Some Remarks on the Jacobian Conjecture and Connections with Hilbert's Irreducibility Theorem

Richard J. Lipton* Evangelos Markakis†
Arno van den Essen‡

Abstract

We have two main results. Let $P : \mathbb{K}^n \to \mathbb{K}^n$ be a polynomial map with constant nonzero Jacobian, where $\mathbb{K}$ is any algebraic extension of $\mathbb{Q}$.

1. The map P has a polynomial inverse if and only if the range of P contains a cartesian product of n universal Hilbert sets.
2. There exists a set S that contains "almost all" rational integers over $\mathbb{K}$ such that P is injective in S.

1 Introduction

The goal of this note is to present some remarks on the famous Jacobian Conjecture. Let $P : \mathbb{K}^n \to \mathbb{K}^n$ be a map over a field $\mathbb{K}$ of characteristic 0, and let $J(P)$ denote the determinant of its Jacobian matrix. We have two main contributions:

*Georgia Tech, College of Computing, Atlanta, GA 30332 and Telcordia Research, Morristown, NJ 07960. Email: rjl@cc.gatech.edu. Research supported by NSF grant CCF-0431023

†University of Toronto, Department of Computer Science, Toronto, ON M5S3G4. Email: vangelis@cs.toronto.edu

‡University of Nijmegen, Department of Mathematics. Email: essen@math.ru.nl

1. Let $P : \mathbb{K}^n \to \mathbb{K}^n$ be a polynomial map with $J(P)$ identically equal to 1, where $\mathbb{K}$ is an algebraic extension of $\mathbb{Q}$. Then, P is surjective if and only if P has a polynomial inverse. In fact we prove something stronger: P has a polynomial inverse if and only if the range of P contains a product of universal Hilbert sets, which is much weaker than being onto.

2. Let $P : \mathbb{K}^2 \to \mathbb{K}^2$ be a polynomial map with $J(P)$ identically equal to 1, where $\mathbb{K}$ is an algebraic extension of $\mathbb{Q}$. Then, P is invertible for "almost all" integers over $\mathbb{K}$.

For the first result two remarks are in order. First, the interesting direction, of course, is the direction from "sufficiently onto" to "invertible", which is based on the existence of universal Hilbert sets. Second, we recently realized that this result essentially follows from van den Dries and McKenna [9]Proposition 1.2. In Section 3, we discuss the similarities and differences between our result and theirs. We would still like to present our proof as it is based on a different approach.

As for the second result, there are two main ingredients in our proof. The first is the use of quantitative forms of Hilbert's irreducibility theorem, i.e., counting the number of integers in a certain interval that preserve irreducibility of polynomials. The second step is reducing our question to showing that a certain polynomial map of finite order has a fixed point. The proof is then completed by using a theorem of Smith on the existence of fixed points of diffeomorphisms with prime order.

As explained above, one of our main tools in both results is the use of various forms of Hilbert's irreducibility theorem and its implications. We believe that the connection between this theorem and the invertibility of polynomial maps is worth further investigation.

2 Definitions and Basic Facts

We first state some basic definitions and results that we need. Suppose that $P : \mathbb{K}^n \to \mathbb{K}^n$ is a polynomial map where $\mathbb{K}$ is a field of characteristic 0. This means, as usual, that $P = (f_1, \ldots, f_n)$ and each f_i is in $\mathbb{K}[x_1, \ldots, x_n]$. We use $J(P)$ to denote the determinant of the Jacobian matrix $(\frac{\partial f_i}{\partial x_j})_{1 \le i,j \le n}$ of the map P. The famous Jacobian Conjecture states that if $J(P) \equiv 1$, then P has a polynomial inverse.

