DEPARTMENT OF MATHEMATICS

UNIVERSITY OF NIJMEGEN The Netherlands

The automorphism group of $\mathbb{C}[T]/(T^m)[X_1,\ldots,X_n]$.

Stefan Maubach

The automorphism group of $\mathbb{C}[T]/(T^m)[X_1, \ldots, X_n]$

Stefan Maubach

Abstract

The automorphism group of $\mathbb{C}[T]/(T^m)[X_1, \ldots, X_n]$ is studied, and a sufficient set of generators is given. Motivations for this theorem are given.

1 Introduction

This paper is about the automorphism group over $\mathbb{C}[T]/(T^m)[X_1, \ldots, X_n]$. Why this interest in this automorphism group? This is mainly motivated by several equivalent formulations of the famous Jacobian Conjecture in terms of the rings $R_m := \mathbb{C}[T]/(T^m)$. (See [4]). Look for these equivalent formulations in the beginning of section 3. From this point of view, knowing more about the automorphisms in $R_m[X_1, \ldots, X_n]$ could be interesting. The main theorem in section 3 is finding a sufficent set of generators for this automorphism group. Section 2 defines used notations and discusses some prerequisites.

2 Notations and small generalisations

First let us define a whole list of notations for this paper.

Definition 2.1.

- k is a field of characteristic zero.

- $R_m := \mathbb{C}[T]/(T^m)$. We will denote $\bar{T}$ by ϵ.

- $A := R[X_1, \ldots, X_n]$ (except in this section, where it can be a commutative R-algebra). $B_m := R_m[X_1, \ldots, X_n]$.

- $Aut_R(A)$ is the R-automorphism group of A. $Aff_R(A) \subset Aut_R(A)$ is the affine automorphism group consisting of maps $(a_1 X_1 + b_1, \ldots, a_n X_n + b_n)$, where $a_i \in R^*, b_i \in R$. $E_R(R[X_1, \ldots, X_n]) \subset Aut_R(A)$ is the collection of automorphisms of the form $(X_1, \ldots, X_{i-1}, X_i + f, X_{i+1}, \ldots, X_n)$ where $f \in R[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.

- $X = (X_1, \ldots, X_n)$, the identity map.

- $X^\alpha := X_1^{\alpha_1} \cdot \cdots \cdot X_n^{\alpha_n}$ for any vector $\alpha \in \mathbb{N}^n$.

1

- If $F \in A^n$ then $F = (F_1, \ldots, F_n)$ where $F_i \in A$; hence F_i is defined as the i-th coordinate of F.

- $P_{i,j}$ is the map interchanging X_i and X_j.

Let R be some commutative ring. A polynomial mapping is an element $F \in R[X_1, \ldots, X_n]^n$. A polynomial automorphism is a polynomial map which has a polynomial inverse G, i.e. $G \circ F = F \circ G = X$. The collection of these polynomial automorphisms is denoted by $Aut(R[X_1, \ldots, X_n])$. Any element $F \in Aut(R[X_1, \ldots, X_n])$ gives an automorphism $R[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n]$ by $P \longrightarrow P(F)$.

3 The automorphism group of $R_m[X]$

To motivate the results in this section we first give some equivalent formulations of the Jacobian Conjecture in terms of these rings. Let $JC(n)$ be the Jacobian Conjecture in dimension n over $\mathbb{C}$. Motivated by results of Bass in [1], Furter in [5], and Derksen in [2], the following result was proved by van de Essen in [4]. His proof is based on results of [3] and a result of Nowicki in [8]. For more details we refer to [4]

Theorem 3.1. *There is equivalence between:*

1. *$JC(n)$ is true.*

2. *For any $d \in \mathbb{N}$ there exists a bound $C(d)$ such that for any $m \in \mathbb{N}$ and any $F \in Aut_{R_m} R_m[X]$ satisfying $deg(F) = d$, $det(JF) = 1$ we have $deg(F^{-1}) \leq C(d)$.*

