doi:10.1006/jmaa.2001.7778, available online at http://www.idealibrary.com on IDEAL®

# Compositions of Polynomials with Coefficients in a Given Field

Alan Horwitz

*Pennsylvania State University, 25 Yearsley Mill Road, Media, Pennsylvania 19063*

*Submitted by Bruce C. Berndt*

Received January 24, 2001

Let $F \subset K$ be fields of characteristic 0, and let $K[x]$ denote the ring of polynomials with coefficients in $K$. Let $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, $a_n \neq 0$. For $p \in K[x]\backslash F[x]$, define $D_F(p)$, the $F$ deficit of $p$, to equal $n - \max\{0 \leq k \leq n : a_k \notin F\}$. For $p \in F[x]$, define $D_F(p) = n$. Let $p(x) = \sum_{k=0}^{n} a_k x^k$ and let $q(x) = \sum_{j=0}^{m} b_j x^j$, with $a_n \neq 0$, $b_m \neq 0$, $a_n, b_m \in F$, $b_j \notin F$ for some $j \geq 1$. Suppose that $p \in K[x]$, $q \in K[x]\backslash F[x]$, $p$ not constant. Our main result is that $p \circ q \notin F[x]$ and $D_F(p \circ q) = D_F(q)$. With only the assumption that $a_n b_m \in F$, we prove the inequality $D_F(p \circ q) \geq D_F(q)$. This inequality also holds if $F$ and $K$ are only rings. Similar results are proven for fields of finite characteristic with the additional assumption that the characteristic of the field does not divide the degree of $p$. Finally we extend our results to polynomials in two variables and compositions of the form $p(q(x, y))$, where $p$ is a polynomial in one variable. 

*Key Words:* polynomial; field; composition; iterate.

## 1. INTRODUCTION

Suppose that $p$ and $q$ are polynomials such that their composition, $p \circ q$, has all rational coefficients. Must the coefficients of $p$ or $q$ be all rational? The idea for this paper actually started with the following more general question. Let $F \subset K$ be fields of characteristic 0, and let $K[x]$ denote the ring of polynomials with coefficients in $K$. Suppose that $p$ and $q$ are polynomials in $K[x]$, and $p \circ q \in F[x]$. Must $p$ or $q$ be in $F[x]$? The answer is yes (see Theorem 7) if the leading coefficient and the constant term of $q$ are each in $F$. Theorem 7 follows easily from a more general result (Theorem 1) concerning the $F$ deficit, denoted by $D_F$, of the composition of two polynomials. $D_F$ is defined as follows: If $p \in K[x]\backslash F[x]$, $\deg(p) = n$, let $x^r$ be the largest power of $x$ with a coefficient not in $F$. We define the $F$ deficit of $p$, $D_F(p)$, to be $n - r$. For $p \in F[x]$, define $D_F(p) = n$. For example, if $F = Q$ (rational



0022-247X/02 $35.00

numbers), $K = R$ (real numbers), and $p(x) = x^5 - 5x^3 + \sqrt{3}x^2 - x + 1$, then $D_F(p) = 3$. Now suppose that the leading coefficients of $p$ and $q$ are in $F$, and that some coefficient of $q$(other than the constant term) is not in F(so that $q \notin F[x]$). Our main result, Theorem 1, states that $D_F(p \circ q) = D_F(q)$. With the weaker assumption that only the *product* of the leading coefficients of $p$ and $q$ is in $F$ we prove the *inequality* $D_F(p \circ q) \geq D_F(q)$ (see Theorem 4). It is interesting to note that if $q \in F[x]$, then we get the different equality $D_F(p \circ q) = D_F(p)D_F(q)$.

We also prove (Theorem 8) some results about the deficit of the *iterates*, $p^{[r]}$, of $p$, which require less assumptions than those of Theorem 1. In particular, $D_F(p^{[r]}) = D_F(p)$ with only the assumption that the leading coefficient of $p$ is in $F$. This assumption is necessary in general as the example $p(x) = ix$ shows with $F = R$ and $K = C$ (complex numbers).

One can, of course, define the $F$ deficit for *any* two sets $F \subset K$. While Theorem 1 does not hold in general if $F$ and $K$ are not fields, we can again prove the inequality $D_F(p \circ q) \geq D_F(q)$ if $F$ and $K$ are rings (see Theorem 12).

For fields of *finite characteristic d*, Theorem 1 follows under the additional assumption that $d$ does not divide $\deg(p)$.

Finally we extend our results to polynomials in two variables(using a natural definition of $D_F$ in that case) and compositions of the form $p(q(x, y))$, where $p$ is a polynomial in one variable. Our proof easily extends to compositions of the form $p(q(x_1, \ldots, x_r))$. However, the analog of Theorem 1 does not hold in general for compositions of the form $p(q_1(x, y), q_2(x, y))$ (even when $q_1 = q_2$), where $p$ is also a polynomial in two variables.

