Arithmetic aspects of polynomial maps

Wodson Mendson

August 15, 2024

Abstract. The Jacobian conjecture is a well-known open problem in affine algebraic geometry that asks if any polynomial endomorphism of the affine space $\mathbb{A}^n_{\mathbb{C}}$ $(n \geq 2)$ with jacobian 1 is an automorphism. We present a survey about some results around this conjecture and we discuss an arithmetic aspect of this conjecture due to Essen-Lipton. We investigate some cases of this arithmetic approach showing the close relationship between the Jacobian Conjecture and the problem of counting $\mathbb{F}_p$-points of an affine scheme.

Contents

1 Introduction

Let k be an algebraically closed field of characteristic zero. The Jacobian Conjecture over k is a classical problem in affine algebraic geometry. It was first formulated by Ott-Heinrich Keller in 1939 and asks whether a polynomial endomorphism ψ of the n-dimensional affine space $\mathbb{A}^n_{\mathrm{k}} = \mathbf{Spec}(\mathrm{k}[x_1, \ldots, x_n])$ with

$$\det((\frac{\partial \psi^*(x_i)}{\partial x_j})_{1 \leq i,j \leq n}) = 1$$

is an automorphism, that is, there is a polynomial endomorphism $\gamma : \mathbb{A}^n_{\mathrm{k}} \longrightarrow \mathbb{A}^n_{\mathrm{k}}$ such that

$$\gamma \circ \psi = id_{\mathbb{A}^n_{\mathrm{k}}} = \psi \circ \gamma.$$

In [2], H. Bass, E. H. Connell, and D. Wright showed that to prove the Jacobian Conjecture it is enough to prove it for endomorphism in the form $\psi = X + H = (x_1 + h_1, \dots, x_n + h_n)$, where h_i is homogeneous of degree 3 for every i with the Jacobian matrix of $H = (h_1, \dots, h_n)$ nilpotent. A refinement, due to Essen-Bondt, ensures that it is sufficient to consider maps in the form $F = X + H$ with $H = (h_1, \dots, h_n)$ homogeneous, $\deg(H) = 3$ with H having jacobian matrix nilpotent **symmetric** (see [4, Theorem 1.1]).

An interesting arithmetical approach to the Jacobian Conjecture was explored on [13]. In that paper, it is proved that the Jacobian Conjecture is related, in some sense, to a problem about counting $\mathbb{F}_p$-rational point of an affine scheme. To explain, let us consider the basic example: let R be a local domain with maximal ideal $\mathbf{m}$ and residue field k. Let $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ be homogeneous of degree one. Assume the Jacobian matrix associated with $f_1, \dots, f_n$ is invertible. Denote this Jacobian matrix by J. Let $M \in \mathcal{M}_n(R)$ be the matrix such that $JM = MJ = 1$. The relation $M \cdot J = id$ implies that there exist $u_1, \dots, u_n \in R$ such that $f_1(u_1, \dots, u_n) = 1$. In particular, since $\overline{f}(\overline{u}_1, \dots, \overline{u}_n) \neq 0$ the induced polynomial map

$$f = (f_1, \dots, f_n) \colon \mathbb{A}^n_R \longrightarrow \mathbb{A}^n_R$$

induces a polynomial map:$\overline{f} = f \otimes R/\mathfrak{m} \colon \mathbb{A}^n_{\mathrm{k}} \longrightarrow \mathbb{A}^n_{\mathrm{k}}$ that is non-zero. For degrees bigger than 1 we have the following conjecture formulated by Essen-Lipton (see [13]).

Unimodular Conjecture. *Let R be a local domain of characteristic zero with maximal ideal* $\mathbf{m}$ *and residue field* k. *Then, for every $n \in \mathbb{Z}_{>2}$ and polynomial map*

$$F = (f_1, \dots, f_n) : \mathbb{A}^n_R \longrightarrow \mathbb{A}^n_R$$

the induced polynomial map obtained by the reduction modulo $\mathfrak{m}$

$$f = (\overline{f_1}, \dots, \overline{f_n}) \colon \mathbb{A}^n_{\mathrm{k}} \longrightarrow \mathbb{A}^n_{\mathrm{k}}$$

is non-zero.

A simple fact is that if k is an infinite field then R satisfies the Unimodular Conjeture (see Proposition 4). When k is finite we get the following reformulation regarding rational points.

Unimodular Conjecture II. *Let R be local domain of characteristic zero with maximal ideal* $\mathbf{m}$ *and finite residue field* k. *Let $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ be polynomials and consider the affine scheme $X =$ **Spec**(A) where $A = R[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$. Denote by $\overline{X}$ the affine scheme **Spec**$(A \otimes k)$ obtained by the reduction modulo* $\mathbf{m}$. *Then, if the Jacobian matrix of $f_1, \dots, f_n$ has determinant invertible then*

$$\#\overline{X}(k) < \#k^n$$

where $\overline{X}(k)$ denotes the set of k-rational points of the scheme $\overline{X}$. Here, $\#k^n$ denotes the number of elements of k^n

Motivated by the Unimodular Conjecture II we define the classes of d-**unimodular domains** and **invariant domains** and we explore conditions where the Unimodular Conjecture II is true. A local domain $(R, \mathfrak{m}, \mathrm{k})$, with k finite, is called d-unimodular if given $f_1, \ldots, f_n \in R[x_1, \ldots, x_n]$ with jacobian 1 and $\deg(f_i) \leq d$ **for some** i we have $\#X(k) < \#\mathrm{k}^n$. In direction, we prove the following:

Theorem A. *Let R be a local domain with maximal ideal $\mathbf{m}$ and finite eresidue field k. Let $f \in \mathcal{MP}_n(R)$ be a polynomial map with jacobian 1. Then, f is $(\#k-1)$ unimodular.*

The interesting fact is that the Unimodular Conjecture is related to the Jacobian Conjecture([13, Theorem 6]):

Theorem 1. *The p-adic integer ring $\mathbb{Z}_p$ does satisfy the Unimodular Conjecture for **almost all primes** p if and only if the Jacobian Conjecture is true.*

We recall that "**almost all primes** p" means all primes of $\mathbb{Z}$ except a finite number. The curious fact is that there is no known example of a prime p such that $\mathbb{Z}_p$ satisfies the **Unimodular Conjecture II**. In this direction, naturally appears the problem:

Problem 1. *Find a unimodular prime $p \in \mathbb{Z}$.*

The Problem 1 above motivates the following question:

Problem 2. *In the statement of the Unimodular Conjecture, can we replace "**almost all primes** p", with "**infinitely many primes** p", or "**a prime** p"?*

We present some results in this direction. In particular, we prove that we can replace "**almost all primes** p", with "**a prime** p" (see Theorem 11) and so that the Jacobian Conjecture is equivalent to finding a prime p such that $\mathbb{Z}_p$ is unimodular. We introduce the notion of Keller-finite domains and establish the following improvement of the Essen-Lipton Theorem using this notion.