3. *For any $d, e \in \mathbb{N}$ there exists a bound $C(d, e)$ such that for any $m \in \mathbb{N}$ and any $F \in Aut_{R_m} R_m[X]$ satisfying $deg(F) = d$, $det(JF) = 1 + N$ and $N^e = 0$ we have $deg(F^{-1}) \leq C(d, e)$.*

4. *For any $d \in \mathbb{N}$ there exists a bound $C(d)$ such that for any R_m-derivation $D \in \eta Der_{R_m} R_m[X]$ satisfying $div(D) = 0$ and $deg(exp(D)) \leq d$ we have $deg(exp(-D)) \leq C(d)$.*

First, let us consider the case $n = 2$. In the field case we have $T(k, n)$ which is called the tame automorphism group of $k[X, Y]$. It is generated by elementary maps $E_k(k[X_1, X_2])$ and affine maps $Aff(k)$. One has the following theorem, due to Jung and van der Kulk ([6],[7],[3]):

Theorem 3.2. *$Aut_k k[X, Y] = T(k, 2)$. More precisely, $Aut_k k[X, Y]$ is the amalgamated free product of $Aff(k)$ and $E(k)$ over their intersection.*

If R is a ring satisfying $\bar{R}$ is a field one could hope to extend this result. However, if we define $T(R, 2)$ in the same way we cannot hope to have $Aut_R R[X, Y] = T(R, 2)$ since $(X + \epsilon X^2, Y)$ is an automorphism in R_m but not in $T(R, 2)$. However, if we allow maps of the form $(X + \epsilon H, Y)$ and $(X, Y + \epsilon H)$ (let us denote the set of these maps by $N(R)$) to be tame we easily have:

Theorem 3.3. $Aut_{R_m} R_m[X, Y] = T(R_m, 2)$, where $T(R_m, 2)$ is the group generated by $Aff(k), E(k)$ and $N(R)$.

Proof. "$\supseteq$" is easy. "$\subseteq$": let $F \in Aut_{R_m} R_m[X, Y]$. By theorem 3.2 we may assume that $F = (F_1, F_2) = (X, Y) + \epsilon^i(H_1, H_2)$ for some $i \in \mathbb{N}$. Now let $\varphi_i = (X - \epsilon^i H_1, Y)$, $\sigma_i = (X, Y - \epsilon^i H_2)$ then $\varphi_i \sigma_i F = (X, Y) + \epsilon^{i+1}(G_1, G_2)$ for some G_i. Doing this several times, we get $\varphi_{m-1} \sigma_{m-1} \cdots \varphi_i \sigma_i F = (X, Y)$, hence $F \in T(R_m, 2)$. $\qquad\square$

In the field case the result is even more useful since it is proved that $T(k, 2)$ is the amalgamated free product of $E(k, 2)$ and $Aff(k, 2)$, hence there is a unique decomposition of each map. If R is a ring for which $\bar{R}$ is a field one cannot hope to extend this result. One would like the extension to be a real extension of the field case. Unfortunately, the following example shows that this is quite impossible.

Example 3.4. Let $R = R_2$. Then
$(X, Y) = (X - \epsilon G(X - f(Y), Y), Y)(X + f(Y), Y)(X + \epsilon G(X + f(Y), Y))(X - f(Y), Y)$
for any $G \in k[T_1, T_2], f \in k[Y]$.

However, one might try to find a "more unique" set of generators for the automorphism group, by not allowing all maps $(X_1, \ldots, X_i + \epsilon H_i, \ldots, X_n)$. The following theorem does this:

Theorem 3.5. Let $n \geq 1$. $Aut_{R_m} B_m$ is generated by the union of the following sets:

1. $Aut_{\mathbb{C}}(A)$;

2. the maps $(X_1 + c\epsilon X_1, X_2, \ldots, X_n)$ all $c \in \mathbb{C}$;

3. the maps $(X_1 + \epsilon X_1^d, X_2, \ldots, X_n), (X_1 + \epsilon X_1^{d+1}, X_2, \ldots, X_n), \ldots$ where d is some positive integer.