Now assume that $\mathbb{K}$ is an algebraic extension of $\mathbb{Q}$ and let $P = (f_1, \ldots, f_n) : \mathbb{K}^n \to \mathbb{K}^n$ be a polynomial map with $J(P) \equiv 1$. The following basic facts will be used later on:

Lemma 1 *The functions $f_1, \ldots, f_n$ are algebraically independent over $\mathbb{K}$.*

Proof : See [10] Proposition 1.1.31. □

Lemma 2 *Each of $x_1, \ldots, x_n$ is algebraic over $\mathbb{Q}[f_1, \ldots, f_n]$.*

Suppose that $\Phi(u_1, \ldots, u_n, z)$ is a polynomial. We say that it *depends* on z provided that when written as a polynomial in z, i.e., as

$$a_m(u_1, \ldots, u_n)z^m + \ldots + a_0(u_1, \ldots, u_n)$$

then $m > 0$ and the polynomial $a_m(u_1, \ldots, u_n)$ is nonzero.

Lemma 2 implies the following:

Lemma 3 *For each x_i, $i = 1, \ldots, n$, there is an irreducible polynomial $\Phi_i(u_1, \ldots, u_n, z)$ with integer coefficients so that $\Phi_i(f_1, \ldots, f_n, x_i) = 0$. Moreover, each $\Phi_i(u_1, \ldots, u_n, z)$ depends on z.*

Lemma 4 *Let $\mathbb{K}$ be any field and let $P : \mathbb{K}^n \to \mathbb{K}^n$ be a polynomial map with $J(P) \equiv 1$. Then, for each $x \in \mathbb{K}^n$, $|P^{-1}(x)|$ is finite.*

Proof : See [10]Theorem 1.1.32. □

We use $P \circ Q$ to denote as usual the functional composition of two maps P and Q. Thus, for any $z \in \mathbb{K}^n$, $(P \circ Q)(z) = P(Q(z))$.

Fact 5 *Let P and Q be polynomial maps from $\mathbb{K}^n$ to $\mathbb{K}^n$. Then,*

$$J(P \circ Q) = J(P)(Q)J(Q).$$

3 Statement of Main Results

In this Section, we state our main results. Let $\mathbb{K}$ be a field. We consider polynomial maps P from $\mathbb{K}^n$ to $\mathbb{K}^n$ that satisfy the jacobian condition, i.e., $J(P) \equiv 1$.

Definition 1 *An infinite set $H \subseteq \mathbb{K}$ is called a universal Hilbert set of order n if for any irreducible polynomial $f(u, x_1, \ldots, x_n)$, the set of a for which $f(a, x_1, \ldots, x_n)$ is reducible, is a finite subset of H.*

Hilbert's irreducibility theorem, see e.g. [8], implies that universal Hilbert sets exist for any algebraic extension $\mathbb{K}$ of $\mathbb{Q}$ and they can be quite "thin". See [8] for results on constructing Hilbert sets.

Our first result shows that if P is "sufficiently onto", then P has a polynomial inverse.

Theorem 6 *Let $P : \mathbb{K}^n \to \mathbb{K}^n$, where $\mathbb{K}$ is any algebraic extension of $\mathbb{Q}$ and P satisfies $J(P) \equiv 1$. If $P(\mathbb{K}^n) \supseteq H_1 \times H_2 \times \ldots \times H_n$, for some universal Hilbert sets $H_1, H_2, \ldots, H_n$ of order n, then P has a polynomial inverse.*

Note that the condition that the range of P only contains $H_1 \times \ldots \times H_n$ is much weaker than onto. Note also that our result yields an equivalence between being sufficiently onto and being invertible since the reverse direction of Theorem 6 is trivial. Our proof works in two steps. We first show that P has a rational inverse. Then, as proved by Keller [6], if $J(P) \equiv 1$ and P has a rational inverse, P in fact has a polynomial inverse. We recently found out that our first step essentially follows from van den Dries and McKenna [9]Proposition 1.2 (our condition on the range of P implies that the range is, as in their terminology, Hilbert-dense). Their proof is based on a compactness argument similar in spirit to Gilmore and Robinson [4]. We would still like to present our proof as we think it is different and based on more elementary arguments.

In our second main result we use the notion of being invertible for "almost all" elements of a set. For a fixed dimension n, we will say that a set $S \subseteq \mathbb{Z}^n$ contains almost all rational integers of $\mathbb{K}^n$ if for all large enough M, the complement of S in $\mathbb{Z}^n$ satisfies:

$$|\bar{S} \cap [-M, M]^n| = o(M^n)$$

We can similarly define what it means for a property Π to hold for almost all integers. In particular, we will say that a map P is injective for almost

all integers if P is injective on a set S that contains almost all integers, i.e., for $x \in S$ and $x' \in S$, $P(x) = P(x')$ implies that $x = x'$.