Theorem 2. *Let p be a prime number. The Jacobian Conjecture is equivalent to the unimodularity of $\mathbb{Z}_p$.*

To prove the theorem above we will define and explore the notion of Keller-finite domains and we will prove that every complete discrete valuation ring is Keller-finite (see Theorem 11).

1.1 Organization of the paper

In Section 2 we fix the notations that will be used in the paper. In Section 3 we survey the main properties of polynomial maps defined over domains. In Section 4 we define the unimodular and invariant domains and explore some properties. In the last section, we define the notion of Keller-finite domains and we prove that every complete discrete valuation ring is a Keller-finite domain. We use this fact to give a new proof of the Essen-Lipton theorem.

2 Notation

- R = domain
- $\overline{\mathrm{k}}$ = an algebraic closure of a field k
- $\langle a_1,\dots,a_n\rangle$ = ideal generated by $a_1,\dots,a_n \in R$
- $\mathcal{Z}(f_1,\dots,f_r)$ = affine scheme/algebric set given by polynomials $f_1,\dots,f_r$
- given $a = (a_1,\dots,a_n)$ and $b = (b_1,\dots,b_n)$ in R^n: $\langle a-b\rangle = \langle a_1-b_1,\dots,a_n-b_n\rangle \subset R$
- $(R,\mathfrak{m},\mathrm{k})$ = local domain with maximal ideal $\mathfrak{m}$ and residue field k
- $\mathcal{MP}_n(R)$ = polynomial maps over R = collection of $(f_1,\dots,f_n)$ with $f_i \in R[x_1,\dots,x_n]$
- $\mathbf{Aut}(R)$ = the collection of invertible polynomial maps over R
- J_f = the Jacobian matrix associated to a polynomial map $(f_1,\dots,f_n)$
- $\mathbb{Z}_p$ = the p-adic ring = the completion of $\mathbb{Z}$ at the maximal ideal $p\mathbb{Z}$
- $\mathbb{Q}_p$ = the fraction field of $\mathbb{Z}_p$
- If S is a finite set, $\#S$ = number of elements of S
- If $f,g \in \mathcal{MP}_n(R)$ then $f\circ g$ denotes the composition $(f_1(g_1,\dots,g_n),\dots,f_n(g_1,\dots,g_n))$

3 Polynomial maps

In this section, we survey some properties of polynomial maps and present an introduction to the Jacobian Conjecture. Complete proofs can be found [12].

Let R be a domain. In this paper, by a polynomial map over R we mean a n-tuple of polynomial $f = (f_1,\dots,f_n)$ with $f_i \in R[x_1,\dots,x_n]$. We denote by $\mathcal{MP}_n(R)$ the collection of polynomial maps over R. We have an identification $\mathcal{MP}_n(R) \cong R[x_1,\dots,x_n]^n$. If $f = (f_1,\dots,f_n) \in \mathcal{MP}_n(R)$ is a polynomial map, we say that f is **Keller map** if the jacobian matrix of f:

$$J_f = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_{n-1}} & \frac{\partial f_1}{\partial x_n} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_{n-1}} & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

is invertible. This is equivalent to say that $\det J_F \in R[x_1,\dots,x_n]^* = R^*$. We say that f **has jacobian** 1 if $\det J_f = 1$. Given $f \in \mathcal{MP}_n(R)$ we say that f is invertible if there is $g \in \mathcal{MP}(R)$ such that $f\circ g = id = g\circ f$, where id is the polynomial map $f = (x_1,\dots,x_n)$. By simple derivation it follows that if f is invertible then $\det J_f \in R[x_1,\dots,x_n]^* = R^*$ and by normalization we can assume $\det J_f = 1$.

The Jacobian Conjecture asks for the converse when $R = \mathbb{C}$.

Jacobian Conjecture. *Any polynomial map* $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(\mathbb{C})$ *with jacobian* 1 *is an invertible polynomial map.*

When R has characteristic $p > 0$ the analog statement is false. We have polynomial maps of the form: $f = (x_1^p - x_1, \dots, x_n^n - x_n) \in \mathcal{MP}_n(\mathbb{F}_p)$. Then, f is not invertible, since is not injective.

Definition 1. *Let* $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(R)$ *be a polynomial map. The* ***degree of*** f *is the integer:*

$$\deg(f) := \boldsymbol{Max}\{\deg(f_1), \dots, \deg(f_n)\}.$$

In the paper **The Jacobian Conjecture: Reduction of degree and formal expansion of the inverse**, Hyman Bass, Edwin H. Connell and David Wright explored the conjecture and proved, in particular, that the Jacobian Conjecture is equivalent to the following conjecture (see [2, Corollary 2.2]).

Conjecture. *Any polynomial map* $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(\mathbb{C})$ *with jacobian* 1 ***and*** $\deg(f) \leq 3$ *is invertible.*

In the [2, Corollary 2.2] it is proved more: we can take $f = (x_1 + h_1, \dots, x_n + h_n)$, where the jacobian matrix of $h = (h_1, \dots, h_n)$ is nilpotent and $\deg(h_i) \leq 3$ for every i.

We denote by $\mathbf{Aut}_n(R)$ the group of polynomial maps that are invertible. If $f \in \mathcal{MP}_n(R)$ and $R \subset S$ for some domain S, we can look f as polynomial map over S. We denote this map by $f \otimes S$, obtained by scalar extension.

We recall some facts about polynomial maps.

