PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The version of the following full text has not yet been defined or was untraceable and may differ from the publisher's version.

For additional information about this publication click this link.
http://hdl.handle.net/2066/18845

Please be advised that this information was generated on 2018-11-24 and may be subject to change.
THE AUTOMORPHISM GROUP OF $\mathbb{C}[T]/(T^m)[X_1, \ldots, X_n]$

Stefan Maubach

Report No. 0002 (January 2000)
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 sufficient 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 $\bar{T} (:= T \mod T^m)$ by $\epsilon$.
  $R^*$ will be the set of invertible elements in $R$.
- $A := R[X_1, \ldots, X_n] B_m := R_m[X_1, \ldots, X_n]$.
- $\text{Aut}_R(A)$ is the $R$-automorphism group of $A$. $\text{Aff}_R(A) \subseteq \text{Aut}_R(A)$ is the affine automorphism group consisting of maps $(a_1 X_1 + b_1, \ldots, a_n X_n + b_n)$, where $a_i \in R^*, b_i \in R$. $E_R(R[X_1, \ldots, X_n]) \subseteq \text{Aut}_R(A)$ is the collection of automorphisms of the form $(X_1, \ldots, X_i, X_i + f(X_{i+1}, \ldots, X_n))$ 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.
$X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ for any vector $\alpha \in \mathbb{N}^n$.

- 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 $\text{Aut}(R[X_1, \ldots, X_n])$. Any element $F \in \text{Aut}(R[X_1, \ldots, X_n])$ gives an automorphism $R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n]$ by $P \to P(F)$.

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 $F \in \text{Aut}_{R_m} R_m[X]$ 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 $F \in \text{Aut}_{R_m} R_m[X]$ 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 $D \in \mathfrak{n} Der_{R_m} R_m[X]$ satisfying $\text{div}(D) = 0$ 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 $\text{Aff}(k)$. One has the following theorem, due to Jung and van der Kulk ([6],[7],[3]):

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

If $R$ is a ring for which $R$ 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 $\text{Aut}_R R[X,Y] = T(R,2)$ 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.** $\text{Aut}_R R_m[X, Y] = T(R_m, 2)$, where $T(R_m, 2)$ is the group generated by $\text{Aff}(k), E(k)$ and $N(R)$.

**Proof.** “$\supset$” is easy. “$\subset$”: let $F \in \text{Aut}_R R_m[X, Y]$. By theorem 3.2 we may assume that $F = (F_1, F_2) = (X, Y) + e^i(H_1, H_2)$ for some $i \in \mathbb{N}$. Now let $\varphi_i = (X - e^iH_1, Y)$, $\sigma_i = (X, Y - e^iH_2)$ then $\varphi_i \sigma_i F = (X, Y) + e^{i+1}(G_1, G_2)$ for some $G_i$. Doing this several times, we get $\varphi_{m-1} \sigma_{m-1} \cdots \varphi_1 \sigma_1 F = (X, Y)$, hence $F \in T(R_m, 2)$. □

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 $\text{Aff}(k, 2)$, hence there is a unique decomposition of each map. If $R$ is a ring for which $R$ 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 $(X, Y) = (X - eG(X - f(Y), Y), Y)(X + f(Y), Y)(X + eG(X + f(Y), Y))(X - f(Y), Y)$ 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 $(X_1, \ldots, X_i + eH_i, \ldots, X_n)$. The following theorem does this:

**Theorem 3.5.** Let $n \geq 1$. $\text{Aut}_R R_m$ is generated by the union of the following sets:

1. $\text{Aut}_C(A)$;
2. the maps $(X_1 + eX_1, X_2, \ldots, X_n)$ all $c \in C$;
3. the maps $(X_1 + eX^d, X_2, \ldots, X_n), (X_1 + eX^{d+1}, X_2, \ldots, X_n), \ldots$ where $d$ is some positive integer.