Here we view $Aut_{\mathbb{C}}(A)$ as a subset of $Aut_R(B_m)$; notice that $\mathbb{C} \subset R_m$. One can prove that the maps 2) of the above theorem together with $Aff_{\mathbb{C}}(A)$ generate $Aff_{R_m}(B_m)$; the lemma's 3.9 and 3.10 indicate this. These remarks give

Corollary 3.6. $Aut_{R_m} R_m[X, Y]$ is generated by $Aff_{R_m} R_m[X, Y], E_{R_m} R_m[X, Y]$ and the maps $(X + \epsilon X^d, Y), (X + \epsilon X^{d+1}, Y), \ldots$ where d is some positive integer.

In this section we will prove the following theorem (which is stronger than theorem 3.5):

Theorem 3.7. $Aut_{R_m} B_m$ is generated by the union of the following sets:

1. $Aut_{\mathbb{C}}(A)$;

2. the maps $(X_1 + c\epsilon X_1, X_2, \ldots, X_n)$ all $c \in \mathbb{C}$;

3. some maps $(X_1 + \epsilon F_1(X_1), X_2, \ldots, X_n), (X_1 + \epsilon F_2(X_1), X_2, \ldots, X_n), \ldots$ where $\lim_{i \to \infty} deg(F_i \mod \epsilon) = \infty$.

Definition 3.8. Denote by $\mathcal{C}_m$ the monoid generated by 1),2) and 3) from the above theorem.

We want to prove that $\mathcal{C}_m = Aut_{R_m}B_m$. The proof of theorem 3.7 will go by the use of several lemma's.

Lemma 3.9. Let $\alpha \in R_m^*$. Then $(\alpha X_1, X_2, \ldots, X_n) \in \mathcal{C}_m$.

Proof. Let $\alpha = c(1 + a_1\epsilon + a_2\epsilon^2 + \ldots + a_{m-1}\epsilon^{m-1})$ for some nonzero $c \in \mathbb{C}$. Let $\beta_1, \ldots, \beta_{m-1}$ be the zeros of the polynomial $Y^{m-1} + a_1Y^{m-2} + a_2Y^{m-3} + \ldots + a_{m-2}Y + a_{m-1}$. Then $(\alpha X_1) = (cX_1) \circ (X_1 - \beta_1\epsilon X_1) \circ \ldots \circ (X_1 - \beta_{m-1}\epsilon X_1)$ since for any $\lambda_1, \lambda_2 \in R_m$ one has $(\lambda_1 X) \circ (\lambda_2 X) = (\lambda_1\lambda_2 X)$. This calculation works in n variables too so we're done. $\square$

Lemma 3.10. $(\alpha X_1 + \beta, X_2, \ldots, X_n) \in \mathcal{C}_m$ for all $\alpha \in R_m^*$, $\beta \in R_m$.

Proof. Let $\alpha^{-1}\beta = \gamma + \delta$ where $\gamma, \delta \in R_m^*$. Then $(\gamma X_1)(X_1 + 1)(\gamma^{-1}X_1)(\delta X_1)(X_1 + 1)(\delta^{-1}X_1) = (X_1 + \gamma + \delta) = (X_1 + \alpha^{-1}\beta)$. So $(\alpha X_1)(X_1 + \alpha^{-1}\beta) = (\alpha X_1 + \beta)$. This calculaton works in n variables too, so we're done. $\square$

Lemma 3.11. Let $F_1, \ldots, F_n \in R_m[X_1, \ldots, X_n]$ be such that $\mathbb{C}[\bar{F}_1, \ldots, \bar{F}_n] = \mathbb{C}[X_1, \ldots, X_n]$ then $R_m[F_1, \ldots, F_n] = R_m[X_1, \ldots, X_n]$.

Proof. Well-known (see [3]). $\square$

Lemma 3.12.