Proposition 1. *Let* $f \in \mathcal{MP}_n(R)$ *and* S *be a domain with* $R \subset S$. *Then*

$$f \otimes S \in \boldsymbol{Aut}(S) \Longleftrightarrow f \in \boldsymbol{Aut}(R).$$

Proof. see [12, Lemma 1.1.8]

□

Theorem 3. ***(Cynk-Rusek)*** *Fix an algebraically closed field* k *of characteristic* $p \geq 0$. *Let* $X \subset \mathbb{A}_{\mathrm{k}}^n$ *be an affine variety and* $f\colon X \longrightarrow X$ *a regular map. The following conditions are equivalent:*

(i) f *is injective;*
(ii) f *is a bijection;*
(iii) f *is an automorphism.*

Proof. See [3, Theorem 2.2],[12, Theorem 4.2.1] or [10, Theorem 3.1] for more details. We will give proof of the implication $(i) \Longrightarrow (ii)$. Suppose by contradiction that there is a non-surjective and injective polynomial map $f\colon X \longrightarrow X$.

Step 1: Formulate the conditions of non-surjectivity, injectivity, and membership using polynomial equations.

Step 2: Let $\{\alpha_i\}_{i \in I}$ the list of coefficients that appear on the equations of Step 1 and consider the cases:

- **char**(k) = $p > 0$: Let $R = \mathbb{F}_p[\{\alpha_i\}_{i\in I}]$ the $\mathbb{F}_p$-algebra obtained by adjuntion of the all coefficients $\{\alpha_i\}_{i\in I}$. Take $\mathfrak{m} \in \mathbf{Spm}(R)$ a maximal ideal of R. By the Nullstellensatz we conclude that $R/\mathfrak{m}$ is a finite extension of $\mathbb{F}_p$. So, by reducing the polynomial relation above we get a polynomial map

$$f \otimes R/\mathfrak{m} \colon \overline{X}(R/\mathfrak{m}) \longrightarrow \overline{X}(R/\mathfrak{m})$$

that is injective and not surjective. But, this is a contraction since $\#X(R/\mathfrak{m})$ is a finite set.

- **char**(k) = 0: Let $R = \mathbb{Z}[\{\alpha_i\}]$ be the subring of k generated by the coefficients $\{\alpha_i\}_{i\in I}$. Let $\mathfrak{m} \in \mathbf{Spm}(R)$ be a maximal ideal of R. Since $R/\mathfrak{m}$ is a finite field (see [11, Lemma 00GC]) we reduce this case to the first case where **char**(k) > 0.

□

Proposition 2. *Let* k *be an algebraically closed field with* $2 \nmid$ ***char***(k)*. Then any polynomial map* $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(\mathrm{k})$ *of degree* $d \in \{1, 2\}$ *with jacobian* 1 *is invertible.*

Proof. If $d = 1$ we can assume by a translation that f_i is homogeneous of degree 1 for every i. So, by linear algebra, f is invertible if and only the Jacobian matrix is invertible. Now, assume $d = 2$. We follow the argument in [2]. By the Theorem 3 it is sufficient to show that f is injective. Suppose, by contradiction, that f is not injective. We can assume that $(0, \dots, 0) = f(0, \dots, 0) = f(h_1, \dots, h_n)$ for some $h \in \mathbb{C}^n$ non-zero. Take $c = 1/2$ and write $f = f_1 + f_2$ the homogeneous decomposition of f. Note that

$$0 = f_1(h) + 2 \cdot c \cdot f_2(h) = \frac{\partial[Tf_1(h) + T^2 f_2(h)]}{\partial T}|_{T=c} = \frac{\partial f(Th)}{\partial T}|_{T=c} = J_f(c \cdot h) \cdot h$$

a contradiction with the jacobian condition: $\det J_f = 1$. □

Lemma 1. *Let* $\alpha_1, ..., \alpha_n \in \overline{\mathbb{Q}}$. *Then for almost all primes* $p \in \mathbb{Z}$ *there is an injection of rings*

$$\phi_p \colon \mathbb{Z}[\alpha_1, ..., \alpha_n] \hookrightarrow \mathbb{Z}_p.$$

Proof. See [12, Theorem 10.3.1] □

Hensel's Lemma. *Let* $(R, \mathfrak{m}, k)$ *be a complete discrete valuation ring and* $f_1, \dots, f_n \in R[x_1, \dots, x_n]$. *Suppose that there is* $\alpha = (\alpha_1, \dots, \alpha_n) \in R^n$ *such that*

$$f_1(\alpha_1, \dots, \alpha_n) \equiv \cdots \equiv f_n(\alpha_1, \dots, \alpha_n) \equiv 0 \mod \mathfrak{m}^{2m+1}$$

where m *is the integer such that* $\det J_f(\alpha) \in \mathfrak{m}^m - \mathfrak{m}^{m+1}$. *Then there is a unique* $\beta = (\beta_1, \dots, \beta_n) \in R^n$ *such that* $f_1(\beta) = \cdots = f_n(\beta) = 0$ *and* $\beta_i \equiv \alpha_i \mod \mathfrak{m}^{m+1}$ *for all* $i = 1, \dots, n$.

Proof. See [6, proposition 5.20]. □

By Hensel's lemma, we get the following

Proposition 3. *Let $(R, \mathfrak{m}, \mathrm{k})$ be a complete discrete valuation ring and let $f = (f_1, \dots, f_n)$ be a Keller map over R. If A is an R-algebra denote by $X(A)$ the set of A-points of the affine scheme $\textbf{\textit{Spec}}(R[x_1, \dots, x_n]/\langle f_1, \dots, f_n\rangle)$. Then there is a bijection $X(R) \cong X(k)$.*

Proof. As f is Keller map we have $Jf(u)$ invertible matrix for every $u = (u_1, \dots, u_n) \in R^n$. The bijection is natural: given $u \in R^n$ we define $\varphi(u) \in X(k)$ the k-point obtained by reduction modulo $\mathfrak{m}$. The Hensel Lemma implies that the projection map $\pi \colon X(R) \longrightarrow X(k)$ is a bijection: injectivity by the uniqueness and surjectivity by lifting points. □

4 Unimodular and invariant domains

Let $(R, \mathfrak{m}, \mathrm{k})$ be a local ring. Given a polynomial map $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(R)$ we denote by $\overline{f} = f \otimes \mathrm{k} \in \mathcal{MP}_n(\mathrm{k})$ the induced map over the residue field k via reduction modulo $\mathfrak{m}$.