Theorem 7 *Let $P : \mathbb{K}^n \to \mathbb{K}^n$, where $\mathbb{K}$ is an algebraic number field and P satisfies $J(P) \equiv 1$. Then P is injective for almost all integer points of $\mathbb{K}^n$.*

As usual, we use the term rational integers to distinguish $\mathbb{Z}$ from the set of algebraic integers over $\mathbb{K}$. The proof of Theorem 7 is more involved and uses quantitative versions of Hilbert's irreducibility theorem, i.e., estimates on the number of integers within a certain interval that preserve irreducibility of polynomials. Another essential tool in our proof is a result of Smith [1] on the existence of fixed points of automorphisms of prime order.

Finally we would like to observe that the starting point in both of our results is the use of Lemma 3 and various forms or implications of Hilbert's irreducibility theorem. We believe that the connection between invertibility of polynomial maps and irreducibility questions should be further explored.

4 Proof of Theorem 6

Proof : We prove the theorem for $\mathbb{K}$ equal to the rationals and for $n = 2$. The general case is similar. Let $P = (f, g) : \mathbb{Q}^2 \to \mathbb{Q}^2$ be a map with $J(P) \equiv 1$. By Lemma 3, there is an irreducible polynomial Φ_1 such that $\Phi_1(f, g, x_1) = 0$ (similarly a polynomial Φ_2 for x_2). Let

$$\Phi_1(f, g, x_1) = a_m(f, g)x_1^m + \ldots + a_0(f, g)$$

Lemma 3 implies that $m > 0$. We claim that there is a choice of rational values $\alpha \in H_1, \beta \in H_2$ for f and g (in fact there is an infinite number of such values), such that the polynomial $\Phi_1'(x_1) \equiv \Phi_1(\alpha, \beta, x_1) \in \mathbb{Q}[x_1]$ is irreducible over $\mathbb{Q}$, it has a rational root and it has the same degree in x_1 as the original Φ_1. To see this, note that for any pair $(\alpha, \beta) = (f(x_1, x_2), g(x_1, x_2))$, for $(x_1, x_2) \in \mathbb{Q}^2$, it is true that x_1 is a rational root of $\Phi_1(\alpha, \beta, x_1)$ and x_2 is a root of $\Phi_2(\alpha, \beta, x_2)$. Suppose we first substitute f with $\alpha \in H_1$ in Φ_1. By the definition of a Hilbert set, there is only a finite number of α's that make $\Phi_1(\alpha, g, x_1)$ reducible. Furthermore, there is only a finite number of α's that make $a_m(\alpha, g)$ identically 0. Once we fix α, then again there can be at most a finite number of choices for β that either make $\Phi_1(\alpha, \beta, x_1)$ reducible or make the highest degree term in x_1 vanish. Since the range of P contains $H_1 \times H_2$,

we can always find a pair (α, β) with the desirable properties. However, if $deg_{x_1}(\Phi_1) > 1$, then we have a contradiction, since $\Phi_1'(x_1)$ is irreducible over $\mathbb{Q}$ and we have assumed that it has a rational root. The same is true if $deg_{x_2}(\Phi_2) > 1$. Hence $deg_{x_1}(\Phi_1) = deg_{x_2}(\Phi_2) = 1$. Then $x_1, x_2 \in \mathbb{Q}(f, g)$, which means that P has a rational inverse. Since $J(P) \equiv 1$, it follows by [6] that P in fact has a polynomial inverse. □

5 Proof of Theorem 7

Let $P = (f_1, ..., f_n)$, where each f_i is a function of $x_1, ..., x_n$. We present the proof with $\mathbb{K} = \mathbb{Q}$. The generalization to any algebraic number field is straightforward. By Lemma 3, we know that for every variable x_i, there exists a polynomial $\Phi_i(u_1, u_2, ..., u_n, z)$ that depends on z, such that

$$\Phi_i(f_1, f_2, ..., f_n, x_i) = 0, \ i = 1, ..., n$$

.