1. Let $H, G \in (B_m)^n$ then $(X + \epsilon^k H) \circ (X + \epsilon^k G) = X + \epsilon^k(H + G) \mod \epsilon^{k+1}$.

2. Let $H, G \in B_m$ then $(X_1 + \epsilon^k H, X_2, \ldots, X_n) \circ (X_1 + \epsilon^k G, X_2, \ldots, X_n) = (X_1 + \epsilon^k(H + G) + \epsilon^{k+1}(\ldots), X_2, \ldots, X_n)$

Proof. Easy since $\epsilon^k H(X + \epsilon(\ldots)) = \epsilon^k H(X) + \epsilon^{k+1}(\ldots)$. $\square$

Lemma 3.13. If $X + \epsilon H \in \mathcal{C}_m$ for all $H \in (B_m)^n$ then $\mathcal{C}_m = Aut_{R_m}A$.

Proof. Let $F \in Aut_{R_m}B_m$. Then $\bar{F} \in Aut_{\mathbb{C}}A$. Since $\bar{F}^{-1}F = X + \epsilon H$ for some $H \in R_m[X_1, \ldots, X_n]^n$ we have $F = \bar{F} \circ (X + \epsilon H)$. Hence $F \in \mathcal{C}_m$. $\square$

Lemma 3.14. If $(X_1 + \epsilon H, X_2, \ldots, X_n) \in \mathcal{C}_m$ for all $H \in B_m$ then $\mathcal{C}_m = Aut_{R_m}B_m$.

Proof. First notice that $P_{1,i}(X + \epsilon H, X_2, \ldots, X_n)P_{1,i} = (X_1, \ldots, X_{i-1}, X_i + \epsilon H(P_{1,i}), X_{i+1}, \ldots, X_n)$ so $(X_1, \ldots, X_{i-1}, X_i + \epsilon H, X_{i+1}, \ldots, X_n) \in \mathcal{C}_m$ for all $H \in B_m$. We are going to proceed by induction.
Suppose $(X_1 + \epsilon H_1, \ldots, X_i + \epsilon H_i, X_{i+1}, \ldots, X_n) \in \mathcal{C}_m$ all $H_i \in R_m[X_1, \ldots, X_n]$. Now choose some $H_{i+1} \in R_m[X_1, \ldots, X_n]$. Let $\tilde{H} := (X_1 + \epsilon H_1, \ldots, X_i + \epsilon H_i, X_{i+1}, \ldots, X_n)$. Then $R_m[\tilde{H}] = B_m$ by lemma 3.11, so there exists $G_{i+1} \in B_m$ such that $H_{i+1} = G_{i+1}(\tilde{H})$. Hence $(X_1, \ldots, X_i, X_{i+1} + \epsilon G_{i+1}, X_{i+2}, \ldots, X_n) \circ \tilde{H} = (X_1 + \epsilon H_1, \ldots, X_{i+1} + \epsilon H_{i+1}, X_{i+2}, \ldots, X_n)$. By induction and lemma 3.13 we are done. $\square$

4

Lemma 3.15. *Suppose for all $k \geq 1$ and any arbitrary monomial M $(= cX^\alpha$ for some $c \in \mathbb{C})$ we have that there exists some map $E_{k,M} \in \mathcal{C}_m$ such that $E_{k,M} = (X_1 + \epsilon^k M + \epsilon^{k+1} H, X_2, \ldots, X_n)$ for some $H \in B_m$ then $\mathcal{C}_m = Aut_{R_m} B_m$.*

Proof. by lemma 3.14 we only have to prove that $(X_1 + \epsilon H, X_2, \ldots, X_n) \in \mathcal{C}_m$ for all $H \in R_m[X_1, \ldots, X_n]$. We will proceed by induction on k.