Definition 2. *We say that R is a* ***unimodular domain*** *if the following holds:*

- *given $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ with jacobian 1 consider the scheme:*

$$X = \textbf{\textit{Spec}}(R[x_1, \dots, x_n]/\langle f_1, \dots, f_n\rangle)$$

  Then $X(\mathrm{k}) \neq \mathbb{A}^n_{\mathrm{k}}$.

We say that a polynomial map $f \in \mathcal{MP}_n(R)$ is ***unimodular*** *if it satisfies the condition above.*

Remark 1. *If $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(R)$ is Keller polynomial map with $c = \det J_f \in R^*$ then $g = (c^{-1} f_1, f_2, \dots, f_n)$ is a Keller map with jacobian 1. In particular, if $(R, \mathfrak{m}, \mathrm{k})$ is an unimodular domain then any Keller polynomial map is a unimodular map.*

Remark 2. *If R is a complete discrete valuation ring with finite residue field then the unimodularity condition is equivalent to $\# X(R) < \# \mathrm{k}^n$. Indeed, by the Proposition 3 we know that $X(R) = X(\mathrm{k})$. In particular, $\# X(R) = \# X(\mathrm{k})$.*

Proposition 4. *Let $(R, \mathfrak{m}, \mathrm{k})$ be a local domain with* k *an infinite field. Then R is an unimodular domain.*

Proof. Let $f \in \mathcal{MP}_n(R)$ be a Keller map. Let $\overline{f} = f \otimes \mathrm{k} \in \mathcal{MP}_n(\mathrm{k})$ be the induced map over the residue field and suppose that $f(\alpha) = 0$ for all $\alpha \in \mathrm{k}^n$. Since k is infinite we have $\overline{f} \equiv 0$. In particular, the coefficients in f are in the maximal ideal $\mathfrak{m}$. In particular, $\det Jf \in \mathfrak{m}[x_1, \dots, x_n]$, a contradiction by jacobian condition: $\det J_f \in R^*$. □

We recall the following proposition (see [13, Proposition 8]).

Proposition 5. *Suppose that the Jacobian Conjecture is true. Then every local domain R of characteristic zero is unimodular.*

Proof. Let $f \in \mathcal{MP}_n(R)$ be a Keller map defined over a local domain R of characteristic zero. Since we assume the Jacobian Conjecture is true over $\mathbb{C}$ we have f an invertible map over R (see [12, lemma 1.1.14]. In particular, there is $g \in \mathcal{MP}_n(R)$ such that $f \circ g = x = (x_1, \dots, x_n)$. By the reduction modulo $\mathfrak{m}$ we conclude that the map $\overline{f} \in \mathcal{MP}_n(\mathrm{k})$ is a bijection, in particular, a non-zero map. □

The Unimodular Conjecture is false for local domains of characteristic $p > 0$ and finite residue field.

Example 1. *Consider the local domain* $(\mathbb{F}_p[[t]], t\mathbb{F}_p[[t]], \mathbb{F}_p)$ *and take the polynomial map* $f = (x_1 - x_1^p, \dots, x_n - x_n^p) \in \mathcal{MP}_n(\mathbb{F}_p[[t]])$. *Note that* f *is a Keller map but the induced map over the residue field is the zero map because* $\alpha^p = \alpha$ *for every* $\alpha \in \mathbb{F}_p$.

Remark 3. *Let* $(R, \mathfrak{m}, \mathrm{k})$ *be a local domain. The following table shows the complete set of relations between* ***char***(R) *and* ***char***(k).

char(R)	***char***(k)	$\#\mathrm{k}$	***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*

4.1 Invariance and unimodularity

Now we will study when the unimodularity of a polynomial map is preserved when we make operations and composition with the map.

Definition 3. *Let* R *be a local domain with of characteristic zero and* $f \in \mathcal{MP}_n(R)$ *be a unimodular map. We say that* f *is an* ***invariant map*** *if it satisfies the following:*

- *Let* $a \in R^n$ *and* $g \in \mathcal{MP}_n(R)$ *be a* ***Keller affine automorphism****, that is,* $g = AX + b$ *with*

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1(n-1)} & a_{1n} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{n(n-1)} & a_{nn} \end{bmatrix}$$

  having $\det A = 1$ *and* $b = (b_1, \dots, b_n)$. *Then* $f \circ g \circ f$ *and* $f - f(a) = (f_1 - f_1(a), \dots, f_n - f_n(a))$ *are unimodular maps for every* $a \in R^n$.

Note that in the Definition 3 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 any Keller unimodular map is an invariant map.

Proposition 6. *Let* R *be a local unimodular domain. Then* R *is invariant.*

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

Definition 4. *Let R be a local domain. Given a map $f \in \mathcal{MP}_n(R)$ we say that*

- *f is **strongly invariant** if it is invariant and for all **Keller affine automorphisms** $g_1, \dots, g_k \in \mathcal{MP}_n(R)$ 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 R is called an **invariant domain** if every unimodular polynomial map (in dimension $n > 1$) is invariant.*

Lemma 2. *If a map $f \in \mathcal{MP}_n(R)$ is strongly invariant then $f \circ g \circ f$ is strongly invariant for all Keller affine automorphism $g \in \mathcal{MP}_n(R)$.*

Proof. Indeed, by induction, it is sufficient to consider the case $k = 2$. For this, let $g_1, g_2 \in \mathcal{MP}_n(R)$ be a Keller affine automorphism and observe 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. □

The next example shows that the condition $\mathbf{char}(R) = 0$ is important.

Example 2. *Let $f_1, \dots, f_n \in \mathbb{F}_p[[t]][x_1, \dots, x_n]$ be defined by $f_j = 1 - x_j^p + x_j$ and consider the polynomial map $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(\mathbb{F}_p[[t]])$. It is easy to check that $\det J_f = 1$ and that f is an unimodular map. But,*

$$f - f(1, \dots, 1) = (-x_1^p + x_1, \dots, -x_n^p + x_n).$$

So, in the case $R = \mathbb{F}_p[[t]]$ it follows that the property of invariance by translation is false.