Here we view $\text{Aut}_C(A)$ as a subset of $\text{Aut}_R(B_m)$; notice that $C \subset R_m$. One can prove that the maps 2) of the above theorem together with $\text{Aff}_C(A)$ generate $\text{Aff}_R(B_m)$; the lemma’s 3.9 and 3.10 indicate this. These remarks give

**Corollary 3.6.** $\text{Aut}_R R_m[X, Y]$ is generated by $\text{Aff}_R R_m[X, Y], E_R R_m[X, Y]$ and the maps $(X + eX^d, Y), (X + eX^{d+1}, Y), \ldots$ 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.** $\text{Aut}_R R_m$ is generated by the union of the following sets:

1. $\text{Aut}_C(A)$;
2. the maps $(X_1 + cX_1, X_2, \ldots, X_n)$ all $c \in C$.
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 $C_m$ the monoid generated by 1), 2) and 3) from the above theorem.

We want to prove that $C_m = \text{Aut}_{R_m} B_m$. The proof of theorem 3.7 will go by the use of several lemma’s.

**Lemma 3.9.** Let $\alpha \in R^*_m$. Then $(\alpha X_1, X_2, \ldots, X_n) \in C_m$.

**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 $Y^{m-1} + a_1 Y^{m-2} + a_2 Y^{m-3} + \ldots + a_{m-2} Y + a_{m-1}$. 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 are done. $\square$

**Lemma 3.10.** $(\alpha X_1 + \beta, X_2, \ldots, X_n) \in C_m$ for all $\alpha \in R^*_m$, $\beta \in R_m$.

**Proof.** Let $\alpha = \gamma + \delta$ 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 calculation works in $n$ variables too, so we are done. $\square$

**Lemma 3.11.** Let $F_1, \ldots, F_n \in R_m[X_1, \ldots, X_n]$ be such that $\mathbb{C}[F_1, \ldots, F_n] = \mathbb{C}[X_1, \ldots, X_n]$ 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 $X + \epsilon H \in C_m$ for all $H \in (B_m)^n$ then $C_m = \text{Aut}_{R_m} A$.

**Proof.** Let $F \in \text{Aut}_{R_m} B_m$. Then $F \in \text{Aut}_{C_m}$ since $F^{-1} F = X + \epsilon H$ for some $H \in R_m[X_1, \ldots, X_n]^n$ we have $F = F \circ (X + \epsilon H)$. Hence $F \in C_m$. $\square$

**Lemma 3.14.** If $(X_1 + \epsilon H, X_2, \ldots, X_n) \in C_m$ for all $H \in B_m$, then $C_m = \text{Aut}_{R_m} B_m$.

**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 $(X_1, \ldots, X_{i-1}, X_i + \epsilon H, X_{i+1}, \ldots, X_n) \in C_m$ for all $H \in B_m$. We are going to proceed by induction.

Suppose $(X_1 + \epsilon H_1, X_2, \ldots, X_n) \in C_m$ 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 $H := (X_1 + \epsilon H_1, \ldots, X_i + \epsilon H_i, X_{i+1}, \ldots, X_n)$. Then $R_m[H] = B_m$ by lemma 3.11, so there exists $G_{i+1} \in B_m$ such that $H_{i+1} = G_{i+1}(H)$. Hence $(X_1, \ldots, X_i, X_{i+1} + \epsilon G_{i+1}, X_{i+2}, \ldots, X_n) \circ H = (X_1 + \epsilon H_1, \ldots, X_i + \epsilon G_{i+1}, X_{i+2}, \ldots, X_n)$. By induction and lemma 3.13 we are done. $\square$
Lemma 3.15. Suppose for all $k \geq 1$ and any arbitrary monomial $M (= cX^\alpha$ for some $c \in \mathbb{C}$) there exists some map $E_{k,M} \in C_m$ such that $E_{k,M} = (X_1 + cX^\alpha + \epsilon^{k+1}H, X_2, \ldots, X_n)$ for some $H \in B_m$. Then $C_m = \text{Aut}_{R_m}B_m$.

Proof. By lemma 3.14 we only have to prove that $(X_1 + cH, X_2, \ldots, X_n) \in C_m$ for all $H \in R_m[X_1, \ldots, X_n]$. We will proceed by induction on $k$.

