SIEGEL'S THEOREM ON INTEGRAL POINTS AND THE JACOBIAN CONJECTURE OVER THE RATIONAL FIELD

NGUYEN VAN CHAU

ABSTRACT. It is shown that a polynomial map $(P,Q) \in \mathbb{Q}[x,y]^2$ with $P_xQ_y - P_yQ_x \equiv 1$ has an inverse map in $\mathbb{Q}[x,y]^2$ if the fiber $P = 0$ contains an infinite subset of $d^{-1}\mathbb{Z}^2$ for an integer d.

1. INTRODUCTION

A polynomial map $F \in \mathbb{C}[X]^n$, $X = (X_1, X_2, \ldots, X_n)$, is a *Keller map* if it satisfies the Jacobian condition $\det DF \equiv 1$. The mysterious Jacobian conjecture, firstly posed by Ott-Heinrich Keller [10] since 1939 and still opened, asserts that every Keller map $F \in \mathbb{C}[X]^n$ has an inverse map in $\mathbb{C}[X]^n$ (see [6] and [4]). This paper is to present a simple application of Siegel's theorem on integral points on affine curves to this conjecture over the rational field.

Recall that a subset of $\mathbb{Q}^n$ is *quasi-integral* if it is contained in $d^{-1}\mathbb{Z}^n$ for an integer d. Obviously, if a Keller map $F = (F_1, F_2, \ldots, F_n) \in \mathbb{Q}[X]^n$ has an inverse $G \in \mathbb{Q}[X]^n$, for each $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \in \mathbb{Q}^{n-1}$, the image $G(\{\alpha\} \times \mathbb{Q})$ is an infinite quasi-integral set contained in the affine curve defined by $F_i = \alpha_i$, $i = 1, 2, \ldots, n-1$, where d is the common denominator of all α_i and coefficients in G.

Our main result here is the following.

Theorem 1.1 (Main Theorem)**.** *Let $(P,Q) \in \mathbb{Q}[x,y]^2$ be a Keller map. If the fiber $P = 0$ contains an infinite quasi-integral subset of $\mathbb{Q}^2$, then (P,Q) has an inverse map in $\mathbb{Q}[x,y]^2$.*

An important and immediate consequence of Theorem 1.1 with together the formal inverse function theorem is the following.

Theorem 1.2. *Every Keller map $(P,Q) \in \mathbb{Z}[x,y]^2$ has an inverse map in $\mathbb{Z}[x,y]^2$ if, for an $\alpha \in \mathbb{Q}$, the fiber $P = \alpha$ contains an infinite quasi-integral subset of $\mathbb{Q}^2$.*

Let us denote

$$C(S,H,\alpha) := \{(a,b) \in S \times S : H(a,b) = \alpha\}$$

for $H \in \mathbb{Q}[x,y]$, $S \subset \mathbb{Q}$ and $\alpha \in \mathbb{Q}$. In view of Theorem 1.1, for any possible counterexample $(P,Q) \in \mathbb{Q}[x,y]^2$ to the Jacobian conjecture, if exists, the inequality

$$\#C(d^{-1}\mathbb{Z}^2, P, \alpha) < +\infty$$

must holds true for all $d \in \mathbb{N}$ and for all but a finite number of $\alpha \in \mathbb{Q}$.

Date: February 4, 2015.

2010 *Mathematics Subject Classification.* 14R15; 11G05 .

The author was partially supported by Vietnam National Foundation for Science and Technology Development (NAFOSTED) grant 101.01-2011.44.

Theorem 1.2 is a slight improvement of the main result in [12], which says that Keller maps $(P,Q) \in \mathbb{Z}[x,y]^2$ with fiber $P=0$ having infinitely many integral points are automorphisms of $\mathbb{Z}^2$. This result is reduced from an interesting observation that if a Keller map $(P,Q) \in \mathbb{Z}[x,y]^2$ is not inverse, then there is a constant $M > 0$ depended only on (P,Q) such that $\#C(\mathbb{Z},P,k) \leq M$ for all $k \in \mathbb{Z}$ (Lemma 2, [12]). Our approach here does not cover this result.

