mathcal{MP}_n(R) \mid F(0) = 0\}$.
- $\mathcal{MP}_n(R)^{(1)} := \{F \in \mathcal{MP}_n(R)^{(0)} \mid J(F)(0) = id_n\}$.
- $\mathcal{MPI}_n(R) := \{F \in \mathcal{MP}_n(R) \mid F \text{ is invertible}\}$.

Remark 1. *To show that $F \in \mathcal{MP}_n(R)$ is invertible we can replace it by $G \circ F \circ H$ where H and G are invertible maps. Furthemore, if F is a Keller map, we can suppose that F is of the form $F = X + H$ where $H = (H_1, \dots, H_n)$ is a polynomial map with $deg(H_i) \geq 2$ for all i.*

Definition 1.1. *Let $F \in \mathcal{MP}_n(R)$. We say that F is an **elementary polynomial map** if $F = (F_1, \dots, F_n)$ where $F_i = X_i + G_i$ with $G_i \in k[X_1, \dots, \hat{X}_i, \dots, X_n]$ (i.e. we omit the variable X_i) for a unique $1 \leq i \leq n$ and $F_j = X_j$ for $i \neq j$. We say that F is a regular map if $F = X + H$ where H is homogeneous with $deg(F) = 3$. F is a symmetric regular map if F is regular and JH is a symmetric matrix.*

Note that an elementary polynomial map is invertible.

Proposition 1.1. *Let $F = (F_1, \dots, F_n) \in \mathcal{MP}_n(R)$. Then F is invertible if and only if $R[X_1, \dots, X_n] = R[F_1, \dots, F_n]$.*

Proof. Follows from the definitions. □

Given a domain R we consider $A := R[[X_1, \dots, X_n]]$ the ring of formal power series over R. Denote the ideal $M = \langle X_1, \dots, X_n \rangle$. By definition, every element in A can be written as $f = f_r + f_{r+1} + \cdots$ where $f_r \in R[X_1, \dots, X_n]$ is homogeneous of degree r. If $f_r \neq 0$, we have $f \in M^r$ and $f \notin M^{r+1}$. In particular, we have $\bigcap_i M^i = 0$. [1]

Formal Inverse Function Theorem. *Let $F = (F_1, \dots, F_n)$ be a system of n formal series in n variables without constant term over a domain R. Suppose that the jacobian $JF(0)$ of F at $(0, \dots, 0) \in R^n$ is a unit in the ring $\mathcal{M}_n(R)$. Then F has an inverse system $G = (G_1, \dots, G_n)$ which is uniquely determined.*

[1] This is more general in noetherian case: given A noetherian domain for any ideal $I \subset A$ we have $\bigcap_i I^i = (0)$. See [1, Chapter 10].

Proof. Let $M := \langle X_1, \ldots, X_n \rangle$. We will show that there is $G_1 \in R[[X_1, \ldots, X_n]]$ such that $G_1(F_1, \ldots, F_n) = X_1$. Without loss of generality we can assume that $F_i = X_i + H_i$ where H_i has only terms in degree ≥ 2. Let $S_1 := X_1$. Then $S_1(F_1, \ldots, F_n) = F_1 \equiv X_1 \mod M^2$. So $S_1(F_1, \ldots, F_n) - X_1 = S_2$ for some $S_2 \in M^2$. In particular, $S_2(F_1, \ldots, F_n) \equiv S_2(X_1, \ldots, X_n) \mod M^3$. Now note that $S_1(F_1, \ldots, F_n) - S_2(F_1, \ldots, F_n) \equiv X_1 + S_2 - S_2 \equiv X_1 \mod M^3$. So $S_1(F_1, \ldots, F_n) - S_2(F_1, \ldots, F_n) - X_1 = S_3$ for some $S_3 \in M^3$. Proceeding in this way, we obtain $S_1, \ldots, S_k \in R[[X_1, \ldots, X_n]]$ such that $S_1(F_1, \ldots, F_2) - \sum_{j \geq 2}^{k} S_j(F_1, \ldots, F_n) - X_1 \in M^{k+1}$. Passing to the M-adic limit, we can determine $G_1 \in R[[X_1, \ldots, X_n]]$ such that $G_1(F_1, \ldots, F_n) \equiv X_1 \mod M^k$ for all k. So $G_1(F_1, \ldots, F_n) = X_1$. Similarly we can determine $G_2, \ldots, G_n \in R[[X_1, \ldots, X_n]]$ such that $G_j(F_1, \ldots, F_n) = X_j$. For uniqueness, note that there is $H = (H_1, \ldots, H_n)$ such that $H \circ G = X$. So $F = H \circ G \circ F = H$ since $G \circ F = X$. Thus G is uniquely determined by F. □

Now we will give some applications of the theorem above.

Corollary 1.1. *Let $F \in \mathcal{MP}_n(R)^{(1)}$ with $R \subset S$ for some domain S. Then, $F \in \mathcal{MPI}_n(S) \Longleftrightarrow F \in \mathcal{MPI}_n(R)$.*

Proof. Suppose that $F \in \mathcal{MPI}_n(S)$. Let G be the formal inverse of F over R and H the inverse over S. Since $H, G \in S[[X_1, \ldots, X_n]]$ and the formal inverse of F over S is unique we have $G = H$. So $G \in R[[X_1, \ldots, X_n]] \cap S[X_1, \ldots, X_n] \subseteq R[X_1, \ldots, X_n]$. □

Lemma 1.1. *Let R be a $\mathbb{Q}$-algebra of finite type. Then, there exists an immersion $\phi : R \hookrightarrow \mathbb{C}$.*

Proof. If R is algebraic over $\mathbb{Q}$, by the primitive element theorem, $K := Frac(R) = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. So if $m(t) \in \mathbb{Q}[t]$ denotes the minimal polynomial, consider the map $\mathbb{Q}[t] \longrightarrow \mathbb{C}$ given by evaluation by α. If R isn't algebraic, denote by $\{\alpha_1, \ldots, \alpha_r\}$ a transcendence basis for K over $\mathbb{Q}$ and make use the fact: $tr.deg_{\mathbb{Q}}(\mathbb{C}) = \infty$. □

Corollary 1.2. *If the Jacobian Conjecture is true over $\mathbb{C}$ then it is true over any domain R with $char(R) = 0$.*

Proof. Let $F \in \mathcal{MP}_n(R)$ be a Keller map and suppose that the Jacobian Conjecture is true over $\mathbb{C}$. Let R' be the subring of R generated (over $\mathbb{Z}$) by all coefficients wich occur in F. Let $\phi : R' \hookrightarrow \mathbb{C}$ be an immersion. By the corollay above we know that F is invertible over R' and by the same corollary we conclude that F is invertible over R. □

1.2 A computational criterion for invertibility

In this section we give a computational criterion, due to Arno Essen (cf.[**?**, poly0]), which determines when a polynomial map is invertible and, in this case, compute the inverse. Initially we recall some topics about Gröbner

Basis. Details can be found in [3].

Let k be a field and consider the ring $A := k[X_1, \ldots, X_n]$. We will denote by X^α the monomial $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. We recall that a monomial order in A is a relation $>$ in the collection of monomials of A with the following properties:

- $>$ is a total order.
- If $X^\alpha > X^\beta$ then $X^\alpha X^\gamma > X^\beta X^\gamma$ for all $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}_{\geq 0}^n$.
- Any subset $S \neq \varnothing$ in the collection of monomials has a minimal element.

Example 1. *(**Lexicographic Order - lex**) Let $X^\alpha = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ and $X^\beta = X_1^{\beta_1} \ldots X_n^{\beta_n}$ be monomials. Define $>_{lex}$ by the rule $X^\alpha >_{lex} X^\beta$ if $\alpha_i = \beta_i$ for $1 \leq i \leq k$ and some k and $\alpha_k > \beta_k$. It is possible to show that $>_{lex}$ defines a monomial order in $k[X_1, \ldots, X_n]$.*

Example 2. *(**Graded Lex Order- grlex**) Let $X^\alpha = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ and $X^\beta = X_1^{\beta_1} \ldots X_n^{\beta_n}$ monomials in $k[X_1, \ldots, X_n]$. Define $>_{grlex}$ by $X^\alpha >_{grlex} X^\beta$ if $|\alpha| = \sum_i \alpha_i > |\beta| = \sum_i \beta_i$ or if $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$. It is possible to show that $>_{grlex}$ defines a monomial order in $k[X_1, \ldots, X_n]$.*

Fix $>$ a monomial order and let $F \in A$. Denote by $LM(F)$ the leading monomial wich occurs in F i.e. $LM(F) > M$ for any other monomial that occurs in F. Define $LC(F)$ the coefficient of $LM(F)$ and $LT(F) := LC(F)LM(F)$.

Let $f(X), g(X) \in k[X] \setminus k$. By the division algorithm, we know that there exist (unique) $q(X), r(X) \in k[X]$ with $r(X) = 0$ or $deg(r(X)) < deg(g(X))$ such that

$$f(X) = q(X)g(X) + r(X).$$

For the ring $k[X_1, \ldots, X_n]$ there is an analogue version

Division Algorithm in $k[X_1, \ldots, X_n]$. *Fix $>$ a monomial order in $k[X_1, \ldots, X_n]$ and let $G = (g_1, \ldots, g_t)$ be an ordered t-tuple of polynomials in $k[X_1, \ldots, X_n]$. Then every polynomial $f \in k[X_1, \ldots, X_n]$ can be written as*

$$f = q_1 g_1 + \cdots + q_t g_t + r$$

where $r = 0$ or $r = \sum_i c_i M_i$ is a linear combination, with coefficients in k, of monomials M_i such that $M_i \notin \langle LT(g_1), \ldots, LT(g_t) \rangle$ for all i. We say that r is the reduction of f by G and write $r := r_G(f)$.

Definition 1.2. *Let $0 \neq I \subset k[X_1, \ldots, X_n]$ be an ideal. Define $LT(I) := \langle cX^\alpha \mid \exists F \in I - \{0\} \quad LT(F) = cX^\alpha \rangle$, an ideal in $k[X_1, \ldots, X_n]$.*

Let $I = \langle F_1, \ldots, F_m \rangle$ be an ideal in $k[X_1, \ldots, X_n]$. By definition it is clear that $\langle LT(F_1), \ldots, LT(F_m) \rangle \subset LT(I)$. The next example shows that, in general, the equality $\langle LT(F_1), \ldots, LT(F_m) \rangle = LT(I)$ is false.

Example 3. *Consider $k^{[3]} = k[X, Y, Z]$ and the ideal $I = (F_1, F_2)$ where $F_1 = X^3 - 2XY$ and $F_2 = X^2Y - 2Y^2 + X$. Fix the a lexicographic order in $k[X, Y, Z]$. Then, $LT(F_1) = X^3$ and $LT(F_2) = X^2Y$. Note*

$$X^2 = XF_2 - YF_1 \Longrightarrow X^2 = LT(X^2) \in LT(I)$$

Now if $X^2 \in \langle LT(F_1), LT(F_2) \rangle$ we have $X^2 \in \langle LT(F_1) \rangle$ or $X^2 \in \langle LT(F_2) \rangle$ and this not occurs. So $X^2 \notin \langle LT(F_1), LT(F_2) \rangle$.

Definition 1.3. *Fix a monomial order in $k[X_1, \ldots, X_n]$. A finite subset $G = \{g_1, \ldots, g_m\}$ of an ideal $0 \neq I \subset k[X_1, \ldots, X_n]$ it is called a **Gröbner basis** if $\langle LT(g_1), \ldots, LT(g_m) \rangle = LT(I)$.*

Theorem 1.1. *Any ideal $0 \neq I \subset k[X_1, \ldots, X_n]$ has a Gröbner basis.*

Definition 1.4. *Let $I \subset k[X_1, \ldots, X_n]$ be an ideal and G a Gröbner basis for I. We say that G is **reduced** if*

(i) $LC(g) = 1$ for all $g \in G$.

(ii) For all $g \in G$, and M a monomial wich occurs in g, we have $M \notin LT(G - \{g\})$.

Theorem 1.2. *Fix $>$ a monomial order in $k[X_1, \ldots, X_n]$. Every non-zero ideal $I \subset k[X_1, \ldots, X_n]$ has a reduced Gröbner basis. Furthemore, the reduced Gröbner basis is unique.*

1.2.1 The criterion of Essen

Let $F = (F_1, \ldots, F_n) \in \mathcal{MP}_n(k)$. So $F_1, \ldots, F_n \in k[X_1, \ldots, X_n]$. Introduce new variables $Y_1, \ldots, Y_n$ and consider the polynomial ring $k[X, Y] := k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ with monomial order $>$ such that $X_n > X_2 > \cdots > X_1 > Y_n > Y_{n-1} > \cdots > Y_1$.

Let $I \subset k[X, Y]$ be the ideal $I = \langle Y_1 - F_1, \ldots, Y_n - F_n \rangle$.

Theorem 1.3. ***(Essen)*** *Let G be the reduced Gröbner basis for the ideal I. Then*

(i) F is invertible if and only if $G = \{X_1 - G_1, \ldots, X_n - G_n\}$ for some polynomials $G_i \in k[Y_1, \ldots, Y_n]$.

(ii) If this is the case, the inverse is given by $G = (G_1, \ldots, G_n) \in \mathcal{MP}_n(k)$.

Proof. Part (ii) follows immediately from (i).

Suppose that $\mathcal{A} = \{X_1 - G_1, \ldots, X_n - G_n\}$ is the reduced Gröbner basis for I, for some $G_1, \ldots, G_n \in k[Y_1, \ldots, Y_n]$. Thus, for each $1 \leq i \leq n$ there is a relation of type

$$Y_i - F_i(X_1, \ldots, X_n) = \sum_i A_i(X, Y)(X_i - G_i(Y_1, \ldots, Y_n))$$

Replacing X_i by $G_i(Y_1, \ldots, Y_n)$ we obtain $Y_i - F_i(G_1(Y), \ldots, G_n(Y)) = 0 \Longrightarrow Y = F(G(Y))$. So we conclude that F is invertible with inverse G.

Now suppose that F is an invertible map with inverse $G = (G_1, \ldots, G_n)$. We want to show that $\{X_1 - G_1(Y_1, \ldots, Y_n), \ldots, X_n - G_n(Y_1, \ldots, Y_n)\}$ is a reduced Gröbner basis for I. By definition of I note that

$$Y_i \equiv F_i \mod I$$

So for any $g \in k[Y_1, \ldots, Y_n]$ we have $g(F_1(X), \ldots, F_n(X)) \equiv g(Y_1, \ldots, Y_n) \mod I$. Since F is invertible, we have that $X_i = G_i(F_1(X), \ldots, F_n(X))$. Hence

$$X_i = G_i(F_1(X), \ldots, F_n(X)) \equiv G_i(Y_1, \ldots, Y_n) \in I.$$

So $X_i = LT(X_i - G_i(Y_1, \ldots, Y_n)) \in LT(I) \Longrightarrow X_i = c_i LT(b_i)$ for some $b_i \in G$ and $c_i \in k[X, Y]$. So $c_i = 1$ and $LT(b_i) = X_i$ for all i.

In particular, for $i = 1$ we have $b_1 = X_1 + h_1(Y)$ for some $h_1(Y) \in k[Y_1, \ldots, Y_n]$ (recall the assumption about the order).

For $i = 2$ we have $b_2 = X_2 + h_2(X_1, Y)$ for some $h_2(X_1, Y) \in k[X_1, Y_1, \ldots, Y_n]$. Now if X_1 occurs effectively in h_2 we conclude that b_2 contains a monomial that belongs to $LT(G - \{b_2\})$. Since G is reduced this cannot occur and so $h_2 \in k[Y_1, \ldots, Y_n]$. We can repeat the argument up to $i \leq n$ and conclude that

$$b_i = X_i + h_i(Y) \qquad h_i(Y) \in k[Y_1, \ldots, Y_n] \qquad \forall \quad 1 \leq i \leq n$$

So $H := \{X_1 + h_1(Y), \ldots, X_n + h_n(Y)\} \subseteq G$. Now note that $I = (G)$ and $J = (H)$ are prime ideals in $k[X, Y]$ with height n. Since $J \subset I$ we conclude $I = J$. By uniqueness we have $H = G$. □

Example 4. *Let $K = k(t)$ the rational functions field over k and consider the polynomial map $F \in \mathcal{MP}_2(K)$ defined by*

$$F(X_1, X_2) = (X_1 - t^3 X_1^3 + 3t^2 X_1^2 X_2 - 3t X_1 X_2^2 + X_2^3 \quad , \quad X_2 - t^4 X_1^3 + 3t^3 X_1^2 X_2 - 3t^2 X_1 X_2^2 + t X_2^3)$$

Considering the ideal

$$I = \langle Y_1 - (X_1 - t^3X_1^3 + 3t^2X_1^2X_2 - 3tX_1X_2^2 + X_2^3) \quad , \quad Y_2 - (X_2 - t^4X_1^3 + 3t^3X_1^2X_2 - 3t^2X_1X_2^2 + tX_2^3)\rangle$$

in the ring $k(t)[X_1, X_2, Y_1, Y_2]$ with lexicographic order $X_2 > X_1 > Y_2 > Y_1$, we see (via Singular, cf.[4]) that the reduced Gröbner basis for I is

$$G = \{X_1 + Y_2^3 - 3tY_2^2Y_1 + 3t^2Y_2Y_1^2 - t^3Y_1^3 - Y_1 \quad , \quad X_2 + tY_2^3 - 3t^2Y_2^2Y_1 + 3t^3Y_2Y_1^2 - Y_2 - t^4Y_1^3\}$$

So by Essen criterion, we have F invertible with inverse map

$$F^{-1}(X_1, X_2) = (X_1 - X_2^3 + 3tX_2^2X_1 - 3t^2X_2X_1^2 + t^3X_1^3 \quad , \quad X_2 - tX_2^3 + 3t^2X_2^2X_1 - 3t^3X_2X_1^2 + t^4X_1^3)$$

Remark 2. *In the example above, note that F is an invertible regular map of the form $F = X + H$ and the inverse is given by $F^{-1} = X - H$. Also, note that $JH^2 = 0$. Later, we shall see that this fact isn't arbitrary but a particular case of a class of invertible maps.*

1.3 Invertible maps

In this section we give a version of the following proposition for affine varieties:

Proposition 1.2. *Let k be a field and L/k an algebraic extension. If $\sigma : L \hookrightarrow L$ is an injective morphism over k then σ is an isomorphism.*

Proof. We will reduce to the finite case.

Let $\alpha \in L$. We want to show that there is $\beta \in L$ such that $\sigma(\beta) = \alpha$. Let $m_\alpha(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in k[T]$ be the minimal polynomial of α over k. Let $E = k(\alpha_1, \ldots \alpha_r)$ (with $\alpha_1 = \alpha$) subfield of L obtained by adjunction of all roots of $m_\alpha(T)$ that are in L. Note that for each $u \in E$ we have $\sigma(u) \in E$. So σ, by restriction, defines an injective map $\sigma|_E : E \hookrightarrow E$ over k. Now, E is of finite dimension over k. In particular, $\sigma|_E$ is an isomorphism. So there is a $\beta \in E$ such that $\sigma(\beta) = \alpha$. □

In what follows, k will denote an algebraically closed field. If $X = Z(F_1, \ldots, F_r) \subset \mathbb{A}_k^n$ is an algebraic set, given a subfield $l \subset k$ we will denote by $X(l)$ the set of l-points i.e. $X(l) := X \cap l^n$.

Theorem 1.4. *Let $X \subset \mathbb{A}_k^n$ be an affine variety and $\alpha : X \longrightarrow X$ an injective endomorphism. Then α is surjective.*

Proof. Initially we shall write the injectivity, non-surjectivity and membership conditions in terms of equations. For this let $G_1, \ldots, G_m \in k[X_1, \ldots, X_n]$ be the equations of X and $\alpha_1, \ldots, \alpha_n$ the components of the map α as elements of $k[X_1, \ldots, X_n]$.

(1) Injectivity: If $(P, Q) \in X \times X$ are such that $\alpha_1(P) = \alpha_1(Q), \ldots, \alpha_n(P) = \alpha_n(Q)$ then $P = Q$. Equivalently, every zero of the ideal

$$I = \langle G_1(X), \ldots, G_m(X), G_1(Y), \ldots, G_m(Y), \alpha_1(X) - \alpha_1(Y), \ldots, \alpha_n(X) - \alpha_n(Y) \rangle$$

is a zero of $J = \langle X_1 - Y_1, \ldots, X_n - Y_n \rangle$. By Nullstellensatz this is equivalently to: for all $i \in \{1, \ldots, n\}$ there is $l_i \in \mathbb{N}$ and polynomials A_{ik}, B_{ik}, C_{ik} such that

$$(X_k - Y_k)^{l_k} = \sum_i A_{ik}(X, Y) G_i(X) + \sum_i B_{ik}(X, Y) G_i(Y) + \sum_i C_{ik}(X, Y)(\alpha_i(X) - \alpha_i(Y)).$$

(2) Membership: For all $P \in X$ we have $\alpha(P) \in X$. So if $P \in \mathbb{A}_k^n$ is a zero of $\langle G_1(X), \ldots, G_m(X) \rangle$ then P is a zero of $\langle G_1(\alpha_1, \ldots, \alpha_n), \ldots, G_m(\alpha_1, \ldots, \alpha_n) \rangle$. By Nullstellensatz this is equivalently to: for all $u \in \{1, \ldots, n\}$ there is $t_i \in \mathbb{N}$ and polynomials r_{iu} such that

$$G_k(\alpha_1, \ldots, \alpha_n)^{t_u} = \sum_i r_{iu}(X) G_i.$$

(3) non-surjectivity: If $Q = (q_1, \ldots, q_n) \notin \alpha(X)$ this is equivalently to: the ideal

$$I_2 := \langle G_1(X), \ldots, G_r(X), \alpha_1(X) - q_1, \ldots, \alpha_n(X) - q_n \rangle$$

has no zero. By Nullstellensatz, this is equivalently to $I_2 = k[X_1, \ldots, X_n]$. So

$$1 = \sum_l h_l(X) G_l(X) + \sum_k u_k(X)(\alpha_k(X) - q_k)$$

for some polynomials h_l, u_k.

Suppose that α isn't surjective. Consider all equations wich occur in (1), (2) and in (3).

Case 1: $char(k) = p > 0$**.**

This case, $\mathbb{F}_p$ is the prime field of k. Consider $\{a_1, \ldots, a_e\} \subset k$ the set of all coefficients that occur in the above relations: (1), (2) and (3). Let $S := \mathbb{F}_p[a_1, \ldots, a_e] \subset k$ be the subring generated by all this coefficients. Let $\mathcal{M} \in Spec_m(S)$ and consider the ring $R = S/\mathcal{M}$.

We have R a $\mathbb{F}_p$-algebra of finite type and by algebraic Nullstellensatz we conclude that R is algebraic over $\mathbb{F}_p$, in particular it is a finite field. Considering $\overline{X}(R)$ the set obtained from X by reduction of equations $\mod \mathcal{M}$ and by $\overline{\alpha}$ the induced map, we obtain a map

$$\overline{\alpha} : \overline{X}(R) \longrightarrow \overline{X}(R)$$

injective by relation (1) but non surjective by (3), a contradiction

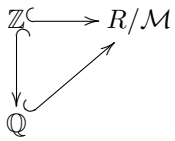
Caso 2: $char(k) = 0$**.**

In this case, consider $\{a_1, \ldots, a_e\} \subset k$ all coefficients that occurs in (1), (2) and (3). Let $S := \mathbb{Z}[a_1, \ldots, a_e] \subset k$ be the subring generated by all this coefficient. Let $\mathcal{M} \in Spec_m(S)$. If $S/\mathcal{M}$ is a finite field we can repeat the argument of case 1 and conclude the proof. So it is sufficient to show the following

Theorem 1.5. [2] *Let R a $\mathbb{Z}$ - algebra of finite type and $\mathcal{M} \in Spec(R)$. Then*

$$R/\mathcal{M} \quad \textit{is a finite field if and only if} \quad \mathcal{M} \in Spec_m(R).$$

Proof. By the algebraic Nullstellensatz it is sufficient to show that $\mathcal{M} \cap \mathbb{Z} \neq 0$. Suppose this false. Then the natural map $\mathbb{Z} \hookrightarrow R/\mathcal{M}$ is injective. In this case, we obtain the following commutative diagram



By theorem 4.3 we conclude that $\mathbb{Q}$ is finitely generated as $\mathbb{Z}$-algebra. A contradiction. □

□

1.3.1 A refinement

Fix k an algebraically closed field with $char(k) = 0$.