Example 3. *Let $g(x) \in \mathbb{F}_p[x]$ be a polynomial that maps $\{0, \dots, p-2\} \mapsto p-1$ and $p-1 \mapsto 0$. For example, take $p = 5$ and consider*

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

It is easy to check that $g \circ g = 0$. Note that $g(0) \neq 0$. Define the polynomial map $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(\mathbb{F}_p[[t]])$ 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 similar to the argument given in [13, Theorem 4] with the observation that it is sufficient to require the invariance property.

Theorem 4. *Let $(R, \mathfrak{m}, \mathrm{k})$ be a complete discrete valuation ring with finite residue field k. Let $f \in \mathcal{MP}_n(R)$ be a strongly invariant map. Then f is injective.*

Proof. Suppose, by contradiction that there is a a strongly invariant polynomial map $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(R)$ with $f(a_1) = \cdots = f(a_m) = c$ $(m > 1)$ for some $a_1, \dots, a_m \in R^n$ 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 $\widetilde{g} \in \mathcal{MP}_n(R)$ with $\#\widetilde{g}^{-1}(c) > (\#k)^n$ a contradiction by Proposition 3.

Since $f(a_1) = f(a_2)$ we have $\langle a_2 - a_1 \rangle = R$ by the [12, Lemma 10.3.11]). On the other hand, since f is an invariant map we guarantee that there exists $b \in R^n$ such that $f(b) - f(a_1)$ is unimodular, that is, $\langle f(b) - f(a_1 \rangle = R$. In particular, $\langle a_2 - a_1 \rangle = \langle f(b) - f(a_1) \rangle = \langle f(b) - c \rangle = R$. So, we have $\{a_2, a_1\} \cong \{f(b), c\}$ (see [13, Transitivity, Proposition 1]). By [13, Theorem 2] we know that there is $h \in \mathcal{MP}_n(R)$, Keller affine automorphism such that $h(c) = a_1$ and $h(f(b)) = a_2$. Now define $g = f \circ h \circ f$. Then the map g is strongly invariant map with $g(a_j) = f(h(c)) = f(a_1) = c$ for all j and $h(b) = f(h(f(b))) = f(a_2) = c$. Note that $b \neq a_j$ for all j. □

As a consequence, we get the following result.

Corollary. *Let $(R, \mathfrak{m}, \mathrm{k})$ be a complete discrete valuation ring with a finite residue field k. Suppose that R is an invariant domain. Then any unimodular Keller polynomial map $f \in \mathcal{MP}_n(R)$ is an injective map.*

Definition 5. *Pick $d \in \mathbb{Z}_{\geq 1}$ and let $(R, \mathfrak{m}, \mathrm{k})$ be a local domain. We say that R is a d-unimodular map if any Keller map $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(R)$ with $\deg(f_i) \leq d$, **for some** i, is unimodular.*

Note that any local domain R is 1-unimodular and R is a unimodular domain if and only if it is d-unimodular for all $d \in \mathbb{N}$. If R is d-unimodular then it is e-unimodular for all $e \leq d$.

If R has characteristic $p > 0$ and k is finite then R is not d-unimodular for infinitely many $d \in \mathbb{Z}$. Indeed, for each $m \in \mathbb{N}$ take $d = (\#k)^m$ and consider the map $f = (x_1 - x_1^d, \dots, x_n - x_n^d) \in \mathcal{MP}_n(R)$.

Proposition 7. *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 $f_1(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n] \setminus \mathbb{Z}$. 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 $p \nmid f_1(d)$. □

It is known that to prove the Jacobian Conjecture it is sufficient to consider polynomial maps of Druzkowski type, that is, maps in the form $f = x+h$ with $h_j = (\sum_k a_{kj} x_k)^3$ and Jh nilpotent (see [12, Theorem 6.3.2]). We call maps of the form $f = x+h$ with $h = \sum_k a_{kj} x_k^3$ quasi-Druzkowski maps.

Proposition 8. *Quasi-Druzkowski maps are unimodular over $\mathbb{Z}_p$.*

Proof. Let f be a quasi-Druzkowski map with $h = (h_1, \dots, h_n)$ where $h_j = \sum_k b_{kj} x_k^3$. We will show that there exist $u_1, \dots, u_n \in \mathbb{Z}_p$ non-zero such that

$$u_1 h_1(x_1, \dots, x_n) + \dots + u_n h_n(x_1, \dots, x_n) = 0.$$

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 $(u_1,\dots,u_n)\in\mathbb{Q}_p^n$ 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, $(1,p,\dots,p)\in\mathbb{Z}_p^n$ is such that $(f_1(1,p,\dots,p),\dots,f_n(1,p,\dots,p))=\mathbb{Z}_p$. □

Remark 4. *It was seen in the previous section that there are local domains $(\mathcal{O},\mathcal{M},k)$ with characteristic $p>0$ that are not unimodular domains. On the other hand, we know that any local domain with an infinite residue field is indeed an unimodular domain. In particular, if we consider the map $f=(x_1-x_1^p,\dots,x_n-x_n^p)$ over $(\overline{\mathbb{F}}_p[[T]],T\overline{\mathbb{F}}_p[[T]],\overline{\mathbb{F}}_p)$ we have $\overline{F}(\alpha)\neq0$ for some $\alpha\in\overline{\mathbb{F}}_p$. 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 analog:

Theorem 5. *Let $f\in\mathcal{MP}_n(\mathbb{Z}_p)$ be a Keller polynomial map. Then there is a complete discrete valuation ring $(\mathcal{O},\mathcal{M},\mathrm{k})$ 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 $\boldsymbol{rank}_{\mathbb{Z}_p}(\mathcal{O})=[\mathrm{k}:\mathbb{F}_p]$.*

Proof. 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 $\overline{f}(\alpha)\neq0$. By taking the field $\mathrm{k}=\mathbb{F}_p(\alpha_1,\dots,\alpha_n)$ obtained by adjunction we can look $\overline{f}$ as a polynomial map which is **non zero** over k. Now we recall the following theorem about unramified extensions of a local field L ([8, Proposition 7.50])