In studying the Jacobian conjecture over the rational field $\mathbb{Q}$ it is worthy to consider the following questions for Keller maps $(P,Q) \in \mathbb{Q}[x,y]^2$:

Question 1.3. *Is (P,Q) inverse if $\#C(\mathbb{Q},P,0) = +\infty$?*

Question 1.4. *Is uniformly bounded the numbers $\#C(\mathbb{Q},P,\alpha)$, $\alpha \in \mathbb{Q}$, if (P,Q) is not inverse?*

Under the Jacobian condition $\det D(P,Q) \equiv 1$, the complex fibers of P are nonsingular curves and P is a primitive polynomial in $\mathbb{C}[x,y]$. It is known that for all except a finite number of $\alpha \in \mathbb{C}$, the fibers $P = \alpha$ are diffeomorphic to same a Riemann surface of genus g_P and of n_P punctures. In view of the celebrated Faltings theorem [7] on rational points on algebraic curves, if $\#C(\mathbb{Q},P,0) = \infty$, the fiber $P=0$ must contain a rational curve or an elliptic curve. Furthermore, if $g_P \geq 2$, one has $\#C(\mathbb{Q},P,\alpha) < +\infty$ for all except a finite number of $\alpha \in \mathbb{Q}$.

The Uniform Bound Conjecture (see, for example, in [5]) says that for every integer $g \geq 2$, there exists a natural number $B(\mathbb{Q};g)$ such that any algebraic curve defined over $\mathbb{Q}$ and of genus g cannot have more than $B(\mathbb{Q},g)$ points in $\mathbb{Q}^2$. If this conjecture is true and if Question 1.3 is positive, then one has a confirmation to Question 1.4, at least for the case $g_P \geq 2$. A confirmation to Question 1.4 will allow us to reduce the Jacobian problem over $\mathbb{Q}$ to a consideration of the existing problem of Keller maps $(P,Q) \in \mathbb{Q}[x,y]^2$ with $\#C(\mathbb{Q},P,\alpha)$ uniformly bounded.

A proof of Theorem 1.1 will be presented in the next section. A version of this theorem for high dimensions will be provided in the last section.

2. Proof of Main Theorem

Let us begin with a brief introduction on the celebrated Siegel's theorem on integral points on affine curves. Let C be an irreducible affine curve in $\mathbb{C}^n$ defined by some polynomials in $\mathbb{Q}[X]$ and g_C denote the geometric genus of a desingularization of C. Siegel's theorem [14] asserts that *if $g_C > 0$ or if $g_C = 0$ and C has more than two irreducible branches at infinity, then C may have at most finitely many integral points*. We will use the following version of Siegel's theorem, concerning with affine curves having infinitely many integral points.

Theorem 2.1. *If C has infinitely many integral points, then*

i) *C has genus zero and has no more than two irreducible branches at infinity, and*
ii) *on each irreducible branch at infinity of C, there is a sequence of integral points of C tending to infinity.*

Property (i) is just Siegel's theorem stated in an equivalent statement. Property (ii) is known later due to Silverman [15]. This property ensures that, in some sense, the behavior at infinity of a regular function on such curve C is completely reflected on its restriction on the set of integral points of C. The consequence below may be well-known for experts and appear somewhere.

Corollary 2.2. *Let C be an irreducible affine curve in $\mathbb{C}^n$, defined over $\mathbb{Q}$. Assume that C has an infinite quasi-integral subset. Then, for any $H \in \mathbb{Q}[X]$, the restriction $H_{|C} : C \longrightarrow \mathbb{C}$ of H on C is either a constant function or a proper function. In particular, if C is smooth and $H_{|C}$ has no singularities, then $H_{|C}$ is an isomorphism of C and $\mathbb{C}$.*

Proof. Let $H \in \mathbb{Q}[X]$ be fixed. By assumptions, there is a number $d \in \mathbb{N}$ such that the intersection $C \cap (d^{-1}\mathbb{Z}^n)$ is infinite and $H \in d^{-1}\mathbb{Z}[X]$. So, by changing variables $X \mapsto dX$ and $H \mapsto dH$, we can assume that C has infinitely many integral points and $H \in \mathbb{Z}[X]$.

First, assume that H is not constant on C. We will prove that the restriction $H_{|C} : C \longrightarrow \mathbb{C}$ is proper. Observe that by Property (ii) in Theorem 2.1 it suffices to show that for each sequence of integral points $a_i \in C$ tending to ∞, the corresponding sequence $H(a_i)$ must tend to ∞. To see it, assume the contrary that H is bounded on a subsequence of a_is. Since any bounded subset of $\mathbb{Z}$ is finite, H must be a constant on an infinite subset of $\{a_i\}$. This implies that H is constant on C - a contradiction. Hence, $H_{|C}$ is proper.