Lemma 1. *Let $X \subset \mathbb{A}^n_k$ be an affine variety. Denote by $(\widetilde{X}, \pi)$ the normalization of X. Let*

$$\mathcal{S}(X) := \{f : X \longrightarrow k \mid f \circ \pi \in \mathcal{O}_{\widetilde{X}}(\widetilde{X})\}.$$

[2] Another elegant proof: Consider the map of affine schemes: $f : Spec(R) \longrightarrow Spec(\mathbb{Z})$. Since $\mathbb{Z}$ is noetherian and we have finitude conditions, by Chevalley theorem (cf.[1]) we know that the map f is constructive i.e. if $X \subset Spec(R)$ is a construtive set then $f(X)$ is constructive. Let $\mathcal{M}$ a closed point in $Spec(R)$. In particular, it is constructive. So $f(\{\mathcal{M}\}) = \{\mathcal{M} \cap \mathbb{Z}\}$ is constructive set. Since $f(\{\mathcal{M}\})$ does not contain any open dense, we can applies [1, IV3.5-propositon 3.5] and conclude that $f(\{\mathcal{M}\})$ isn't dense. In particular, can't be the generic point of $Spec(\mathbb{Z})$ i.e. $f(\{\mathcal{M}\}) \neq \{0\}$. Algebraic Nullstellensatz finishes the proof.

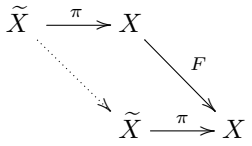
Then $\mathcal{S}(X)$ is a noetherian $\mathcal{O}_X(X)$-module.

Proof. By properties of normalization, we know that $\mathcal{O}_{\widetilde{X}}(\widetilde{X})$ is noetherian as $\mathcal{O}_X(X)$-module (it is of finite type). Consider the map of $\mathcal{O}_X(X)$-modules

$$L : \mathcal{S}(X) \longrightarrow \mathcal{O}_{\widetilde{X}}(\widetilde{X}) \qquad f \in \mathcal{S}(X) \mapsto f \circ \pi.$$

It is easy to check that L is an injective map. So $\mathcal{S}(X)$ can be looked at as an $\mathcal{O}_X(X)$-submodule of $\mathcal{O}_{\widetilde{X}}(\widetilde{X})$ (that is noetherian). Thus $\mathcal{S}(X)$ is noetherian. □

Let X be an affine variety and $(\widetilde{X}, \pi)$ its normalization. Let $F : X \longrightarrow X$ be a morphism. Consider the following diagram



By properties of normalization, there is a unique morphism $\widetilde{F} : \widetilde{X} \longrightarrow \widetilde{X}$ fitting in the dotted arrow above.

Lemma 2. *(i) If F is injective then $\widetilde{F}$ is injective.*

(ii) If $\widetilde{F}$ is surjective then F is surjective.

Proof. (i): Suppose that F is an injective map. By theorem above, we have F is a bijection. Initially, we show that $\widetilde{F}$ is a dominant map. Indeed, suppose this false. Then since $\widetilde{X}$ is irreducible, we have $\dim \overline{\widetilde{F}(\widetilde{X})} < \dim \widetilde{X}$. Now, note that $\pi \circ \tilde{F}$ is a dominant map:

$$\overline{\pi(\widetilde{F}(\tilde{X}))} = \overline{F(\pi(\widetilde{X}))} = \overline{X} = X.$$

Thus,

$$\dim X = \dim \overline{\pi(\widetilde{F}(\widetilde{X}))} = \dim \pi(\overline{\widetilde{F}(\widetilde{X})}) \leq \dim \overline{\widetilde{F}(\widetilde{X})} < \dim \widetilde{X} = \dim X$$

a contradiction.

So $\widetilde{F} : \widetilde{X} \longrightarrow \widetilde{X}$ is a dominant map between varieties of same dimension. Furthemore $\widetilde{F}$ is quasi-finite map, since $F \circ \pi$ is too. So by Theorem 4.7, for any point $P \in \widetilde{X}$ we have $\#F^{-1}(P) \leq deg(\widetilde{F})$. Now, $1 = deg(F)deg(\pi) = deg(F \circ \pi) = deg(\pi \circ \widetilde{F}) = deg(\widetilde{F}) \Longrightarrow deg(\widetilde{F}) = 1$. In particular $\widetilde{F}$ is injective.

(ii) Suppose that $\widetilde{F}$ is surjective. Then

$$F(X) = F(\pi(\widetilde{X})) = \pi(\widetilde{F}(\widetilde{X})) = \pi(\widetilde{X}) = X$$

i.e. F is surjective.

□

Definition 1.5. *In notation as in **lemma 1** above, we define* $S_n(X) := \{F : X \longrightarrow X \mid F_i \circ \pi \in \mathcal{O}_{\tilde{X}}(\tilde{X}) \quad \forall i = 1, \ldots, n\}$. *Note that* $S_n(X) \cong \bigoplus_{i=1}^{n} S(X)$, *as* $\mathcal{O}_X(X)$*-module, and so* $S_n(X)$ *is noetherian as* $\mathcal{O}_X(X)$*-module.*

Theorem 1.6. ***(Cynk-Rusek)*** *Let* $X \subset \mathbb{A}_k^n$ *be an affine variety and* $F : X \longrightarrow X$ *a regular map. The following conditions are equivalent:*

(i) F *is injective.*

(ii) F *is a bijection.*

(iii) F *is an automorphism.*

Proof. The implication (i) $\Longrightarrow$ (ii) follows from the theorem above. We will show (ii)$\Longrightarrow$ (iii). Suppose that $F : X \longrightarrow X$ is a bijection and consider the map $\widetilde{F}$ induced in normalization. By the lemma above, we have $\widetilde{F}$ an injective map. Applying the Zariski Main Theorem (see section 4.4) we conclude $\widetilde{F}$ is an isomorphism. Let F^{-1} be the set-theoretic inverse of F. By commutativity of the diagram

$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{\pi} & X \\ & \searrow^{\widetilde{F}} \quad \swarrow_{F} & \\ & \widetilde{X} \xrightarrow{\pi} X & \end{array}$$

we have $\pi \circ \widetilde{F}^{-1} = F^{-1} \circ \pi$. So we conclude $\pi \circ \widetilde{F}^{-d} = F^{-d} \circ \pi$. So $F^{-d} \in S_n(X)$ for all $d \in \mathbb{N}$. Consider the $\mathcal{O}_X(X)$-submodules: $S_n(X)^{(e)} := \mathcal{O}_X(X)F^{-1} + \cdots + \mathcal{O}_X(X)F^{-e}$. The collection $\{S_n(X)^{(e)}\}_{e \in \mathbb{N}}$ is an ascending chain of submodules

$$S_n(X)^{(1)} \subset S_n(X)^{(2)} \subset S_n(X)^{(e)} \cdots$$

Since $S(X)$ is noetherian there exists $d \in \mathbb{N}$ such that $F^{-d-1} \in S_n(X)^{(d)}$. So

$$F^{-d-1} = \sum_{j=1}^{d} r_j F^{-j} \quad r_j \in \mathcal{O}_X(X).$$

In particular we have $F^{-1} = \sum_{j=1}^{d} r_j F^{d-j} = r_1 F^{d-1} + r_2 F^{d-2} + \cdots + r_d X \Longrightarrow F^{-1}$ is a regular map i.e. F is an

automorphism.

The implication (iii)$\Longrightarrow$(i) is trivial.

□

Corollary 1.3. *(**Wang**) Let k be an algebraically closed field with $char(k) = 0$. Let $F \in \mathcal{MP}_n(k)$ be a Keller map with $deg(F) \leq 2$. Then, F is invertible.*

Proof. By 1.6 it is sufficient to show that F is injective. Suppose that this is false. Pick $P, Q \in k^n$ such that $F(P) = F(Q)$ with $P \neq Q$. Without loss of generality, we can suppose that $P = 0$ and $F(0) = 0 = F(Q)$. Write $F = F_{(1)} + F_{(2)}$ where $F_1 =$ linear part of F and $F_2 =$ quadratic part. Denote by $F^{(i)}$ the i-th componenent of F. Then

$$0 = F^{(i)}(Q) = F^{(i)}_{(1)}(Q) + F^{(i)}_{(2)}(Q) = F^{(i)}_{(1)}(Q) + 2t_0F^{(i)}_{(2)}(Q), \qquad t_0 := 1/2.$$

Now, note that $F^{(i)}_{(1)}(Q)+2t_0F^{(i)}_{(2)}(Q) = (tF^{(i)}_{(1)}(Q)+t^2F^{(i)}_{(2)}(Q))'|_{t=t_0} = (F^{(i)}_{(1)}(tQ)+F^{(i)}_{(2)}(tQ))'|_{t=t_0} = (F^{(i)}(tQ))'|_{t=t_0} =< \nabla F^{(i)}(t_0Q), Q >$. In terms of matrix we conclude that $JF(1/2Q).Q = 0$ a contradiction since F is a Keller map. □

The next theorem is fundamental in chapter 3:

Theorem 1.7. *(**Connell - van den Dries**) Let $F \in \mathcal{MP}_n(\mathbb{C})$ be a counterexample for the Jacobian Conjecture. Then there is $N \in \mathbb{N}$ with $N > n$ and a couterexample $G \in \mathcal{MP}_N(\mathbb{C})$ with coefficients in $\mathbb{Z}$ such that $\det(JF) = 1$.*

We make use of the following

Lemma 1.2. *Let k be a field with $char(k) = 0$ and $K|k$ a Galois extension of degree $m > 1$. Let $F \in \mathcal{MP}_n(K)$ be a Keller map and suppose that F isn't injective. Then there is a non-injective Keller map $G \in \mathcal{MP}_{nm}(k)$.*

Proof. Let $\{e_1, \ldots, e_n\}$ be a k-basis of K and denote $\sigma_0, \ldots, \sigma_{m-1}$ the elements of the group $Gal(K/k)$. Introduce new variables $X_{11}, \ldots, X_{1m}, \ldots, X_{n1}, \ldots, X_{nm}$ and consider the polynomials $G_{ij} \in k[X_{11}, \ldots, X_{nm}]$ defined by relations

$$G_{k1}e_1 + \cdots + G_{km}e_m = F_k(X_{11}e_1 + \cdots + X_{1m}e_m, \ldots, X_{n1}e_1 + \cdots + X_{nm}e_m)$$

Consider the polynomial map $G = (G_{11}, \ldots, G_{nm}) : k^{nm} \longrightarrow k^{nm}$. Since F isn't injective it follows that G isn't injective. We affirm that $\det JG = 1$. For this, consider the polynomial map $\widetilde{F} : K^{nm} \longrightarrow K^{nm}$ given by $P \mapsto (F^{\sigma_0}(P), \ldots, F^{\sigma_{m-1}}(P))$. By definition, if $F_k = \sum_l \alpha_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n}$ we set $F_k^{\sigma_p} = \sum_l \alpha^{\sigma_p}_{i_1 \ldots i_n} X^{i_1}_{pn+1} \cdots X^{i_n}_{pn+n} \in k[X_{pn+1}, \ldots, X_{pn+n}]$ for $0 \leq p \leq m-1$ and $1 \leq k \leq n$. Finally, $F^\sigma := (F_1^\sigma, \ldots, F_n^\sigma)$ if $\sigma \in Gal(K/k)$.

By construction, we have

$$JF^{\sigma} = \begin{pmatrix} JF^{\sigma_0} & 0 & 0 & \dots & 0 \\ \vdots & JF^{\sigma_1} & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & JF^{\sigma_{m-1}} \end{pmatrix}$$

So $\det(\widetilde{F}) = \prod_{j=0}^{m-1} \det JF^{\sigma_j} = \prod_{j=0}^{m-1} \sigma_j(\det JF) = 1$. Now consider $L : K^{nm} \longrightarrow K^{nm}$ the polynomial map obtained by taking $L_{i(n+j)} := \sigma_i(e_1)Y_{j1} + \cdots + \sigma_i(e_m)Y_{jm}$ for $0 \leq i \leq m-1$ and $1 \leq j \leq n$. Note that [3] $L \circ G = \widetilde{F} \circ L \Longrightarrow G = L^{-1} \circ \widetilde{F} \circ L$ and so $\det JG = \det J\widetilde{F} = 1$. This finishes the proof.

□

Proof. (**of 1.7**) Let $F \in \mathcal{MP}_n(\mathbb{C})$ be a counterexample for the Jacobian Conjecture. By 1.6 we know that F isn't injective. Thus there are $P, Q \in \mathbb{C}^n$ such that $F(P) = F(Q)$. Without loss of generality we can suppose that $P = (0, \dots, 0)$ and $Q = (1, 0, \dots, 0)$ with $F(P) = 0$. In particular we have $F = X + F_{(2)} + F_{(3)} + \cdots$.

Replace each coefficient a_i that occurs in terms in F of degree ≥ 2 by a new variable Y_i. In this case, we obtain a map $\widetilde{F}$ with coefficients in the ring $\mathbb{Z}[Y_1, \dots, Y_l, X_1, \dots, X_n]$ $(= \mathbb{Z}[X, Y]$ for simplicity). Furthemore, we have $\det J\widetilde{F} = 1 + p(X, Y)$ for some $p(X, Y) = \sum_{i=1}^{k} D_i(Y)X^{\alpha_i} \in \mathbb{Z}[Y, X]$. The condition $\widetilde{F}(1, 0, \dots, 0) = \widetilde{F}(0, \dots, 0)$ can be expressed by polynomial relations $C_1, \dots, C_p$, in the variables $Y_1, \dots, Y_l$. Also, the condition $\det \widetilde{F} = 1$ can be expressed in polynomial relations $D_1(Y), \dots, D_k(Y)$. Now note that since F satisfies $F(1, \dots, 0) = F(0, \dots, 0)$ and $\det JF = 1$ and has coefficients in $\mathbb{C}$ we know that there is a solution (over $\mathbb{C}$) for the algebraic system:

$$D_1 = D_2 = \cdots = D_k = C_1 = \cdots = C_p = 0.$$

So considering the ideal $I = \langle D_1, \dots, D_k, C_1, \dots, C_p \rangle \subset \overline{\mathbb{Q}}[Y_1, \dots, Y_l]$ we know $1 \notin I \Longrightarrow Z(I) \neq \varnothing$ (by Nullstellensatz). So there is a conterexample with coefficients in $\overline{\mathbb{Q}}$. By adjunction of coefficients in $\mathbb{Q}$ and taking the normal closure K we obtain a counterexample $F = X + F_{(2)} + F_{(3)} \cdots$ for the Keller Problem with coefficients in K (Galois extension) with $F(1, 0, .., 0) = F(0, \dots, 0)$. By the lemma above we obtain $G : \mathbb{Q}^{nm} \longrightarrow \mathbb{Q}^{nm}$ a polynomial map which is not injective and with $\det JG = 1$ where $m = [K : \mathbb{Q}]$.

Finally let $r \in \mathbb{N}$ such that $G'_i = X_i + rG_{i1} + rG_{i2} + \cdots + \in \mathbb{Z}[X_1, \dots, X_{nm}]$ for all $1 \leq i \leq n$ and consider the map $G' = (G'_1, \dots, G'_{nm}) : \mathbb{Q}^{nm} \longrightarrow \mathbb{Q}^{nm}$.

[3] we make use of the linear independence of characters: $c_0\sigma_0 + \cdots + c_{m-1}\sigma_{m-1} = 0$ with $c_0, \dots, c_{m-1} \in k \Longrightarrow c_1 = \cdots = c_{m-1} = 0$

We affirm that G' isn't injective and satifies $\det JG' = 1$. Note that $G_i'(X) = r^{-1}G_i(rX) \in \mathbb{Q}[X] \Longrightarrow G(X)' = r^{-1}G(rX)$. In particular, the map G' over $\mathbb{Q}$ isn't injective. We have $J(G(X)') = J(r^{-1}G(rX)) = r^{-1}rJ(G)(rX) = (JG)(rX)$. So by condition $\det JG = 1$ we obtain $\det(J(G(X)')) = 1$ and this finishes the proof.

□

Corollary 1.4. *The Jacobian Conjecture is true over $\mathbb{C}$ if and only it is true over $\mathbb{Z}$.*

1.4 Particular cases

In this section we study some classes of polynomial maps which satisfy the condition of the Jacobian Conjecture. We start with some facts about domains of finite type.

Let k be a field and A a domain with $k \subseteq A \subseteq k[X_1, \ldots, X_n]$ and $\dim A = 1$. We will show that A is a k-algebra of finite type. For this, we remark that we can assume $n = 1$. More precisely,

Lemma 1.3. *Let A be a domain with $\dim A = 1$ such that $k \subset A \subset k[X_1, \ldots, X_n]$. Then, there is a map of k-algebras $\varphi : k[X_1, \ldots, X_n] \longrightarrow k[Z]$ that induces an immersion $\varphi : A \longrightarrow k[Z]$. So we can suppose that $n = 1$.*

Proof. Fix the maximal ideal $M = (X_1, \ldots, X_n) \subset k[X_1, \ldots, X_n]$ and consider $P := A \cap M$. If $P = 0$ then $A \hookrightarrow k[X_1, \ldots, X_n]/M \cong k$ and so $A = k$ a contradiction (since $\dim A = 1$). So $P \neq 0$. Define $P_m := \langle X_1^m - X_n \rangle \in Spec(k[X_1, \ldots, X_n])$ for $m \in \mathbb{N}$. Fix $G \in P \cap M$ a non zero element and chose m such that $X_1^m - X_n \nmid G$. Then, by this choice, and since $\dim A = 1$ we obtain $P_m \cap A = 0$. So the map $\varphi : k[X_1, \ldots, X_n] \twoheadrightarrow k[X_1, \ldots, X_n]/P_m \cong k[X_1, \ldots, X_{n-1}]$ induces an injective map $A/P_m \cap A = A \hookrightarrow k[X_1, \ldots, X_{n-1}]$. By iteration, we obtain the result.

□

Theorem 1.8. *Let A a domain with $\dim A = 1$ and $k \subset A \subset k[X_1, \ldots, X_n]$ for some field k. Then A is a k-algebra of finite type and $\overline{A}$ is a polynomial ring in one variable over k. Here, $\overline{A}$ is the integral closure of A in $Frac(A)$.*

Proof. By lemma 1.3 we can suppose $n = 1$ i.e. $k \subset A \subset k[X]$. We will show, initially, that A is a k-algebra of finite type. For this, take $g \in A \setminus k$ and consider the k-algebra $k[g]$. We have $k[g] \subseteq k[X]$ an integral extension: indeed, X satisfies $p(X) = 0$ where $p(T) = g(T) - g(X) \in k[g][T]$. In particular, we have $k[X]$ is a finitely generated $k[g]$-module. Since A is a $k[g]$-submodule we have A a $k[g]$-module finitely generate. In particular, it is of finite type over k

Let $L := Frac(A)$. Since $k \subset L \subset k(X)$ we have $L = k(Z)$, for some rational function Z [4]. Let $\overline{A}$ denote the integral closure of A in L. By Theorem 4.2, we have

$$\overline{A} = \bigcap_{\mathcal{O} \in S(A)} \mathcal{O} = \bigcap k[Z]_{p(Z)}$$

where the intersection is taken over all irreducibles in $k[Z]$ and

$$S(A) := \{\mathcal{O} \subset L \mid \mathcal{O} \text{ is a valuation ring that contains } A\}.$$

Now, note that all valuation rings of $k(X)$ contain A, with possible exception of the ring in infinity. This follows from the fact that $A \subset k[X]$ since every valuation ring of "finite distance" of $k(X)$ is of form $k[X]_{p(X)}$ with $p(X)$ irreducible.

Since every valuation ring of $k(Z)$ is a contraction of some discrete valuation of $k(X)$ [5] we conclude that all valuation rings of $k(Z)$ contain A, with the exception of those that come from $k[1/X]_{1/X}$. Now, note that if $\mathcal{O}$ is a DVR of $k(Z)$ that comes from $k[1/X]_{1/X}$ by looking the residues fields we have:

$$k \hookrightarrow \mathcal{O}/P \hookrightarrow \frac{k[1/X]_{1/X}}{(1/X)} = k$$

So the possible DVRs that come from $k(Z)$ that do not contain A are of form $k[Z]_{p(Z)}$ for some $p(Z)$ irreducible linear and $k[1/Z]_{1/Z}$. In the last case, we have $\overline{A} = \bigcap k[Z]_{p(Z)} = k[Z]$ and in the first case, we make use of the fact $k(Z) = k(1/Z)$ and so we obtain $\overline{A} = k[1/Z]$.

□

Theorem 1.9. ***(Formanek)*** *Let $F \in \mathcal{MP}_n(k)$ be a Keller map with k a field with $char(k) = 0$. Suppose that there is a $F_{n+1} \in k[X_1, \ldots, X_n]$ such that $k[F_1, \ldots, F_n, F_{n+1}] = k[X_1, \ldots, X_n]$. Then F is an invertible map.*

Proof. Let $Y_1, \ldots, Y_n, Y_{n+1}$ be variables over k. For simplicity, define $A := k[Y_1, \ldots, Y_n, Y_{n+1}]$ and consider the map of k-algebras $\alpha : A \twoheadrightarrow k[X_1, \ldots, X_n]$ given by $Y_i \mapsto F_i$ for $i = 1, \ldots, n+1$. Let $P \in Spec(A)$ be the kernel of α. Recall that $ht(P) = 1$ (apply the formula $\dim A = \dim A/P + ht(P)$, true for all domains of finite type over a field k). So since A is factorial we have $P = (F)$ for some $F \in A$.

Pick $T_1, \ldots, T_n \in A$ such that $\alpha(T_j) = X_j$. We have $Y_j - F_j(T_1, \ldots, T_n) \in Ker(\alpha) = P$. So there are

[4] Recall: **Lüroth Theorem.** *Let $k(t)$ be the field of rational functions over a field k and L subfield with $k \subsetneq L \subset k(t)$. Then, there is $s \in k(t)$ such that $L = k(s)$.*

[5] Let A a DVR with $K := Frac(R)$ and $L|K$ a finite extension. Let R the integral closure of A in L. Suppose that R is a finite A-module. Then R is a semilocal ring and each DVR over A is obtained by taking R_P for some $P \in Spec(R)$. In the case in question, $A = k[Z]$ and by general results we know that R is finite over A.

$R_1, \ldots, R_{n+1} \in A$ such that $Y_j = F_j(T_1, \ldots, T_n) + R_j F$. Write, $F = H_r Y_{n+1}^r + \cdots + H_0$ with $H_0, \ldots, H_r \in k[Y_1, \ldots, Y_n]$. Note that $H_j \neq 0$ for some $j > 0$ (Keller condition ($\det JF \in k^*$) implies that $F_1, \ldots, F_n$ are algebraically independent over k.)

Applying the operator $\partial/\partial Y_j$ for $j = 1, \ldots, n+1$ we obtain

$$\frac{\partial Y_i}{\partial Y_j} = \sum_{k=1}^{n} \frac{\partial F_i}{\partial X_k}(T_1, \ldots, T_n)\frac{\partial T_k}{\partial Y_j} + \frac{\partial R_i}{\partial Y_j}F + \frac{\partial F}{\partial Y_j}R_i \qquad 1 \leq i, j \leq n+1$$

In terms of matrices, we have

$$Id_{n+1} = \begin{pmatrix} \frac{\partial F_1(T_1,\ldots,T_n)}{\partial X_1} & \vdots & \vdots & \frac{\partial F_1(T_1,\ldots,T_n)}{\partial X_n} & R_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial F_n(T_1,\ldots,T_n)}{\partial X_1} & \vdots & \vdots & \frac{\partial F_n(T_1,\ldots,T_n)}{\partial X_n} & R_n \\ \frac{\partial F_{n+1}(T_1,\ldots,T_n)}{\partial X_1} & \vdots & \vdots & \frac{\partial F_{n+1}(T_1,\ldots,T_n)}{\partial X_n} & R_{n+1} \end{pmatrix} \begin{pmatrix} \frac{\partial T_1}{\partial Y_1} & \vdots & \vdots & \frac{\partial T_1}{\partial Y_{n+1}} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial T_n}{\partial Y_1} & \vdots & \vdots & \frac{\partial T_n}{\partial Y_{n+1}} \\ \frac{\partial F}{\partial Y_1} & \vdots & \vdots & \frac{\partial F}{\partial Y_{n+1}} \end{pmatrix} + F \begin{pmatrix} \frac{\partial R_1}{\partial Y_1} & \vdots & \vdots & \frac{\partial R_1}{\partial Y_{n+1}} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial R_n}{\partial Y_1} & \vdots & \vdots & \frac{\partial R_n}{\partial Y_{n+1}} \\ \frac{\partial R_{n+1}}{\partial Y_1} & \vdots & \vdots & \frac{\partial R_{n+1}}{\partial Y_{n+1}} \end{pmatrix}$$

Applying α in the above identiy and observing that $\alpha(\frac{\partial F_j(T_1,\ldots,T_n)}{\partial X_p}) = \frac{\partial F_j(X_1,\ldots,X_n)}{\partial X_p}$ for all $1 \leq p \leq n$ and $1 \leq i \leq n+1$ we obtain the following identity over $k[X_1, \ldots, X_n]$:

$$Id_{n+1} = \begin{pmatrix} \frac{\partial F_1(X_1,\ldots,X_n)}{\partial X_1} & \vdots & \vdots & \frac{\partial F_1(X_1,\ldots,X_n)}{\partial X_n} & (**) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial F_n(X_1,\ldots,X_n)}{\partial X_1} & \vdots & \vdots & \frac{\partial F_n(X_1,\ldots,X_n)}{\partial X_n} & (**) \\ (**) & \vdots & \vdots & (**) & (**) \end{pmatrix} \begin{pmatrix} (**) & \vdots & \vdots & (**) \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ (**) & \vdots & \vdots & (**) \\ (**) & \vdots & \vdots & \alpha(\frac{\partial F}{\partial Y_{n+1}}) \end{pmatrix}$$

Multiplying by the adjoint matrix and using the fact that $(F_1, ..., F_n)$ is a Keller map we obtain $\alpha(\frac{\partial F}{\partial Y_{n+1}}) \in k^* \Longrightarrow \alpha(\frac{\partial F}{\partial Y_{n+1}}) = c$, for some $c \in k^*$. So $\frac{\partial F}{\partial Y_{n+1}} - c \in P$. By comparison of degrees we have $\frac{\partial F}{\partial Y_{n+1}} - c = 0 \Longrightarrow \frac{\partial F}{\partial Y_{n+1}} = c \Longrightarrow F = cY_{n+1} + H_0(Y_1, \ldots, Y_n)$. In particular, $0 = cF_{n+1} + H_0(F_1, \ldots, F_n) \Longrightarrow F_{n+1} = -c^{-1}H_0(F_1, \ldots, F_n)$. So $k[F_1, \ldots, F_n, F_{n+1}] = k[F_1, \ldots, F_n] = k[X_1, \ldots, X_n] \Longrightarrow (F_1, \ldots, F_n)$ is an invertible polynomial map.