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

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

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 $\mathrm{k}|\mathbb{F}_p$ 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 [1, Proposition 5.17]) we know that $\mathcal{O}$ is a free $\mathbb{Z}_p$-module and $rank_{\mathbb{Z}_p}(\mathcal{O})=[K:\mathbb{Q}_p]=[\mathrm{k}:\mathbb{F}_p]$. So $f\otimes\mathcal{O}\in\mathcal{MP}_n(\mathcal{O})$ is a Keller map with a non-zero induced map over the residue field. □

Lemma 3. *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 [12, A Galois descent] works. The relevant fact is that $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of $\mathbf{rank}_{\mathbb{Z}_p}(\mathcal{O}_K) = m$. □

By Theorem 4 we know that if $\mathbb{Z}_p$ is an unimodular domain then any Keller map $f \in \mathcal{MP}_n(\mathbb{Z}_p)$ is injective. We can show a more general result

Theorem 6. *Assume that $\mathbb{Z}_p$ is an 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.*

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 $\alpha \neq \beta \in \mathcal{O}^n$ are such that $f(\alpha) = f(\beta)$ consider the ring $R = \mathbb{Z}_p[\alpha, \beta]$ obtained by adjunction of α and β and let K the fraction field of R. The extension $K|\mathbb{Q}_p$ is finite and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in K$. 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 $\mathcal{O}_K$ and non-injective. By the Lemma 3, we get $g \in \mathcal{MP}_N(\mathbb{Z}_p)$ a Keller unimodular map non-injective, for some $N \in \mathbb{N}$. Now, since we are assuming that $\mathbb{Z}_p$ is an invariant domain and by Theorem 4 we know that g is an injective map. A contradiction. □

4.2 $\mathbb{F}_p$-points of hypersurfaces and unimodularity

We start this subsection by reminding the following result about $\mathbb{F}_p$-points of affine hypersurfaces in the affine space $\mathbb{A}^n_{\overline{\mathbb{F}}_p}$ (see [5, Corollary 2.7])

Theorem 7. *Let $X = \mathcal{Z}(f) \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$ be an affine irreducible hypersurface. Consider the set of $\mathbb{F}^n$-points of X, that is,*

$$X(\mathbb{F}_p) = \{(\alpha_1, \dots, \alpha_n) \in \mathbb{A}^n_{\overline{\mathbb{F}}_p} \mid f(\alpha_1, \dots, \alpha_n) = 0\} \cap \mathbb{F}_p^n.$$

Then $\#X(\mathbb{F}_p) \leq \deg(f) p^{n-1}$.

Using this result we can easily proof that the p-adic ring $\mathbb{Z}_p$ is $(p-1)$-unimodular.

Proposition 9. *Let $(R, \mathfrak{m}, \mathrm{k})$ be a complete discrete valuation ring with residue field k finite. Then, any Keller polynomial map $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(R)$ is $(\#\,\mathrm{k}-1)$-unimodular if $\deg(f_i) < \#k$, for some i.*

Proof. Let X be the scheme defined by the equations $f_1, \dots, f_n$. First, consider the algebraic set $\overline{X} = \{(x_1, \dots, x_n) \in \mathbb{A}^n_{\overline{\mathbb{F}}_p} \mid \overline{f}_1(x) = \cdots = \overline{f}_n(x) = 0\}$. Note that the hypersurface $\mathcal{Z}(f_i) \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$ contains $\overline{X}$. In particular, $\#\overline{X}(\mathbb{F}_p) \leq \#\mathcal{Z}(f_i)(\mathrm{k}) \leq \deg(f_i)\#\,\mathrm{k}^{n-1}$. Now, by the Proposition 3 we conclude that

$$\#X(R) = \#\overline{X}(\mathrm{k}) \leq \deg(f_i)\#\,\mathrm{k}^{n-1} < \#\,\mathrm{k}^n.$$

This finishes the proof. □

Corollary. *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 $\mathbb{F}_p[[T]]$.

Proposition 10. *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 $d = 1$ just take $K = \mathbb{Q}_p$. Suppose that $d > 1$. We know that for any Keller polynomial map $f \in \mathcal{MP}_n(\mathbb{Z}_p)$ of degree d we have

$$\#\mathcal{Z}(f_1, \dots, f_n) \leq \deg(f)^n = d^n$$

where $\mathcal{Z}(f_1, \dots, f_n)$ 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 5 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 an unimodular map and $\mathcal{O}_K$ is a d-invariant domain. □

Proposition 11. *Suppose that for all $n \in \mathbb{N}$ and all $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(\mathbb{Z}_p)$ Keller map with* $\deg(f) < n$ *is unimodular. Then $\mathbb{Z}_p$ is an 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

$$f^{[[m]]} = (f_1, \dots, f_n, f_1, \dots, f_n, \dots, f_1, \dots, f_n) \in \mathcal{MP}_{mn}(\mathbb{Z}_p)$$

which consists of m-repetitions of the tuple $f_1, \dots, f_n$ where 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 $f \in R[x_1, \dots, x_n]$. Define $d(f) :=$ the number of monomials in degree > 3 that occur in f. If $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(R)$ we define $d(F) := \sum_j d(f_j)$.

Proposition 12. *Let $p \in \mathbb{Z}_{>3}$ be a prime number and $f \in \mathcal{MP}_n(\mathbb{Z}_p)$ a Keller map. Suppose that*

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

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 (see [2, (Proposition 3.1] 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 $f^{[m]} = (f, x_{n+1}, \dots, x_{n+m})$. 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 we have $\#X_G(\mathbb{Z}_p) < 3^{n+m}$ and we get $m = 2^{d(f)}$ by the proof of reduction theorem. The inequality $(*)$ implies $3^{m+n} \leq p^n$ and so we have f a unimodular map. □

Theorem 8. *$\mathbb{Z}_p$ is an invariant domain for almost all prime p if and only if the Jacobian Conjecture is true.*

Proof. The implication $\Longleftarrow$ it follows from Proposition 5. Suppose that $\mathbb{Z}_p$ is invariant for almost all prime p. By [12, Proposition 1.1.19] we know that it is sufficient to show that the Jacobian Conjecture is true over $\mathbb{Z}$. Suppose, by contradiction, that there is some Keller map $f = (f_1, \ldots, f_n) \in \mathcal{MP}_n(\mathbb{Z})$ non-invertible. Since f has coefficients in $\mathbb{Z} \subset \mathbb{Z}_p$ it follows that g is unimodular over $\mathbb{Z}_p$ for almost all primes p (see Proposition 7). Also, we know by the hypothesis that $f \otimes \overline{\mathbb{Q}}$ is non-injective (see Theorem 3). In particular, by Lemma 1, we have f non-injective over $\mathbb{Z}_p$ for infinitely many primes p. Fix 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. Contradiction by Theorem 4. □

A refinement of Lemma 1 allows us to replace **infinitely many primes** by **almost all primes**. This is the following lemma.