Let $u = (u_1, ..., u_n)$ and $f = (f_1, ..., f_n)$. Suppose that in each $\Phi_i(u, z)$ we substitute u by f. We can then see Φ_i as a polynomial in z with coefficients from $\mathbb{Q}[f_1, ..., f_n]$:

$$\Phi_i(f, z) = a_{m_i}(f)z^{m_i} + a_{m_i-1}(f)z^{m_i-1} + ... + a_0(f)$$

We can further substitute $f_1, ..., f_n$ as functions of $x = (x_1, ..., x_n)$ and factor the resulting polynomial over $\mathbb{Q}(x)$. We will then obtain a polynomial in $\mathbb{Q}(x)[z]$:

$$\Phi_i(f, z) = (z - \phi_{i1}(x))(z - \phi_{i2}(x))...(z - \phi_{i,r_i}(x))A_i(x, z) \qquad (1)$$

where the ϕ_{ij}'s are rational functions of x and each A_i is a product of irreducible polynomials. Suppose that A_i contains l_i irreducible polynomials that depend on z (A_i may also contain factors that depend only on x but such terms do not affect our analysis). Note that each polynomial Φ_i has at least one factor, i.e., $r_i \geq 1$ because x_i is a root (since $\Phi_i(f, x_i) = 0$). Finally, we can also assume that each ϕ_{ij} has integer coefficients.

Let $u = (u_1, ..., u_n)$ be the value of f at a point, say $u = P(x^*)$, where $x^* = (x_1^*, ..., x_n^*) \in \mathbb{Q}^n$. We want to see when can we say that u has no other preimage. We will show that there exists a set S that contains almost all

points of $\mathbb{Z}^n$, such that for any $x^* \in S$, the corresponding value u has no other preimage within that set.

From now on, we assume that $x^* \in \mathbb{Z}^n$, the dimension n is some fixed integer and that each x_i^* is in $[-M, M]$, for some large enough M. Throughout our proof, we will eliminate integer points from $[-M, M]^n$ for which our arguments do not apply. We call such points "bad" points. We will show that there is a constant m_0 such that for all $M \geq m_0$, the number of bad points is $o(M^n)$. This will directly imply that the map P is injective on a set that contains almost all integer points.

Substituting x^* in each Φ_i yields the following univariate polynomials:

$$\Phi_i(z) \quad = \quad (z - \alpha_{i1})...(z - \alpha_{i,r_i})A_i(z) \tag{2}$$

where $\alpha_{ij} = \phi_{ij}(x^*),\ j = 1, \ldots, r_i,\ A_i(z) = A_i(x^*, z)$.

We first note that for almost all integer points $x^* \in \mathbb{Z}^n$, the polynomials $A_i(z)$ are products of irreducible polynomials over $\mathbb{Q}$ and hence have no rational roots. This follows from the result of [2], a quantitative form of Hilbert's irreducibility theorem. In particular, if we have an irreducible polynomial $B(x, z)$ in $n+1$ variables and we substitute x with integer values in the interval $[-M, M]$, there can be at most $O(M^{n-1/2} \log M)$ bad points x^* that make $B(x^*, z)$ reducible, out of a total of $O(M^n)$ possible points (see [8] Chapter 4 for related results). Since each A_i was a product of l_i irreducible polynomials, there are in total at most $c(\sum_i l_i)M^{n-1/2} \log M$ bad points, for some constant c. By picking large enough M, this is $o(M^n)$.

Consider an integer point x^* such that all the factors of $A_i(x^*, z)$ are irreducible over $\mathbb{Q}$. Then the only rational roots of each $\Phi_i(z)$ are the α_{ij}'s. Notice also that for each preimage of u, say $\hat{x}$, it holds that $\hat{x}_i$ is a root of $\Phi_i(z)$. This comes from the fact that Φ_i satisfies $\Phi_i(f, \hat{x}_i) = 0$. Hence, there is at least one point, say without loss of generality $\alpha^* = (\alpha_{11}, \alpha_{21}, ..., \alpha_{n1})$, that is equal to x^*. To see if u has any other integer preimage, we only need to check if there exists any other tuple of α_{ij}'s, say $\hat{\alpha} = (\alpha_{1,j_1}, ..., \alpha_{n,j_n}) \neq \alpha^*$ for which $\hat{\alpha} \in \mathbb{Z}^n$ and $P(\hat{\alpha}) = u$. If there is no such pair, then u has no other integer preimage apart from x^*.