□

Theorem 1.10. *Let $F = X + H \in \mathcal{MP}_n(k)$ be a polynomial map with k a $\mathbb{Q}$-algebra. Assume H homogeneous of degree d. Suppose that $JH^2 = 0$. Then F is invertible with inverse given explicitly by $F^{-1} = X - H$.*

Remark 3. *Let $A = \oplus_{n\in\mathbb{N}} A_d$ be a graded ring (not necessarily commutative). Let $d \in A$ be homogeneous of degree $e > 1$. Then*

$$d \text{ is nilpotent} \Longleftrightarrow 1 - d \in A^*.$$

The implication $\Longrightarrow$follows from the formula: $(1-d)(1+d+d^2+\cdots+d^n) = 1-d^{n+1}$. Now, suppose that $1-d \in A^*$ but d isn't nilpotent. Let $\alpha \in A$ be the inverse of $1-d$ and consider the formula $(1-d)(1+d+d^2+\cdots+d^n) = 1-d^{n+1}$. Multiplying in the left by α we obtain

$$s_n := 1 + d + d^2 + \cdots + d^n = \alpha - \alpha d^{n+1}.$$

From $\alpha(1 - d) = 1$ we obtain $\alpha = 1 + \alpha d$. Note that $deg(\alpha) = 0$. Plugging in the above relation we obtain $s_n = \alpha - (1 + \alpha d)d^{n+1} = \alpha - d^{n+1} - \alpha d^{n+2}$. By iteration, and using the fact d isn't nilpotent we see that s_n has terms of arbitrarily large degree, a contradiction. So d is nilpotent.

Considering $A = k[X_1, \ldots, X_n]^n$ with its natural graded structure we see that given a map $F = X + H$ with H homogeneous we have

$$J(H) \text{ is nilpotent if and only if } J(F) \in GL_n(k[X_1, \ldots, X_n]).$$

With notations as above, let $H = (H_1, \ldots, H_n)$ with $H_i \in k[X_1, \ldots, X_n]$. Consider the **Euler operator:**

$$\triangle : k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_n], \qquad P \longmapsto \sum_{i=1}^{n} \frac{\partial P}{\partial X_i} H_i.$$

The following properties are easy to check:

- $\triangle$ is k-linear.
- $\triangle(PQ) = P\triangle(Q) + Q\triangle(P)$ for any $P, Q \in k[X_1, \ldots, X_n]$.

In what follows, $\triangle^m := \triangle \circ \triangle \circ \cdots \circ \triangle$ (n times).

Lemma 1.4. *Suppose that $\triangle(H_1) = \cdots = \triangle(H_n) = 0$. Then for all $P \in k[X_1, \ldots, X_n]$*

$$\triangle^m(P) = \sum_{i_1,\ldots,i_m} \frac{\partial^m(P)}{\partial X_{i_1} \partial X_{i_2} \cdots \partial X_{i_m}} H_{i_1} \cdots H_{i_m}.$$

Proof. Induction. □

Lemma 1.5. *Let $F = X + H$ and $G = X - H$ be polynimial maps (as above). The following are equivalent:*

(i) F is ivertible with inverse G.

(ii) $H_i(X-H) = H_j$ *for all* $i = 1, \dots, n$.

(iii) $\triangle H_i = 0$ *for all* $i = 1, \dots, n$.

Proof. $(ii) \Longrightarrow (i)$: We have $F(G) = F(X-H) = X - H + H(X-H) = X - H + H = X$ and so F is invertible with inverse G.

$(iii) \Longrightarrow (ii)$: By Taylor expansion and by lemma above we have $H_i(X-H) = H_i - \triangle H_i - \triangle^2 H_i/2 + \cdots$. Since $\triangle H_i = 0$ for all i we obtain (ii).

$(i) \Longrightarrow (iii)$: We have $X = F(X-H) = X - H + H(X-H) \Longleftrightarrow H_i(X-H) = H_i$ for all $i = 1, \dots, n$. Considering the Taylor expansion we obtain

$$H_i(X-H) = H_i - \triangle H_i - \triangle^2 H_i/2 + \cdots$$

By hypothesis we know $H_i(X-H) = H_i$ and so $\triangle H_i + \triangle^2 H_i/2 + \cdots$. By comparison of degrees we see that $\triangle^m H_i = 0$ for all $i = 1, \dots, n$. □

Proof. (**of 1.10**) The condition $JH^2 = 0$ implies

$$\begin{pmatrix} \frac{\partial H_1(X_1,\dots,X_n)}{\partial X_1} & \vdots & \vdots & \frac{\partial H_1(X_1,\dots,X_n)}{\partial X_n} \\ \vdots & \vdots & \vdots & \ddots \\ \frac{\partial H_n(X_1,\dots,X_n)}{\partial X_1} & \vdots & \vdots & \frac{\partial H_n(X_1,\dots,X_n)}{\partial X_n} \end{pmatrix} \begin{pmatrix} dH_1 \\ \vdots \\ \vdots \\ dH_n \end{pmatrix} = \begin{pmatrix} d\sum_j \frac{\partial H_1(X_1,\dots,X_n)}{\partial X_j} H_j \\ \vdots \\ d\sum_j \frac{\partial H_n(X_1,\dots,X_n)}{\partial X_j} H_j \end{pmatrix} = \begin{pmatrix} d\triangle H1 \\ \vdots \\ \vdots \\ d\triangle H_n \end{pmatrix} = 0$$

So $d\triangle H_k = 0 \Longrightarrow H_k = 0$ for all $k = 1, \dots, n$. The result follows from the lemma above.

□

Lemma 1.6. *Let* k *be a field with* $char(k) = 0$ *and* $T \in A := k[X_1, \dots, X_n]$. *Denote by* $D_j := \frac{\partial}{\partial X_j}$ *the* j*-th canonical derivation. Let* V *be the* k*-vecor space generated by* $D_1T, \dots, D_nT$ *and* $r := \dim_k V$. *Then there is a linear change of coordinates* $X_k \mapsto L_k$ *such that if* $S := T(L)$ *then* $\{D_1S, \dots, D_rS\}$ *is a basis of* V *and* S *is independent of* $X_{r+1}, \dots, X_n$. *Furthemore,* $D_1S, \dots, D_rS$ *are algebraically independent over* $k[S]$.

Proof. If $r = \dim_k V$ we can suppose, without loss of generality, that $\{D_1T, \dots, D_rT\}$ is a basis for V. So for $r+1 \leq j \leq n$: $D_{r+j}T = \sum_{i=1}^{r} \alpha_{ij} D_iT$ for some constants $\alpha_{ij} \in k$. Through such constants, we can find a matrix A such that the induced map $L : k^n \longrightarrow k^n, X \mapsto AX$ is such that if $S := T(L)$ then $D_{r+j}S = 0$ for $1 \leq j \leq n-r$. So we conclude $(char(k) = 0)$ that S is independent of $X_{r+1}, \dots, X_n$. Suppose that $\sum_{i=1}^{r} P_i(S) D_iS = 0$ for

some $P_1(S),\dots,P_r(S) \in k[S]$. Erasing the common factors we can suppose that $\gcd(P_1(S),\dots,P_r(S)) = 1$. By reduction mod S we obtain $0 = \sum_{i=1}^r P_i(S)D_iS \equiv \sum_{i=1}^r P_i(0)D_iS \mod S \Longrightarrow \sum_{i=1}^r P_i(0)D_iS \in (S)$. By comparison of degree we obtain $\sum_{i=1}^r P_i(0)D_iS = 0$ a contradiction. □

Theorem 1.11. *Let k be a field with $char(k) = 0$ and $F \in \mathcal{MP}_n(k)$ a map of the form $F = X + H$ with $H(0) = 0$. Suppose that JH is nilpotent with rank $= 1$. Then F is an invertible polynomial map.*

Proof. Let $H = (H_1,\dots,H_n)$ be the components of H and consider the k-algebra $R = k[H_1,\dots,H_n]$. Let $L = k(H_1,\dots,H_n)$ be the fraction field of R and $K = k(X_1,\dots,X_n)$. Consider the following exact sequence

$$\Omega_{L/k} \otimes_L K \xrightarrow{\alpha} \Omega_{K/k} \xrightarrow{\beta} \Omega_{K/L} \longrightarrow 0$$

By definition of α we have $\alpha(\Omega_{L/k} \otimes_L K)$ is a K-subspace of $\Omega_{K/k}$ with generators $d_{K/k}(H_1),\dots,d_{K/k}(H_n)$. Hence $\dim_K Im(\alpha) = rank_K J(H) = 1$. So

$$\dim_K \Omega_{K/L} = \dim_K(\Omega_{K/k}) - \dim Im(\alpha) = tr.deg_k(K) - 1$$

Since $\dim_K \Omega_{K/L} = tr.deg_L(K)$ (see dimension formula 4.2) we have $tr.deg_k(L) = 1$. So $\dim_{Krull} R = tr.deg_k(L) = 1$. By theorem 1.8 we have that the integral closure, $\overline{R}$, of R in $Frac(R)$ is a polynomial ring. Now note that if $P \in \overline{R}$ then P is integral over $k[X_1,\dots,X_n]$ and since that this last ring is integrally closed we obtain $P \in k[X_1,\dots,X_n]$. So $\overline{R} = k[T]$ for some $T \in k[X_1,\dots,X_n]$.

By the lemma above there is a linear change of variables $X_i \mapsto L_i$ such that if $S := T(L)$ then S is independent of $X_{r+1},\dots,X_n$ and $D_1S,\dots,D_rS$ are algebraically linearly independent over $k[S]$. Write $H = (H_1,\dots,H_n) = (Q_1,\dots,Q_n)$ with $Q_1,\dots,Q_n \in k[T]$. If $G = L^{-1} \circ F \circ L$ we have

$$G = X + L^{-1} \circ H \circ L = X + L^{-1} \circ Q(T(L)) = X + L^{-1}(Q(S)).$$

Define $R := (R_1,\dots,R_n)$ with $R_i := L^{-1} \circ Q(T) \in k[T]$. Then $L^{-1}(Q(S)) = R(S) = (R_1(S),\dots,R_n(S))$. The Jacobian matrix of $R(S)$ is nilpotent, of the form

$$\begin{pmatrix} R_1'(S)D_1S & R_1'(S)D_2S & \ddots & \vdots & \vdots & R_1'(S)D_nS \\ R_2'(S)D_1S & R_2'(S)D_2S & \ddots & \vdots & \vdots & R_2'(S)D_nS \\ & & \ddots & \vdots & \vdots & \\ R_n'(S)D_1S & R_n'(S)D_2S & \ddots & \vdots & \vdots & R_n'(S)D_nS \end{pmatrix}$$

In particular, we have $0 = tr(J(R(S))) = \sum_{i=1}^n R_i'(S)D_iS$. Since $D_{r+1}S = \cdots = D_nS = 0$ we obtain

$\sum_{i=1}^{r} R_i'(S)D_iS = 0 \Longrightarrow R_1'(S) = \cdots = R_r'(S) = 0 \Longrightarrow R_1, \ldots, R_r \in k$. Since $H(0) = 0$ we have $R(0) = 0$ and so, $R_1 = \cdots = R_r = 0$. So G is a map of the form $G = (X_1, \ldots, X_r, X_{r+1} + R_{r+1}(S), \ldots, X_n + R_n(S))$ with $R_{r+j}(S)$ independent of $X_{r+1}, \ldots, X_n \Longrightarrow G$ (and so F) is invertible. □

Chapter 2

Reductions

In this chapter we give some results about reductions. The main objective is to show that the Jacobian Conjecture (over $\mathbb{C}$) is true if it is so for any regular polynomial map $F = X + H$ with H homogeneous and of degree 3 with JH nilpotent. This result will be refined: it is sufficient to consider polynomial maps in the form $F = X + H$ where H is homogeneous, $deg(H) = 3$ and with JH nilpotent and **symmetric**.

2.1 Classical reduction theorem

Let R be a ring (as always, commutative with 1) and consider the polynomial ring $R^{[n]} := R[X_1, \ldots, X_n]$. Let $M = X_1^{e_1} \cdots X_n^{e_n}$ be a monomial and define $e_j(M) := e_j$ for $1 \leq j \leq n$. If $f \in R^{[n]}$ we denote

$$\widetilde{M}(f) := \{M \mid \ M \text{ is a monomial wich occurs in } f \ \}$$

and we define

$$e(f) := \sum_{M \in \widetilde{M}(f)} \sum_{i=1}^{n} \mathbf{Max}\{e_j(M) - 1, 0\}^2.$$

Definition 2.1. *Given $g \in R^{[n]}$ we say that g is of linear type if $e(g) = 0$.*

Definition 2.2. *Let $F \in \mathcal{MP}_n(R)$ with $F = (F_1, \ldots, F_n)$. The **linearity index** of F is defined by*

$$e(F) := \sum_{i=1}^{n} e(F_i).$$

Let $F \in \mathcal{MP}_n(R)$ be a polynomial map and $m \in \mathbb{Z}_{\geq 0}$. Consider the map

$$\alpha_m : \mathcal{MP}_n(R) \longrightarrow \mathcal{MP}_{n+m}(R), \qquad F \longmapsto (F, X_{n+1}, \ldots, X_{n+m})$$

For simplicity we denote $\alpha_m(F)$ by $F^{[m]}$ and we call it the m-expansion of the map F.

It is easy to check the following properties:

(i) $detJF = detJF^{[m]}$.

(ii) F is invertible if and only if $F^{[m]}$ is invertible.

In the sequel $\mathcal{ME}_n(R)$ will denote the group generated by all elementary n-dimensional maps (via composition) over R. We also write

$$\mathcal{ME}_n^{(0)}(R) := \mathcal{ME}_n(R) \cap \mathcal{MP}_n^{(0)}(R) \qquad \text{and} \qquad \mathcal{ME}_n^{(1)}(R) := \mathcal{ME}_n(R) \cap \mathcal{MP}_n^{(1)}(R).$$

Theorem 2.1. ***(Bass-Connell-Wright)***[1] *Let R be a ring and $F \in \mathcal{MP}_n^{(1)}(R)$ a Keller map. Then there are $m \in \mathbb{Z}_{\geq 0}$, $G, H \in \mathcal{ME}_{n+m}^0(R)$ and $E(T) \in \mathcal{MP}_{n+m}(R[T])$ (T is a variable) such that*

(i) $E(1) = G \circ F^{[m]} \circ H$. So if E is invertible $\Longrightarrow$ F is invertible.

(ii) Consider the polynomial map gotten from $E(T)$,

$$\begin{array}{rccc} \widetilde{E} : R^{n+m+1} & \longrightarrow & R^{n+m+1} \\ (X, T) & \longmapsto & (E(T), T). \end{array}$$

Then $\widetilde{E} = X + H$ with H homogeneous of degree 3, JH nilpotent and

$$E \text{ is invertible} \Longleftrightarrow \widetilde{E} \text{ is invertible.}$$

The proof is in 3 steps:

- reduction of degree.
- reduction to nilpotent case.
- reduction to homogeneous case.

[1] see [2, (2.1)Theorem]

Proposition 2.1. *Let $F \in \mathcal{MP}_n(R)$. Then there exist $m \in \mathbb{Z}_{\geq 0}$ and maps $G, H \in \mathcal{ME}^{(1)}_{n+m}(R)$ such that $F' = G \circ F^{[m]} \circ H$ has degree ≤ 3. Furthemore, it is possible to take $H \in \mathcal{ME}^{(0)}_{n+m}(R)$ such that F' is of linear type.*

Proof. Let d be the degree of F and denote by g the number of monomials of degree d that occur in F. If $d \leq 3$, finish. Suppose that $d > 3$. We will show the proposition by induction in the pair (d, g). Let M be a monomial wich occurs in F with degree d. Without loss of generality we can assume that M occurs in F_1. Write $M = PQ$ where P and Q are monomials with degree $\leq d-2$ and consider the maps $G, H \in \mathcal{ME}^{(1)}_{n+2}(R)$ defined by

$$G = (X_1 - X_{n+1}X_{n+2}, X_2, \ldots, X_n, X_{n+1}, X_{n+2}) \qquad H = (X_1, \ldots, X_n, X_{n+1} + P, X_{n+2} + Q).$$

We have $F' := G \circ F^{[2]} \circ H = (F_1 - X_{n+1}P - X_{n+2}Q - X_{n+1}X_{n+2} - PQ, F_2, \ldots, F_n, X_{n+1} + P, X_{n+2} + Q)$. Consider the pair (d', g') associated to F'. By construction, we have $d' < d$ or $d' = d$. In any case we have $g' < g$ and by induction hypothesis there are maps $\widetilde{G}, \widetilde{H} \in \mathcal{ME}^{(1)}_{n+2+m}(R)$ such that $\widetilde{F} = \widetilde{G} \circ (F')^{[m]} \circ \widetilde{H} = \widetilde{G} \circ G^{[m]} \circ F^{[m+2]} \circ H^{[m]} \circ \widetilde{H}$ have degree ≤ 3. This finishes the first part.

Let $F \in \mathcal{MP}_n(R)$ be a polynomial map with degree ≤ 3. Suppose that $e(F) > 0$ and let M be a monomial wich occurs in F_1 such that $X_j^2 | M$ for some $1 \leq j \leq n$. Write $M = PQ$, with $X_j | P$ and $X_j | Q$. We can assume that $P = X_j$ and $Q = X_j N$ with $N \in \{X_1, \ldots, X_n\}$ or $N \in R$. By using G and H as above we have $F' := G \circ F^{[2]} \circ H = (\widetilde{F}_1, \ldots, \widetilde{F}_{n+2}) = (F_1 - X_{n+1}P - X_{n+2}Q - X_{n+1}X_{n+2} - PQ, F_2, \ldots, F_n, X_{n+1} + P, X_{n+2} + Q)$ with $G \in \mathcal{ME}^{(1)}_{n+2}(R)$ and $H \in \mathcal{ME}^{(0)}_{n+2}(R)$. Now if $N = X_k$ with $k \neq j$ or $N \in R$ we have $e(\widetilde{F}_1) = e(F_1) - 2$ and $e(\widetilde{F}_l) = e(F_l)$ for $1 \leq l \leq n$ and $e(\widetilde{F}_{n+1}) = e(\widetilde{F}_{n+2}) = 0$. In this case $e(\widetilde{F}) < e(F)$.

If $N = X_j$ we have $P = X_j$ and $Q = X_j^2$. So, $e(\widetilde{F}_1) = e(F_1) - 1$ and $e(\widetilde{F}_l) = e(F_l)$ for $1 \leq l \leq n$, $e(\widetilde{F}_{n+1}) = 0$ and $e(\widetilde{F}_{n+2}) = 1$. In this case, $e(\widetilde{F}) = e(F)$. In order to decrease $e(F)$ write $Q = P'Q'$ with $P' = Q' = X_j$ and consider the map $S = (X_1, \ldots, X_{n+2}, X_{n+3} + P', X_{n+4} + Q')$ and $T = (X_1, \ldots, X_{n+1}, X_{n+2} - X_{n+3}X_{n+4}, X_{n+3}, X_{n+4})$. We have

$$F'' := T \circ (F')^{[2]} \circ S = T \circ (\widetilde{F_1}, \ldots, \widetilde{F}_{n+2}, X_{n+3} + P', X_{n+4} + Q')$$

$$= (\widetilde{F_1}, \ldots, \widetilde{F}_{n+2} - X_{n+3}X_{n+4} - P'Q' - X_{n+3}Q' - X_{n+4}P', X_{n+3} + P', X_{n+4} + Q').$$

It is easy to check that $e(F'') < e(F)$.

Thus in any case we see that it is possible to reduce the index $e(F)$. By induction we can find $G \in \mathcal{ME}^{(1)}(R)$ and $H \in \mathcal{ME}^{(0)}_{n+m}$ such that $G \circ F^{[m]} \circ H$ has degree ≤ 3 and is of linear type. □

Let $F \in \mathcal{MP}_n(R)$ be a Keller map. By the result above there are $G, H \in \mathcal{ME}_{n+m}(R)$ with $H(0) = G(0) = 0$ and

$JG(0) = id_n$ such that $F' := G \circ F^{[m]} \circ H$ has maximum degree 3. So to control invertibility we can suppose that $F = F'$. Write $F = F_{(1)} + F_{(2)} + F_{(3)}$ where $F_{(i)}$ is the homogeneous component of F in degree i. Since F is a Keller map we have, in particular, that $\det JF(0) = \det JF_{(1)} \in R^*$. So by composition with an automorphism we can suppose that $F = X + F_{(2)} + F_{(3)}$. Let T be a new variable over R and consider the polynomial map $E(T) : R[T]^n \longrightarrow R[T]^n,\ X \longmapsto X + TF_{(2)}(X) + T^2F_{(3)}(X)$. Note that

$$JE(T) = id_n + TJF_{(2)} + T^2JF_{(3)} = JF(TX)$$

So $E(T)$ is a Keller map over $R[T]$.

Consider new variables $Y = (Y_1, \ldots, Y_n)$ and let $G(T), H(T) \in \mathcal{ME}_{n+m}(R[T])$ be defined by

$$G(T) = (X + TY, Y) \qquad\qquad H(T) = (X, Y - TF_{(3)})$$

We have

$$\widetilde{E}(T) := G(T) \circ E(T)^{[n]} \circ H(T) = G(T) \circ (E(T), Y - TF_{(3)}) = (E(T) + T(Y - TF_{(3)}), Y - TF_{(3)})$$

$$= (E(T) + TY - T^2F_{(3)}, Y - TF_{(3)}).$$

So $\widetilde{E}(T) = (X + TF_{(2)} + TY, Y - TF_{(3)}) = (X, Y) + T(F_{(2)} + Y, -F_{(3)}) = (X, Y) + TN$. By construction $\widetilde{E}(T)$ is invertible if and only if $E(T)$ is invertible. Furthemore, the invertibility of $\widetilde{E}(1)$ implies the invertibility of the map F. Also, we have $\widetilde{E}(1) = G(1) \circ F^{[m]} \circ H(1)$ and so we obtain the item (i) of theorem above.

Considering the jacobian map J_{2n} we have

$$J_{2n}\widetilde{E}(T) = id_{2n} + TJ_{2n}N \in GL_{2n}(R[X_1, \ldots, Y_n, T])$$

where

$$J_{2n}N = \begin{pmatrix} J_nF_{(2)} & id_n \\ -J_nF_{(3)} & 0 \end{pmatrix}$$

Proposition 2.2. *$J_{2n}N \in \mathcal{M}_{2n}(R[X_1, \ldots, Y_n, T]$ is a nilpotent matrix.*

Proof. Consider the matrix ring $\mathcal{M}_{2n}(R[X_1, \ldots, X_n, T])$ with graded structure by T-degree:

$$\mathcal{M}_{2n}(R[X_1, \ldots, X_n, T]) = \bigoplus_{d \in \mathbb{N}} \mathcal{M}_{2n}(R[X_1, \ldots, X_n, T])_d$$

where $\mathcal{M}_{2n}(R[X_1,\dots,X_n,T])_d := \mathcal{M}_{2n}(R[X_1,\dots,X_n)T^d$. Note that $TJ_{2n}N$ is a homogeneous element of degree 1. So, the result follows from Remark 3

□

We can summarize the results above in the following

Proposition 2.3. *Let R be a ring. Then the Jacobian Conjecture over R is true if and only if it is so for any $n \in \mathbb{N}$ and all regular map $F = X + N \in \mathcal{MP}_n(R)$ with JN nilpotent and $deg(F) \leq 3$.*

Now let $F = X+N$ be a map as in the proposition above and set $N = N_{(1)}+N_{(2)}+N_{(3)}$ with $N_{(i)}$ the homogeneous component of degree i. Let T be a variable over R and consider $F(T) = X + T^2N_{(1)} + TN_{(1)} + N_{(3)} = X + \widetilde{N}$. Let $\widetilde{F} : R^{n+1} \longrightarrow R^{n+1}$ be the map given by $(X,T) \mapsto (F(T),T) = (X,T) + (T^2N_{(2)} + TN_{(1)} + N_{(3)}, 0)$. We have

$$J_{n+1}\widetilde{F} = id_{n+1} + J_{n+1}(\widetilde{N},0) = id_{n+1} + \begin{pmatrix} T^2J_n(N_{(2)}) + TJ_n(N_{(1)}) + J_n(N_{(3)}) & 2TN_{(2)} + N_{(1)} \\ 0 & 0 \end{pmatrix}$$

Lemma 2.1. *Let $A = \bigoplus_{d\in\mathbb{N}} A_d$ be a graded ring and T a variable over A. Consider a graded structure in $A[T]$ by*

$$A[T] = \bigoplus_{d\in\mathbb{N}} A[T]_{(d)}$$

with $A[T]_{(d)} := A_0T^d \oplus A_1T^{d-1} \oplus \cdots \oplus A_d$. Define $A_{(d)} := A_0 \oplus A_1 \oplus \cdots \oplus A_d$.