Suppose that for any map $F := (X_1 + \epsilon H, X_2, \ldots, X_n)$ we can construct some map $F' = (X_1 + \epsilon H', X_2, \ldots, X_n) \in \mathcal{C}_m$ such that $F - F' = (\epsilon^k H'', 0, \ldots, 0)$ some $H'' \in R_m[X_1, \ldots, X_n]$. Let $H'' = \sum_{j=1}^s M_j + \epsilon G$ where $G \in B_m$ and M_j are monomials. Now we are going to compose several maps which are the identity in all variables except the first one; therefore we write down only the first variable. Using lemma 3.12.2 a few times we get

$$
\begin{aligned}
F_1'' := \quad & F_1' \circ (E_{k,M_1})_1 \circ \ldots \circ (E_{k,M_s})_1 \quad \text{mod } \epsilon^{k+1} \\
= \quad & (F_1 - (\epsilon^k \textstyle\sum_{j=1}^s M_j)) \circ (X_1 + \epsilon^k \textstyle\sum_{j=1}^s M_j) \quad \text{mod } \epsilon^{k+1} \\
= \quad & F_1 \quad \text{mod } \epsilon^{k+1}.
\end{aligned}
$$

Hence we can construct F'' which is equal to $F + (\epsilon^{k+1} \tilde{H}, 0, \ldots, 0)$ some $\tilde{H} \in B_m$. . By induction we are done since $\epsilon^m = 0$. $\qquad\square$

Lemma 3.16. *If $G \in \mathcal{C}_m$ of the form G $\text{mod } \epsilon^{k+1} = (X_1 + \epsilon^k X_1^d, X_2, \ldots, X_n)$ for any $d \geq 2$ then $\mathcal{C}_m = Aut_{R_m} B_m$.*

Proof. By lemma 3.15 we only have to prove that we can construct maps $E_{k,M}$ of the form $(X_1 + \epsilon^k M + \epsilon^{k+1} H, X_2, \ldots, X_n)$ for some $H \in R_m[X_1, \ldots, X_n]$. Now notice that if $c' \in \mathbb{C}$ such that $c'^{d-1} = c$ then

$$
\begin{aligned}
&({c'}^{-1} X_1, X_2, \ldots, X_n)(X_1 + \epsilon^k X_1^d, X_2, \ldots, X_n)(c' X_1, X_2, \ldots, X_n) = \\
&(X_1 + c\epsilon^k X_1^d, X_2, \ldots, X_n).
\end{aligned}
$$

Furthermore defining $L := (X_1 + a_2 X_2 + \ldots + a_n X_n, X_2, \ldots, X_n)$ we have

$$
\begin{aligned}
(*) \qquad & L^{-1}(X_1 + c\epsilon^k X_1^d, X_2, \ldots, X_n) L \\
& (X_1 + c\epsilon^k (X_1 + a_2 X_2 + \ldots + a_n X_n)^d, X_2, \ldots, X_n).
\end{aligned}
$$

So maps of the form $(X_1 + c\epsilon^k (X_1 + a_2 X_2 + \ldots + a_n X_n)^d, X_2, \ldots, X_n)$ $\text{mod } \epsilon^{k+1}$ can be constructed (where only the first coordinate is not the identity). By lemma 3.12.2 we can make maps of the form $(X_1 + c\epsilon^k H + \epsilon^{k+1}(\ldots), X_2, \ldots, X_n)$ where H is any linear combination of polynomials of the form $(X_1 + a_2 X_2 + \ldots + a_n X_n)^d$. Since these polynomials generate the k-vectorspace of homogeneous polynomials in n variables of degree d we can find a map $E_{k,M}$ as stated for any monomial of degree d. Since d is arbitrary ≥ 2 we are done. $\qquad\square$

Now we will give some technical statements for the case that $n = 1$ ($B_m = R_m[X]$, one variable). These will be used in the proof of lemma 3.18 which will be the last step in the proof of theorem 3.7. This is the only lemma in which one has to do a lot of (dirty) calculation; one cannot evade some hard work in some places. (At least, I cannot.)

Lemma 3.17.