There are connections between some of the results in this paper and earlier work of Horwitz in [1] and [2], where we asked questions such as: If the composition of two power series, $f$ and $g$, is even, must $f$ or $g$ be even? One connection with this paper lies in the following fact: If $F = R$ and $K = C$, then $F[x]$ is invariant under the linear operator $L(f)(z) = \bar{f}(\bar{z})$. Of course, the even functions are invariant under the linear operator $L(f)(z) = f(-z)$. Note that in each case $L \circ L = I$. This connection does not extend to fields $F$ in general, however, since such an operator $L$ may not exist. The methods and results we use in this paper are somewhat similar to those of [1] and [2], but there are some key differences. Also, we only consider polynomials in this paper, since there is really no useful notion of the $F$ deficit for power series which are not polynomials.

## 2. MAIN RESULTS

Let $F \subset K$ be sets, with $F[x]$ equal to the set of all polynomials with coefficients in $F$.

DEFINITION 1. Let $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, $a_n \neq 0$. For $p \in K[x] \setminus F[x]$, define $D_F(p)$, the $F$ deficit of $p$, to equal $n - \max\{0 \leq k \leq n : a_k \notin F\}$. For $p \in F[x]$, define $D_F(p) = n$.

Note that $D_F(p) = n$ if and only if $a_k \in F\ \forall\, k \geq 1$ and $D_F(p) = 0$ if and only if $a_n \notin F$.

Most of the results in this paper concern the case where $F$ and $K$ are *fields*.

We shall need the following easily proven properties. For any fields $F \subset K$

$$u \in F,\ v \in K \setminus F \Rightarrow uv \in K \setminus F (\text{if } u \neq 0) \text{ and } u + v \in K \setminus F \tag{1}$$

and for fields of characteristic 0

$$v \in K \setminus F \Rightarrow nv \in K \setminus F \text{ for any } n \in Z_+. \tag{2}$$

Assume for the rest of this section that $F$ is a proper nonempty *subfield* of $K$, which is a field of *characteristic zero*. Later in the paper we discuss the case where $K$ is a field of finite characteristic or just a ring.

The following result shows that, under suitable assumptions, $q$ and $p \circ q$ have the same $F$ deficit.

THEOREM 1. *Suppose that* $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, *$p$ not constant,* $q(x) = \sum_{j=0}^{m} b_j x^j \in K[x] \setminus F[x]$ *with* $a_n \neq 0$, $b_m \neq 0$, $a_n, b_m \in F$, $b_j \notin F$ *for some* $j \geq 1$. *Then* $p \circ q \notin F[x]$ *and* $D_F(p \circ q) = D_F(q)$.

*Proof.* Let $d = D_F(q) < m$. Since $b_m \in F$, $d \geq 1$. By the definition of $D_F$, $b_{m-d} \notin F$, but $b_{m-(d-1)}, \ldots, b_m \in F$. Also, since $p$ is not constant, $n \geq 1$. We have

$$(p \circ q)(x) = \sum_{k=0}^{n} a_k \left( \sum_{j=0}^{m} b_j x^j \right)^k. \tag{3}$$

Consider the coefficient of $x^{mn-d}$ in $(p \circ q)(x)$. Since $mn - d > mn - m = m(n-1)$, this coefficient will only arise from the summand above with $k = n$, namely $a_n (q(x))^n$, which equals

$$a_n \left( \sum_{i_0 + \cdots + i_m = n} \frac{n!}{(i_0)! \cdots (i_m)!} (b_0)^{i_0} \cdots \left(b_m x^m\right)^{i_m} \right). \tag{4}$$

To get an exponent of $mn - d$ in (4), $\sum_{k=0}^{m} k i_k = mn - d$. Along with $\sum_{k=0}^{m} i_k = n$ this implies

$$m i_0 + (m-1) i_1 + \cdots + i_{m-1} = d. \tag{5}$$

Note that since $b_j \notin F$ for some $j \geq 1$, $d < m$, which implies that $m - (d + 1) \geq 0$. Now $mi_0 + (m-1)i_1 + \cdots + (d+1)i_{m-(d+1)} > d$ if some $i_j \neq 0$ for $0 \leq j \leq m - (d+1)$. That proves

$$i_j = 0 \text{ for } 0 \leq j \leq m - (d+1). \tag{6}$$

By (5) and (6), $di_{m-d} + (d-1)i_{m-(d-1)} + \cdots + i_{m-1} = d$. Since $b_j \in F$ for $j \geq m - (d-1)$, the only way to get a coefficient in (4) *not* in $F$ is if $i_{m-d} \neq 0$, which implies that $i_{m-d} = 1$, $i_{m-d+1} = i_{m-d+2} = \cdots = i_{m-1} = 0$. Also, from $i_{m-d} + i_{m-d+1} + \cdots + i_m = n$ we have $i_m = n - 1$. Hence the only way to obtain $x^{mn-d}$ in (4) using $b_{m-d}$ is $n(b_{m-d}x^{m-d})^1(b_m x^m)^{n-1}$. Now $b_{m-d}b_m^{n-1} \notin F$(by (1)), and all of the other terms in (4) which contribute to the coefficient of $x^{mn-d}$ involve $b_{m-(d-1)}, \ldots, b_m$. Hence, by (1) and (2), the coefficient of $x^{mn-d}$ in (4) is not in $F$, and it follows that $p \circ q \notin F[x]$. Now we want to show that the coefficient of $x^r$ in (3) will lie in $F$ if $r > mn - d$. Write $r = mn - d'$, where $d' < d$. Since $mn - d' > mn - d$, this coefficient will only arise in (3) with $k = n$. Arguing as above, to get an exponent of $mn - d'$ in (4), it follows that $i_j = 0$ for $0 \leq j \leq m - (d' + 1)$. Since $m - (d' + 1) \geq m - d$, $i_j = 0$ for $0 \leq j \leq m - d$, which implies that the coefficient of $x^r$ in (4) only involves $b_k$ with $k > m - d$. Since $b_{m-(d-1)}, \ldots, b_m \in F$, the coefficient of $x^r$ in (3) is also in $F$, and thus $D_F(p \circ q) = d$. ∎