The map $\alpha_d : A_{(d)} \longrightarrow A[T]_{(d)}$ given by $a_0 + \cdots + a_d \mapsto a_0T^d + \cdots + a_d$ is an isomorphism of groups. Furthemore $a \in A_{(d)}$ is nilpotent if and only if $\alpha_d(a)$ is nipotent.

Proof. The first item is easy. Given $a \in A_d$ denote $\alpha_d(a) := a^{(d)}$ for simplicity. Pick $e \in \mathbb{N}$ and $b \in A_{(e)}$. We affirm that $(ab)^{(e+d)} = a^{(d)}b^{(e)}$. Indeed, note that $\alpha^{-1}_{d+e}(a^{(d)}b^{(e)}) = (a^{(d)}b^{(e)})(1) = a^{(d)}(1)b^{(e)}(1) = ab$ and so $(ab)^{(e+d)} = a^{(d)}b^{(e)}$. In particular taking $a = b$ and $n \in \mathbb{N}$ we have

$$(a^n)^{(nd)} = (a^{(d)})^n$$

and so a is nilpotent $\iff a^{(d)}$ is nilpotent. □

Proposition 2.4. *$J_{n+1}(\widetilde{N},0)$ is nilpotent.*

Proof. Consider the ring $A := \mathcal{M}_n(R[X_1,\dots,X_n])$ with graded structure by X-degree. We have $T^2J_n(N_{(2)}) + TJ_n(N_{(1)}) + J_n(N_{(3)}) \in A[T]_{(3)}$ and by the lemma above $T^2J_n(N_{(2)}) + TJ_n(N_{(1)}) + J_n(N_{(3)})$ is nilpotent if and

only if $J_nN = J_n(N_{(2)}) + J_n(N_{(1)}) + J_n(N_{(3)})$ is nilpotent. Since J_nN is nilpotent we get the result. □

A consequence of this is the following

Reduction Theorem. *Suppose that, for all $n \in \mathbb{N}$ and all $F \in \mathcal{MP}_n(R)$ of the form $F = X + H$ with H cubic homogeneous and JN nilpotent, F is invertible. Then for all $n \in \mathbb{N}$ and for any map $F \in \mathcal{MP}_n(R)$ with $JF \in GL_n(R[X_1, \ldots, X_n])$, F is invertible.*

2.2 Druzkowski maps

Definition 2.3. *Let R be a domain and $F \in \mathcal{MP}_n(R)$. We say that F is a **Druzkowski** map if $F = X + H$ with $H = (H_1, \ldots, H_n)$ cubic homogeneous of the form $H_j = (\sum_k a_{kl}X_k)^3$ for some constants $a_{ij} \in R$.*

We can apply the reduction theorem to show the following

Theorem 2.2. *Let R be a $\mathbb{Q}$-algebra. Suppose that for all $n \in \mathbb{Z}_{\geq 2}$ and $F \in \mathcal{MP}_n(R)$ all Keller Druzkowski maps are invertible. Then the Jacobian Conjecture over R is true.*

Proof. Let $F \in \mathcal{MP}_n(R)$ be a Keller regular map, i.e., $F = X + H$ with JH nilpotent matrix and H homogeneous of degree 3. We will show that F is invertible.

Given $X, Y, Z \in R[X_1, \ldots, X_n]$ note the following formulas

$$XY^2 = 1/6(-2X^3+(X-Y)^3+(X+Y)^3) \quad \text{and} \quad XYZ = ((X-Y-Z)^3-(X+Y-Z)^3-(X-Y+Z)^3+(X+Y+Z)^3)/24.$$

So we can rewrite $H_j \in R[X_1, \ldots, X_n]$ in the form

$$H_l = \sum_{k=1}^{s_j} \alpha_{lk} L_{lk}^3$$

where $L_{lk} \in \mathbb{Q}X_1 + \cdots + \mathbb{Q}X_n \subset \mathbb{Q}[X_1, \ldots, X_n]$. Let $s := s_1 + \cdots + s_n$ be the total quantity of terms of type L_{ij}^3. Introduce new variables $Y_i^{(j)}$ and consider the map $F_L \in \mathcal{MP}_{n+s}(R)$ defined by

$$F_L = (F_1, \ldots, F_n, Y_1^{(1)} + L_{11}^3, \ldots, Y_{s_1}^{(1)} + L_{1s_1}^3, \ldots, Y_1^{(n)} + L_{n1}^3, \ldots, Y_{s_n}^{(n)} + L_{ns_n}^3).$$

By construction we have that F is invertible if F_L is invertible. Consider the elementary map

$$E_1 = (X_1 - \sum_{k=1}^{s_1} \alpha_{1k} Y_k^{(1)}, X_2, \ldots, X_n, Y_1^{(1)}, \ldots, Y_{r_1}^{(1)}, \ldots, Y_1^{(n)}, \ldots, Y_{r_n}^{(n)}).$$

Note that

$$E_1 \circ F_L = (F_1 - \sum_{k=1}^{s_1} \alpha_{1k} Y_k^{(1)} - \sum_{k=1}^{r_1} \alpha_{1k} L_{1k}^3, X_2, \ldots, X_n, Y_1^{(1)} + L_{11}^3, \ldots, Y_{s_1}^{(1)} + L_{1s_1}^3, \ldots, Y_1^{(n)} + L_{n1}^3, \ldots, Y_{s_n}^{(n)} + L_{ns_n}^3).$$

Now, considering the elementary map $E_2 = (X_1, X_2 - \sum_{k=1}^{s_2} \alpha_{2k} Y_k^{(2)}, \ldots, X_n, Y_1^{(1)}, \ldots, Y_{r_1}^{(1)}, \ldots, Y_1^{(n)}, \ldots, Y_{r_n}^{(n)})$ and composing with $E_1 \circ F_L$ we can erase the term $\sum_{k=1}^{s_2} \alpha_{2k} L_{2k}^3$ in the second component.

Proceeding this way we obtain a map of the form

$$F' = (X_1 - \sum_{k=1}^{s_1} \alpha_{1k} Y_k^{(1)}, \ldots, X_n - \sum_{k=1}^{s_n} \alpha_{nk} Y_k^{(n)}, Y_1^{(1)} + L_{11}^3, \ldots, Y_{s_1}^{(1)} + L_{1s_1}^3, \ldots, Y_1^{(n)} + L_{n1}^3, \ldots, Y_{s_n}^{(n)} + L_{ns_n}^3).$$

and if F' is invertible then so is F. By composition with elementary maps we see that F' is invertible if and only if the map

$$S = (X_1, \ldots, X_n, Y_1^{(1)} + \widetilde{L}_{11}^3, \ldots, Y_{s_1}^{(1)} + \widetilde{L}_{1s_1}^3, \ldots, Y_1^{(n)} + \widetilde{L}_{n1}^3, \ldots, Y_{s_n}^{(n)} + \widetilde{L}_{ns_n}^3).$$

for $\widetilde{L}_{ij} \in \mathbb{Q}X_1 + \cdots + \mathbb{Q}X_n$. This finishes the proof. □

2.3 The symmetric case

In this section we will study polynomial maps over $\mathbb{C}$. If $X_1, \ldots, X_n$ are variables we denote the ring $\mathbb{C}[X_1, \ldots, X_n]$ by $\mathbb{C}[X]$.

Let $f \in \mathbb{C}[X]$ and consider the hessian matrix

$$\mathcal{H}(f) = \begin{pmatrix} f_{X_1X_1} & f_{X_1X_2} & \vdots & \vdots & \vdots & f_{X_1X_n} \\ f_{X_2X_1} & f_{X_2X_2} & \vdots & \vdots & \vdots & f_{X_2X_n} \\ f_{X_3X_1} & f_{X_3X_2} & \vdots & \vdots & \vdots & f_{X_3X_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{X_nX_1} & f_{X_nX_2} & \vdots & \vdots & \vdots & f_{X_nX_n} \end{pmatrix}$$

where $f_{X_iX_j} := \frac{\partial^2 f}{\partial X_i \partial X_j}$.

Given a polynomial map $H = (H_1, \ldots, H_n) : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ introduce new variables $Y_1, \ldots, Y_n$ and define

$$f_H := (-i)H_1(X_1 + iY_1, \ldots, X_n + iY_n)Y_1 + \cdots + (-i)H_n(X_1 + iY_1, \ldots, X_n + iY_i)Y_n \in \mathbb{C}[X, Y].$$

Considering the map $S = (X_1 - iY_1, \dots, X_n - iY_n, Y_1, \dots, Y_n)$ we have

$$g_H := f_H \circ S = (-i) \sum_{k=1}^{n} H_k(X) Y_k.$$

Furthemore,

$$\mathcal{H}(g_H) = \begin{pmatrix} (**) & -i(JH)^t \\ -iJH & 0 \end{pmatrix}.$$

Lemma 2.2. *Let $A \in \mathcal{M}_n(\mathbb{C})$ and $f \in \mathbb{C}[X]$. Define $f \circ A := f(AX)$. Then*

$$\mathcal{H}(f \circ A) = A^t \mathcal{H}(f)|_{AX} A.$$

Proof. Chain rule. □

Lemma 2.3. *Let $H = (H_1, \dots, H_n) \in \mathcal{MP}_n(\mathbb{C})$ and suppose that JH is symmetric. Then there exists $f \in \mathbb{C}[X]$ such that $H_i = f_{X_i}$ for all $i = 1, \dots, n$.*

Proof. Let $H_i = \sum_\alpha a_\alpha^{(i)} X^\alpha$. By hypothesis we know $\frac{\partial H_i}{\partial X_j} = \frac{\partial H_j}{\partial X_i}$. Comparing the coefficients we obtain $\alpha_j a^{(i)}_{\alpha_1 \cdots (\alpha_i - 1) \cdots \alpha_n} = \alpha_i a^{(j)}_{\alpha_1 \cdots (\alpha_j - 1) \cdots \alpha_n}$. Take $f = \sum_\alpha b_\alpha X^\alpha$ where $b_\alpha = a_{\alpha_1 \cdots (\alpha_i - 1) \cdots \alpha_n} / \alpha_i$ for $\alpha_i > 0$ and $b_\alpha = 0$ if $\alpha = (0, \dots, 0)$. □

Proposition 2.5. *Let $H = (H_1, \dots, H_n) \in \mathcal{MP}_n(\mathbb{C})$ be a polynomial map and f_H the associated polynomial. Then*

$$\mathcal{H}(f_H) \text{ is nilpotent } \iff JH \text{ is nilpotent }.$$

Proof. By simplicity denote f_H by f and $f_H \circ S$ by g. We know that $\mathcal{H}(f)$ is nilpotent if and only if

$$\det(T id_{2n} - \mathcal{H}(f)) = T^{2n}.$$

Let $Q := \frac{1}{2} \sum_k (X_k^2 + Y_k^2)$. Note that $Q \circ S = \frac{1}{2} \sum_k ((X_k - iY_k)^2 + Y_k^2) = \frac{1}{2} \sum_k X_k^2 - i \sum_k X_k Y_k$ and so

$$\mathcal{H}(Q \circ S) = \begin{pmatrix} id_n & -i(id_n) \\ -i(id_n) & 0 \end{pmatrix}$$

Also, we have

$$\mathcal{H}(g) = \begin{pmatrix} (**) & -i(JH)^t \\ -iJH & 0 \end{pmatrix}$$

So, $\det(\mathcal{H}(TQ\circ S-g))=\det(S^t\mathcal{H}(TQ-f)|_{S(X,Y)}S)=\det(\mathcal{H}(TQ-f)|_{S(X,Y)})=\det(Tid_{2n}-\mathcal{H}(f))|_{S(X,Y)}$.

On the other hand, since

$$\mathcal{H}(TQ\circ S-g)=\begin{pmatrix}(**) & i[Tid_n-(JH)^t]\\ i[Tid_n-JH] & 0\end{pmatrix}$$

we have $\det(\mathcal{H}(TQ\circ S-g))=\det(Tid_n-JH)\det(Tid_n-JH^t)=\det(Tid_n-JH)^2$.

So JH is nilpotent if and only if $\det(Tid_n-JH)=T^n\iff\det(Tid_{2n}-\mathcal{H}(f))=T^{2n}\iff\mathcal{H}(f)$ is nilpotent. □

Now consider the following

Hessian Conjecture. *If $F=(X_1,\dots,X_n)+(f_{X_1},\dots,f_{X_n})$ for some $f\in\mathbb{C}[X]$ with $\mathcal{H}(f)$ nilpotent then F is invertible.*

Note that if the Jacobian Conjecture is true for dimension n then so is the Hessian Conjecture since nilpotency of $\mathcal{H}(f)$ implies Keller condition $\det(F)=1$. The surprising fact is that the converse holds in the following sense:

Theorem 2.3. *Suppose that $HP_{2n}(\mathbb{C})$ is true. Then all regular polynomial map $F=X+H$ with JH nilpotent in dimension n is invertible, i.e.,*

$$HP_{2n}(\mathbb{C})\Longrightarrow JP_n(\mathbb{C}).$$

Proof. Let $F=X+H$ be a regular map in dimension n. By the proposition above we have that JH is nilpotent if and only if $\mathcal{H}(f)$ is nilpotent where

$$f=(-i)H_1(X_1+iY_1,\dots,X_n+iY_n)Y_1+\cdots+(-i)H_n(X_1+iY_1,\dots,X_n+iY_n)Y_n.$$

So since we assume that $HP_{2n}(\mathbb{C})$ is true we conclude that the map

$$F=(X_1+f_{X_1},\dots,X_n+f_{X_n},Y_1+f_{Y_1},\dots,Y_n+f_{Y_n})$$

is invertible. In particular, $F\circ G$ is invertible where $G=(X_1-iY_1,\dots,X_n-iY_n,Y_1,\dots,Y_n)$. Now, we note that $F\circ G=F(X_1-iY_1,\dots,X_n-iY_n,Y_1,\dots,Y_n)=(G_1,\dots,G_n,G_{n+1},\dots,G_{2n})$ where

$$G_p=X_p-iY_p+(-i)\sum_k\frac{\partial H_k(X_1,\dots,X_n)}{\partial X_p}Y_k\qquad 1\le p\le n.$$

$$G_{n+l}=Y_l+\sum_k\frac{\partial H_k(X_1,\dots,X_n)}{\partial X_l}Y_k-iH_l(X_1,\dots,X_n)\qquad 1\le l\le n.$$

By composition with G^{-1} we have that

$$G^{-1}\circ F\circ G = (E_1,\dots,E_{2n}) = (G_1+iG_{n+1},\dots,G_n+iG_{2n},G_{n+1},\dots,G_{2n}) = (X_1+H_1,\dots,X_n+H_n,(**),\dots,(**))$$

is an invertible map. In particular, $F = (X_1 + H_1,\dots,X_n + H_n)$ is an invertible polynomial map. □

Using the theorem above and the reduction theorem we obtain

Symmetric Reduction Theorem. ***(Bondt-Essen)*** *It is sufficient to prove the Jacobian Conjecture for all polynomial maps $F : k^n \longrightarrow k^n$ of the form " gradient", i.e., $F = X + (f_{x_1},\dots,f_{x_n})$ where f is homogeneous of degree 4 and the hessian matrix $\mathcal{H}(f)$ is nilpotent (equivalently, it is sufficient to consider the case where F is symmetric regular i.e. in the form $F = X + H$ with H homogeneous of degree 3, $J(H)$ nilpotent and* ***symmetric*** *matrix).*

Remark 4. *Let k be a field. Recall that k is an ordered field if there is a partition $k = P^- \cup \{0\} \cup P^+$ such that $x, y \in P^+ \Longrightarrow x + y, xy \in P^+$. Note that $1 \in P^- \Longrightarrow (-1) \in P^+ \Longrightarrow (-1)^2 = 1 \in P^+$ a contradiction. So, $1 \in P^+ \Longrightarrow 1 + 1 \cdots + 1 \in P^+ \Longrightarrow char(k) = 0$.*

In relation to the theorem above, the following result is interesting:

- *Let k be an ordered field. If $M \in \mathcal{M}_n(k[X_1,\dots,X_n])$ is a nilpotent symmetric matrix then $M = 0$.*

Indeed, let $M \in \mathcal{M}_n(k)$ be nilpotent and symmetric. Suppose that $M \neq 0$. Then, there is $l \in \mathbb{N}$ such that $M^l = 0$ and $N := M^{l-1} \neq 0$. Since $N \neq 0$ we have that some row is non zero, say $(u_{11},\dots,u_{1n})$. Since $N^2 = 0$ and N is symmetric we have $u_{11}^2 + \cdots + u_{1n}^2 = 0$. But this is a contradiction, since k is ordered. Now let $M \in \mathcal{M}_n(k[X_1,\dots,X_n])$ be nilpotent and symmetric. By evaluation on $(a_1,\dots,a_n) \in k^n$ we have $M(a_1,\dots,a_n) = 0$. If M_{ij} denote the (i,j)-element in M then M_{ij} is a polynomial that is zero in k^n. Since k is infinite field $(char(k) = 0)$ we have $M_{ij} \equiv 0$ for all $1 \leq i, j \leq n$. So, $M = 0$.

Chapter 3

Jacobian Conjecture via $\mathbb{Z}_p$

In this chapter we describe an approach to the Jacobian Conjecture via p-adic integers and we formulate the Unimodular Conjecture of [12, Essen-Lipton]. We propose a new conjecture, the Invariance Conjecture, and we show the equivalences

$$\text{Jacobian Conjecture over } \mathbb{C} \text{ is true } \iff \text{Unimodular Conjecture over } \mathbb{Z}_p \text{ is true for almost all primes } p$$

$$\text{Jacobian Conjecture over } \mathbb{C} \text{ is true} \iff \text{ Invariance Conjecture over } \mathbb{Z}_p \text{ is true for almost all primes } p \ .$$

In the end of this chapter we make some contributions to the Unimodular Conjecture.

3.1 Completion

Let R be a ring and $I \subset R$ an ideal with $\cap_{n\in\mathbb{N}} I^n = 0$ [1]. We can define a topology in R declaring that $V \subset R$ is a neighborhood of $a \in R$ iff $a + I^n \subset V$ for some $n \in \mathbb{N}$. Provided with this structure, we obtain a topological ring (sum/product are continuous). This topology is called the I-adic topology.

Given a sequence $s = \{a_n\} \subset R$ we say that s is a Cauchy sequence if for any $n \in \mathbb{N}$ there is m_0 such that if $m, r > m_0$ then $a_m - a_r \in I^n$. We remark that a convergent sequence is Cauchy, but there are Cauchy sequences which are not convergent.

[1] In this chapter, we are interested only in the case where the I-adic topology is Hausdorff. This is equivalent to the condition $\cap_{n\in\mathbb{N}} I^n = 0$.

Example 5. *Let $R = \mathbb{Z}$ with I-adic topology where $I = 5\mathbb{Z}$. We will construct a sequence $\{a_n\}$ such that*

$$a_n^2 + 1 \equiv 0 \mod 5^n \qquad a_{n+1} \equiv a_n \mod 5^n.$$

For this, take $a_1 = 2$ and suppose that we have a_m defined for all $m \leq n$. Define $a_{n+1} := a_n + b5^n$, with b to be determined. We show that there is a $b \in \mathbb{Z}$ such that $a_{n+1}^2 + 1 = (a_n + 5^n b)^2 + 1 \equiv 0 \mod 5^{n+1}$ i.e. $d + 2ba_n \equiv 0 \mod 5$, with $d = (a_n^2+1)/5^n \in \mathbb{Z}$. Now, since $(a_n, 5) = 1$ we can solve the congruence above and obtain the integer wanted.

By construction, we have $\{a_n\}$ Cauchy. But it isn't convergent. Indeed, if $\{a_n\}$ converge to α then, taking the limit in the relation $a_n^2 + 1 = 0 \mod 5^n$, by continuity we have $\alpha^2 + 1 = 0$ in $\mathbb{Z}$, a contradiction.

Definition 3.1. *Let I be an ideal of R and consider the projective system $\{\Phi_m^n, R/I^n\}$ where, for $m \geq n$, $\Phi_m^n : R/I^m \twoheadrightarrow R/I^n$ are the natural projections. The completion of R with respect to I-adic topology is by definition $\widetilde{R} := \varprojlim_{n\in\mathbb{N}} R/I^n$.*

Theorem 3.1. *Let $I \subset R$ with R commutative ring and I an ideal with $\cap_{n\in\mathbb{N}} I^n = 0$. Consider the I-adic topology in R. Then, $\widetilde{R}$ is a topological Hausdorff complete ring with topology given by ideal $\widetilde{I} = I\widetilde{R}$.*

Proof. see [1, chapter 10]. □

Definition 3.2. *Let $p \in \mathbb{Z}$ be a prime and consider the p-adic topology in $\mathbb{Z}$. The p-adic ring is the completion of $\mathbb{Z}$ with respect to p-adic topology, denoted $\mathbb{Z}_p$.*

Theorem 3.2. *$\mathbb{Z}_p$ is a discrete valuation ring with uniformizer p and residue field $\mathbb{F}_p$.*

Proof. The associeted valuation is defined in the following way: If $0 \neq a = (a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ define $ord_p(a) := \mathbf{Min}\{n \in \mathbb{N} \mid a_n \neq 0\}$. If $a = 0$, by convention we define $ord_p(a) = \infty$. We can check that ord_p define a discrete valuation in $\mathbb{Z}_p$. For the second affirmation, note that the following sequence

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\phi} \mathbb{Z}_p \xrightarrow{\pi} \mathbb{F}_p \longrightarrow 0$$

is exact where the map ϕ is the multiplication by p and π is the natural projection. □

Hensel Lemma. *Let $(\mathcal{O}, \mathcal{M}, k)$ be a complete discrete valuation ring and $F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n) \in \mathcal{O}[X_1, \ldots, X_n]$. Choose $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{O}^n$ such that*

$$F_1(\alpha_1, \ldots, \alpha_n) \equiv \cdots \equiv F_n(\alpha_1, \ldots, \alpha_n) \equiv 0 \mod \mathcal{M}^{2m+1}$$

where $m := ord_{\mathcal{M}}(\det JF(\alpha)) < \infty$. *Then there is unique* $\beta = (\beta_1, \ldots, \beta_n) \in \mathcal{O}^n$ *such that* $F_1(\beta) = \cdots = F_n(\beta) = 0$ *and* $\beta_i \equiv \alpha_i \mod \mathcal{M}^{m+1}$ *for all* $i = 1, \ldots, n$.

Proof. See [5]. □

By Hensel lemma we get the following

Proposition 3.1. *Let* $f_1, \ldots, f_n \in \mathcal{O}[X_1, \ldots, X_n]$ *satisfying the Keller condition where* $(\mathcal{O}, \mathcal{M}, k)$ *is a complete DVR. If* R *is an* $\mathcal{O}$*-algebra denote by* $X(R)$ *the set of* R*-points. Then there is a bijection* $X(\mathcal{O}) \cong X(k)$.

Proof. As f is Keller we have $m = ord_{\mathcal{M}}(\det JF(\alpha)) = 0$ for all $\alpha \in \mathcal{O}^n$. The bijection is natural: given $P \in \mathcal{O}^n$ define $\varphi(P) \in X(k)$ the k-point obtained by reduction $\mod \mathcal{M}$. Hensel lemma implies that $\varphi : X(R) \longrightarrow X(k)$ is a bijection: injectivity by uniqueness and surjectivity by lifting. □

Proposition 3.2. *Let* R *be a noetherian domain and* $I \subset R$ *an ideal. Then,* $\cap_{n\in\mathbb{N}} I^n = 0$.

Proof. see [1]. □

Lemma 3.1. *Let* $Q(T) = a_n T^n + \cdots + a_0 \in \mathbb{Z}[T]$ *be an irreducible polynomial and* $E \subset \mathbb{Z}$ *a finite set of rational primes. Then there is a prime* $p \in \mathbb{Z} \setminus E$ *and* $\alpha \in \mathbb{Z}_p$ *such that* $Q(\alpha) = 0$.