1. *If there exists some map $E_{k,d} \in \mathcal{C}_m$ where $d \geq 2$ such that $E_{k,d} \mod \epsilon^{k+1} = (X + \epsilon^k X^d)$ then there exists a map $F \in \mathcal{C}_m$ such that*

$$F \mod \epsilon^{k+2} = (X + \epsilon^{k+1} \sum_{i=0}^{s} h_i X^i)$$

   and $h_d = 1$.

2. *If there exists a map $F \in \mathcal{C}_m$ with*

$$F \mod \epsilon^{k+1} = (X + \epsilon^k \sum_{i=1}^{s} h_i X^i)$$

   where $s > d$, $h_d = 1$ $(d \geq 2)$ then there exists some $\widetilde{F} \in \mathcal{C}_m$ satisfying

$$\widetilde{F} \mod \epsilon^{k+1} = (X + \epsilon^k \sum_{i=1}^{s} \tilde{h}_i X^i)$$

   where $\tilde{h}_d = 1$, $\tilde{h}_s = 0$ (and if $h_i = 0$ then $\tilde{h}_i = 0$).

Proof.

1. Choose some $c \in \mathbb{C}$. Let $a \in \mathbb{C}$ be such that $a^{d-1} = c$. Then

$$(a^{-1}X)E_{k,d}(aX) = (X + c\epsilon^k X^d) \mod \epsilon^{k+1}.$$

   So we have $E_{k,d,c} \in \mathcal{C}_m$ such that $E_{k,d,c} \mod \epsilon^{k+1} = (X + c\epsilon^k X^d)$ for any $c \in \mathbb{C}$. Now choose $\alpha \in R_m$ such that $\alpha = 1 + c\epsilon$ for some $c \in \mathbb{C}$. Notice that $\alpha^d \mod \epsilon^2 = 1 + cd\epsilon$ and $\alpha^{-d} \mod \epsilon^2 = 1 - cd\epsilon$ (in fact, "analytically speaking" d could be any real number). So now we have some $F \in \mathcal{C}_m$ such that

$$
\begin{aligned}
& F \mod \epsilon^{k+2} \\
= {} & E_{k,d,-1}(\alpha^{-1}X)E_{k,d,1}(\alpha X) \\
= {} & (X - \epsilon^k X^d - \epsilon^{k+1}G)(\alpha^{-1}X)(X + \epsilon^k X^d + \epsilon^{k+1}H)(\alpha X)
\end{aligned}
$$

   where G, H are certain polynomials $\in \mathbb{C}[X]$ and $c \in \mathbb{C}$ arbitrarily chosen. But writing out the last equation we get:

$$
\begin{aligned}
& F \mod \epsilon^{k+2} \\[4pt]
= {} & (X - \epsilon^k X^d - \epsilon^{k+1}G(X))(\alpha^{-1}X)(X + \epsilon^k X^d + \epsilon^{k+1}H(X))(\alpha X) \\[4pt]
= {} & (\alpha^{-1}X - \epsilon^k \alpha^{-d}X^d - \epsilon^{k+1}G(\alpha^{-1}X))(\alpha X + \epsilon^k \alpha^d X^d + \epsilon^{k+1}H(\alpha X)) \\[4pt]
= {} & (\alpha^{-1}X - \epsilon^k(1 - cd\epsilon)X^d - \epsilon^{k+1}G(X))(\alpha X + \epsilon^k(1 + cd\epsilon)X^d + \epsilon^{k+1}H(X)) \\[4pt]
= {} & (\alpha^{-1}X - \epsilon^k X^d + \epsilon^{k+1}(cdX^d - G(X)))(\alpha X + \epsilon^k X^d + \epsilon^{k+1}(cdX^d + H(X)))
\end{aligned}
$$