If $q \in K[x]/F[x]$ and $b_0 \in F$, then $b_j \notin F$ for some $j \geq 1$. Theorem 4 then implies

COROLLARY 2. *Suppose that* $p(x) = \sum_{k=0}^n a_k x^k \in K[x]$, *p not constant*, $q(x) = \sum_{j=0}^m b_j x^j \in K[x] \backslash F[x]$. *Suppose that* $a_n \neq 0$, $b_m \neq 0$, $a_n, b_m, b_0 \in F$. *Then* $p \circ q \notin F[x]$ *and* $D_F(p \circ q) = D_F(q)$.

EXAMPLE 1. Let $F = Q, K = R$, $p(x) = x^3 + 2x^2 - \sqrt{2}x + 1$, $q(x) = x^2 + \sqrt{3}x + 5$. Then

$$\begin{aligned} p(q(x)) = x^6 + 3\sqrt{3}x^5 + 26x^4 + 37\sqrt{3}x^3 + (-\sqrt{2} + 146)x^2 \\ + (95\sqrt{3} - \sqrt{2}\sqrt{3})x + 176 - 5\sqrt{2}. \end{aligned}$$

Hence $D_F(p \circ q) = 1 = D_F(q)$.

Theorem 1 assumes that $q \notin F[x]$. For $q \in F[x]$ we have

THEOREM 3. *Suppose that* $p(x) = \sum_{k=0}^n a_k x^k \in K[x]$, $q(x) = \sum_{j=0}^m b_j x^j \in F[x]$, *with* $a_n \neq 0$, $b_m \neq 0$. *Then* $D_F(p \circ q) = D_F(p)D_F(q)$.

*Proof.* If $p$ is constant, then $p \circ q$ is constant, and thus $D_F(p \circ q) = 0 = D_F(p)D_F(q)$. So assume now that $p$ is not constant.

Case 1: $a_n \in F$ and $p \notin F[x]$.

Let $d = D_F(p) \Rightarrow d > 0$, $a_{n-d} \notin F$, and $a_{n-d+1}, \ldots, a_n \in F$. Consider the coefficient of $x^{mn-md}$ in $(p \circ q)(x)$. This coefficient will only arise in (3) with $k \geq n-d$. Since $a_k \in F$ for $k > n-d$, the only way to get a coefficient not in $F$ is with $a_{n-d}(q(x))^{n-d} = a_{n-d}b_m^{n-d}x^{mn-md} + \cdots$. Since $a_{n-d}b_m^{n-d} \notin F$, the coefficient of $x^{mn-md}$ is not in $F$. It also follows easily that if $r > mn - md$, then the coefficient of $x^r$ in (3) is in $F$. Thus $D_F(p \circ q) = mn - (mn - md) = md = D_F(p)D_F(q)$.

Case 2: $a_n \notin F$.
Then $D_F(p) = 0$ and $a_n b_m^n \notin F \Rightarrow D_F(p \circ q) = 0 = D_F(p)D_F(q)$.

Case 3: $p \in F[x]$.
Then $D_F(p \circ q) = mn = D_F(p)D_F(q)$. ∎

EXAMPLE 2. Let $F = Q$, $K = R$, $p(x) = x^4 - \sqrt{2}x$, and $q(x) = x^2 + 3x$. Then $p(q(x)) = x^8 + 12x^7 + 54x^6 + 108x^5 + 81x^4 - \sqrt{2}x^2 - 3\sqrt{2}x$. Hence $D_F(p \circ q) = 6 = (3)(2) = D_F(p)D_F(q)$.

*Remark* 1. Theorem 3 implies that if $q \in F[x]$, then $D_F(p \circ q) \geq D_F(q)$.

*Remark* 2. Theorem 1 does not hold in general if $a_n$ and/or $b_m$ are not in $F$. For example, let $F = Q$, $K = R$, $p(x) = \sqrt{2}x^3 + x^2 - x + \sqrt{5}$, $q(x) = 3\sqrt{2}x^2 + \sqrt{3}x + 5$. Then $D_F(p \circ q) = 1$ and $D_F(q) = 0$, and thus $D_F(p \circ q) \neq D_F(q)$. However, with the weaker assumption that $a_n b_m \in F$, one can prove an inequality.

THEOREM 4. *Suppose that* $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, *$p$ not constant,* $q(x) = \sum_{j=0}^{m} b_j x^j \in K[x]$, *with* $a_n \neq 0$, $b_m \neq 0$, $a_n b_m \in F$. *Then* $D_F(p \circ q) \geq D_F(q)$.