Suppose that for any map $F := (X_1 + \epsilon H, X_2, \ldots, X_n) \in C_m$ such that $F - F' = (\epsilon^{k+1}H, 0, \ldots, 0)$ 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

$$F'' := F_1 \circ (E_{k, M_1})_1 \circ \ldots \circ (E_{k, M_s})_1 \mod \epsilon^{k+1}$$

$$= (F_1 - (\epsilon^k \sum_{j=1}^s M_j)) \circ (X_1 + \epsilon^k \sum_{j=1}^s M_j) \mod \epsilon^{k+1}$$

$$= F_1 \mod \epsilon^{k+1}.$$ 

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

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

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

$$\left(\epsilon^{d-1}X_1, X_2, \ldots, X_n\right) \left(X_1 + \epsilon^kX^d, X_2, \ldots, X_n\right) = \left(X_1 + \epsilon^kX^d, X_2, \ldots, X_n\right).$$

Furthermore defining $L := (X_1 + a_2X_2 + \ldots + a_nX_n, X_2, \ldots, X_n)$ we have

$$(*) \quad L^{-1}(X_1 + \epsilon^kX^d, X_2, \ldots, X_n)L = (X_1 + \epsilon^k(X_1 + a_2X_2 + \ldots + a_nX_n)^d, X_2, \ldots, X_n).$$

So maps of the form $(X_1 + \epsilon^k(X_1 + a_2X_2 + \ldots + a_nX_n)^d, X_2, \ldots, X_n) \mod \epsilon^{k+1}$ can be constructed (where only the first coordinate is not the identity). By lemma 3.12.2 we can make maps of the form $(X_1 + \epsilon^kH + \epsilon^{k+1}(\ldots), X_2, \ldots, X_n)$ where $H$ is any linear combination of polynomials of the form $(X_1 + a_2X_2 + \ldots + a_nX_n)^d$. Since these polynomials generate the $k$-vector space 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 $\geq 2$ we are done. □

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 $E_{k,d} \mod e^{k+1} = (X + e^k X^d)$ then there exists a map $F \in \mathcal{C}_m$ such that

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

and $h_d = 1$.

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

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

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

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

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

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

So we have $E_{k,d,\cdot} \in \mathcal{C}_m$ such that $E_{k,d,c} \mod e^{k+1} = (X + ce^k X^d)$ for any $c \in \mathbb{C}$. Now choose $a \in \mathbb{R}_m$ such that $a = 1 + \alpha$ for some $c \in \mathbb{C}$. Notice that $a^d \mod e^d = 1 + cde$ and $a^{-d} \mod e^d = 1 - cde$ (in fact, “analytically speaking” $d$ could be any real number). So now we have some $F \in \mathcal{C}_m$ such that

$F \mod e^{k+2} = E_{k,d,\alpha^{-1}}(a^{-1} X) E_{k,d,1}(aX)

= (X - e^k X^d - e^{k+1} G(\alpha^{-1} X) \sum_{i=0}^{s} h_i X^i)(X + e^k X^d + e^{k+1} H)(aX)$

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:

$F \mod e^{k+2} = (X - e^k X^d - e^{k+1} G(\alpha^{-1} X)(X + e^k X^d + e^{k+1} H)(\alpha X))$

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

$= (\alpha^{-1} X - e^k (1 - cde) X^d - e^{k+1} G(X))(\alpha X + e^k (1 + cde) X^d + e^{k+1} H(X))$

$= (\alpha^{-1} X - e^k X^d + e^{k+1} (cdX^d - G(X)))(\alpha X + e^k X^d + e^{k+1} (cdX^d + H(X)))$
\[
X + \alpha^{-1}e^kX^d + \alpha^{-1}e^{k+1}(cdX^d + H(X)) - \alpha^k(\alpha X + e^kX^d) + e^{k+1}(cd\alpha X - G(\alpha X))
\]
\[
= (X + (1 - \alpha)e^kX^d + e^{k+1}(cdX^d + H(X))) - e^k((1 + \alpha)X + e^kX^d) + e^{k+1}(cdX^d - G(X))
\]
\[
= (X + e^kX^d + e^{k+1}((cd - c)X^d + H(X)) - \alpha^k(X + \alpha X + e^kX^d) + e^{k+1}(cdX^d - G(X)).
\]