Proof. By Hensel lemma, it is sufficient to show that there exists a prime $p \notin E$ and $b \in \mathbb{Z}$ such that

$$Q(b) \equiv 0 \mod p\mathbb{Z}_p \qquad \text{and} \qquad Q'(b) \not\equiv 0 \mod p\mathbb{Z}_p.$$

For this, denote d the discriminant of $Q(T)$. We remark that $d \in \mathbb{Z} \setminus \{0\}$ since $d := \mathbf{resultant}(Q, Q') \in \mathbb{Z}$ and the separability of Q implies $d \neq 0$. Define $e := 2d \prod_{p\in E} p$ and for $l \in \mathbb{N}$ denote $m_l := a_0 e^l$. We have,

$$Q(m_l) = a_0(a_n a_0^{n-1} e^{ln} + \cdots + a_1 e^l + 1) = a_0 \widetilde{Q}(m_l) \qquad (*).$$

Now, since $\widetilde{Q}(t) \in \{1, 0, -1\}$ occurs for a finite number of $t \in \mathbb{Z}$, we can take $l \in \mathbb{N}$ such that $\widetilde{Q}(m_l) \neq 1, 0, -1$. Let $p \in \mathbb{Z}$ be a prime such that $p \mid \widetilde{Q}(m_l)$. In particular, we have $Q(m_l) \equiv 0 \mod p\mathbb{Z}_p$. Note that $p \nmid e$. Indeed, if $p \mid e$ we have, by $(*)$, $p \mid 1$ a contradiction. In particular, $p \nmid d \Longrightarrow Q'(m_l) \not\equiv 0 \mod p\mathbb{Z}_p$. So, we get the result. □

Proposition 3.3. *Let* $E \subset \mathbb{Z}$ *be a finite set of rational primes and* $\alpha \in \overline{\mathbb{Q}}$. *Then there is a prime* $p \in \mathbb{Z} \setminus E$ *and an injective homomorphism* $\phi : \mathbb{Z}[\alpha] \hookrightarrow \mathbb{Z}_p$.

Proof. Let $m_\alpha(T) \in \mathbb{Q}[T]$ be the minimal polynomial of α. We have $m_\alpha(T) = c(m_\alpha(T))f(T)$ for some primitive polynomial $f(T) \in \mathbb{Z}[T]$[2]. We affirm that

$$\mathbb{Q}[T]f(T) \cap \mathbb{Z}[T] = f(T)\mathbb{Z}[T].$$

The inclusion $\supset$ is trivial. Let $h(T) \in \mathbb{Q}[T]f(T) \cap \mathbb{Z}[T]$ and write $h(T) = \frac{1}{a}A(T)f(T)$ with $A(T)$ primitive. By Gauss lemma we know that the product of primitive polynomials is primitive. So, $c(h(T)) = 1/a \in \mathbb{Z}$ and $a \in \{1, -1\} \Longrightarrow h(T) \in \mathbb{Z}[T]f(T)$.

So

$$\mathbb{Z}[\alpha] \cong \frac{\mathbb{Z}[T]}{f(T)\mathbb{Z}[T]} \hookrightarrow \frac{\mathbb{Q}[T]}{f(T)\mathbb{Q}[T]}.$$

Let $p \notin E$ be a prime such that $f(a) = 0$ for some $a \in \mathbb{Z}_p$ and consider the map $\Phi : \mathbb{Q}[T] \longrightarrow \mathbb{Q}_p$, evaluation by a where $\mathbb{Q}_p := Frac(\mathbb{Z}_p)$

Since $f(T)$ is irreducible we have $ker(\Phi) = f(T)\mathbb{Q}[T]$ and so

$$\frac{\mathbb{Q}[T]}{f(T)\mathbb{Q}[T]} \hookrightarrow \mathbb{Q}_p.$$

By composition of isomorphims we get $\mathbb{Z}[\alpha] \hookrightarrow \mathbb{Z}_p$.

□

Immersion Lemma. *Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Then for infinitely many primes $p \in \mathbb{Z}$ there is an injective homomorphism*

$$\varphi_p : \mathbb{Z}[\alpha_1, \ldots, \alpha_n] \hookrightarrow \mathbb{Z}_p.$$

Proof. Consider $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, the field obtained by adjunction. By the primite element theorem, we have $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$. In particular, we can find $d \in \mathbb{Z}$ such that $d\alpha_i \in \mathbb{Z}[\alpha]$ for all $i \in \{1, \ldots, n\}$. Consider the multiplicative system $S = \{d^n \mid n \in \mathbb{N}\}$. We have

$$\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \hookrightarrow S^{-1}\mathbb{Z}[\alpha].$$

Denote $E := \{q \mid q \text{ prime with } q|d\}$. By the lemma above, we know that there is a prime number $p \notin E$ and an injective homomorphism $\varphi_p : \mathbb{Z}[\alpha] \hookrightarrow \mathbb{Z}_p$. Since all elements of S are invertible in $\mathbb{Z}_p$, the map φ_p induces an injection $S^{-1}\mathbb{Z}[\alpha] \hookrightarrow \mathbb{Z}_p$. By composition, we get $\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \hookrightarrow \mathbb{Z}_p$. Replacing E by $E' = E \cup \{p\}$ and by

[2]Recall the content of polynomials: Given $f(T) = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathbb{Q}[T]$ by definition $c(f(T)) := \prod_p p^{ord_p(f)}$, where the product take all primes in $\mathbb{Z}$ and $ord_p(f) := \mathbf{Min}\{ord_p(a_i) \mid 0 \leq i \leq n\}$. If $f, g \in \mathbb{Q}[T]$, Gauss lemma implies $C(fg) = C(f)C(g)$

repetion of the argument above we get a prime $q \notin E'$ and an injection $\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \hookrightarrow \mathbb{Z}_q$. So, $\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \hookrightarrow \mathbb{Z}_p$ for infinite primes. □

3.2 A reformulation of the Jacobian Conjecture

We start with some lemmas.

Lemma 3.2. *Let R be a domain and $F \in R[X_1, \ldots, X_n]^n$ with $F(0) = 0$. Let $P = (p_1, \ldots, p_n), Q = (q_1, \ldots, q_n) \in R^n$ be distinct points.*

(i) If $F(P) = F(Q)$ and $\det JF(0) \in R^*$ then the ideal $\langle p_1, \ldots, p_n, q_1, \ldots, q_n \rangle = R$.

(ii) If $F(P) = F(Q)$ and $\det JF \in R^*$ then the ideal $\langle p_1 - q_1, \ldots, p_n - q_n \rangle = R$.

Proof. Note that we can suppose R is a noetherian ring. Indeed, by adjunction of all elements that occurs in F, $\det JF$ and the coordinates of P and Q to the prime subring of R we obtain a subring $A \subset R$ of finite type over a noetherian ring. So achieve a noetherian ring.

Suppose that $F(P) = F(Q)$ and $\det JF(0) \in R^*$ but $\langle p_1, \ldots, p_n, q_1, \ldots, q_n \rangle \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \in Spec_m(R)$. Denote $\widetilde{R}$ the $\mathfrak{m}$-adic completion of R. By injectivity of the natural map $R \longrightarrow \widetilde{R}$ we can suppose $P, Q \in \widetilde{R}$. Let G be the formal inverse of F over $\widetilde{R}$. It is easy to see that $G(F(P))$ and $G(F(Q))$ are well defined elements in $\widetilde{R}$. In particular, $P = G(F(P)) = G(F(Q)) = Q$ a contradiction.

Given F with $F(P) = F(Q)$ and $\det JF \in R^*$ consider $F_Q := F(X + Q) - F(Q)$ and note that that $F_Q(P - Q) = F(P) - F(Q) = 0$ and $F_Q(0) = 0$. Also, we have $\det JF_Q = \det JF(X + Q) \in R^* \Longrightarrow \det JF_Q(0) \in R^*$. So by (i) we obtain $\langle p_1 - q_1, \ldots, p_n - q_n \rangle = R$.

□

Proposition 3.4. *(Connell - van den Dries) Let R be a domain and $F \in \mathcal{MP}_n(R) = R[X_1, \ldots, X_n]^n$ with $F(0) = 0$ and $\det JF \in R^*$. Let $I \subsetneq R$ be an ideal and consider the induced map $\overline{F} : (R/I)^n \longrightarrow (R/I)^n$. If $\overline{F}$ is injective then so is F.*

Proof. Suppose this false and let $P = (p_1, \ldots, p_n), Q = (q_1, \ldots, q_n) \in R^n$ be distinct points such that $F(P) = F(Q)$. By Keller condition and the lemma above we have

$$1 = \alpha_1(p_1 - q_1) + \cdots + \alpha_n(p_n - q_n) \text{ for some } \alpha_1, \ldots, \alpha_n \in R.$$

By reduction $\mod I$ we have $\overline{1} = \overline{\alpha_1}\overline{(p_1 - q_1)} + \cdots + \overline{\alpha_n}\overline{(p_n - q_n)}$. On the other hand, the injectivity of $\overline{F}$ implies that $p_i - q_i \in I$ for all i. This implies $1 \in I$ a contradiction. □

Lemma 3.3. *Let $F \in \mathcal{MP}_n(\mathbb{Z})$ be such that the induced map $F \in \mathcal{MP}_n(\mathbb{Z}_p)$ is injective for almost all primes $p \in \mathbb{Z}$. Then $d := \det JF \in \mathbb{Z} \setminus \{0\}$ and F is invertible over $\mathbb{Z}[d^{-1}]$.*

Proof. Consider F as a map over $\overline{\mathbb{Q}}$ (by scalar extension). We claim that $F \in \mathcal{MP}_n(\overline{\mathbb{Q}})$ is injective. Suppose this false and let $P = (p_1, \ldots, p_n), Q = (q_1, \ldots, q_n) \in \overline{\mathbb{Q}}$ be distinct points such that $F(P) = F(Q)$. By the immersion lemma 3.3, we know that there is an injective homomorphism $\varphi_p : \mathbb{Z}[P, Q] \hookrightarrow \mathbb{Z}_p$ for infinitely many primes $p \in \mathbb{Z}$. So $F(\varphi_p(P)) = \varphi_p(F(P)) = \varphi_p(F(Q)) = F(\varphi_p(Q))$. Since F is injective over $\mathbb{Z}_p$ (for almost all primes) we have $\varphi_p(P) = \varphi_p(Q) \Longrightarrow P = Q$, a contradiction. So $F \in \mathcal{MP}_n(\overline{\mathbb{Q}})$ is injective. By Cynk-Rusek theorem 1.6 we know that F is, of course, an isomorphim. In particular, $\det JF \in \overline{\mathbb{Q}}^* \cap \mathbb{Z}[X_1, \ldots, X_n] = \mathbb{Z} \setminus \{0\}$. By the inverse formal theorem 1.1 we know that F has a formal inverse over $\mathbb{Z}[d^{-1}]$. Since F is invertible over $\overline{\mathbb{Q}}$ it follows that the inverse over $\mathbb{Z}[d^{-1}]$ is polynomial. □

Theorem 3.3. *The Jacobian Conjecture is equivalent to the following statement:*

- *For almost all primes $p \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 2}$, for any map $F \in \mathcal{MP}_n(\mathbb{Z})$ with $\det JF = 1$ the induced map $\overline{F} \in \mathcal{MP}_n(\mathbb{F}_p)$ is injective.*

Proof. Suppose that the Jacobian Conjecture is true and take $F \in \mathcal{MP}_n(\mathbb{Z})$ a polynomial map with the condition $\det JF = 1$. By the inverse formal theorem we know that F is an invertible map over $\mathbb{Z}$ if and only if is invertible over $\mathbb{C}$. By hypothesis we have the Jacobian Conjecture true and so F is an invertible map. Denote G the inverse. By reduction $\mod p$ the relations $F \circ G = X$ and $G \circ F = Y$ imply that the induced map $\overline{F} \in \mathcal{MP}_n(\mathbb{F}_p)$ is a bijection.

Now suppose that for almost all primes $p \in \mathbb{Z}$, and all $n \in \mathbb{Z}_{\geq 2}$ any map $F \in \mathcal{MP}_n(\mathbb{Z})$ with $\det JF = 1$ is injective. Let $F \in \mathcal{MP}_n(\mathbb{C})$ be a Keller map that isn't injective, i.e., a counterexemple for the Jacobian Conjecture. We can assume $F \in \mathcal{MP}_n(\mathbb{Z})$ with $\det JF = 1$ (by Connell-van den Dries theorem, see chapter 1, 3.4). By a translation we can assume $F(0) = 0$. The map F is injective over $\mathbb{Z}_p$. By the lemma above this implies that F is invertible over $\mathbb{Z}[d^{-1}]$ where $d = 1$. So F is invertible over $\mathbb{Z}$. Contradiction.

□

3.3 The Unimodular Conjecture

Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain and consider a linear map $F : \mathcal{O}^n \longrightarrow \mathcal{O}^n$ i.e. $F = (F_1, \ldots, F_n)$ with $F_i \in \mathcal{O}[X_1, \ldots, X_n]$ homogeneous of degree 1. Suppose that the matrix $B := JF$ is invertible and let $A \in Mat_n(\mathcal{O})$ be such that $AB = BA = id_n$. The relation $BA = id_n$ implies that there exist $u_1, \ldots, u_n \in \mathcal{O}$ such that $F_1(u_1, \ldots, u_n) = 1$. In particular, by reduction $\mod \mathcal{M}$ we have $\overline{F} : k^n \longrightarrow k^n$ a non-zero map. The general case is an open problem, the so called

Unimodular Conjecture. *Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain with $char(\mathcal{O}) = 0$ and $F \in \mathcal{MP}_n(\mathcal{O})$ $(n > 1)$ a Keller map. Then the induced map $\overline{F} \in \mathcal{MP}_n(k)$ is a non-zero map.*

Given $F \in \mathcal{MP}_n(\mathcal{O})$ over a local domain $(\mathcal{O}, \mathcal{M}, k)$ we will denote by $f \in \mathcal{MP}_n(k)$ the induced map over the residue field k.

Definition 3.3. *Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain. We say that $\mathcal{O}$ is a **unimodular domain** if the Unimodular Conjecture is true for $\mathcal{O}$. We say that a polynomial map $F \in \mathcal{MP}_n(\mathcal{O})$ is **unimodular** if it satisfies the condition on Unimodular Conjecture.*

Proposition 3.5. *(WM)*[3] *Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain with k an infinite field. Then $\mathcal{O}$ is unimodular.*

Proof. Let $F \in \mathcal{MP}_n(\mathcal{O})$ be a Keller map. Let $f \in \mathcal{MP}_n(k)$ be the induced map over the residue field and suppose that $f(\alpha) = 0$ for all $\alpha \in k^n$. Since k is infinite we have $f \equiv 0$. So the coefficients that occur in F belong to the maximal ideal $\mathcal{M}$. In particular, $\det JF \in \mathcal{M}[X_1, .., X_n]$ a contradiction by Keller condition: $\det JF = 1$.

□

Theorem 3.4. *Suppose that the Jacobian Conjecture over $\mathbb{C}$ is true. Then every local domain $(\mathcal{O}, \mathcal{M}, k)$ with $char(\mathcal{O}) = 0$ is unimodular.*

Proof. Let $F \in \mathcal{MP}_n(\mathcal{O})$ be a Keller map over a local domain $\mathcal{O}$ with $char(\mathcal{O}) = 0$. Since we assume that Jacobian Conjecture is true over $\mathbb{C}$ we have F an invertible map over $\mathcal{O}$ (see corollary 1.2). So, there is a unique $G \in \mathcal{MP}_n(\mathcal{O})$ such that $F \circ G = X$. By reduction $\mod \mathcal{M}$ we see that the map $f \in \mathcal{MP}_n(k)$ is a bijection, in particular, non-zero map. □

We remark that the Unimodular Conjecture is false for local domains with $char(\mathcal{O}) = p > 0$ and residue field finite. For example: consider the local domain $(\mathbb{F}_p[[T]], T\mathbb{F}_p[[T]], \mathbb{F}_p)$ and take the polynomial map $F = (X_1 - X_1^p, \ldots, X_n - X_n^p) \in \mathcal{MP}_n(\mathbb{F}_p[[T]])$. Note that F is a Keller map but the induced map over the residue field is the zero map, since $\alpha^p = \alpha$ for all $\alpha \in \mathbb{F}_p$.

[3] This is more general than [12, Theorem 4]

Remark 5. *Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain. The following table shows the complete set of relations between $char(\mathcal{O})$ and $char(k)$.*

$char(\mathcal{O})$	$char(k)$	$\#k$	*type*
$p = 0$	$q > 0$	∞	*unimodular*
$p = 0$	$q > 0$	$< \infty$	*unknown*
$p = 0$	$q = 0$	∞	*unimodular*
$p > 0$	$q = p$	$< \infty$	*non-unimodular*
$p > 0$	$q = p$	∞	*unimodular*

*Thus the interesting case is $(char(\mathcal{O}), char(k), \#k, type) = (0, p, < \infty, unknown)$ where $p > 0$. Indeed, we will see later (Essen-Lipton theorem) that **unknown** = **unimodular** if and only if the Jacobian Conjecture over $\mathbb{C}$ is true.*

3.3.1 n-dimensional 2-sets

Definition 3.4. [4] *Let R be a domain. We denote by $S_R(n, 2)$ the category where the objects are of the form (P, Q) (ordered) with $P \neq Q \in R^n$ and a morphism $F : (P_1, Q_1) \longrightarrow (P_2, Q_2)$ is restriction of a polynomial map in $\mathcal{MP}_n(R)$ with the condition $F(P_1) = P_2$ and $F(Q_1) = Q_2$. Each object (P, Q) in $S_R(n, 2)$ is called an **n-dimensional 2-set.***

In what follows, given $P = (p_1, \ldots, p_n)$ and $Q = (q_1, \ldots, q_n)$ in R^n we denote by $\langle Q - P \rangle$ the ideal

$$\langle p_1 - q_1, \ldots, p_n - q_n \rangle \subset R.$$

Theorem 3.5. *Let $X = (a, b)$ and $Y = (c, d)$ n-dimensional 2-sets. Then*

(i) $Hom(X, Y) \neq \varnothing \iff \langle d - c \rangle \subset \langle b - a \rangle$.

(ii) $X \cong Y \iff \langle d - c \rangle = \langle b - a \rangle$.

Proof. Suppose that $Hom(X, Y) \neq \varnothing$ and pick $F \in \mathcal{MP}_n(R)$ such that $F(a) = c$ and $F(b) = d$. Let $G = (X - c) \circ F$ so that $G(a) = 0$ $G(b) = d - c$. Since $G_i(a) = 0$ we have

$$G_i(X_1, \ldots, X_n) = f_{i1}(X_1, \ldots, X_n)(X_1 - a_1) + \cdots + f_{in}(X_1, \ldots, X_n)(X_n - a_n).$$

So, $d_i - c_i = G_i(b_1, \ldots, b_n) \in \langle b_1 - a_1, \ldots, b_n - a_n \rangle$ for all $i = 1, \ldots, n \Longrightarrow \langle d - c \rangle \subset \langle a - b \rangle$. Reciprocally, if $\langle d - c \rangle \subset \langle b - a \rangle$ then

$$d_j - c_j = e_{1j}(b_1 - a_1) + \cdots + e_{nj}(b_n - a_n)$$

[4] see [12, 2-transitivity]

for some $e_{ij} \in R$. Define $G_j := e_{1j}(X_1 - a_1) + \cdots + e_{nj}(X_n - a_n)$ and take $F = (X + c) \circ G$.

(ii) follows from (i) trivially. □

Theorem 3.6. *Let R be a PID. Suppose that $\langle a, b\rangle \cong \langle c, d\rangle$. Then, there exists an affine automorphism $S \in \mathcal{MP}_n(R)$ with $\det JS = 1$ such that $S(a) = c$ and $S(b) = d$.*

Proof. Since R is a PID we have $\langle b - a\rangle = \langle g\rangle$ for some $g \in R$. Write $b_i - a_i = gv_i$ for $v_i \in R$ with $i = 1, \ldots, n$ and note that $\langle v_1, \ldots, v_n\rangle = R$. In particular, it follows that $(v_1, \ldots, v_n)$ is a unimodular sequence. So there is $B = (b_{ij}) \in Gl_n(R)$ with $\det B = 1$ the first row of which is the n-tuple $v = (v_1, \ldots, v_n)$ [5]. Let $A = (a_{ij}) \in Gl_n(R)$ such that $AB = BA = id_n$ and define for $1 \leq k \leq n$

$$F_k(X_1, \ldots, X_n) = a_{1k}(X_1 - a_1) + \cdots + a_{nk}(X_n - a_n).$$

Consider the affine automorphism $F = (F_1, \ldots, F_n) \in \mathcal{MP}_n(R)$. We have $F_k(a) = 0$ and $F_k(b) = a_{1k}(b_1 - a_1) + \cdots + a_{nk}(b_n - a_n) = a_{1k}gv_1 + \cdots + a_{nk}gv_n = g(a_{1k}v_1 + \cdots + a_{nk}v_n) = g\delta_{1k}$. In particular, $F(a) = 0$ and $F(b) = (g, 0, \ldots, 0) = ge_1$. Repeating the argument, change $\langle b - a\rangle$ by $\langle d - c\rangle$ and take the affine automorphism $G \in \mathcal{MP}_n(R)$ such that $G(c) = 0$ and $G(d) = ge_1$. So, define $S := G^{-1} \circ F$. By construction, S is an affine automorphism with $S(a) = c$ and $S(b) = d$. □

Proposition 3.6. *Let R be a local unimodular domain and $F \in \mathcal{MP}_n(R)$ a Keller map. Then for all $a \in R^n$ there is $d \in R^n$ such that $F(d) - F(a)$ is unimodular.*

Proof. Consider $F_a = F(X + a) - F(a)$. Note that F_a is a Keller map and since R is unimodular there is $b \in R^n$ such that $F_a(b)$ is unimodular. Now take $d := b + a$. □

Theorem 3.7. *Let R be a local unimodular PID and $F \in \mathcal{MP}_n(R)$ Keller map non-injective. Then for each $m \in \mathbb{Z}_{\geq 2}$ there is a Keller map $G \in \mathcal{MP}_n(R)$ and $P \in R^n$ with $\#G^{-1}(P) \geq m$.*

Proof. This will be shown in the next section in more general form. □

Proposition 3.7. *Let $(\mathcal{O}, \mathcal{M}, k)$ be a complete discrete valuation ring with finite residue field. Let $F \in \mathcal{MP}_n(\mathcal{O})$ be a Keller map. Then for all $Q \in \mathcal{O}^n$ we have $\#F^{-1}(Q) \leq \#(k)^n$.*

Proof. By a translation we can suppose $Q = (0, \ldots, 0)$. So, finding the fiber $F^{-1}(Q)$ is equivalent to solve the algebraic system over $\mathcal{O}$:

$$F_1 = \cdots = F_n = 0.$$

[5] This follows from the structure of modules of finite type over a PID.

By Hensel lemma we can prove that the natural map

$$F^{-1}(Q) = \{\alpha \in \mathcal{O}^n \mid F_1(\alpha) = \cdots = F_n(\alpha) = 0\} \longrightarrow \{b \in k^n \mid \overline{F_1}(b) = \cdots = \overline{F_n}(b) = 0\}$$

is injective and so $\#F^{-1}(Q) \leq \#(k)^n$. □

We will now prove the following

Theorem (Essen-Lipton). *$\mathbb{Z}_p$ is a unimodular domain for almost all primes p if and only if the Jacobian Conjecture is true (over $\mathbb{C}$).*

Proof. The implication $\Longleftarrow$ follows from 3.4. Now suppose that $\mathbb{Z}_p$ is a unimodular domain for almost all primes p. By a result of Connell-van den Dries (see chapter 1, 1.7) it is sufficient to show that the Jacobian Conjecture is true over $\mathbb{Z}$. So let $F \in \mathcal{MP}_n(\mathbb{Z})$ be a polynomial map with $\det JF = 1$. Since $\mathbb{Z} \hookrightarrow \overline{\mathbb{Q}}$ is sufficient to prove that the map over the extension $F \otimes \overline{\mathbb{Q}} \in \mathcal{MP}_n(\overline{\mathbb{Q}})$ is injective. Indeed, if this occurs then F is an isomorphim (Cynk-Rusek) over $\overline{\mathbb{Q}}$ and so F^{-1} is a polynomial map over $\mathbb{Z}$, via the formal inverse function theorem.

Suppose by contradiction that F isn't injective. Then there are distinct $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \overline{\mathbb{Q}}^n$ such that $F(a) = F(b)$. By the immersion lemma we know that there exist an injective homomorphism $\varphi_p : \mathbb{Z}[a_1, \ldots, a_n, b_1, \ldots, b_n] \hookrightarrow \mathbb{Z}_p$ for infinitely many primes p. So the map $F \otimes \mathbb{Z}_p$ isn't injective for infinitely many primes p. Fix such a prime p for which $\mathbb{Z}_p$ is a unimodular domain. By theorem 3.7, we can find $G \in \mathcal{MP}_n(\mathbb{Z}_p)$ Keller map and $Q \in \mathbb{Z}_p^n$ such that $\#G^{-1}(Q) \geq p^{2n} > p^n$, a contradiction by proposition 3.7. So F is injective.