*Proof.* Case 1: $q \notin F[x]$ and $b_m \in F$.
By (1), $a_n \in F$ as well. If $b_j \notin F$ for some $j \geq 1$, then by Theorem 1, $D_F(p \circ q) = D_F(q)$. Now suppose that $b_j \in F$ for all $j \geq 1$. It is not hard to show that the coefficient of any power of $x > m(n-1)$ cannot involve $b_0$, and hence $D_F(p \circ q) \geq mn - m(n-1) = m = D_F(q)$.

Case 2: $q \notin F[x]$ and $b_m \notin F$. Then $D_F(q) = 0$ and the inequality follows immediately.

Case 3: $q \in F[x]$. Then $D_F(p \circ q) \geq D_F(q)$ by Theorem 3 (see the remark following the proof). ∎

*Remark* 3. Theorem 4 does not hold in general if $a_n b_m \notin F$. For example, let $F = Q$, $K = R$, $p(x) = \sqrt{2}x^3 + x^2 - x + 1$, and $q(x) = x^2 + \sqrt{3}x + 5$. Then clearly $D_F(p \circ q) = 0$ while $D_F(q) = 1$.

As an application of Theorem 1 we have the following result. Note that we do not assume that the leading coefficient of $p$ is in $F$.

PROPOSITION 5. *Suppose that* $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, *p not constant*, $q(x) = \sum_{j=0}^{m} b_j x^j \in K[x]\backslash F[x]$, *with* $a_n \neq 0$, $b_m \neq 0$, *and* $b_m \in F$. *If* $b_j \notin F$ *for some* $j \geq 1$, *then* $p \circ q \notin F[x]$.

*Proof.* If $a_n \notin F$, then $a_n b_m^n \notin F$, which implies that $p \circ q \notin F[x]$ since $a_n b_m^n$ is the coefficient of $x^{mn}$ in $p \circ q$. If $a_n \in F$, then $p \circ q \notin F[x]$ by Theorem 1. ∎

LEMMA 6. *Suppose that* $q(x) = \sum_{j=0}^{m} b_j x^j \in F[x]$ *and* $p \circ q \in F[x]$, $p(x) = \sum_{k=0}^{n} a_k x^k$, $a_n \neq 0$, $b_m \neq 0$, *q not constant*. *Then* $p \in F[x]$.

*Proof.* Note that $D_F(q) = m \geq 1 > 0$. Then by Theorem 3, $D_F(p) = \frac{D_F(p \circ q)}{D_F(q)} = \frac{mn}{m} = n$, and thus $a_k \in F$ for $k \geq 1$. Since $p \circ q \in F[x]$, $p(q(0)) = \sum_{k=0}^{n} a_k b_0^k \in F$. Since $b_0 \in F$, this implies that $a_0 \in F$. Hence $p \in F[x]$. ∎

Now we answer the following question mentioned in the Introduction. Suppose that $p \circ q \in F[x]$. Must $p$ or $q$ be in $F[x]$?

THEOREM 7. *Suppose that* $p, q \in K[x]$ *with* $p \circ q \in F[x]$, $q(x) = \sum_{j=0}^{m} b_j x^j$, $a_n \neq 0, b_m \neq 0, b_0, b_m \in F$. *Then* $p \in F[x]$ *or* $q \in F[x]$. *In addition, if* $p \circ q$ *is not constant, then* $p \in F[x]$ *and* $q \in F[x]$.

*Proof.* Suppose $p \circ q \in F[x]$. If $p \circ q$ is constant, then $p$ and/or $q$ is constant. If $p(x) = c$, then $(p \circ q)(x) = c$, which implies that $c \in F$ and hence $p \in F[x]$. If $q(x) = c$, then $c \in F$ since $b_0 \in F$ and hence $q \in F[x]$. Now suppose that $p \circ q$ is not constant. Then $q$ is not constant. If $q \notin F[x]$, then $b_j \notin F$ for some $j \geq 1$. By Proposition 5, $p \circ q \notin F[x]$, a contradiction. Hence $q \in F[x]$. Lemma 6 then shows that $p \in F[x]$ as well. ∎

*Remark* 4. Note that no restriction is needed on the leading coefficient of $p$. However, some restriction on the *leading coefficient* and *constant* term of $q$ are needed in order for Theorem 7 to hold in general. Simple examples are $p(x) = x - c$, $q(x) = x + c$ or $p(x) = (1/c)x$, $q(x) = cx$, with $c \in K$, $c \notin F$.

*Remark* 5. Theorem 7 does not hold in general if $F$ equals the complement of a field. For example, if $F =$ irrational numbers, let $p(x) = x^2$, $q(x) = \pi x^2 + x + \pi$. Then neither $p$ nor $q$ has all irrational coefficients, and the leading coefficient and constant term of $q$ are irrational. However, $p(q(x)) = \pi^2 x^4 + 2\pi x^3 + (2\pi^2 + 1)x^2 + 2\pi x + \pi^2$, which has all irrational coefficients.

*Remark* 6. If $S$ is any subset of $K$(not necessarily a subfield), we say that $S$ is a *deficit set* if Theorem 1 holds with $F$ replaced by $S$ throughout. For example, if $K = C =$ complex numbers, then it is not hard to show that $S = R \cup I =$ set of all real or imaginary numbers is a deficit set. It would be interesting to determine exactly what a deficit set must look like for a given field $K$.