Suppose that there is indeed a point $\hat{\alpha} = (\alpha_{1,j_1}, ..., \alpha_{n,j_n}) \neq \alpha^*$ for which $\hat{\alpha} \in \mathbb{Z}^n$ and $P(\hat{\alpha}) = u$. We claim that this cannot happen for a lot of integer points x^*. Note that $\hat{\alpha}$ is equal to $(\phi_{1,j_1}(x^*), ..., \phi_{n,j_n}(x^*))$. Hence we have that $P(\phi_{1,j_1}(x^*), ..., \phi_{n,j_n}(x^*)) = P(x^*)$. Let Q be the map $Q = (\phi_{1,j_1}, ..., \phi_{n,j_n})$.

Obviously Q is not the identity map, since $\hat{\alpha} = Q(x^*)$. We first show that for almost all integers, we may assume that the map Q is in fact a polynomial map. For this we will make use of the following well known lemma, which says that varieties can hit only a small fraction of integer points in $[-M, M]^n$ (e.g., see [8] Lemma 1, p. 298):

Lemma 8 *Let V be the variety: $V = \{x \in \mathbb{R}^n : R(x) = 0, R \in \mathbb{Q}[x]\}$. For any $n \geq 1$ and any $\epsilon > 0$, the number of integer points in $[-M, M]^n$ that belong to V is $O(M^{n-1})$.*

The constant in the asymptotic expression of Lemma 8 depends on the maximum degree of a variable in $R(x)$.

Lemma 9 *Let $a(x_1, ..., x_n)/b(x_1, ..., x_n)$ be a rational function with integer coefficients such that $a(x) \not\equiv c(x)b(x)$, i.e., a/b is not a polynomial function. Then for every $n \geq 1$, the number of integer pairs $x^* \in [-M, M]^n$ for which $a(x^*)/b(x^*)$ is an integer is $O(M^{n-1/2} \log M)$.*

Proof : Fix $n \geq 1$. Assume without loss of generality that b is irreducible. For a point $x^* = (x_1^*, ..., x_n^*)$, let $y^* = (x_2^*, ..., x_n^*)$. We estimate separately for each $y^* \in [-M, M]^{n-1}$, the number of x_1^*'s such that $b(x_1^*, y^*)$ divides $a(x_1^*, y^*)$. There are two cases to consider for y^*. First suppose that $b(x, y^*)$ becomes reducible. The result of Cohen [2], implies that there can be at most $O(M^{n-3/2} \log M)$ such y^*'s. Hence in the worst case there can be at most $O(M^{n-1/2} \log M)$ such pairs (x_1^*, y^*) for which the rational function takes an integer value. Assume now that $b(x, y^*)$ remains irreducible, which happens for $O(M^{n-1})$ values of y^*. Let $R(y^*)$ be the resultant of $a(x, y^*)$ and $b(x, y^*)$, which is a polynomial in y^* (for a definition of the resultant, see [7]). It is easy to check that if the resultant is identically 0, then $a(x)$ is a multiple of $b(x)$ and a/b is a polynomial map, a contradiction to our assumptions. Hence the resultant is not identically 0 and we consider two subcases. Suppose that $R(y^*) = 0$. By Lemma 8, this can happen for at most $O(M^{n-2})$ values of y^*. Therefore there can be at most $O(M^{n-1})$ points (x_1^*, y^*) that fall under this subcase. Assume now that $R(y_0) \neq 0$, which is true for $O(M^{n-1})$ values of y^*. This implies that $a(x, y^*)$ and $b(x, y^*)$ are relatively prime and there is a $d \in \mathbb{Z}$ and polynomials $q, s \in \mathbb{Z}[x]$ such that:

$$q(x)a(x, y^*) + s(x)b(x, y^*) = d$$

For $b(x_1^*, y^*)$ to divide $a(x_1^*, y^*)$, it has to be the case that $b(x_1^*, y^*)$ is equal to a divisor of d (or minus a divisor of d). However for any $\delta > 0$, the number of divisors of any large enough number n is $O(n^\delta)$ [5]. We also know that d is at most a polynomial in y^* by the way it was constructed and therefore for any $\epsilon > 0$, we can choose large enough constant m_0, so that for $M \geq m_0$ there are at most $c\ M^\epsilon$ divisors of d, for some constant c. Then for each (x_1^*, y^*) that we are interested in, x_1^* has to be a solution to $b(x, y^*) = d'$ for some divisor d' of d. Hence there are at most $deg_x b(x, y^*) = O(1)$ such choices for each divisor d'. In total, for each y^* in this subcase, we can have at most $O(M^\epsilon)$ values for x_1^* that make $b(x^*)$ divide $a(x^*)$. Therefore the total number of points x^* is $O(M^{n-1+\epsilon})$. Finally, summing up all the integer points that we counted in each case, we get a total of $O(M^{n-1/2} \log M)$. $\square$

Coming back to the discussion before Lemma 8 and 9, consider a tuple of functions $(\phi_{1,j_1}, ..., \phi_{n,j_n})$. If at least one of them is a rational function, then by Lemma 9, for almost every point $x^* \in \mathbb{Z}^n$, the point $(\phi_{1,j_1}(x^*), ..., \phi_{n,j_n}(x^*))$ is not an integer point. Since there are at most Πr_i such tuples containing at least one rational map, it follows that for almost every integer point $x^* \in \mathbb{Z}^n$, the second preimage of u, $\hat{\alpha} = (\alpha_{1,j_1}, ..., \alpha_{n,j_n})$, as defined above, belongs to $\mathbb{Z}^n$ only if the corresponding map $Q = (\phi_{1,j_1}, ..., \phi_{n,j_n})$ is a polynomial map. Hence after throwing away $o(M^n)$ bad points we may assume that Q is a polynomial map satisfying $(P \circ Q)(x^*) = P(x^*)$. We consider the following two cases:

Case 1 $P \circ Q$ is not identical to P. In this case, the equation $P(Q(x)) - P(x) = 0$ defines a non-trivial variety. But by Lemma 8, varieties can hit only a small fraction of integer points in $[-M, M]^n$. By ignoring these points, we have that all the remaining points cannot have any other integer preimage and we are done since in our analysis we have only ignored a total of $o(M^n)$ integer points.

Case 2 $P \circ Q \equiv P$ This case is more complicated. We will derive a contradiction by showing that Q has to be the identity map. First note that since $P(Q) \equiv P$ over $\mathbb{Q}$, the same will hold over $\mathbb{C}$. From now on we look at P and Q as polynomial maps from $\mathbb{C}^2$ to $\mathbb{C}^2$. Note also that by Fact 5, we have $J(Q) \equiv 1$.

We use P^t to denote the t-fold composition of the map P with itself. Thus, $P^2 = P \circ P$. In the rest of our analysis, we make repeated use of the following lemma:

Lemma 10 *If the map Q has a fixed point, then Q is the identity map.*

Proof : The proof is based on the inverse function theorem. Suppose Q has a fixed point, say $Q(a) = a$, where $a \in \mathbb{C}^n$. Since $J(Q) \equiv 1$, by the inverse function theorem, we know that P is locally invertible at a neighborhood of a, i.e., there exists an open set U containing a and an open set V containing $P(a)$, such that $V = P(U)$ and P is one-to-one, when restricted to U. We can pick a small enough open subset of U, say $D \subseteq U$, such that for every $a' \in D$, $Q(a') \in U$. Since $P(Q) \equiv P$, we have that

$$P(Q(a')) = P(a') \ \ \forall a' \in D$$

But P is one-to-one, when restricted to U. It follows that $Q(a') = a'$ on the open set D, i.e., Q is the identity map on the open set D. But since Q is a polynomial map, Q has to be the identity map everywhere. □

Lemma 10 enables us to prove the following property of the map Q.