□

3.4 The Invariance Conjecture

Invariance Conjecture. *Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain with $char(\mathcal{O}) = 0$ and $F \in \mathcal{MP}_n(\mathcal{O})$ a Keller unimodular map. Let $G \in Aut_n(\mathcal{O})$ be an affine Keller automorphism i.e. $G = AX + b$ where $A \in Sl_n(\mathcal{O})$. Then $F \circ G \circ F$ and $F - F(a)$ are unimodular maps for all $a \in \mathcal{O}^n$.*

Remark 6. *Note that in the above conjecture we ask the unimodular property to be invariant under translation and composition of a special type. Note also that, as in the unimodular case, if the residue field k is infinite then the Invariance Conjecture is true for any complete discrete valuation ring $(\mathcal{O}, \mathcal{M}, k)$ with $char(\mathcal{O}) = p \geq 0$.*

Definition 3.5. *Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain. Given a map $F \in \mathcal{MP}_n(\mathcal{O})$ we say that*

- *F is an **invariant map** if F is Keller, unimodular and satisfies the Invariance Conjecture condition.*

- F *is* ***strongly invariant*** *if it is invariant and for all Keller affine automorphisms* $G_1, \ldots, G_k \in Aut_n(\mathcal{O})$ *the map* $F_1 \circ F_2 \circ F_3 \circ \cdots \circ F_k$ *is invariant where* $F_j = G_j \circ F$.

The domain $\mathcal{O}$ *is called an* ***invariant domain*** *if every polynomial map that is Keller and unimodular (in dimension* $n > 1$*) is invariant.*

Lemma 3.4. *If a map* $F \in \mathcal{MP}_n(\mathcal{O})$ *is strongly invariant then* $F \circ G \circ F$ *is strongly invariant for all Keller affine automorphism* $G \in Aut_n(\mathcal{O})$.

Proof. Indeed, by induction it is sufficient to consider the case $k = 2$. For this, let $G_1, G_2 \in Aut_n(\mathcal{O})$ be a Keller affine automorphisms and remark that $G_1 \circ (F \circ G \circ F) \circ G_2 \circ (F \circ G \circ F) = (G_1 \circ F) \circ (G \circ F) \circ (G_2 \circ F) \circ (G \circ F)$. So it is invariant by hypothesis on F. □

Proposition 3.8. *Let* $(\mathcal{O}, \mathcal{M}, k)$ *be a local unimodular domain. Then* $\mathcal{O}$ *is invariant.*

Proof. By hypothesis a Keller map $F \in \mathcal{MP}_n(\mathcal{O})$ is unimodular. Since unimodularity is invariant under composition and translation we have the result. □

The condition $char(\mathcal{O}) = 0$ is important.

Example 6. *Let* $F_1, \ldots, F_n \in \mathbb{F}_p[[T]][X_1, \ldots, X_n]$ *be defined by* $F_j = 1 - X_j^p + X_j$ *and consider the polynomial map* $F = (F_1, \ldots, F_n) \in \mathcal{MP}_n(\mathbb{F}_p[[T]])$. *It is easy to check that* $\det JF = 1$ *and that* F *is unimodular. But*

$$F - F(1, \ldots, 1) = (-X_1^p + X_1, \ldots, -X_n^p + X_n).$$

So, in case $(\mathcal{O}, \mathcal{M}, k) = (\mathbb{F}_p[[T]], T\mathbb{F}_p[[T]], \mathbb{F}_p)$ *it follows that the property of invariance by translation is false.*

Example 7. *Let* $g(X) \in \mathbb{F}_p[X]$ *be a polynomial wich maps* $\{0, \ldots, p-2\} \mapsto p-1$ *and* $p-1 \mapsto 0$. *For example, take* $p = 5$ *and consider*

$$g(X) = -1 + X - 1X^2 + X^3 + 4X^4 \in \mathbb{F}_5[X].$$

It is easy to check that $g \circ g = 0$. *Note that* $g(0) \neq 0$. *Define the polynomial map* $F = (F_1, \ldots, F_n) \in \mathcal{MP}_n(\mathbb{F}_p[[T]])$ *with* $F_j = X_j - X_j^p + g(X_j^p)$. *We have* F *a Keller map with the induced map over the residue field non-zero. But by construction we have* $F \circ F = 0$. *Thus, in characteristic* $p > 0$ *the invariance by composition is false.*

In the next theorem the argument is simitar to the argument given in [12, Theorem 4] with the observation that is sufficient to require the invariance property.

Theorem 3.8. *(WM) Let $(\mathcal{O}, \mathcal{M}, k)$ be a complete discrete valuation ring with finite residue field. Let $F \in \mathcal{MP}_n(\mathcal{O})$ be a strongly invariant map. Then F is injective.*

Proof. Suppose false and let F be a strongly invariant map over $\mathcal{O}$ with $F(a_1) = \cdots = F(a_m) = c$ $(m > 1)$ for some $a_1, \ldots, a_m \in \mathcal{O}^n$ with $a_i \neq a_j$, if $i \neq j$. We will show that there is a strongly invariant map G with $\#G^{-1}(c) > m$. By iteration we will get a Keller map $\widetilde{G} \in \mathcal{MP}_n(\mathcal{O})$ with $\#G^{-1}(c) > (\#k)^n$ a contradiction by proposition 3.7 above.

Since $F(a_1) = F(a_2)$ we have $\langle a_2 - a_1 \rangle = R$ (lemma 3.2 above). On the other hand, since F is an invariant map it is ensured that there exists $b \in \mathcal{O}^n$ such that $F(b) - F(a_1)$ is unimodular, i.e., $\langle F(b) - F(a_1) \rangle = R$. In particular, $\langle a_2 - a_1 \rangle = \langle F(b) - F(a_1) \rangle = \langle F(b) - c \rangle = R$. So, we have $(a_2, a_1) \cong (F(b), c)$. By theorem 3.6 we know that there is $H \in \mathcal{MP}_n(\mathcal{O})$, Keller affine automorphism such that $H(c) = a_1$ and $H(F(b)) = a_2$. Now define $G = F \circ H \circ F$. We have G strongly invariant map with $G(a_j) = F(H(c)) = F(a_1) = c$ for all j and $G(b) = F(H(F(b))) = F(a_2) = c$. Note that $b \neq a_j$ for all j. □

Theorem 3.9. *(WM) Let $(\mathcal{O}, \mathcal{M}, k)$ be a complete discrete valuation ring with finite residue field. Suppose that $\mathcal{O}$ is an invariant domain. Then any unimodular Keller polynomial map $F \in \mathcal{MP}_n(\mathcal{O})$ is injective.*

3.5 Some results

Definition 3.6. *Pick $d \in \mathbb{Z}_{\geq 1}$ and let $(\mathcal{O}, \mathcal{M}, k)$ a local domain. We say that $\mathcal{O}$ is a d-unimodular map if any Keller map $F \in \mathcal{MP}_n(\mathcal{O})$ in dimension $n > 1$ with $deg(F) \leq d$ is unimodular.*

Note that any local domain $\mathcal{O}$ is 1-unimodular and $\mathcal{O}$ is a unimodular domain if and only if it is d-unimodular for all $d \in \mathbb{N}$. If $\mathcal{O}$ is d-unimodular then it is e-unimodular for all $e \leq d$. We will see later that $\mathbb{Z}_p$ is 3-unimodular for any prime $p > 3$. In case $char(\mathcal{O}) = p > 0$ and k finite we have that $\mathcal{O}$ isn't d-unimodular for infinitely many $d \in \mathbb{Z}$. Indeed, for each $m \in \mathbb{N}$ take $d = (\#k)^m$ and consider the map $F = (X_1 - X_1^d, \ldots, X_n - X_n^d) \in \mathcal{MP}_n(\mathcal{O})$.

Proposition 3.9. *(WM) Let $F \in \mathcal{MP}_n(\mathbb{Z})$ be a non constant polynomial map. Then for almost all primes $p \in \mathbb{Z}$ we have $F \otimes \mathbb{Z}_p$ unimodular map over $\mathbb{Z}_p$.*

Proof. Indeed, suppose $F_1(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n] \setminus \mathbb{Z}$. We can choose $d \in \mathbb{Z}^n$ such that $F_1(d) \neq 0$. Note that $F_1(d) \in \mathbb{Z}_p^*$ for all p such that $p \nmid F_1(d)$.

□

We have seen that to prove the Jacobian Conjecture it is sufficient to consider polynomial maps of Druzkowski type, i.e., maps in the form $F = X + H$ with $H_j = (\sum_k a_{kj}X_k)^3$ and JH nilpotent. We call maps of the form $F = X + H$ with $H = \sum_k a_{kj}X_k^3$ quasi-Druzkowski maps.

Proposition 3.10. *(WM) For almost all primes p, the Unimodular Conjecture over $\mathbb{Z}_p$ is true for quasi-Druzkowski maps.*

Proof. Let F be a quasi-Druzkowski map with $H = (H_1, \ldots, H_n)$ where $H_j = \sum_k b_{kj}X_k^3$. We will show that there exist $u_1, \ldots, u_n \in \mathbb{Z}_p$, not all null , such that

$$u_1H_1(X_1, \ldots, X_n) + \cdots + u_nH_n(X_1, \ldots, X_n) = 0.$$

Indeed, for this it is sufficient to find a non trivial solution for the homogeneous system:

$$u_1b_{11} + u_2b_{12} + \cdots + u_nb_{1n} = u_1b_{21} + u_2b_{22} + \cdots + u_nb_{2n} = \cdots = u_1b_{n1} + u_2b_{n2} + \cdots + u_nb_{nn} = 0.$$

Now since JH is nilpotent we have, in particular, $\det(b_{ij}) = 0$ and so there is a non-trivial solution $(u_1, \ldots, u_n) \in \mathbb{Q}_p^n$ for the system above. Without loss of generality we can suppose that $u_1 \in \mathbb{Z}_p^*$ and $u_j \in \mathbb{Z}_p$, if $j > 1$. Now consider $s := u_1 + u_2p \cdots + u_np \in \mathbb{Z}_p^*$. Note that, $(1, p, \ldots, p) \in \mathbb{Z}_p^n$ is such that

$$\langle F_1(1, p, \ldots, p), \ldots, F_n(1, p, \ldots, p)\rangle = \mathbb{Z}_p.$$

□

Remark 7. *The proposition above will be generalized later (see corollary 3.2).*

It was seen in the previous section that there are local domains $(\mathcal{O}, \mathcal{M}, k)$ with $char(\mathcal{O}) = p > 0$ that are not unimodular domains. On the other hand we know that any local domain with infinite residue field is indeed a unimodular domain. In particular, if we consider the map $F = (X_1 - X_1^p, \ldots, X_n - X_n^p)$ over $(\overline{\mathbb{F}_p}[[T]], T\overline{\mathbb{F}_p}[[T]], \overline{\mathbb{F}_p})$ we have $\overline{F}(\alpha) \neq 0$ for some $\alpha \in \overline{\mathbb{F}_p}$ (= algebraically closure of $\mathbb{F}_p$). So, if we take $L =$ the field obtained by adjunction of α to $\mathbb{F}_p$ we see that our F is unimodular over the local domain $(L[[T]], TL[[T]], L)$. For the p-adic case there is an analogue:

Theorem 3.10. *(WM) Let $F \in \mathcal{MP}_n(\mathbb{Z}_p)$ be a Keller map. Then there is a complete discrete valuation ring $(\mathcal{O}, \mathcal{M}, k)$ that dominates $\mathbb{Z}_p$ such that $F \otimes \mathcal{O}$ is a unimodular map. Furthermore, $\mathcal{O}$ is a free $\mathbb{Z}_p$-module with*

$$rank_{\mathbb{Z}_p}(\mathcal{O}) = [k : \mathbb{F}_p].$$

Proof. In the proof we use a result of algebraic number theory.

Consider the map $\overline{F} \in \mathcal{MP}_n(\mathbb{F}_p)$ induced over the residue field. By the previous remark we know that there exists $\alpha \in \overline{\mathbb{F}_p}^n$ such that $\overline{F}(\alpha) \neq 0$. By taking the field $k := \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ obtained by adjunction we can look at $\overline{F}$ as a polynomial map which is **non zero** over k. Now we recall the following theorem about unramified extensions of a local field L [6]:

Theorem. *Let L be a local field with residue field l. There exists a 1-1 correspondence between the following sets*

$$\{\textit{finite extensions unramified over } L\ \} \ \cong\ \{\textit{finite separable extensions of } l\}$$

given by $L' \mapsto l'$, where l' is the residue field associated to L'. Furthermore, in this correspondence we have $[L' : L] = [l' : l]$.

Applying the theorem above to $L = \mathbb{Q}_p$ with $l = \mathbb{F}_p$ we see that the extension $k|\mathbb{F}_p$ corresponds to a local field $K|\mathbb{Q}_p$ such that k is the residue field of K. Denote by $(\mathcal{O}, \mathcal{M}, k)$ the ring of integers of K. The ring $\mathcal{O}$ is the integral closure of $\mathbb{Z}_p$ in K and by a general result (cf.[1, proposition 5.17]) we know that $\mathcal{O}$ is a free $\mathbb{Z}_p$-module and $rank_{\mathbb{Z}_p}(\mathcal{O}) = [K : \mathbb{Q}_p] = [k : \mathbb{F}_p]$. So $F \otimes \mathcal{O} \in \mathcal{MP}_n(\mathcal{O})$ is a Keller map with non zero induced map over the residue field. □

The theorem below was gotten in an attempt of the author to show the following

Conjeture. [7] *Denote by $\mathcal{O}$ the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$. Let $F : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ be a Keller map such that $F \otimes \mathcal{O}$ is injective. Then F is an isomorphim.*

Lemma 3.5. *Let $K|\mathbb{Q}_p$ be a finite Galois extension with $m := [K : \mathbb{Q}_p] > 1$. Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K. Let $F \in \mathcal{MP}_n(\mathcal{O}_K)$ be a non-injective Keller unimodular map. Then there exists a non-injective Keller unimodular map $G \in \mathcal{MP}_{mn}(\mathbb{Z}_p)$.*

Proof. The same argument of lemma 1.2 works. The relevant fact is that $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of $rank_{\mathbb{Z}_p}(\mathcal{O}_K) = m$. □

By proposition 3.7 we know that if $\mathbb{Z}_p$ is a unimodular domain then any Keller map over $\mathbb{Z}_p$ is injective. We can show a more general result

Theorem 3.11. *(WM) Assume that $\mathbb{Z}_p$ is invariant domain for some prime p. Then for all Keller unimodular maps $F \in \mathcal{MP}_n(\mathbb{Z}_p)$ and $K|\mathbb{Q}_p$ finite extension we have $F \otimes \mathcal{O}_K$ is an injective map.*

[6] See appendix, theorem 4.10
[7] see mathoverflow "Polynomial maps over $\mathbb{Z}$" for an incomplete argument due to Jason Starr

Proof. It is sufficient to show that $F \otimes \mathcal{O}$ is an injective map where $\mathcal{O}$ denotes the integral closure of $\mathbb{Z}_p$ in $\overline{\mathbb{Q}_p}$. Indeed, if $\alpha \neq \beta \in \mathcal{O}$ are such that $F(\alpha) = F(\beta)$ consider the ring $R = \mathbb{Z}_p[\alpha, \beta]$ obtained by adjunction and let $K := Frac(R)$. We have $K|\mathbb{Q}_p$ a finite extension such that $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in K$. Note that $\alpha_i, \beta_i \in \mathcal{O}_K$ for all i. Without loss of generality we can suppose that $K|\mathbb{Q}_p$ is a Galois extension. So, $F \otimes \mathcal{O}_K$ is a Keller unimodular map over $\mathcal{O}_K$ that isn't injective. By the lemma above, we obtain $G \in \mathcal{MP}_N(\mathbb{Z}_p)$ a Keller unimodular map that isn't injective. Now since we assume that $\mathbb{Z}_p$ is a invariant domain and G is strongly invariant map, by theorem 3.8, we know that G is an injective map. A contradiction. □

In the direction of the Unimodular Conjecture we have the interesting result:

Theorem 3.12. *(WM) Let $(\mathcal{O}, \mathcal{M}, k)$ be a local domain with $q := \#k < \infty$. Then $\mathcal{O}$ is a $(q-1)$-unimodular domain.*

Note that there are no restrictions about $char(\mathcal{O})$.

Proof. Let $F : \mathcal{O}^n \longrightarrow \mathcal{O}^n$ be a Keller map with $deg(F) \leq q-1$. Denote by f_j the polynomial in $k[X_1, \ldots, X_n]$ obtained by reduction of $F_j \mod \mathcal{M}$. By Keller condition we have f_j is a non zero polynomial, for all indices j. So we obtain a polynomial map $f = (f_1, \ldots, f_n) : k^n \longrightarrow k^n$. We must prove that there exists $\alpha \in k^n$ such that $f(\alpha) \neq 0$.

By passing to algebraic closure consider the algebraic set $X \subset \overline{k}^n$ defined by equations $f_1 = \cdots = f_n = 0$. We affirm that $\dim X = 0$ [8]. Indeed, note that $X = f^{-1}(0)$, where f is the map over $\overline{k}$ defined by tuple $f_1, \ldots, f_n$. The Keller condition implies that $[\overline{k}(X_1, \ldots, X_n) : \overline{k}(f_1, \ldots, f_n)] < \infty$ (see [11, proposition 1.1.31]) and by [11, theorem 1.1.32] we know $\#f^{-1}(Q) \leq [\overline{k}(X_1, \ldots, X_n) : \overline{k}(f_1, \ldots, f_n)]$ for all $Q \in \overline{k}^n$. In particular, $\#X = \#f^{-1}(0) < \infty$. So $\dim X = 0$.

Now we make use of the following [9]

Bezout Inequality. *Let $X \subset \mathbb{A}^n_{\overline{k}}$ be an affine algebraic set given by the equations $f_1 = \cdots = f_r = 0$. Denote by $X(k)$ the set of k-points. If $\dim X = 0$ then*

$$\#X(k) \leq \#X \leq deg(f_1) \cdots deg(f_r).$$

[8] second proof: consider the $\overline{k}$-algebra $R = \overline{k}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n \rangle$ and take $M \in Spec_m(R)$ a maximal ideal. By local noetherian ring theory we know that $\dim R_m \leq dim_{\overline{k}} T_P X$ for all $P \in X$ where $T_P X := Hom_{\overline{k}}(\mathcal{M}_{X,P}/\mathcal{M}^2_{X,P}, \overline{k})$ is the tangent space. By Jacobian criterion we have $dim_{\overline{k}} T_P X = n - rank(JF(P)) = n - n = 0$. So we conclude $\dim R_m = 0$. In particular, $\dim R = 0$ and so that R is an artinian $\overline{k}$-algebra. In particular, $Spec_m(R)$ is finite set. By correspondence, we conclude that X is a finite set. So $\dim X = 0$.

[9] see appendix.

Applying the theorem above we have

$$\#X(k) \leq deg(f_1) \cdots deg(f_n) \leq deg(F)^n < q^n$$

where we use the hypothesis: $q > deg(F)$. So $S = k^n \setminus X(k) \neq \varnothing$. Let $\alpha \in S$. By definition $f_j(\alpha) \neq 0$ for some index j. In particular, the map $f : k^n \longrightarrow k^n$ isn't zero. So F is a unimodular map. □

Corollary 3.1. *(WM) For all prime p, $\mathbb{F}_p[[T]]$ and $\mathbb{Z}_p$ are $(p-1)$-unimodular domains .*

Note that the bound $p-1$ is "maximal" for $\mathbb{F}_p[[T]]$.

Corollary 3.2. *(WM) $\mathbb{Z}_p$ is 3-unimodular domain for all prime $p > 3$. In particular, for almost all primes p the Unimodular Conjecture is true for maps of degree ≤ 3 over $\mathbb{Z}_p$.*

Proof. Since $p > 3$ we have $p - 1 \geq 3$ and so the result follows from theorem above. □

In dimension $n = 2$ and in characteristic 0 the theorem above can be refined. Indeed, we have the following

Theorem 3.13. *(WM) Let $f = (f_1, f_2) \in \mathcal{MP}_2(\mathcal{O})$ be a Keller map over a complete DVR $(\mathcal{O}, \mathcal{M}, k)$ with $q := \#k < \infty$ and $char(\mathcal{O}) = 0$. If $deg(f_1) < q^2$ then f is unimodular.*

Remark 8. *This is particular for $char(\mathcal{O}) = 0$. Indeed, consider the map*

$$f = (X_1 - X_1^p, X_2 - X_2^p) \in \mathcal{MP}_2(\mathbb{F}_p[[T]]).$$

f is a Keller map but is not unimodular. Furthermore $deg(f_1) = p < p^2$.

In order to prove the theorem above we use the following result:

Theorem (Yitang Zhang). [10] *Let $f = (f_1, f_2) \in \mathcal{MP}_2(K)$ be a Keller map over an algebraically closed field K with $char(K) = 0$. Then $[K(X, Y) : K(f_1, f_2)] \leq \boldsymbol{Min}\{deg(f_1), deg(f_2)\}$.*

Proof. (of theorem 3.13) Let $f = (f_1, f_2)$ be a Keller map over $\mathcal{O}$. By proposition 3.1 we have a bijection

$$S_1 := \{(u, v) \in \mathcal{O}^2 \mid f_1(u, v) = f_2(u, v) = 0\} \cong \{(a, b) \in k^2 \mid g_1(a, b) = g_2(a, b) = 0\} =: S_2$$

where g_1 and g_2 are the reductions of $f_1, f_2 \mod \mathcal{M}$.

[10] see: Zhang, Y.: " The Jacobian conjecture and the degree of field extension-Thesis, (1991)".

By [11, theorem 1.1.32] we know that $\#S_1 \leq [K(X,Y) : K(f_1, f_2)]$ where $K = \overline{Frac(\mathcal{O})}$. By Zhang theorem and hypothesis we have $\#S_1 \leq \mathbf{Min}\{deg(f_1), deg(f_2)\} \leq q^2 - 1$. In particular there is $Q \in k^2 \setminus S_2$. So f is a unimodular map. □

Theorem 3.14. *(WM)* [11] *Let $p \in \mathbb{Z}$ be a prime. For each $d \in \mathbb{Z}_{\geq 1}$ we can find a finite extension $K|\mathbb{Q}_p$ such that the ring of integers $\mathcal{O}_K$ is a d-unimodular domain.*

Proof. Let $d \in \mathbb{N}$. If $d = 1$ take $K = \mathbb{Q}_p$. Suppose that $d > 1$. We know that for any Keller map $F \in \mathcal{MP}_n(\mathbb{Z}_p)$ of degree d we have

$$\#X = deg(X) \leq deg(F)^n = d^n$$

where X is the algebraic set in $\mathbb{A}^n_{\overline{\mathbb{F}_p}}$ given by reduction of $F \mod p$. Let n be an integer such that $p^n > d$ and fix $\mathbb{F}_{p^n}$ the unique extension of $\mathbb{F}_p$ of degree n in $\overline{\mathbb{F}_p}$. We have seen in the proof of theorem 3.10 that there is a finite extension $K|\mathbb{Q}_p$ such that the residue field of $\mathcal{O}_K$ is $\mathbb{F}_{p^n}$. By construction, for all Keller map $G \in \mathcal{MP}_n(\mathcal{O}_K)$ with $deg(G) \leq d$ we have $\#\{g_1 = \cdots = g_n = 0\} \leq deg(G)^n \leq d^n < (p^n)^n$. So G is a unimodular map and $\mathcal{O}_K$ is a d-invariant domain. □

Proposition 3.11. *(WM) Suppose that for all $n \in \mathbb{N}$ and $F = (F_1, \ldots, F_n) \in \mathcal{MP}_n(\mathbb{Z}_p)$ Keller map with $deg(F) < n$ is unimodular. Then $\mathbb{Z}_p$ is a unimodular domain.*

Proof. Let $F \in \mathcal{MP}_n(\mathbb{Z}_p)$ be a Keller map with $n \leq deg(F)$. Let $m \in \mathbb{Z}$ be an integer (to be determined) and consider the map

$$F^{[[m]]} = (F_1, \ldots, F_n, F_1, \ldots, F_n, \ldots, F_1, \ldots, F_n) \in \mathcal{MP}_{mn}(\mathbb{Z}_p)$$

which consists of m-repetitions of the tuple $F_1, \ldots, F_n$ where in each occurrence of such tuple we introduce n-distinct variables. By construction we have $F^{[[m]]}$ a Keller map and F is a unimodular map if and only if so is $F^{[[m]]}$. We can choose large m such that $deg(F) < mn$. Thus, we get the unimodularity of F. □

Let R be a domain and $f \in R[X_1, \ldots, X_n]$. Define $d(f) :=$ number of monomials in degree > 3 that occur in f. If $F = (F_1, \ldots, F_n) \in \mathcal{MP}_n(R)$ we define $d(F) := \sum_j d(F_j)$.

Proposition 3.12. *(WM) Let $p \in \mathbb{Z}_{>3}$ be a prime number and $f \in \mathcal{MP}_n(\mathbb{Z}_p)$ a Keller map. Suppose that*

$$d(f) \leq log(2)^{-1} log(nlog(p/3)/log(3)) \qquad (*)$$

[11] This proposition motivates the following question:

- Let p be a prime and consider the p-adic ring. Is there a finite extension $K/\mathbb{Q}_p$ such that $\mathcal{O}_K$, the ring of integers, is a unimodular domain?

where log is the natural logarithm. Then f is unimodular.