6

$$= (X + \alpha^{-1}\epsilon^k X^d + \alpha^{-1}\epsilon^{k+1}(cdX^d + H(X))) - \epsilon^k(\alpha X + \epsilon^k X^d)^d +$$
$$\epsilon^{k+1}(cd(\alpha X)^d - G(\alpha X)))$$

$$= (X + (1 - c\epsilon)\epsilon^k X^d + \epsilon^{k+1}(cdX^d + H(X))) - \epsilon^k((1 + c\epsilon)X + \epsilon^k X^d)^d +$$
$$e^{k+1}(cdX^d - G(X)))$$

$$= (X + \epsilon^k X^d + \epsilon^{k+1}((cd - c)X^d + H(X)) - \epsilon^k(X + c\epsilon X + \epsilon^k X^d)^d +$$
$$\epsilon^{k+1}(cdX^d - G(X)).$$

Now we have to differentiate between $k = 1$ and $k > 1$ since in the latter case $\epsilon^k(X + c\epsilon X + \epsilon^k X^d)^d = \epsilon^k X^d + dc\epsilon^{k+1}X^d \mod \epsilon^{k+2}$ and in the case $k = 1$ one has $\epsilon^k(X + c\epsilon X + \epsilon^k X^d)^d = \epsilon(X + c\epsilon(X + X^d))^d = \epsilon(X^d + \epsilon dX^{d-1}(X + X^d))$ $\mod \epsilon^2 = \epsilon X^d + \epsilon^2(dX^d + dX^{2d-1})$. Let us do the case $k > 1$:

$$F \mod \epsilon^{k+2}$$

$$= (X + \epsilon^k X^d + \epsilon^{k+1}((cd - c)X^d + H(X)) - \epsilon^k(X + c\epsilon X + \epsilon^k X^d)^d +$$
$$\epsilon^{k+1}(cdX^d - G(X))$$

$$= (X + \epsilon^k X^d + \epsilon^{k+1}((cd - c)X^d + H(X)) - (\epsilon^k X^d + dc\epsilon^{k+1}X^d) +$$
$$\epsilon^{k+1}(cdX^d - G(X))$$

$$= (X + \epsilon^{k+1}((-c)X^d + H(X)) + \epsilon^{k+1}(cdX^d - G(X))$$

$$= (X + \epsilon^{k+1}((-c + cd)X^d + H(X) - G(X)).$$

Since c is completely free (and G, H are fixed) we can obtain the desired result. The case $k = 1$ is not really different: replace "$H(X) - G(X)$" by "$H(X) - G(X) - dX^{2d-1}$" and observe that the coefficient of X^d equals $\epsilon^2(2cd - c - d)$.

2. Choose some $c \in \mathbb{C}$ such that $c^{s-1} = -1$ and $c^{d-1} \neq -1$. Now let $F' := (c^{-1}X)F(cX)F$. Then

$$F' \mod \epsilon^{k+1}$$

$$= (c^{-1}X)(X + \epsilon^k \sum_{i=1}^s h_i X^i)(cX)(X + \epsilon^k \sum_{i=1}^s h_i X^i)$$

$$= (X + \epsilon^k \sum_{i=1}^s g_i X^i)(X + \epsilon^k \sum_{i=1}^s h_i X^i)$$

$$= (X + \epsilon^k \sum_{i=1}^s g_i X^i + \epsilon^k \sum_{i=1}^s h_i X^i)$$

where $g_i := c^{i-1}h_i$. Define $h'_i := g_i + h_i$ for all i. Then $h'_s = g_s + h_s = c^{s-1}h_s + h_s = -h_s + h_s = 0$. Also if $h_i = 0$ then $g_i = 0$ and hence $h'_i = 0$. Furthermore $h'_d = g_d + h_d = c^{d-1}h_d + h_d = (c^{d-1} + 1) \neq 0$. Choose $a \in \mathbb{C}$ such

that $a^{d-1} = (c^{d-1} + 1)^{-1}$. Now define $\widetilde{F} := (a^{-1}X)F'(aX)$. Then

$$\widetilde{F} \mod \epsilon^{k+1}$$

$$= (a^{-1}X)(X + \epsilon^k \sum_{i=1}^{s-1} h_i' X^i)(aX)$$

$$= (X + \epsilon^k \sum_{i=1}^{s-1} a^{i-1} h_i' X^i)$$

$$= X + \epsilon^k \sum_{i=1}^{s-1} \tilde{h}_i X^i$$

where $\tilde{h}_i := a^{i-1} h_i'$. Hence $\tilde{h}_d = 1$, and if $h_i' = 0$ then $\tilde{h}_i = 0$.