### 2.1. *Iterates*

We now prove the analogs of Theorems 1, 4, and 7 when $p = q$. In this case we require less assumptions. In particular, for the analog of Theorem 4, we require no assumptions whatsoever. Let $p^{[r]}$ denote the $r$th iterate of $p$.

THEOREM 8. *Suppose that $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]\backslash F[x]$, with $a_n \neq 0$, $a_n \in F$. Then, for any positive integer $r$, $p^{[r]} \notin F[x]$ and $D_F(p^{[r]}) = D_F(p)$.*

*Proof.* Note that if $n = 0$, then $a_0 \in F \Rightarrow p \in F[x]$. Hence $n \geq 1$. If $n = 1$, then $p(x) = a_1 x + a_0$, $a_1 \in F$, $a_0 \notin F$. It is not hard to show that

$$p^{[r]}(x) = (a_1)^r x + a_0 \sum_{k=0}^{r-1} (a_1)^k.$$

Now $a_0 \sum_{k=0}^{r-1}(a_1)^k \notin F$ since $\sum_{k=0}^{r-1}(a_1)^k \in F$. Hence $p^{[r]}(x) \notin F[x]$ and $D_F(p^{[r]}) = 1 = D_F(p)$. Assume now that $n \geq 2$. First we prove the theorem for $p \circ p$,

$$(p \circ p)(x) = \sum_{k=0}^{n} a_k \left( \sum_{j=0}^{n} a_j x^j \right)^k. \tag{7}$$

If $a_j \notin F$ for some $j \geq 1$, then $D_F(p \circ p) = D_F(p)$ by Theorem 1 with $p = q$. So suppose now that $a_j \in F$ for $j \geq 1$ and $a_0 \notin F$. First let $k = n$ in (7) to get

$$a_n \left( \sum_{i_0 + \cdots + i_n = n} \frac{n!}{(i_0)! \cdots (i_n)!} (a_0)^{i_0} \cdots (a_n x^n)^{i_n} \right). \tag{8}$$

It follows easily that the highest power of $x$ in (8) involving $a_0$ is $n(n-1)$, obtained by letting $i_0 = 1$, $i_j = 0$ for $2 \leq j \leq n-1$, $i_n = n-1$. The coefficient of $x^{n(n-1)}$ in (8) is $n a_0 a_n^{n-1} \notin F$ by (1) and (2). The only other way to obtain $x^{n(n-1)}$ is by letting $k = n-1$ in (7) and letting $i_n = n-1$ in $a_{n-1}(\sum_{i_0+\cdots+i_n=n-1} \frac{(n-1)!}{(i_0)!\cdots(i_n)!}(a_0)^{i_0} \cdots (a_n x^n)^{i_n})$. This gives a coefficient of $x^{n(n-1)}$, which does *not* involve $a_0$. Hence the coefficient of $x^{n(n-1)}$ in $p \circ p$ equals $n a_0 a_n^{n-1} + c$, where $c \in F$. By ( 1), $n a_0 a_n^{n-1} + c \notin F$. Finally, it is not hard to show that any power of $x$ in (7) greater than $n(n-1)$ cannot involve $a_0$. Thus $D_F(p \circ p) = n^2 - n(n-1) = n = D_F(p)$. Now consider $p^{[r]} = p^{[r-2]} \circ q$, where $r \geq 3$, and $q = p \circ p = \sum_{j=0}^{m} b_j x^j$, $m = n^2$. Since $D_F(p \circ p) = D_F(p) \leq n$, $D_F(p \circ p) < n^2$ since $n \geq 2$. Hence $b_j \notin F$ for some $j \geq 1$. Since $b_m = a_n^{n+1} \in F$ and the leading coefficient of $p^{[r-2]}$ is also in $F$, $D_F(p^{[r]}) = D_F(p^{[r-2]} \circ q) = D_F(q)$(by Theorem 1) $= D_F(p \circ p) = D_F(p)$. It also follows that $p^{[r]} \notin F[x]$ since $D_F(p^{[r]}) = D_F(p) \leq n < n^2$. ∎

*Remark* 7. If $f(x) = (x/ax - 1)$, then $f(f(x)) = x \in F(x) =$ ring of formal power series in $x$. However, $f \notin F(x)$ if $a \notin F$, which implies that the first part of Theorem 8 fails in general for formal power series (we have not defined $D_F(f)$ for $f \in F(x)$).

*Remark* 8. Theorem 8 is not simply a trivial application of Theorem 1 using induction on $r$, with $q = p^{[r-1]}$. The reason is that one requires $b_j \notin F$ for some $j \geq 1$ to apply Theorem 1.

EXAMPLE 3. Let $F = R, K = C$, and $p(x) = x^3 + 4x^2 - 3ix + 2i$. Then $p(p(x)) = x^9 + 12x^8 + (48 - 9i)x^7 + (68 - 66i)x^6 + (5 - 96i)x^5 + (-8 + 72i)x^4 + (132 - 56i)x^3 + (-84 - 2i)x^2 + (39 + 36i)x - 10 - 6i \Rightarrow D_F(p \circ p) = 2 = D_F(p)$.