Now, assume that C is smooth and $H_{|C}$ has no singularities. Since $H_{|C}$ is proper, $H_{|C} : C \longrightarrow \mathbb{C}$ determines a unramified covering of $\mathbb{C}$. Thus, by the simple connectedness of $\mathbb{C}$, $H_{|C}$ is isomorphic. □

Lemma 2.3. *Let $(P,Q) \in \mathbb{C}[x,y]^2$ be a Keller map. If the fiber $P = 0$ has a component diffeomorphic to $\mathbb{C}$, then (P,Q) is inverse.*

Proof. Assume that C is a component of the fiber $P = 0$, diffeomorphic to $\mathbb{C}$. As $J(P,Q) \equiv 1$, the restriction $Q_{|C} : C \longrightarrow \mathbb{C}$ gives a unramified covering of $\mathbb{C}$, and hence, is bijective. It implies that the restriction $(P,Q)_{|C} = (0, Q_{|C})$ is injective. By Abhyankar-Moh-Suzuki embedding theorem [1] , C is a line in a suitable algebraic coordinate of $\mathbb{C}^2$. The invertibility of (P,Q) now follows from a well-known result due to Gwrozdiewicz [9], which asserts that every Keller map of $\mathbb{C}^2$ is inverse if its restriction to a line is injective (see Theorem 1 in [9], Theorem 10.2.31 in [6]). □

Proof of Theorem 1.1. Let $(P,Q) \in \mathbb{Q}[x,y]^2$ be a given Keller map such that the fiber $P = 0$ contains an infinite quasi-integral set of $\mathbb{Q}^2$. In view of Siegel's theorem, the fiber $P = 0$ must contain an irreducible component C of genus zero and at most two irreducible branches at infinity. Since $J(P,Q) \equiv 1$, C is smooth and the restriction $Q_{|C}$ has no singularities. Therefore, by Corollary 2.2, the component C is diffeomorphic to $\mathbb{C}$. Hence, by Lemma 2.3, (P,Q) has an inverse map in $\mathbb{Q}[x,y]^2$. □

3. HIGH DIMENSIONAL CASE

Recall that a value $c \in \mathbb{C}^m$ is a *generic value* of a polynomial map $h : \mathbb{C}^n \longrightarrow \mathbb{C}^m$ if there is an open neighborhood U of c such that the restriction $h : h^{-1}(U) \longrightarrow U$ determines a locally trivial fibration. Let E_h denote the the complement of the set of all generic values of h. By definitions, the restriction $h : \mathbb{C}^n \setminus h^{-1}(E_h) \longrightarrow \mathbb{C}^m \setminus E_h$ determines a locally trivial fibration. It is well-known that E_h is either empty or an algebraic hypersurface of $\mathbb{C}^m$ (for example, see [16]).

Theorem 3.1. *Let $F = (F_1, F_2, \dots, F_n) \in \mathbb{Q}[X]^n$ be a Keller map. Suppose that for a generic value $\alpha \in \mathbb{Q}^{n-1}$ of the map $\hat{F} = (F_1, F_2, \dots, F_{n-1}) : \mathbb{C}^n \longrightarrow \mathbb{C}^{n-1}$, the fiber $\hat{F} = \alpha$ contains an infinite quasi-integral set of $\mathbb{Q}^n$. Then, F has an inverse map in $\mathbb{Q}[X]^n$.*

Proof. For $\lambda \in \mathbb{C}^{n-1}$, let us denote $C_\lambda := \hat{F}^{-1}(\lambda)$, $L_\lambda := \{\lambda\} \times \mathbb{C}$ and f_λ the restriction to C_λ of F. Since $JF \equiv 1$, the fibers C_λ are smooth and the maps $f_\lambda : C_\lambda \longrightarrow L_\lambda \subset \mathbb{C}^n$ have no singularities. By definitions, the map $\hat{F} : \mathbb{C}^n \setminus \hat{F}^{-1}(E_{\hat{F}}) \longrightarrow \mathbb{C}^{n-1} \setminus E_{\hat{F}}$ is a locally trivial fibration. So, the fibres C_λ, $\lambda \in \mathbb{C}^{n-1} \setminus E_{\hat{F}}$, are nonsingular affine curves of same a topological type.