Lemma 4. *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. It is sufficient to prove the following **Fact.** Let $f(T) \in \mathbb{Z}[T] \setminus \mathbb{Z}$ 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 9. *$\mathbb{Z}_p$ is an invariant domain for infinitely many primes p if and only if the Jacobian Conjecture is true.*

Proof. The implication $\Longleftarrow$ is trivial. Suppose, by contradiction, that $\mathbb{Z}_p$ is an invariant domain for infinitely many primes p but the Jacobian Conjecture is false. Let $f \in \mathcal{MP}_N(\mathbb{Z})$ be a counterexample with $\det JF = 1$ (see [12, Proposition 1.1.19]). In particular, $f \otimes \overline{\mathbb{Q}}$ is not injective. Let $\alpha \neq \beta \in \overline{\mathbb{Q}}^N$ be such that $f(\alpha) = f(\beta)$. By the Lemma 4, 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 an invariant domain. So, we obtain $f \otimes \mathcal{O}_{K,p}$ a Keller map, non-injective over the domain $\mathcal{O}_{K,p}$. By Lemma 3 we know that there exists a Keller map g over $\mathbb{Z}_p$ that non-injective. A contradiction by Theorem 4.1. □

As a consequence, we get the following interesting result.

Corollary. *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 ($\Longleftarrow$) follows from Proposition 6. Suppose ($\Longrightarrow$) is false. Then for infinitely many primes p, we have $\mathbb{Z}_p$ as an invariant and non-unimodular domain. Since $\mathbb{Z}_p$ is invariant for infinitely many primes we have that the Jacobian Conjecture is true by Theorem 9. Contradiction by Essen-Lipton theorem. □

5 Keller-finite domains

This section introduces the notion of Keller-finite domains and explores their relation with the Jacobian Conjecture. Using this notion we give a simple proof of a result that refines the Essen-Lipton Theorem in some sense (see Theorem 11).

We start with the main definition.

Definition 6. *Let R be a domain and $n \in \mathbb{N}$. We say that R is a* ***Keller-finite domain in dimension*** *n if it satisfies the following property:*

- *given $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ with jacobian 1 the R-module*

$$R[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$$

is finitely generated.

We say that R is a ***Keller-finite domain*** *if R is Keller domains in dimension n for every $n \in \mathbb{Z}_{\geq 1}$.*

The first observation is that any field is Keller finite. This is the following proposition.

Proposition 13. *Any field K is a Keller domain.*

Proof. Passing to the an algebraic closure of K we can assume K algebraically closed. Let $R = K[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$ and let $\mathfrak{m}$ be a maximal ideal of R. By the [1, Corollary 11.15] we know that $\dim R_{\mathfrak{m}} \leq \dim_K \mathfrak{m}/\mathfrak{m}^2$ and using the jacobian criterion we have $\dim_K \mathfrak{m}/\mathfrak{m}^2 = n - \mathbf{rank}(Jf(\mathfrak{m})) = n - n = 0$. In particular, $\dim R_{\mathfrak{m}} = 0$. So, R is an Artinian K-algebra. In particular, $\dim_K R$ is finite. □

Proposition 14. *Consider the local ring $R = \mathbb{F}_q[[t]]$ of power series with coefficients on $\mathbb{F}_q$. Then R is not a Keller-finite domain.*

Proof. We will show that for every $n \in \mathbb{Z}_{>0}$ there are $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ with jacobian 1 such that the quotient

$$S = R[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$$

is not finitely generated as a R-module. Since S is a R-algebra note that S is finitely generated as R-module if and only if S is integral over R. Pick the polynomials

$$f_i = x_i - tx_i^q \quad \text{for every } i \in \{1, \dots, n\}.$$

Note that $\overline{x_i} \in S$ is not integral over R for every i. Indeed, suppose that there is a relation:

$$\overline{x_i}^n + a_{n-1}\overline{x_i}^{n-1} + \cdots + a_0 = 0$$

in S for some i. We can assume $i = 1$. Then we have

$$x_1^n + a_{n-1}x_1^{n-1} + \cdots + a_0 \in \langle x_1 - tx_1^q, x_2 - tx_2^q, \dots, x_n - tx_n^q \rangle.$$

So, there are $u_1(t; x_2, \dots, x_n), \dots, u_n(t; , x_2, \dots, x_n) \in \mathbb{F}_p[[t]][x_2, \dots, x_n]$ such that

$$x_1^n + a_{n-1}x_1^{n-1} + \cdots + a_0 = \sum_{i=0}^{m} u_i(t; x_2, \dots, x_n)x_1^i - t\sum_{i=0}^{m} u_i(t; x_2, \dots, x_n)x_1^{q+i}$$

We conclude by looking at the right side of the equation above that the leading monomial is of the form $tu_k(t; x_2, \dots, x_n)x_1^{q+k}$ for some k. But the left side is monical on x_1. This gives us a contradiction. □

In the next proposition, we explore local domains.

Remark 5. *Let $(R, \mathfrak{m}, k)$ be a local ring with residue field k and fraction field K. Let M be a R-module such that $M \otimes k$ and $M \otimes K$ are finite dimensional vector spaces. This is not enough to conclude that M is a finitely generated R-module.*

Example 4. *Let p be a prime number and consider the p-adic ring $\mathbb{Z}_p$. Consider the $\mathbb{Z}_p$-module*

$$M = \mathbb{Q}_p = \mathbb{Z}_p[1/p] = \mathbb{Z}_p[t]/\langle tp - 1 \rangle.$$

Note that M is not finitely generated as $\mathbb{Z}_p$-module since $\overline{t}$ is not integral over $\mathbb{Z}_p$. But $\dim_k M \otimes k = 0$ *and* $\dim_K M \otimes K = 1$.