Lemma 11 *The map Q has a finite order, i.e., there exists a positive integer $t \geq 1$ such that Q^t is the identity map.*

Proof : Pick $z \in \mathbb{C}^n$ and let $u = P(z)$. Consider the terms $z, Q(z), Q^2(z), \ldots$. By Lemma 4 we know that $|P^{-1}(z)|$ is finite. On the other hand, $u = P(z) = P(Q(z)) = P(Q^2(z)) = \ldots$. Hence there exist $r > s$ such that $Q^r(z) = Q^s(z)$. This means that the map Q^{r-s} has a fixed point and it also satisfies $J(Q^{r-s}) \equiv 1$ and $P \circ Q^{r-s} = P$. Lemma 10 completes the proof. □

The final argument in our proof uses the following Theorem, proved by Smith (see [1]):

Theorem 12 *[1] Let $P : \mathbb{R}^n \to \mathbb{R}^n$ be a diffeomorphism of prime order. Then P has a fixed point.*

By Lemma 11, there exists $t \geq 1$ such that Q^t is the identity map. Consider the minimum such t. We want to show that $t = 1$. So assume $t \geq 2$. Write $t = pd$, with p prime. Then Q^d is a diffeomorphism of R^{2n} of prime order. By Theorem 12 it follows that Q^d has a fixed point. So by lemma 10, Q^d is the identity map, a contradiction with the minimality of t(clearly $d < t$, since p is prime and hence $p > 1$).

Hence Q is the identity map, a contradiction. Therefore x^* is the only preimage of u. In various steps of our analysis we only needed to ignore integer pairs in $[-M, M]^n$ that were no more than $o(M^n)$. Hence what remains is a set S of $O(M^n)$ points such that for any $x \in S$, P has no other preimage within S. This completes the proof of Theorem 7.

6 Conclusions

We have obtained some connections between Hilbert's irreducibility theorem (in various forms) and invertibility of polynomial maps over algebraic number fields.

We think it is possible to generalize Theorem 7 and show that P is injective for almost all algebraic integers over $\mathbb{K}$. One of the steps that requires a different analysis towards this is Lemma 9. Another way to enlarge the set on which P is injective in the statement of Theorem 7 could be to start with a complete factorization of the polynomials $\Phi_i(f, z)$, in which the ϕ_{ij} functions would be algebraic functions of x and perform a similar analysis. In fact we believe that the jacobian conjecture is equivalent to the following statement:

Conjecture 13 *The jacobian conjecture is equivalent to proving the following statement: Let $P : \mathbb{C}^n \to \mathbb{C}^n$ with:*

1. *$J(P) \equiv 1$,*
2. *there exists an algebraic function defined on some open set $\mathcal{U}$, such that $P \circ Q = P$,*
3. *Q has finite order.*

Then the map Q has a fixed point.

References

[1] G. Bredon. *Introduction to Compact transformation groups.* Academic Press, 1972.

[2] S. D. Cohen. The distribution of galois groups and hilbert's irreducibility theorem. *Proc. London Math. Soc.*, 41(3):227–250, 1981.

[3] M. Fried. On hilbert's irreducibility theorem. *Journal of Number Theory*, 6:211–231, 1974.

[4] P. Gilmore and A. Robinson. Metamathematical considerations on the relative irreducibility of polynomials. *Canadian Journal of Mathematics*, 7:483–489, 1955.

[5] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1960.

[6] O. H. Keller. Ganze cremona-transformationen. *Monatsh. math. Phys.*, 47:299–306, 1939.

[7] S. Lang. *Algebra*. Addison-Wesley, 1993.

[8] A. Schinzel. *Polynomials with Special Regard to Reducibility*. Cambridge University Press, 2000.

[9] L. van den Dries and K. McKenna. Surjective polynomial maps and a remark on the jacobian problem. *Manuscripta Math.*, 67:1–15, 1990.

[10] A. van den Essen. *Polynomial Automorphisms and the Jacobian Conjecture*. Birkhauser, 2000.