Proof. Let $f \in \mathcal{MP}_n(\mathbb{Z}_p)$ be a Keller map. By the reduction theorem we can find invertible maps $G, H \in \mathcal{MP}_{n+m}(\mathbb{Z}_p)$ for some $m \in \mathbb{N}$ such that $g := G \circ f^{[m]} \circ H$ has degree ≤ 3 where $f^{[m]} = (f, X_{n+1}, \ldots, X_{n+m})$. Furthermore, we know that $G(0) = H(0) = 0$. Denote by $X_f(\mathbb{Z}_p)$ and $X_g(\mathbb{Z}_p)$ the set of $\mathbb{Z}_p$-points of f and g respectively. It is easy to check that $\#X_f(\mathbb{Z}_p) = \#X_g(\mathbb{Z}_p)$. Now, since $\mathbb{Z}_p$ is a 3-unimodular domain (corollary 3.2) we have $\#X_g(\mathbb{Z}_p) < 3^{n+m}$. By the proof of reduction theorem we get $m = 2^{d(f)}$. The inequality $(*)$ implies $3^{m+n} \leq p^n$ and so we have f a unimodular map. □

Theorem 3.15. *(WM) $\mathbb{Z}_p$ is an invariant domain for almost all prime p if and only if the Jacobian Conjecture (over $\mathbb{C}$) is true.*

Proof. The implication $\Longleftarrow$ follows from 3.4. Suppose that the Invariance Conjecture is true over $\mathbb{Z}_p$ for almost all prime p. By a result of Connel-var den Dries (see chapter 1, 1.7) we know that is sufficient to show the Jacobian Conjecture over $\mathbb{Z}$. So, suppose some Keller map $F \in \mathcal{MP}_n(\mathbb{Z})$ isn't invertible. Since F has coefficients in $\mathbb{Z}$ it follows that F is unimodular over $\mathbb{Z}_p$ for almost all primes p. Also, we know by hypothesis that $F \otimes \overline{\mathbb{Q}}$ isn't injective. By immersion lemma, F isn't injective over $\mathbb{Z}_p$ for infinitely many primes p. Fix such a prime p such that $\mathbb{Z}_p$ is an invariant domain. So, we obtain $F \otimes \mathbb{Z}_p$ a Keller map non-injective over the invariant complete local domain. A contradiction by theorem 3.8. □

3.5.1 A refinement

Strong Immersion Lemma. *(WM) Let $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}$ be algebraic numbers. Then there is a finite set E of rational primes such that for all prime $p \notin E$ we have an injective homomorphism*

$$\mathbb{Z}[\alpha_1, \ldots, \alpha_m] \hookrightarrow \mathcal{O}_{K,p}$$

where $\mathcal{O}_{K,p}$ is the ring of integers of some finite $K|\mathbb{Q}_p$.

Proof. The proof is similar to proof the immersion lemma. It is sufficient to prove the following

Fact. *Let $f(T) \in \mathbb{Z}[T]$ be an irreducible polynomial. Then for almost all prime p there is a finite extension $K|\mathbb{Q}_p$ and $\alpha \in \mathcal{O}_{K,p}$ such that $f(\alpha) = 0$.*

Let d be the discriminant of the polynomial f and $E := \{p \mid p \text{ is prime with } p \mid d\}$. Let $p \in \mathbb{Z} \setminus E$ be a prime and take $\overline{f}(T) \in \mathbb{F}_p[T]$, via reduction $\mod p$. Let $\alpha \in \overline{\mathbb{F}_p}$ be a root of $\overline{f}(T)$ and take $\mathbb{F}_{p^k}$ the definition field of α.

Then

$$\overline{f}(\alpha) = 0 \text{ and } \overline{f}'(\alpha) \neq 0 \text{ by condition } p \notin E.$$

Now we recall that there exists a finite extension $K|\mathbb{Q}_p$ such that $\mathcal{O}_{K,p}$ is a complete discrete valuation with residue field $\mathbb{F}_{p^k}$. Since $\mathcal{O}_{K,p}$ is a complete ring we can use the Hensel lemma to conclude that there is some $a \in \mathcal{O}_{K,p}$ such that $f(a) = 0$. □

Theorem 3.16. *(WM) $\mathbb{Z}_p$ is an invariant domain for infinitely many primes p if and only if the Jacobian Conjecture (over $\mathbb{C}$) is true.*

Proof. The implication $\Longleftarrow$ is trivial. Suppose that $\mathbb{Z}_p$ is invariant domain for infinitely many primes p but the Jacobian Conjecture is false. Let $F \in \mathcal{MP}_N(\mathbb{Z})$ be a counterexemple with $\det JF = 1$. In particular, $F \otimes \overline{\mathbb{Q}}$ isn't injective. Let $\alpha \neq \beta \in \overline{\mathbb{Q}}^N$ be such that $F(\alpha) = F(\beta)$. By the strong immersion lemma we know that $R := \mathbb{Z}[\alpha, \beta] \hookrightarrow \mathcal{O}_{K,p}$ for almost all primes p. Fix a prime p such that $R \hookrightarrow \mathcal{O}_{K,p}$ and such that $\mathbb{Z}_p$ is invariant domain. So, we obtain $F \otimes \mathcal{O}_{K,p}$ a Keller map, not injective, over the domain $\mathcal{O}_{K,p}$. By lemma 3.5 we know that there exists a Keller map G over $\mathbb{Z}_p$ that isn't injective. A contradiction by theorem 3.9. □

Theorem 3.17. *(WM) There is a finite set of primes E such that for all prime $p \in \mathbb{Z} \setminus E$ we have*

$$\mathbb{Z}_p \text{ is an invariant domain} \Longleftrightarrow \mathbb{Z}_p \text{ is a unimodular domain.}$$

Proof. The implication $\Longleftarrow$ is easy. Suppose $\Longrightarrow$ false. Then for infinitely many primes p we have $\mathbb{Z}_p$ is an invariant non-unimodular domain. Since $\mathbb{Z}_p$ is invariant for infinitely many primes we have that the Jacobian Conjecture is true by theorem 3.16. On the other hand since $\mathbb{Z}_p$ is not unimodular for infinitely many primes we know, by Essen-Lipton theorem, that the Jacobian Conjecture is false. Contradiction. □

Chapter 4

Appendix

In this chapter we include for the reader's convenience some results in algebraic geometry and commutative algebra that have been used in the dissertation. Details can be found in the references. In all text the word ring signifies commutative ring with unity unless otherwise stated.

4.1 k-algebras of finite type

We start with the

Definition 4.1. *Let K be a field. A valuation ring of K is a subring $\mathcal{O}$ of K such that given $x \in K \setminus \{0\}$ we have $x \in \mathcal{O}$ or $1/x \in \mathcal{O}$.*

Proposition 4.1. *Let K be a field and $\mathcal{O}$ a valuation ring. Then $\mathcal{O}$ is an integrally closed local domain.*

We say that a valuation ring $\mathcal{O}$ is a discrete valuation ring if the maximal ideal is principal.

Theorem 4.1. *Let k be a field and $K = k(T)$ the rational functions field over k. Let $\mathcal{O}$ be a valuation ring that contains k. Then $\mathcal{O}$ is a discrete valuation ring and $\mathcal{O} = k[T]_{p(T)}$ for some irreducible polynomial $p(T) \in k[T]$ or $\mathcal{O} = k[1/T]_{1/T}$, the "infinity" discrete valuation.*

Proof. Let $\mathcal{O}$ be a valuation ring with $\mathcal{O} \supset k$ and maximal ideal $\mathcal{M}$. We divide in cases:

(i) $T \in \mathcal{O}$: In this case, $k[T] \subset \mathcal{O}$ and if $P := \mathcal{M} \cap k[T] = (p(T))$ we have $k[T]_{p(T)} \subset \mathcal{O}$. Since discrete valuation rings are maximal with respect the domination relation, we have $\mathcal{O} = k[T]_{p(T)}$.

(ii) If $T \notin \mathcal{O}$, a similar argument applied to T^{-1} shows $\mathcal{O} = k[1/T]_{1/T}$. □

The following result has many interesting applications:

Extension Theorem. *Let k be an algebraically closed field and R a domain with $K = Frac(R)$. Let $\phi : R \longrightarrow k$ be a ring map. Then, there is a valuation ring $(\mathcal{O}, \mathcal{M})$ of K containing R and $\Phi : \mathcal{O} \longrightarrow k$, an extension of ϕ, such that $Ker(\Phi) = \mathcal{M}$.*

Proof. Consider the set S that consists of pairs (A, Φ) where A is a (proper) subring of K containing R and $\Phi : A \longrightarrow k$ is an extension of ϕ. Note that $S \neq \varnothing$ since $(R, \phi) \in S$. Introduce a partial order in S by $(A_1, \Phi) \leq (A_2, \Phi_2)$ if $A_1 \subset A_2$ and Φ_2 is an extension of Φ_1. This implies that S is an inductive set and by Zorn lemma there exists $(\mathcal{O}, \Phi)$ a maximal element. I affirm that $\mathcal{O}$ is a valuation ring. Note that it is local ring with maximal ideal $\mathcal{Q} := Ker(\Phi)$. Indeed, pick $x \in R$ with $x \notin \mathcal{Q}$ and consider the ring $A_1 := \mathcal{O}[x^{-1}]$. Since $x \notin \mathcal{Q}$ we have $\Phi(x) \neq 0$. Define $\psi : A_1 \longrightarrow k$ given by $a_0 + \cdots + a_n x^{-n} \mapsto \Phi(a_0) + \cdots + \Phi(a_n)\Phi(x)^{-n}$. This map is well defined and yields a map extending Φ. By maximality we have $x^{-1} \in \mathcal{O}$. So $\mathcal{O} - \mathcal{O}^* = \mathcal{Q}$. It is easy to show that $\mathcal{O}$ is a valuation ring.

□

Algebrically Nullstellensatz. *Let k be a field and A a k-algebra of finite type. Let $\mathcal{M}$ be a maximal ideal A. Then, $A/\mathcal{M}$ is a finite extension of k.*

Proof. Write $A' = A/\mathcal{M} = k[\alpha_1, \ldots, \alpha_n]$ and suppose that $d = tr.deg_k(A')$. Without loss of generality we can suppose that $\alpha_1, \ldots, \alpha_d$ are algebraically independent over k. So $R := k[\alpha_1, \ldots, \alpha_d]$ is a polynomial ring in d variables. Thus for each $d + 1 \leq i \leq n$ there is a relation (minimal) of type

$$a_{0i}(\alpha_1, \ldots, \alpha_d)\alpha_i^{e_i} + a_{1i}(\alpha_1, \ldots, \alpha_d)\alpha_i^{e_i - 1} + \cdots + a_{e_i i}(\alpha_1, \ldots, \alpha_d) = 0.$$

Since $\overline{k}$ (= algebraic closure of k) is infinite there exists $P = (a_1, \ldots, a_d) \in \overline{k}^n$ such that $a_{0j}(P) \neq 0$ for all $j \in \{d + 1, \ldots, n\}$.

Define $\phi : R \longrightarrow \overline{k}$ given by $\alpha_i \mapsto a_i$. By the extension theorem there is a DVR $\mathcal{O}$ of $k(\alpha_1, \ldots, \alpha_d)$ wich contains R and $\Phi : \mathcal{O} \longrightarrow \overline{k}$ extension of ϕ with $ker(\Phi) = \mathcal{M}_{\mathcal{O}}$. We affirm that $\mathcal{O}$ contains $\alpha_{d+1}, \ldots, \alpha_n$. Indeed, suppose this false for some $d + 1 \leq i \leq n$. In particular, $\alpha_i^{-1} \in \mathcal{O} - \mathcal{O}^* = \mathcal{M} = Ker(\Phi)$.

Then making use of the relation $a_{0i}(\alpha_1, \ldots, \alpha_d)\alpha_i^{e_i} + a_{1i}(\alpha_1, \ldots, \alpha_d)\alpha_i^{e_i - 1} + \cdots + a_{e_i i}(\alpha_1, \ldots, \alpha_d) = 0$ we obtain $a_{0i}(\alpha_1, \ldots, \alpha_d) + a_{1i}(\alpha_1, \ldots, \alpha_d)\alpha_i^{-1} + \cdots + a_{e_i i}(\alpha_1, \ldots, \alpha_d)\alpha^{-e_i} = 0$.

Applying Φ we obtain a relation of type $a_{0i}(a_1, \ldots, a_d) = 0$ that is impossible by construction. So, $A' \subset \mathcal{O} \Longrightarrow \mathcal{O} = A'$. Since A' is a field we should have $Ker(\Phi) = 0$ and thus A' is a subfield of $\overline{k}$. In particular, $A'|k$ is an algebraic extension. □

Corollary 4.1. *Let $\mathcal{M}$ be a maximal ideal in $k[X_1, \ldots, X_n]$ (with $k = \overline{k}$). Then there is $\alpha_1, \ldots, \alpha_n \in k$ such that*

$$\mathcal{M} = (X_1 - \alpha_1, \ldots, X_n - \alpha_n).$$

Corollary 4.2. *Let $X = Z(I) \subset \mathbb{A}_k^n$ be a closed subset (in Zariski topology) with $\overline{k} = k$. Denote $\mathcal{I}(X) := \{f \in k[X_1, \ldots, X_n] \mid f(P) = 0 \text{ for all } P \in X\}$.*

$$\mathcal{I}(X) = \sqrt{I}.$$

Theorem 4.2. *Let A be a domain with fraction field K. Denote $\overline{A}$ the integral closure of A in K. Then*

$$\overline{A} = \bigcap_{\mathcal{O} \in S} \mathcal{O} \quad em \quad K$$

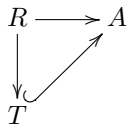
where $S := \{\mathcal{O} \mid \mathcal{O} \text{ is a valuation ring of } K \text{ and } A \subset \mathcal{O}\}$.

Proof. Since valuation ring is integrally closed we have $\overline{A} \subset \mathcal{O}$ provided that $\mathcal{O}$ is a valuation ring of K and $A \subset \mathcal{O}$. Now suppose that $x \in K$ with $x \notin \overline{A}$. Consider $\overline{K}$, the algebraic closure of K, and define the map

$$\phi : A[x^{-1}] \longrightarrow \overline{K} \qquad a_0 + \cdots + a_n x^{-n} \mapsto a_0.$$

By extension theorem we know that ϕ extend to a map $\Phi : \mathcal{O} \longrightarrow L$, where $\mathcal{O}$ is a valuation ring of K and, furthermore, $\mathcal{M}_{\mathcal{O}} = Ker(\Phi)$. In particular, we have $x^{-1} \in Ker(\Phi) \Longrightarrow x^{-1} \notin \mathcal{O}^* \Longrightarrow x \notin \mathcal{O}$. □

Theorem 4.3. *Suppose that R is a noetherian ring and A an R-algebra of finite type. Let $T \subset A$ be an R-algebra such that A is finite as T-module. Then, T is an R-algebra of finite type.*



Proof. Let $A = R[x_1, \ldots, x_n]$ for generators $x_1, \ldots, x_n$ and $A = Tu_1 + \cdots + Tu_r$ as T-module. We have $x_i = \sum_{j=1}^r t_{ij} u_j$ for all i an some $t_{ij} \in T$ and $u_l u_k = \sum_p t_{lkp} u_p$ for some elements $t_{ikp} \in T$. Consider $T_0 = R[\{t_{ij}, t_{lkp} \mid 1 \leq i, j, k, l \leq n\}]$ the subalgebra of T. We affirm that A is finitely generated as T_0-module. Assume, this for a moment. Since T_0 is notherian and A is finitely generated as T_0-module we have A a noetherian T_0-module. So, since T is a T_0-submodule, we have that T is finitely generated as T_0-module. Since T_0 is of finite type over R we concluded that T if of finite type over R.

Now, we show that A is finitely generated as T_0-module. Let $a \in A$. Then there is $p(X_1, .., X_n) \in R[X_1, \ldots, X_n]$ such that $a = p(x_1, \ldots, x_n)$. Using the relations $x_i = \sum_{j=1}^r t_{ij} u_j$ and $u_l u_k = \sum_p t_{lkp} u_p$ we have that we can write

a in the form $a = v_1u_1 + \cdots + v_ru_r$ with $v_i \in T_0$. So, $A = T_0u_1 + \cdots + T_0u_r$ and so A is module-finite over T_0. $\square$

4.2 Kähler differentials

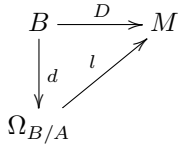
Let B be an A-algebra. Given a B-module M an A-derivation consists of an A-linear map $D : B \longrightarrow M$ that satisfies the rule of Leibniz

$$D(bb') = bD(b') + b'D(b) \qquad \forall \quad b, b' \in B.$$

We denote by $Der_A(B, M)$ the set of all A-derivation of B in M.

Theorem 4.4. *$Der_A(B, M)$ is a B-module and there is a B-module $\Omega_{B/A}$ together with a derivation $d : B \longrightarrow \Omega_{B/A}$ and with the following universal property:*

Given M, a B-module, and any A-derivation $D : B \longrightarrow M$ there is a unique B-linear map $l : \Omega_{B/A} \longrightarrow M$ such that the following diagram is commutative



More precisely, $Der_A(B, M) \cong Hom_B(\Omega_{B/A}, M)$ for all B-module M.

Proof. Consider the map of A-algebras

$$\phi : B \otimes_A B \longrightarrow B \qquad b \otimes b' \mapsto bb'.$$

Let $I := Ker(\phi)$

Define $\Omega_{B/A} := I/I^2$. Consider $\Omega_{B/A}$ as B-module via $b\overline{b_1 \otimes b_2} := \overline{bb_1 \otimes b_2}$.

In view of the exact sequence

$$0 \longrightarrow I \longrightarrow B \otimes_A B \longrightarrow B \longrightarrow 0$$

we get $0 \longrightarrow I/I^2 \longrightarrow C \longrightarrow B \longrightarrow 0$ where $C := B \otimes B/I^2$. Consider the maps $\beta_1, \beta_2 : B \longrightarrow C$ given by $b \mapsto b \otimes 1 \mod I^2$ and $b \mapsto 1 \otimes b \mod I^2$ respectivaly. We define $d_{B/A} : B \longrightarrow \Omega_{B/A}$ by $\gamma \mapsto \beta_1(\gamma) - \beta_2(\gamma)$. It can be shown that pair $(\Omega_{B/A}, d_{B/A})$ satisfies the universal property in the statement.

$\square$

By universal property it follows that $(\Omega_{B/A}, d_{B/A})$ is unique up to isomorphism.

Proposition 4.2. *Let A be a k-algebra (k isn't necessarily a field) and B an A-algebra. Then there is an exact sequence*

$$\Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0$$

where $\alpha : d_{A/k}(a) \otimes b \mapsto b d_{B/k}(a)$ and $\beta : d_{B/k}(b) \mapsto d_{B/A}(b)$.

Definition 4.2. *Let $K|k$ be a finitely generated field extension and $d = tr.deg_k(K)$. We say that K is separable over k if exists $t_1, \ldots, t_d \in K$ such that $K|k(t_1, \ldots, t_d)$ is finite and separable.*

Theorem 4.5. *Let $K|k$ be field extension finitely generated. The following are equivalent*

(i) K is separable over k.

(ii) The sequence $0 \longrightarrow \Omega_{k/\mathbb{Z}} \otimes_k K \xrightarrow{\alpha} \Omega_{K/\mathbb{Z}} \xrightarrow{\beta} \Omega_{K/k} \longrightarrow 0$ is exact.

(iii) $\dim_K(\Omega_{K/k}) = tr.deg_k(K)$.

Proof. [7, proposition 5.2-Iversen] □

Dimension Formula. *Let A be a domain of finite type over a field k with $char(k) = 0$ or perfect. Let $K := Frac(A)$. Then*

$$\dim A = tr.deg_k K = \dim_K \Omega_{K/k}.$$

Proof. By Noether Normalization lemma we can find $X_1, \ldots, X_n \in A$, algebraically independent over k, such that the extension $k[X_1, \ldots, X_n] \hookrightarrow A$ is integral. In particular, $\dim A = \dim k[X_1, \ldots, X_n] = n$. Denote $L = k(X_1, \ldots, X_n)$. Then $L|K$ is an algebraic extension and so $tr.deg_k K = tr.deg_k L = n$. So, $\dim A = tr.deg_k K$. The formula $tr.deg_k K = \dim_K \Omega_{K/k}$ is a consequence of the theorem above. □

4.3 Finite maps

In this section, k will denote an algebraically closed field. Given A a domain of finite type over k we will denote by $Spec_m(A)$ the subset of $Spec(A)$ that consists of closed points If $A = k[X_1, \ldots, X_n]/J$ then there is a homeomorphism $Spec_m(A) \cong Z(J)$:

$$\alpha : Spec_m(A) \longrightarrow Z(J) \qquad \overline{(X_1 - a_1, \ldots, X_n - a_n)} \mapsto (a_1, \ldots, a_n).$$

Proposition 4.3. *Let $A \xrightarrow{f} B$ be a map of k-algebras of finite type. Let $\mathcal{M} \in Spec_m(B)$. Then, $\mathcal{M} \cap A$ is a maximal ideal of A.*

Proof. Let $\mathcal{M}$ a maximal ideal of B. By Nullstellensatz we have $B/\mathcal{M}$ is a finite extension of k. So, taking $Im(\pi) = \pi(A)$, where $\pi : A \longrightarrow B \longrightarrow B/\mathcal{M}$, we have that $\pi(A)$ is a k-algebra with $\dim_k \pi(A) < \infty$. So, $\pi(A)$ is a field. Since $\pi(A) \cong A/\mathcal{M} \cap A$ we have $\mathcal{M} \cap A \in Spec_m(A)$. □

So, given a map of k-algebras $A \xrightarrow{f} B$ we obtain a map in closed points $f^{\#} : Spec_m(B) \longrightarrow Spec_m(A)$.

Let $X \subset \mathbb{A}^n_k$ and $Y \subset \mathbb{A}^m_k$ affine varieties and $f : X \longrightarrow Y$ a morphism. Let $f^{\#} : \mathcal{O}_Y(Y) \longrightarrow \mathcal{O}_X(X)$ the map induced in regular functions given by $g \in \mathcal{O}_Y(Y) \mapsto g \circ f \in \mathcal{O}_X(X)$. So, we obtain a structure of $\mathcal{O}_Y(Y)$ algebra in $\mathcal{O}_X(X)$.

Definition 4.3. *We say that the morphism f if finite if $\mathcal{O}_X(X)$ is integral over $\mathcal{O}_Y(Y)$.*

In particular, if $f : X \longrightarrow Y$ is a finite dominant map we have $\dim X = \dim Y$. Note that, if X is a subvariety of X then $f|_{X'} : X' \longrightarrow Y$ is a finite map.

Theorem 4.6. *Let $f : X \longrightarrow Y$ be a map of affine varieties. Then*

(i) f is finite $\Longrightarrow$ f quasi-finite i.e. f has finite fibers.

(ii) f finite $\Longrightarrow$ f closed.

(iii) f finite and dominant $\Longrightarrow$ f surjective.

Proof. [8, Milne] □

Theorem 4.7. *Let $f : X \longrightarrow Y$ a finite dominant map of affine varieties and assume that Y is normal.*

(i) $\forall P \in Y$ we have $\#f^{-1}(P) \leq deg(f)$.

(ii) The set $S = \{P \in Y \mid \#f^{-1}(P) = deg(f)\}$ is open in Y.

Proof. Let $B = \mathcal{O}_X(X)$, $A = \mathcal{O}_Y(Y)$ and $g : A \longrightarrow B$ the induced map in k algebras. Let $f^{-1}(P) = \{Q_1, \ldots, Q_r\}$ and $u \in \mathcal{O}_X(X)$ such that $u(Q_i) \neq u(Q_j)$ if $i \neq j$. Let $F(T) \in \mathcal{O}_Y(Y)[T]$ be the minimal polynomial of u over $k(Y)$ (function field of Y). Since Y is normal we conclude that the coefficients of $F(T)$ are regular functions in Y. We have

$$F(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

for some $a_0, \ldots, a_{n-1} \in \mathcal{O}_Y(Y)$. Now, note that $n \leq deg(f)$ and $F(u)(Q_j) = u(Q_j)^n + a_{n-1}(P)u(Q_j)^{n-1} + \cdots + a_0(P) = 0$ and so, $u(Q_1), \ldots, u(Q_r)$ are roots of $T^n + a_{n-1}(P)T^{n-1} + \cdots + a_0(P) \in k[T]$. In particular, $r \leq n \leq deg(f)$.