Proposition 15. *Let $(R, \mathfrak{m}, k)$ be a discrete valuation ring with residue field k, fraction field K and uniformizer $t \in R$. Let $f_1, \dots, f_n \in R$ with the jacobian 1. Let $S = R[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$ the quotient. Then,* $\dim_k S \otimes k \leq \dim_K S \otimes K$

Proof. Let $\{u_1, \dots, u_n\}$ be elements of R such that $\{\overline{u}_1, \dots, \overline{u}_n\}$ is k-independent. We will show that $\{u_1, \dots, u_n\}$ is K-independent. Suppose that there are $a_1, \dots, a_n \in K$ such that

$$a_1u_1 + \cdots + a_nu_n = 0.$$

Cleaning denominators we can assume $a_i \in R$ for every i. Moreover, we can assume that $a_i \mod t \neq 0$ for some i. So, reducing $\mod \mathfrak{m}$ we get a non-trivial linear relation over k: $\overline{a_1} \cdot \overline{u_1} + \cdots + \overline{a_n} \cdot \overline{u_n} = 0$, a contradiction. □

In the next theorem, we show that any complete discrete valuation ring of characteristic zero does satisfy the Keller-finite condition. We start with the following lemma.

Lemma 5. *Let R be a ring and M be a R-module. Let $I \subset R$ be an ideal and assume that*

- *R is complete with the I-adic topology,*
- *$\bigcap_{n\geq 0} I^n M = (0)$, and*
- *M/IM is a R/I-module finitely generated*

Then M is finitely generated as a R-module.

Proof. See [11, Lemma 10.96.12]. □

Theorem 10. *Any complete discrete valuation ring of characteristic zero, $(R, \mathfrak{m}, \mathrm{k})$, is a Keller-finite domain.*

Proof. Let $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ with invertible jacobian and consider the quotient

$$A = R[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle.$$

We must to show that A is a finitely generated R-module. By the Lemma 5 it is sufficient to show that the intersection of every power of the ideal $I = tA$ is trivial, where t is a generator of $\mathfrak{m}$. This is because R complete and $\mathbb{F}_p[x_1, ..., x_n]/\langle f_1, \dots, f_n \rangle$ a $\mathbb{F}_p$-vector space of finite dimension by Proposition 13.

Now, denote by J the intersection of all power of I. By the Krull Intersection Theorem (see [9, Theorem 3.16], it is sufficient to show that I is inside in every maximal ideal of A. But, since R is a Jacobson ring so is A, because A is finitely generated as R-algebra. In particular, the "contraction" (= inverse image under the quotient map) of the maximal ideal of A to R is also a maximal ideal. But, R is local with maximal ideal $\langle t \rangle$. So, if $\mathcal{M}$ is a maximal ideal of A then, $R \cap \mathcal{M} = \langle t \rangle$. But, this means that t is inside $\mathcal{M}$. So, we are done by the Lemma 5. □

A consequence is the following theorem

Theorem 11. *The Jacobian Conjecture is true if and only if $\mathbb{Z}_p$ is unimodular* ***for some prime*** *p.*

Proof. Suppose that $\mathbb{Z}_p$ is unimodular for some prime p. Assume, by contradiction, that the Jacobian Conjecture is false. By [12, Proposition 1.1.19] we know that there is a counterexample in the form $f = (f_1, \dots, f_n) \in \mathcal{MP}_n(\overline{\mathbb{Q}_p})$ with jacobian 1 and coefficients on $\mathbb{Z}_p$. In particular, f is not injective. So, there is $\alpha_1 \neq \alpha_2 \in L^n$ such that $f(\alpha_1) = f(\alpha_2)$ for some finite extension $L|\mathbb{Q}_p$. By a translation, we can assume $f(\alpha_1) = 0$. Now, by the Theorem 10 we have $\mathcal{O}_L$ a Keller-finite domain. So, $\mathcal{O}_L[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$ finitely generated as an $\mathcal{O}_L$-module. By the valuative criterion (see [7, Theorem 4.7]) there exists a bijection $X(\mathcal{O}_L) \cong X(L)$, where X is the affine scheme defined by the equations $f_1, \dots, f_n$. But, since we are assuming that $\mathbb{Z}_p$ is unimodular then by Theorem 4 it follows that $f \otimes \mathcal{O}_L$ is an injective polynomial map. In particular, $\#X(L) = \#X(\mathcal{O}_L) \leq 1$. Contradiction, since $\#X(L) \geq 2$ ($\alpha_1, \alpha_2 \in X(L)$). □

Acknowledgements. W.Mendson thanks Ehsan Tavanfar for the discussion and references of useful topics in the proof of the Theorem 10. The author acknowledges the support of CNPq and Universidade Federal Fluminense (UFF).

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802

[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** (1982), no. 2, 287–330. MR 663785

[3] S. Cynk and K. Rusek, *Injective endomorphisms of algebraic and analytic sets*, Ann. Polon. Math. **56** (1991), no. 1, 29–35. MR 1145567

[4] Michiel De Bondt and Arno Van den Essen, *A reduction of the jacobian conjecture to the symmetric case*, Proceedings of the American Mathematical Society **133** (2005), no. 8, 2201–2205.

[5] Sudhir R Ghorpade, *A note on nullstellensatz over finite fields*, Contemporary Mathematics **738** (2019).

[6] Marvin J. Greenberg, *Lectures on forms in many variables*, W. A. Benjamin, Inc., New York-Amsterdam, 1969. MR 0241358

[7] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[8] James S. Milne, *Algebraic number theory*, available from his website (2017).

[9] ———, *A primer of commutative algebra*, 2020.

[10] Jean-Pierre Serre, *How to use finite fields for problems concerning infinite fields*, Contemporary Mathematics **14** (2009), 183.

[11] The Stacks project authors, *The stacks project*, `https://stacks.math.columbia.edu`, 2021.

[12] Arno van den Essen, *Polynomial automorphisms and the Jacobian conjecture*, Progress in Mathematics, vol. 190, Birkhäuser Verlag, Basel, 2000. MR 1790619

[13] Arno van den Essen and Richard J. Lipton, *A p-adic approach to the Jacobian Conjecture*, J. Pure Appl. Algebra **219** (2015), no. 7, 2624–2628. MR 3313498