We now prove an inequality which holds for *all* $p$ in $K[x]$.

THEOREM 9. *Let* $p \in K[x]$. *Then* $D_F(p^{[r]}) \geq D_F(p)$.

*Proof.* If $p \in F[x]$, then $p^{[r]} \in F[x]$, which implies that $D_F(p^{[r]}) = n^r \geq n = D_F(p)$. If $p \in K[x]\backslash F[x]$ and $a_n \in F$, then by Theorem 8, $D_F(p^{[r]}) = D_F(p)$. Finally, if $a_n \notin F$, then $D_F(p) = 0 \leq D_F(p^{[r]})$. ∎

We now prove the analog of Theorem 7 for iterates.

THEOREM 10. *Suppose that* $p \in K[x]$, $p(x) = \sum_{k=0}^{n} a_k x^k$, $a_n \neq 0$, $a_n \in F$. *Assume also that* $p^{[r]} \in F[x]$ *for some positive integer* $r$. *Then* $p \in F[x]$.

*Proof.* If $p \notin F[x]$, then $p^{[r]} \notin F[x]$ by Theorem 8. ∎

*Remark* 9. Theorem 10 does not hold in general if $a_n \notin F$. For a counterexample, if there exists $a \in F$ with $a^{1/r} \notin F$, then let $p(x) = a^{1/r}x$.[1]

## 3. SEVERAL VARIABLES

As earlier, assume throughout that $F$ is a proper nonempty subfield of $K$, which is a field of characteristic zero. We now extend the definition of the $F$ deficit to polynomials in two variables. Write $p(x, y) = \sum_{k=0}^{n} p_k(x, y)$, where each $p_k$ is homogeneous of degree $k$, $p_n \neq 0$. If $p \in K[x, y]\backslash F[x, y]$, define $D_F(p) = n - \max\{k : p_k \notin F[x, y]\}$. For $p \in F[x, y]$, define $D_F(p) = n$. Then Theorems 1 and 4, with similar assumptions, do not hold in general for compositions of the form $p(q(x), q(x))$, where $q$ is a polynomial in one variable and $p$ is a polynomial in two variables. For example, let $F = R, K = C, p(x, y) = x^2 - y^2 + 1$, and $q(x) = x^2 + ix$. Then $p(q(x), q(x)) = 1$ and thus $D_F(p(q, q)) = 0 < 1 = D_F(q)$. Indeed,

[1]If $F =$ algebraic numbers and $K =$ real numbers, then such an $a$ does not exist.

Theorems 1 and 4 even fail for iterates of the form $p(p(x, y), p(x, y))$. For example, let $F = Q, K = R$, and $p(x, y) = y^2 - x^2 + \sqrt{3}x - \sqrt{5}y$. Then $p(p(x, y), p(x, y)) = \sqrt{3}y^2 - \sqrt{3}x^2 + 3x - \sqrt{3}\sqrt{5}y - \sqrt{5}y^2 + \sqrt{5}x^2 - \sqrt{5}\sqrt{3}x + 5y$, which implies that $D_F(p(p, p)) = 0 < 1 = D_F(p)$.

However, we can prove similar theorems for compositions of the form $p(q(x, y))$, where $p$ is a polynomial in *one* variable.

THEOREM 11. *Suppose that* $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x], 0 \neq a_n \in F$, *$p$ not constant. Suppose that* $q \in K[x, y] \backslash F[x, y]$, $q(x, y) = \sum_{j=0}^{m} q_j(x, y)$, *where each $q_j$ is homogeneous of degree $j$ with* $0 \neq q_m \in F[x, y]$. *If* $q_j(x, y) \notin F[x, y]$ *for some* $j \geq 1$, *then* $p \circ q = p(q(x, y)) \notin F[x, y]$ *and* $D_F(p \circ q) = D_F(q)$.

*Proof.* Our proof is very similar to the proof of Theorem 1, except that we have to work with the homogeneous polynomials $q_j(x, y)$ instead of the monomials $x^j$. This only complicates things a little.

$$p(q(x, y)) = \sum_{k=0}^{n} a_k \left( \sum_{j=0}^{m} q_j(x, y) \right)^k . \tag{9}$$

Let $d = D_F(q) < m$. By the definition of $D_F$, $q_{m-d} \notin F[x, y]$, $q_{m-(d-1)}, \ldots, q_m \in F[x, y]$. Also, $p$ not constant $\Rightarrow n \geq 1$ and $q_n \in F[x, y] \Rightarrow d > 0$. Now $(q_j(x, y))^k$ is homogeneous of degree $jk$, and $k < n$ implies that $jk \leq j(n-1) \leq m(n-1) < mn - d$. Hence a term of degree $mn - d$ can only arise in (9) if $k = n$, which gives

$$\begin{aligned} a_n(q(x, y))^n &= \left( \sum_{j=0}^{m} q_j(x, y) \right)^n \\ &= a_n \left( \sum_{i_0 + \cdots + i_m = n} \frac{n!}{(i_0)! \cdots (i_m)!} (q_0)^{i_0} \cdots (q_m)^{i_m} \right). \end{aligned} \tag{10}$$