Let $P \in Y$ such that $deg(f) = \#f^{-1}(P) = \#\{Q_1, \ldots, Q_r\}$. We want to show that there is an open set $U \ni P$,such that for any $P' \in U$ we have $deg(f) = \#f^{-1}(P')$. Pick $u \in \mathcal{O}_X(X)$ a regular function such that $u(Q_i) \neq u(Q_j)$ if $i \neq j$. Denote by $F(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathcal{O}_Y(Y)[T]$ the minimal polynomial of u. Then $deg(f) = r \leq deg(F) \leq deg(f) \Longrightarrow deg(F) = deg(f)$. Let $d := disc(F(T))$, the discriminant of $F(T)$. Since $T^n + a_{n-1}(P)T^{n-1} + \cdots + a_0(P)$ has $deg(F)$ distinct roots, we have that $d \in \mathcal{O}_Y(Y)$ is such that $d(P) \neq 0$. So, there is an open U_P over P such that $T^n + a_{n-1}(P')T^{n-1} + \cdots + a_0(P')$ has distinct roots. Consider the commutative diagram:

$$\begin{array}{ccc} \mathcal{O}_Y(Y) & \xrightarrow{f^{\#}} & \mathcal{O}_X(X) \\ \downarrow{\scriptstyle \pi} & \nearrow_{g} & \\ \mathcal{O}_Y(Y)[T]/(F(T)) & & \end{array}$$

Here, g is defined by $\overline{T} \mapsto u$. This diagram induces, by restriction

$$\begin{array}{ccc} Spec_m(\mathcal{O}_X(X)) & \xrightarrow{\widetilde{f}} & Y = Spec_m(\mathcal{O}_Y(Y)) \supset U_P \\ \downarrow{\scriptstyle g^*} & \nearrow_{\pi^*} & \\ Spec_m(\mathcal{O}_Y(Y)[T]/(F(T))) & & \end{array}$$

Let $P \in U_P$. The fiber with respect to the map π^* has $deg(f)$ elements. Furthermore, the map g^* is surjective. Indeed, g^* is finite and dominant since the map in regular functions is injective. In particular, $\#f^{-1}(P) \geq deg(f)$ and by (i) we have the equality $\#f^{-1}(P) = deg(f)$. □

4.4 Normalization

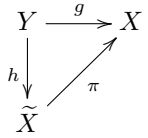
Let X be an affine variety over a field k $(= \overline{k})$ with coordinate ring $\mathcal{O}_X(X)$. Denote by $\mathcal{A}$ the integral closure of $\mathcal{O}_X(X)$. It is well know that $\mathcal{A}$ is a domain of finite type over k and so it is the coordinate ring of a variety $\widetilde{X}$. The inclusion $i : \mathcal{O}_X(X) \hookrightarrow \mathcal{A}$ induces a finite map $\pi : \widetilde{X} \longrightarrow X$.

It can be shown that the pair $(\widetilde{X}, \pi)$ is unique, up to isomorphism, and has the following properties:

(i) $\mathcal{O}_{\widetilde{X}}(\widetilde{X})$ is an integrally closed domain.

(ii) Suppose that Y is a normal affine variety and $g : Y \longrightarrow X$ is a morphism. Then there exists a unique morphism

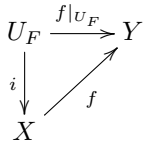
$h : Y \longrightarrow \widetilde{X}$ such that the following diagram is commutative



The pair $(\widetilde{X}, \pi)$ is called **the normalization of** X.

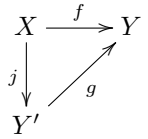
Let X be a variety and $X \xrightarrow{f} Y$ a finte dominant map of affine varieties. In particular we have f quasi-finite. Let $Q \in Y$ and consider $F := f^{-1}(Q) = \{P_1, \ldots, P_n\}$.

Take the open set $U_F = X \setminus F$. By restriction, we obtain a map $U_F \xrightarrow{f} Y$, quasi-finite but **non-finite**. So, we obtain the following diagram:



where i is inclusion, in particular an open embedding. The next theorem shows that, conversely, any quasi-finite map factors through a finite map

Zariski Main Theorem. *Every quasi-finite map* $X \xrightarrow{f} Y$ *is factored* $X \xrightarrow{j} Y' \xrightarrow{g} Y$ *where* j *is an open immersion and* g *is a finite map. If* Y *is normal and* f *a dominant map then the statement is true with* (Y', g) *being the normalization of* Y.



We will not prove the above theorem; details can be found in [10, Mumford] or in [8, Milne].

Example 8. *Let* X *be an affine variety and* $f : X \longrightarrow Y$ *a bijective morphism. It is possible that* f *isn't an isomorphism. Indeed, consider* $Y = \mathbb{A}^1_k$ *and* $X = \{(x, y) \in \mathbb{A}^2_k \mid y^2 - x^3 = 0\}$ *(*$k = \mathbb{C}$*). The map* $f : Y \longrightarrow X$ *given by* $t \mapsto (t^2, t^3)$ *is a bijective morphism but not isomorphism. Indeed, consider the map in coordinate rings:* $f^{\#} : \mathcal{O}_X(X) = k[t^2, t^3] \hookrightarrow k[t] = \mathcal{O}_Y(Y)$. *Note that this map isn't an isomorphism since* $\mathcal{O}_Y(Y)$ *is integrally closed and this is false for* $\mathcal{O}_X(X)$.

The problem is that X is singular over $(0, 0)$:

Corollary 4.3. *Let* $f : Y \longrightarrow X$ *be a bijective map of affine varieties with* X *normal. Then,* f *is an isomorphism.*

Proof. Since f is a bijection, in particular it is dominant. So, by Zariski Main Theorem we have that f is factored by $f = \pi \circ j$ where $\pi = id$ and $j = f$ is an open immersion. In particular, f is an isomorphism. □

4.5 Bounds for k-points

In this section k is a field and K is its algebraic closure. The objective is to give a bound for k-points in an algebraic set $X \subset \mathbb{P}^n_K$ (or in $\mathbb{A}^n_K$). In what follows we will identify $\mathbb{A}^n_K$ as an open subset in $\mathbb{P}^n_K$ via the homeomorphism $\mathbb{A}^n_K \longrightarrow D(X_0) \subset \mathbb{P}^n_K$ given by $(a_1, \ldots, a_n) \mapsto [1 : a_1 : \cdots : a_n]$.

Definition 4.4. *Let $X \subset \mathbb{P}^n$ be an algebraic set. Let $Z_1, \ldots, Z_m$ be the irreducible components of X. The cumulative degree of X is defined by $deg_c(X) := \sum_{l=1}^{m} deg(Z_l)$. Here, if Z is a variety $deg(Z)$ means the degree of Z (via Hilbert polynomial cf.[6, chapter 1]).*

Remark 9. *We have $deg(X) \leq deg_c(X)$. Indeed, by [6, proposition 7.6-chapter 1] we know that $deg(X_1 \cup X_2) = deg(X_1) + deg(X_2)$ if $\dim(X_1 \cap X_2) < r$ where X_1 and X_2 are algebraic subsets of $\mathbb{P}^n$ and $r = \dim X_1 = \dim X_2$. Furthermore if $\dim X_2 < \dim X_1$ then $deg(X_1 \cup X_2) = deg(X_1)$. Indeed, let $S := K[X_0, \ldots, X_n]$ be the homogeous coordinate ring for $\mathbb{P}^n_K$ and let I_{X_1} and I_{X_2} the associated ideals. Then we have an exact sequence of graded rings:*

$$0 \longrightarrow S/I_{X_1} \cap I_{X_2} \xrightarrow{f \mapsto (f,-f)} S/I_{X_1} \oplus S/I_{X_2} \xrightarrow{(h,g) \mapsto h+g} S/I_{X_1} + I_{X_2} \longrightarrow 0$$

By properties of Hilbert polynomials in exact sequences we have $H_{X_1}(t) + H_{X_2}(t) = H_{X_1 \cup X_2}(t) + H_{X_1 \cap X_2}(t)$. Since $\dim X_i = deg(H_{X_i}(t))$ we obtain $deg(H_{X_1}(t)) = deg(H_{X_1 \cup X_2}(t))$ and so $deg(X_1) = deg(X_1 \cup X_2)$. In particular, if $Z_1, \ldots, Z_m$ are the components of X we have

$$deg(X) = \sum_{\dim Z_k = \dim X} deg(Z_k) \leq deg_c(X).$$

Recall that a subset $X \subset \mathbb{P}^n_K$ is called a locally closed subset if $X = F \cap U$ where F is a closed subset in $\mathbb{P}^n$ and U is a open subset. This is equivalent to the equality: $X = \overline{X} \cap U$ for some open subset in $\mathbb{P}^n_K$. Examples: closed subsets in $\mathbb{A}^n_K$. We define cumulative degree and degree of a locally closed subset X by taking $deg_c(X) := deg_c(\overline{X})$ and $deg(X) := deg(\overline{X})$. Note that $deg(\mathbb{A}^d) = deg(\mathbb{P}^d) = 1$ since that $H_{\mathbb{P}^d}(t) = \frac{t^d}{d!} + \text{terms in degree} < d$.

Proposition 4.4. *Let $X \subset \mathbb{P}^n$ be a locally closed subset.Then,*

- *$deg_c(X) = deg(X)$ if X is a variety.*
- *If X is finite then $deg_c(X) = \#X$.*

- *If X is a variety with $\dim X > 0$ and $H \subset \mathbb{P}^n_K$ is a hypersurface with $X \nsubseteq H$ then $deg(X \cap H) = \sum_k m_k deg(C_k)$ where $C_1, \ldots, C_m$ are the irreducible components of $X \cap H$ and $m_k \in \mathbb{Z}_{\geq 1}$.*

Proof. The first item is trivial. For the second item, it is sufficient to compute the degree of the subset $Z := \{Q\} \subset \mathbb{P}^n_K$. But this is trivial since that $H_Z(t) = 1 \in \mathbb{Q}[t]$ and so $deg(Z) = 0!$(leader coefficient of $H_Z(t)) = 1$. The last item is a version of Bezout theorem and a proof can be found in [6, Hartshorne]. □

Lemma 3. *Let $X \subset \mathbb{P}^n_K$ be a locally closed subset and $\varnothing \neq U \subset X$ open in X. Then $deg_c(U) \leq deg_c(X)$. Furthermore, if U is dense in X then $deg_c(U) = deg_c(X)$*

Proof. Let $U_1, \ldots, U_k$ be the irreducible components of U. Let F_i denote the closure of U_i in X. We will show that $F_1, \ldots, F_k$ are the distint irreducible components of X. Let $X_1, \ldots, X_m$ be the irreducible componenets of X. Suppose that $U \cap X_i \neq \varnothing$ for $i \in \{1, \ldots, s\}$ and $X_i \cap U = \varnothing$ for $i > s$. It suffices to show that $X_i \cap U$ are the irreducible components of U. For $\overline{X_i \cap U} = X_i$.

Indeed, note that since X_i is irreducible we have that the open subset $X_i \cap U$ is dense and irreducible. Thus $X_i \cap U \nsubseteq X_j \cap U$ for $1 \leq i, j \leq s$. Now if $U = U_1 \cup \cdots \cup U_k$ we have $deg_c(U) = \sum_{j=1}^s deg(\overline{\overline{U}_i}) = \sum_{j=1}^s deg(\overline{X_j}) \leq \sum_{j=1}^m deg(\overline{X_j}) = deg_c(X)$. For the last statement observe that if U is dense in X then $X_i \cap U \neq \varnothing$ for all i and so $s = m$.

□

Lemma 4. *If $X \subset \mathbb{P}^n_K$ is locally closed then $deg(X) = deg(\overline{X})$.*

Of course, we have $X = \overline{X} \cap U$ for some open U. So X is an open dense subset in $\overline{X}$. By lemma above we obtain $deg(X) = deg(\overline{X})$.

Theorem 4.8. *Let $X \subset \mathbb{P}^n$ a locally closed subset and $H_1, \ldots, H_m$ hypersurfaces in $\mathbb{P}^n_K$. Then*

$$deg_c(X \cap H_1 \cap \cdots \cap H_m) \leq deg_c(X) \prod_j deg(H_j).$$

Proof. By induction we can suppose that $m = 1$. We can assume that X is a closed subset. Of course we have $X = \overline{X} \cap U$ for some U open subset of $\mathbb{P}^n_K$. So X is open dense in $\overline{X}$ and thus $X \cap H_1$ is open subset of $\overline{X} \cap H_1$. By lemma above we have $deg_c(X \cap H_1) \leq deg_c(\overline{X} \cap H_1)$.

If $X \subset H_1$ then $deg_c(X \cap H_1) = deg_c(X) \leq deg_c(X) deg(H_1)$. Suppose that $X \nsubseteq H_1$ and that X and H_1 are variety. Let $C_1, \ldots, C_l$ the irreducible components of $X \cap H_1$. Then by proposition above we have

$$deg_c(X \cap H_1) = \sum_j deg(C_j) \leq \sum_j m_j deg(C_j) = deg(X) deg(H_1) = deg_c(X) deg(H_1).$$

If $X_1, \cdots, X_j$ are the irreducible components of X note that each irreducible component of $X \cap H_1$ is equal to $X_j \cap H_1$ for some j. In particular

$$deg_c(X \cap H_1) \leq \sum_l deg(X_l \cap H_1) = \sum_l deg(X_l)deg(H_1) = [\sum_l deg(X_l)]deg(H_1) = deg_c(X)deg(H_1).$$

The case H_1 reducible is similar. □

Bezout Inequality. *Let $X \subset \mathbb{A}^n_K$ an affine algebraic subset defined by equations $f_1 = \cdots = f_r = 0$. Suppose that* $\dim X = 0$. *Then $\#X(k) \leq \#X(K) \leq deg(f_1) \cdots deg(f_r)$.*

Proof. By induction is sufficient to consider the case $r = 1$. Denote h the closed subset described by f_1. Let Z be a locally closed subset in $\mathbb{A}^n_K$ and denote H the closure of h in $\mathbb{P}^n_K$. We have $h = H \cap \mathbb{A}^n_K$ and so $Z \cap h$ is an open subset of $Z \cap H$. By lemma above we have $deg_c(Z \cap h) \leq deg_c(Z \cap H)$ and by theorem above $deg_c(Z \cap h) \leq deg_c(Z)deg(H) = deg_c(Z)deg(h)$.

So $deg_c(Z \cap h_1 \cap \cdots \cap h_r) \leq deg_c(Z)deg(h_1) \cdots deg(h_r)$. In particular, if $Z = \mathbb{A}^n_K$ we have

$$\#X(k) \leq \#X(K) \leq deg_c(\mathbb{A}^n_K \cap H_1 \cap \cdots \cap H_r) \leq deg_c(\mathbb{A}^n_K)deg(f_1) \cdots deg(f_r) = deg(f_1) \cdots deg(f_r).$$

□

4.6 Ramification

Let K be a field and v a discrete valuation (always normalizated) of K. We say that K is a local field (with respect to v) if K is complete and k_v, the residue field, is finite. In this section, we give a summary of results on local fields. Details can be found in [9, Milne]. We recall that if v is a discrete valuation in a field K we have an associated discrete valuation ring $\mathcal{O}_v := \{a \in K \mid v(a) \geq 0\}$ with maximal ideal $\mathcal{M}_v := \{a \in \mathcal{O}_v \mid v(a) > 0\}$.

Proposition 4.5. *Let K be a field with discrete valuation v (not necessarily local field). Let $L|K$ be a finite separable extension and denote $\mathcal{O}$ the integral closure of $\mathcal{O}_v$ in L. Then there exists a bijection*

$$\varphi : Spec_m(\mathcal{O}) \longrightarrow \mathbb{P}(L, v)$$

where $\mathbb{P}(L, v) := \{w : L^* \longrightarrow \mathbb{Z} \mid w$ is a discrete valuation normalized in L such that $w|v$ $\}$.

Proof. The map is defined in the following way.

Let $\mathcal{M} \in Spec_m(\mathcal{O})$ and consider the ring $\mathcal{O}_\mathcal{M}$ obtained by localization over $\mathcal{M}$. Note that $\mathcal{O}_\mathcal{M}$ is noetherian ring (the extension is separable), $\dim \mathcal{O}_\mathcal{M} = 1$ and it is integrally closed. In particular it is a local Dedekind domain and so a discrete valuation ring in L. Let $v_\mathcal{M}$ be the associated normalizated discrete valuation. The map is $\varphi : \mathcal{M} \mapsto v_\mathcal{M}$.

We affirm that φ is a bijection. Indeed, let $\mathcal{A}$ be a discrete valuation ring of L with maximal ideal P and $\mathcal{A} \supset \mathcal{O}_v$. Note that $m := P \cap \mathcal{O} \neq 0$. Indeed, let $0 \neq \alpha \in P$. Since $L|K$ is algebraic we have $d\alpha \in \mathcal{O}$ for some $d \in \mathcal{O}_v \setminus \{0\}$. In particular $d\alpha \in m$.

By localization property we obtain the inclusion dominant $\mathcal{A} \supset \mathcal{O}_m$. Since DVR are maximal subrings with respect to relation of domination we obtain $\mathcal{A} = \mathcal{O}_m$. So the map φ is sujective. It is easy to check that φ is injective. □

Let K be a complete field with respect to a valuation v. Let $L|K$ be a separable finite extension and denote $\mathcal{A}$ the integral closure of $\mathcal{O}_v$ in L.

Theorem 4.9. *Notation as above L is a local field and there exists a unique discrete valuation in L that extends the discrete valuation of K.*

Proof. It is a general result that $\mathcal{A}$ is a Dedekind domain. By proposition above we know that $Spec_m(\mathcal{A}) \cong \mathbb{P}(L, v)$. We want to prove that $\#\mathbb{P}(L, v) = 1$. For this suppose $\mathcal{M}_1$ and $\mathcal{M}_2$ are distinct maximal ideals in $\mathcal{A}$. Take $b \in \mathcal{A}$ such that $\mathcal{M}_1 \cap \mathcal{O}_v[b] \neq \mathcal{M}_2 \cap \mathcal{O}_v[b]$. For example, $b \in \mathcal{M}_1 \setminus \mathcal{M}_2$. Let $m_b(T) \in \mathcal{O}_v[T]$ be the minimal polynomial of b. By Hensel lemma, ($\mathcal{O}_v$ is complete!) we know that $\overline{f}(T) \in k_v[T]$ is a power of an irreducible polynomial $f(T) \in k_v[T]$. In particular, $\mathcal{O}_v[b]/\mathcal{M}_v\mathcal{O}_v[b] \cong \mathcal{O}_v[T]/(\mathcal{M}_v, m_b(T)) \cong k_v[T]/(\overline{m_b}(T))$, a local ring with maximal ideal $(f(T))/(\overline{m_b}(T))$. But $\mathcal{M}_1 \cap \mathcal{O}_v[b]/\mathcal{M}_v\mathcal{O}_v[b] \neq \mathcal{M}_2 \cap \mathcal{O}_v[b]/\mathcal{M}_v\mathcal{O}_v[b]$ are maximal ideals in $\mathcal{O}_v[b]/\mathcal{M}_v\mathcal{O}_v[b]$. A contradiction.

We have L complete. Of course, let $r = [L : K]$ and take $\{e_1, \ldots, e_r\}$ a K-basis for L. To give a Cauchy sequence $\{a_n\} \subset L$ is equivalent to give r-Cauchy sequences $\{a_n^{(1)}\}, \ldots, \{a_n^{(r)}\}$ and $\{a_n\}$ is convegent if and only if $\{a_n^{(l)}\}$ is convegent for all l. □

By Dedekind ring theory we know that $[L : K] = ef$ where

$$f = [\mathcal{A}/P : \mathcal{O}_v/\mathcal{M}] \quad \text{and} \quad e = ord_P(t).$$

Here, P is the maximal ideal of $\mathcal{A}$ = the integral closure of $\mathcal{O}_v$ in L and t is a uniformizer for $\mathcal{O}_v$ We say that $L|K$ is an unramified extension if $e = 1$.

Remark 10. *Ramification can be studied in terms of discriminants. More precisely, let $K|L$ be a separable finite extension, where L is a local field with valuation ring $\mathcal{O}_v$, and denote by $\mathcal{A}$ the ring of integers of K. By the primitive element theorem we know that $K = L(\alpha)$ for some $\alpha \in \overline{L}$ integral over $\mathcal{O}_v$. Suppose that $\mathcal{A} = \mathcal{O} \oplus \mathcal{O}\alpha \oplus \cdots \oplus \mathcal{O}\alpha^{n-1}$ i.e. $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ it is a basis for $\mathcal{A}$. Let $m_\alpha(T) \in \mathcal{O}_v[T]$ the associated minimal polynomial. Let $d \in \mathcal{O}_v$ the discriminant of $m_\alpha(T)$, i.e., $d =$ **resultant**$(m_\alpha(T), m'_\alpha(T))$. Then $K|L$ is unramified if and only if $d \in \mathcal{O}_v^*$.*

Theorem 4.10. *Let L be a local field with discrete valuation v and residue field l_v. There is a 1-1 correspondence between*

$$\{ \text{ unramified finite extension of } L\} \longrightarrow \{\text{finite extension of } l_v\}.$$

given by $K \mapsto k_v$.

Proof. (sketch) For surjectivity, let $k|l_v$ a finite extension and take α such that $k = l_v(\alpha)$. Let $m(T) \in \mathcal{O}_v[T]$ a monic polynomial such that $\overline{m}(T) \in l_v[T]$ is a minimal polynomial of α. By Hensel lemma we know that there is some $a \in \mathcal{O}_v$ simple root of $m(T)$ in $\mathcal{O}_v$. Take $K := L(a)$.

Let $K|L$ be an unramified finite extension. By the definition above, we have $k_v|l_v$ a finite separable extension with $[k_v : l_v] = [K : L]$. We affirm that the map $K \mapsto k_v$ induces the bijection above. For injectivity, suppose that K and S are fields that $k_v = s_v$. Then, taking the composite (in $\overline{L}$) we have $K.S$ an unramified extension with residue k_v, [9, Lemma 6.5], and so $[S.K : L] = [k_v : l_v] = [K : L] \Longrightarrow S \subset S.K \subset K$. By a similar argument, we conclude that $K \subset S$ and so $K = S$. □

Chapter 5

Some problems

Here, we list some problems we wish to find a solution:

Problem 1. *Recall the reduction theorem in chapter 2: In order to show the Jacobian Conjecture it is sufficient to consider the maps of degree* ≤ 3*. So, we may ask*

- *Is there an analogue of the reduction theorem for Unimodular Conjecture?*

Problem 2. *Find a prime* $p \in \mathbb{Z}$ *such that* $\mathbb{Z}_p$ *is unimodular.*

In chapter 3 it was seen that for each integer $d \in \mathbb{Z}$ there exists a finite extension $K|\mathbb{Q}_p$ such that $\mathcal{O}_K$ is d-unimodular. This motivates the following

Problem 3. *Given a prime* $p \in \mathbb{Z}$ *find (or show that this is impossible) a finite extension* $K|\mathbb{Q}_p$ *such that* $\mathcal{O}_K$ *is a unimodular domain.*

The following problem is equivalent to the Jacobian Conjecture [1]

Problem 4. *Let* $F \in \mathcal{MP}_n(\mathbb{Z})$ *a Keller map. Let* $\mathcal{O}$ *be the integral closure of* $\mathbb{Z}$ *in* $\overline{\mathbb{Q}}$*. Then,* $F \otimes \mathcal{O}$ *is injective.*

We can compare the problem above with the following

Theorem 5.1. *Let* $F \in \mathcal{MP}_n(\mathbb{Z})$ *be a Keller map. Suppose that* $F \otimes \overline{\mathbb{Q}}$ *is injective. Then* F *is an isomophism.*

The proof of this theorem uses Cynk-Rusek theorem of chapter 1.

Problem 5. *In theorem 3.17, what can be said about* $\#E$*?*

[1] indeed, the theorem of Connell-van den Dries in chapter 1 is more general: Let $P \in Spec(\mathcal{O})$ and consider $\mathcal{A} := \mathcal{O}_P$ localization over P. If the Jacobian Conjecture over $\mathbb{C}$ is false then there is a Keller map $F \in \mathcal{MP}_n(\mathbb{Z})^{(0)}$, counterexemple, and such that for all $d \in \mathcal{A} - \mathcal{A}^*$ we have a Keller injective ${}^dF \in \mathcal{MP}_n(\mathcal{A})$. Here, $({}^dF)_l := F_{1l} + dF_{2l} + \cdots + d^{deg(F_l)-1}F_{deg(F_l)l}$ where $F = (F_1, \ldots, F_n)$.

Bibliography

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. 1, 2, 3.1, 3.1, 3.5

[2] Hyman Bass, Edwin H. Connell, and David Wright. The Jacobian conjecture: reduction of degree and formal expansion of the inverse. *Bull. Amer. Math. Soc. (N.S.)*, 7(2):287–330, 1982. 1

[3] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra. 1.2

[4] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR 4-1-0 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de, 2016. 4

[5] Marvin J. Greenberg. *Lectures on forms in many variables*. W. A. Benjamin, Inc., New York-Amsterdam, 1969. 3.1

[6] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. 4.4, 9, 4.5

[7] Birger Iversen. *Generic local structure of the morphisms in commutative algebra*. Lecture Notes in Mathematics, Vol. 310. Springer-Verlag, Berlin-New York, 1973. 4.2

[8] James S Milne. Algebraic geometry. *available from his website*, 2017. (document), 4.3, 4.4

[9] James S Milne. Algebraic number theory. *available from his website*, 2017. 4.6, 4.6

[10] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, expanded edition, 1999. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello. 4.4

[11] Arno van den Essen. *Polynomial automorphisms and the Jacobian conjecture*, volume 190 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2000. 3.5, 3.5

[12] Arno van den Essen and Richard J. Lipton. A p-adic approach to the Jacobian Conjecture. *J. Pure Appl. Algebra*, 219(7):2624–2628, 2015. (document), 3, 3, 4, 3.4