Now we have to differentiate between \(k = 1\) and \(k > 1\) since in the latter case \(e^k(X + \alpha X + e^kX^d)d = e^kX^d + d\alpha e^{k+1}X^d \mod e^{k+2}\) and in the case \(k = 1\) one has \(e^k(X + \alpha X + e^kX^d)d = (X + \alpha\alpha(X + X^d))d = e(X^d + cdX^{-1}(X + X^d)) \mod e^2 = eX^d + e^2(dx^d + dx^{2d-1})\). Let us do the case \(k > 1\):

\[
F \mod e^{k+2}
\]
\[
= (X + e^kX^d + e^{k+1}((cd - c)X^d + H(X)) - e^k(X + \alpha X + e^kX^d) + e^{k+1}(cdX^d - G(X))
\]
\[
= (X + e^kX^d + e^{k+1}((cd - c)X^d + H(X)) - (e^kX^d + \alpha d e^{k+1}X^d) + e^{k+1}(cdX^d - G(X))
\]
\[
= (X + e^{k+1}((c - ce)X^d + H(X)) + e^{k+1}(cdX^d - G(X))
\]
\[
= (X + e^{k+1}((c - (cd)X^d + H(X)) - G(X)).
\]

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 \(e^2(2cd - c - d)\).

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

\[
F' \mod e^{k+1}
\]
\[
= (c^{-1}X)(X + e^k\sum_{i=1}^{s} h_iX^i)(eX)(X + e^k\sum_{i=1}^{s} h_iX^i)
\]
\[
= (X + e^k\sum_{i=1}^{s} g_iX^i)(X + e^k\sum_{i=1}^{s} h_iX^i)
\]
\[
= (X + e^k\sum_{i=1}^{s} g_iX^i + e^k\sum_{i=1}^{s} h_iX^i)
\]
where \(g_i := e^{i-1}h_i\). 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 \( \tilde{F} := (a^{-1} X)^d (aX) \). Then
\[
\tilde{F} \mod e^{k+1}
= (a^{-1} X) (X + e^k \sum_{i=1}^{d-1} h'_i X^i) (aX)
= (X + e^k \sum_{i=1}^{d-1} a^{i-1} h'_i X^i)
= X + e^k \sum_{i=1}^{d-1} \tilde{h}_i X^i
\]
where \( \tilde{h}_i := a^{i-1} h'_i \). Hence \( \tilde{h}_d = 1 \), and if \( h'_i = 0 \) then \( \tilde{h}_i = 0 \).

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 \( E_{k,d} = (X + e^k X^d) \mod e^{k+1} \).

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
\[
F \equiv a^{k-1} a^{-1} X + e^k \sum_{i=0}^{d-1} \tilde{h}_i X^i
\]
where \( h_d = 1 \). Now by applying lemma 3.17.2 several times we have constructed a map \( F' \) which looks like
\[
F' \equiv a^k \sum_{i=0}^{d} \tilde{h}_i X^i.
\]
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 \( E_{k,d,c} := (X + ec^k X^d) \mod e^{k+1} = (a^{-1} X) E_{k,d}(aX) \) where \( a \in \mathbb{C} \) such that \( a^{d-1} = c \). Now using lemma 3.12 a few times we have
\[
F \circ E_{k,d-1,-h_d-1} \circ E_{k,d-2,-h_d-2} \circ \cdots \circ E_{k,2,-h_2} \circ (X - h_1 e^k X) \circ (X - h_0 e^k) \mod e^{k+1} = (X + e^k X^d)
\]
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.

Acknowledgements
I would like to thank Arno van den Essen for doing a lot of corrections (over and over again) and some stimulating discussions.

References