Note that $m - d \geq 1 \Rightarrow m - (d+1) \geq 0$. Arguing exactly as in the proof of Theorem 1, to get an exponent of $mn - d$ in (10)

$$i_j = 0 \text{ for } 0 \leq j \leq m - (d+1). \tag{11}$$

Thus the only way to get a coefficient in (10) *not* in $F$ is if $i_{m-d} \neq 0$, which implies that $i_{m-d} = 1$, $i_{m-d+1} = i_{m-d+2} = \cdots = i_{m-1} = 0$. Also, from $i_{m-d} + i_{m-d+1} + \cdots + i_m = n$ we have $i_m = n - 1$. (10) then becomes $n a_n q_{m-d} q_m^{n-1}$, which we shall now show has at least one coefficient not in $F$. Let $g = q_{m-d} q_m^{n-1}$, which is homogeneous of degree $mn - d$. Write

$q_m^{n-1}(x,y) = \sum_{k=0}^{m(n-1)} c_k x^k y^{m(n-1)-k}$, $q_{m-d}(x,y) = \sum_{r=0}^{m-d} b_r x^r y^{m-d-r}$. Note that $c_k \in F$ for all $k$, while $b_r \notin F$ for some $r$. Let

$$M = \max\{r : 0 \le r \le m-d, b_r \notin F\},$$
$$N = \max\{k : 0 \le k \le m(n-1), c_k \ne 0\}.$$

Clearly $M$ and $N$ are well defined, $b_M \notin F$, and $c_N \in F$. Consider the coefficient of $x^{M+N} y^{mn-d-M-N}$ in $g$. One way to obtain this coefficient is $(b_M x^M y^{m-d-M})(c_N x^N y^{m(n-1)-N}) = b_M c_N x^{M+N} y^{mn-d-M-N}$. There are other ways to obtain this coefficient if $N > 0$ and $M < m-d$. Since $c_k = 0$ for $k > N$, one must choose $c_k x^k y^{m(n-1)-k}$ from $q_m^{n-1}$ with $k < N$ and $b_r x^r y^{m-d-r}$ from $q_{m-d}$ with $r > M$, which all involve coefficients in $F$. Since $b_M c_N \notin F$, the coefficient of $x^{M+N} y^{mn-d-M-N}$ in $g$ is not in $F$. Thus the coefficient of $x^{M+N} y^{mn-d-M-N}$ in $n a_n q_{m-d} q_m^{n-1}$ is not in $F$, which implies that $p(q(x,y)) \notin F[x,y]$.

Now write $(p \circ q)(x,y) = \sum_{l=0}^{mn} h_l(x,y)$, where each $h_l$ is homogeneous of degree $l$. Again, arguing exactly as in the proof of Theorem 1, since $q_{m-(d-1)}, \ldots, q_m \in F[x,y]$, it follows that $h_l \in F[x,y]$ for $l > mn-d$. This implies that $D_F(p \circ q) = mn - d$. ∎

*Remark* 10. Theorem 11 can be easily extended to compositions of the form $p(q(x_1, \ldots, x_r))$.

## 4. RINGS

Theorem 1 does not hold in general if $F$ is just a *ring*. For example, if $F = Z$, the ring of integers and $K = Q$, let $p(x) = x^2 + (2/3)x$ and $q(x) = 6x^2 + (3/2)x$. Then $a_2, b_2$, and $b_0$ are in $Z$, and $p(q(x)) = 36x^4 + 18x^3 + (25/4)x^2 + x$, which implies that $2 = D_F(p \circ q) \ne D_F(q) = 1$. Theorem 4 also does not hold if $F$ is a ring. However, if $F \subset K$, where $F$ and $K$ are rings of finite or infinite characteristic, we can prove

THEOREM 12. *Suppose that $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, $p$ not constant, $q(x) = \sum_{j=0}^{m} b_j x^j \in K[x] \backslash F[x]$, with $a_n \ne 0$, $b_m \ne 0$, $a_n, b_m \in F$, $b_j \notin F$ for some $j \ge 1$. Then $D_F(p \circ q) \ge D_F(q)$.*

*Proof.* Letting $d = D_F(q)$, the proof follows exactly as in the proof of Theorem 1, except that we cannot conclude that $b_{m-d} b_m \notin F$ if $F$ is only a ring. However, it does still follow that the coefficient of $x^r$ in (3) will lie in $F$ if $r > mn - d$. Hence, even if $b_{m-d} b_m \in F$, it follows that $D_F(p \circ q) \ge d$. ∎

## 5. FIELDS OF FINITE CHARACTERISTIC

Theorem 1 also does not hold in general if the field $F$ has *finite* characteristic. For example, suppose that $K$ is a finite field of order 4; $F = Z_2 \subset K$. Let $p(x) = x^2$ and let $q(x) = x^2 + 3x$. Then $p(q(x)) = x^4 + (3+3)x^3 + (3 \times 3)x^2 = x^4 + 2x^2$. Thus $D_F(q) = 1$ while $D_F(p \circ q) = 2$. The problem here is that the characteristic of $K$ divides the degree of $p$. If we assume that this does not happen, we have