Now, assume that α is a generic value of $\hat{F}$ such that the fiber $\hat{F} = \alpha$ contains an infinite quasi-integral set of $\mathbb{Q}^n$. By Siegel's theorem, C_α is an affine curve of genus zero and is diffeomorphic to either $\mathbb{C}$ or $\mathbb{C}^*$. We will consider cases: (a) C_α is diffeomorphic to $\mathbb{C}$; (b) C_α is diffeomorphic to $\mathbb{C}^*$

(a). In this case, for every $\lambda \in \mathbb{C}^{n-1} \setminus E_{\hat{F}}$, the map $f_\lambda : C_\lambda \longrightarrow L_\lambda \subset \mathbb{C}^n$ is diffeomorphic. It follows that $\#F^{-1}(a) = 1$ for all points a of the open dense algebraic subset $\mathbb{C}^n \setminus (E_{\hat{F}} \times \mathbb{C})$ of $\mathbb{C}^n$. Therefore, F is injective, as F is locally diffeomorphic by the Jacobian condition. Then, by Ax-Grothendieck Theorem (Theorem 10.4.11 in [8], see also [2, 11]), F is bijective, and hence, by the formal inverse function, F has an inverse map in $\mathbb{Q}[X]^n$.

(b). We will show that this case can never happen.

First, fix an arbitrary $\lambda \in \mathbb{C}^{n-1} \setminus E_{\hat{F}}$ and consider the map $f_\lambda : C_\lambda \longrightarrow L_\lambda$. Let Γ_1 and Γ_2 be the two unique irreducible branches at infinity of C_λ and b_1 and b_2 are the corresponding limiters of sequences $F_n(a_k)$ where $a_k \in \Gamma_i$ tend to infinity. Obviously, at least one of b_i is ∞. If both of b_i are ∞, f_λ must be proper, and hence, is a diffeomorphism from C_λ onto L_λ. Thus, we can assume that $b_1 = \infty$ and $b_2 := b_\lambda \in \mathbb{C}$.

Next, consider the restriction

$$f_\lambda : C_\lambda \setminus F^{-1}(\lambda, b_\lambda) \longrightarrow L_\lambda \setminus \{(\lambda, b_\lambda)\}, \qquad (*)$$

which determines a covering. Applying the Riemann-Huzwicz relation to this covering, we obtain

$$\chi(C_\lambda \setminus F^{-1}(\lambda, b_\lambda)) = \deg_{geo.} f_\lambda . \chi(L_\lambda \setminus \{(\lambda, b_\lambda)\}) - \sum_{p \in C_\lambda \setminus F^{-1}(\lambda, b_\lambda)} \deg_p f_\lambda - 1.$$

Here, $\chi(V)$, $\deg_{geo.} f_\lambda$ and $\deg_p f_\lambda$ denote the Euler-Poincare characteristic of an affine curve V, the geometric degree of f_λ and the local degree of f_λ at $p \in C_\lambda$, respectively. Note that $\chi(L_\lambda \setminus \{(\lambda, b_\lambda)\})) = 0$ and f_λ has no singularities. From the above equality it follows that $\chi(C_\lambda \setminus F^{-1}(\lambda, b_\lambda)) = 0$. Therefore, since C_λ is diffeomorphic to $\mathbb{C}^*$, the set $F^{-1}(\lambda, b_\lambda))$ is empty and the covering (*) is unramified.

The above arguments show that

$$L_\lambda \cap E_F = \{(\lambda, b_\lambda)\} \subset E_0$$

for all $\lambda \in \mathbb{C}^{n-1} \setminus E_{\hat{F}}$, where $E_0 := \{a \in \mathbb{C}^n : F^{-1}(a) = \emptyset\}$ - an closed algebraic subset of the hypersurface E_F in $\mathbb{C}^n$. Then, considering the projection $E_F \xrightarrow{\pi} \mathbb{C}^{n-1}$, $\pi(X) := (X_1, X_2, \ldots, X_{n-1})$, we can see that $\pi^{-1}(\mathbb{C}^{n-1} \setminus E_{\hat{F}})$ is a subset of E_0 and $\pi^{-1}(\mathbb{C}^{n-1} \setminus E_{\hat{F}}) \xrightarrow{\pi} \mathbb{C}^{n-1} \setminus E_{\hat{F}}$ is bijective. Since $\mathbb{C}^{n-1} \setminus E_{\hat{F}}$ is an open dense algebraic subset of $\mathbb{C}^{n-1}$, $\pi^{-1}(\mathbb{C}^{n-1} \setminus E_{\hat{F}})$ is an open dense algebraic subset of E_F. This follows that E_0 contains a hypersurface that is impossible. Indeed, if E_0 contains a hypersurface defined by a polynomial $H \in \mathbb{C}[X]$, by the definition of E_0, it must be that $H(F(X)) \equiv c \neq 0$ and that $DH(F(X))DF(X) \equiv 0$. The latter contradicts to the Jacobian condition. □