$\square$

Lemma 3.18. *For the case $n = 1$ ($B_m = R_m[X]$, one variable) we have for any $k, d \in \mathbb{N}$ that there exists some $E_{k,d} \in \mathcal{C}_m$ such that $E_{k,d} = (X + \epsilon^k X^d) \mod \epsilon^{k+1}$.*

Proof. Notice that for $d = 0, 1$ we can refer to lemma 3.10. So let $d > 1$. This lemma will be done by induction.
Suppose for any $k' < k$ we have maps $E_{k',d}$ as in the theorem.
Suppose for any $d' < d$ we have maps $E_{k,d'}$ as in the theorem.
We have to prove that we can construct a map $E_{k,d}$. By induction we have some map $E_{k-1,d}$. So by lemma 3.17.1 we get some map F of the form

$$F \mod \epsilon^{k+1} = X + \epsilon^k \sum_{i=0}^{s} h_i X^i$$

where $h_d = 1$. Now by applying lemma 3.17.2 several times we have constructed a map F' which looks like

$$F \mod \epsilon^{k+1} = X + \epsilon^k \sum_{i=0}^{d} h_i X^i.$$

By induction we have maps $E_{k,d-1}, \ldots, E_{k,1}, E_{k,0}$. Now define for any $c \in \mathbb{C}$ the maps $E_{k,d,c} := (X + c\epsilon^k X^d) \mod \epsilon^{k+1} = (a^{-1}X)E_{k,d}(aX)$ where $a \in \mathbb{C}$ such that $a^{d-1} = c$. Now using lemma 3.12 a few times we have

$$F \circ E_{k,d-1,-h_{d-1}} \circ E_{k,d-2,-h_{d-2}} \circ \ldots \circ E_{k,2,-h_2} \circ (X - h_1 \epsilon^k X) \circ (X - h_0 \epsilon^k)$$
$$\mod \epsilon^{k+1} = (X + \epsilon^k X^d)$$

and hence we are done by induction. $\square$

Proof. (of theorem 2) Lemma 3.18 gives us the ability to construct maps as required in lemma 3.16. (The fact that lemma 3.18 is in one dimension is of no consequence, that was just to make notations easier.) Since the requirements of lemma 3.16 are fulfilled, we are done. $\square$

References

[1] H.Bass. The Jacobian Conjecture and inverse degrees. Arithmetic and geometry, Prog. Math **1983** . 36, 65-75

[2] H.Derksen. Inverse degrees and the Jacobian Conjecture, Comm. in Algebra **1994**. 22, 12, 4793-4794.

[3] A. van den Essen. Polynomial automorphisms and the Jacobian Conjecture. In Prog. Math , Vol.190, Birkhäuser **2000**.

[4] A. van den Essen. On Bass' Inverse Degree Approach to the Jacobian Conjecture and Exponential Automorphisms. To appear in the Proceedings of the International Conference on Computational and Combinatorial Algebra, held at the University of Hong Kong, May 24-29,1999.

[5] J.-Ph. Furter. On the degree of the inverse of an automorphism of the affine space. J. of Pure and Appl. Algebra **1998**. 130, 11, 1-8.

[6] H.Jung. Uber ganze birationale Transformationen der Ebene, J.Reine Angew. Math. **1942**. 184, 161-174.

[7] W. van der Kulk. On polynomial rings in two variables, Nieuw Archief voor Wiskunde **1953**. 3 I, 33-41.

[8] A.Nowicki. Polynomial derivations and their rings of constants, Univ. of Toruń, **1994**.