THEOREM 13. *Let $F \subset K$ be fields of characteristic $t$. Suppose that $p(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, $p$ not constant, $q(x) = \sum_{j=0}^{m} b_j x^j \in K[x] \backslash F[x]$, with $a_n \neq 0$, $b_m \neq 0$, $a_n, b_m \in F$, $b_j \notin F$ for some $j \geq 1$. If $t \nmid n$, then $p \circ q \notin F[x]$ and $D_F(p \circ q) = D_F(q)$.*

*Proof.* We need the fact that if $r \in Z_+$ with $r < t$, then $ru \neq 0$ for any $u \in K$. This easily implies that $nu \neq 0$ if $t \nmid n$. It follows that if $u \notin F$, then $nu \notin F$ if $t \nmid n$. Hence, letting $d = D_F(q)$ and $u = b_{m-d} b_m \notin F$ we have $n b_{m-d} b_m \notin F$. Now the proof follows exactly as in the proof of Theorem 1. ∎

One can also prove versions of Theorems 4 and 7 for fields of finite characteristic. Theorem 7 also requires the additional assumption that $t \nmid n$. ∎

## 6. APPLICATIONS

The main theorems in this paper give information about the coefficients of $p \circ q$ and the iterates of $p$. All of the examples we give here use $F =$ rationals, $K =$ reals, though of course it is possible to construct examples from other fields of characteristic 0, from finite fields, or from rings. For example, let $p(x) = x^2 + c$, where $c$ is irrational. By Theorem 8, $D_F(p) = 2 \Rightarrow D_F(p^{[r]}) = 2$ for any $r \in Z_+$, which implies that the coefficient of $x^{2^r - 2}$ in $p^{[r]}(x)$ is irrational, while the coefficient of $x^{2^r - 1}$ in $p^{[r]}(x)$ must be rational.

Also, suppose that, given $r(x) \in K[x]$, one wants to determine if nonlinear polynomials $p, q \in K[x]$ exist with $r = p \circ q$. Given $p$ or $q$ as well, Theorems 1 or 7 can sometimes be used to give a quick negative answer. For example, let $r(x) = x^6 + ax^5 + bx^4 + \cdots$, where $a$ is rational and $b$ is irrational, and $q(x) = x^3 + Bx^2 + \cdots$, where $B$ is irrational. If $r = p \circ q$, then the leading coefficient of $p$ equals 1, and by Theorem 1, $D_F(q) = D_F(r) = 2$. But $D_F(q) = 1$ and thus no such $p$ exists.

The applications given here are probably of limited value. It would be nice to find other, perhaps more useful, applications of the theorems in this paper.

## 7. ENTIRE FUNCTIONS

The obvious extension of $F[x]$ to the class of *entire* functions $E$ is

$$S_F = \left\{ f \in E : f(z) = \sum_{k=0}^{\infty} a_k z^k,\ \ a_k \in F\ \forall k \right\}.$$

While there is no reasonable notion of $D_F(f)$ when $f$ is not a polynomial, one can attempt to extend Theorem 7 to $E$. The question then becomes: Suppose that $f(z)$ is entire and $q(z)$ is a polynomial, with leading coefficient and constant term in $F$. If $f \circ q \in S_F$, must $f \in S_F$ or $q \in S_F$? The following theorem gives a negative answer to this question for a large class of fields $F$.

THEOREM 14. *Let $F$ be a subfield of $C$, with either $F = R$ or $\pi^2 \notin F$. Then there exist an entire function $f(z)$ and a polynomial $q(z) = a_2 z^2 + a_1 z + a_0$ such that*:

(1) $f \notin S_F$ *and* $q \notin S_F$

(2) $a_0$ *and* $a_2$ *are both in* $F$

(3) $f \circ q \in S_F$.

*Proof.* Case 1: $F = R$.

Let $f(z) = \cos(i\pi\sqrt{z+2i}) = \cosh(\pi\sqrt{z+2i})$ and $q(z) = z^2 + 2(1+i)z$. Since $\cos(\sqrt{z})$ is an entire function, $f \in E$. Also, $a_0$ and $a_2$ are both real and $f(q(z)) = -\cosh(\pi(z+1)) \in S_F$. However, $f'(0) = (\pi/2(1+i))\sinh(\pi(1+i)) = (\pi(i-1)/4)\sinh\pi$, which is not real. Hence $f \notin S_F$ and $q \notin S_F$, but $f \circ q \in S_F$.

Case 2: $\pi^2 \notin F$.

Let $f(z) = \cos(\sqrt{z+\pi^2})$ and $q(z) = z^2 + 2\pi z$. Then $f(q(z)) = -\cos z \in S_F$. Now $q \notin S_F$ since $\pi \notin F$ and $f \notin S_F$ since $f''(0) = 1/4\pi^2 \notin F$.

## ACKNOWLEDGMENT

We thank the referee for suggesting the notion of the $F$ deficit and its use in strengthening the original version of Theorem 1.

## REFERENCES

1. Alan L. Horwitz, Even compositions of entire functions and related matters, *J. Austral. Math. Soc. Ser. A* **63** (1997), 225–237.
2. Alan L. Horwitz and Lee A. Rubel, When is the composition of two power series even?, *J. Austral. Math. Soc. Ser. A* **56** (1994), 415–420.