To conclude the article, we would like to present some remarks related to Theorem 1.1 and Theorem 3.1.

i) Note that Siegel's theorem is stated and valid for number fields. Property (ii) in Theorem 2.1 is also valid for arbitrary number field. Its proof is implicit in the proof of the main results in [13] and in the algorithms finding integral points presented in [3].

ii) As can be seen in its proof, Theorem 3.1 still holds true for when $\mathbb{Q}$ is replaced by an arbitrary number field.

iii) A key point in the proof of Corollary 2.2 is that any bounded subset of $\mathbb{Z}$ is finite. This is true for integral rings of imaginary quadratic fields $\mathbb{Q}(\sqrt{-m})$, $m \in \mathbb{N}$. Thus, Theorem 1.1 is valid for the fields $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-m})$. The statement of this theorem for number fields would be true if we could prove that for Keller maps $(P,Q) \in \mathbb{C}[x,y]^2$, any fiber of P cannot have a component diffeomorphic to $\mathbb{C}^*$, which is one of most special situations of the Jacobian conjecture.

Acknowledgments: The author wishes to express his thank to the professors Arno Van den Essen, Ha Huy Vui and Pierrette Cassou-Noguès for valuable discussions. The author would like to thank the VAST-JSPS and the VIASM for their helps.

REFERENCES

[1] S. S. Abhyankar and T. T. Moh, *Embeddings of the line in the plane*, J. Reine Angew. Math. **276** (1975), 148–166.
[2] J. Ax, *The elementary theory of finite fields*, Annals of Mathematics (2nd ser.) (Annals of Mathematics), **88** (2) (1968), 239–271.
[3] P. Alvanos, D. Poulakis, *Solving genus zero Diophantine equations over number fields*, Journal of Symbolic Computation, **46** (2011), 54–69.
[4] H. Bass, E. Connell and D. Wright, *The Jacobian conjecture: reduction of degree and formal expansion of the inverse*, Bull. Amer. Math. Soc. (N.S.) **7** (1982), 287–330.
[5] L. Caporaso, J. Harris and M. Barry, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35.
[6] A. Van den Essen, Polynomial automorphisms and the Jacobian conjecture, Progress in Mathematics **190**, Birkhauser, Basel, 2000.
[7] G. Faltings, *Endlichkeitsstze fr abelsehe Varietten ber Zahlkrpern*, Invent. Math. **73** (1983), 349–366.
[8] A. Grothendieck, *lments de gomtrie algbrique. IV. tude locale des schmas et des morphismes de schmas. III.* , Inst. Hautes tudes Sci. Publ. Math. **28** (1966).
[9] J. Gwrozdiewicz, *Injectivity on one line*, Bull. Soc. Sci. Lodz, **7**(1993), 59–60, Series Recherches sur les deformationes XV.
[10] O. Keller, *Ganze Cremona-Transformatione*, Monatsh. Math. Phys. **47** (1939), 299–306.
[11] K. McKenna and L. van den Dries,*Surjective polynomial maps, and a remark on the Jacobian problem*, Manuscripta Mathematica **67** (1) (1990), 1–15.
[12] Nguyen Van Chau, *Integer points on a curve and the plane Jacobian problem*, Ann. Polon. Math. **88** (2006), no. 1, 53–58.
[13] D. Poulakis and E. Voskos, *Solving genus zero Diophantine equations with at most two infinite valuations*, J. Symbolic Comput. **33** (4) (2002), 479–491.
[14] C. L. Siegel, *Uber einige Anwendungen Diophantischer Approximationen*, Abh. Preuss Akad. Wiss. Phys.-Math. Kl., 1929, Nr. 1; Ges. Abh., Band **1**, 209–266.
[15] J. H. Silverman, *On the distribution of integer points on curves of genus zero*, Theor. Computer Sc. **235** (2000) 163–170.
[16] A. N. Varchenko, *Algebro-geometrical equisingularity and local topological classification of smooth mappings*. Proceedings of the International Congress of Mathematicians (Vancouver, B.C., 1974), Vol. **1**, pp. 427–431. Canad. Math. Congress, Montreal, Que., 1975.

INSTITUTE OF MATHEMATICS, VIETNAM ACADEMY OF SCIENCE AND TECHNOLOGY, 18 HOANG QUOC VIET, 10307 HANOI, VIETNAM.

E-mail address: nvchau@math.ac.vn