POLYNOMIAL DECOMPOSITION OVER RINGS

by

Brian Kenneth Wyman

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2010

Doctoral Committee:

Professor Michael E. Zieve, Chair
Professor Todd M. Austin
Professor Mel Hochster
Professor Jeffrey C. Lagarias
Professor Karen E. Smith

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Mike Zieve, for asking questions, for answering questions, and for his confidence and support throughout this research. He has worked tirelessly, and I as well as this thesis have greatly benefitted from this. I would also like to extend my thanks to Karen Smith for her support and assistance throughout my time at Michigan. Thanks to Julian Rosen for a discussion that helped develop the proof of GCD existence, as well to as my committee for their comments, which surely improved the quality of exposition in this thesis.

Thanks to Jim Davis, Bill Ross, and Ellen Leblanc for giving me my mathematical foundations.

Lastly, thanks to Jocelyn for her friendship, companionship, love, and support. You are the best.

TABLE OF CONTENTS

CHAPTER I

Introduction

It is well-known that the ring of polynomials (in one variable) over a field is a Euclidean domain, so that the multiplicative semigroup of this ring has unique prime factorization, and hence for instance any two elements have a greatest common divisor and a least common multiple. In this thesis we shall consider a different operation on the collection of nonzero polynomials over a field, namely the operation of functional composition: $f(x) \circ g(x) := f(g(x))$. This collection of polynomials again forms a semigroup, which turns out to enjoy several appealing properties. For instance, any two polynomials (over a field) have a greatest common divisor and a least common multiple under this operation. Moreover, for certain fields (such as $\mathbb{C}$ or $\mathbb{Q}$) there are even results describing the full extent of nonuniqueness of "prime factorization" in this semigroup.

These questions were originally studied for polynomials with complex coefficients, in the context of finding polynomial solutions of functional equations. The founders of modern iteration theory (Fatou, Julia, and Ritt) made intensive studies of these questions; for instance, the Julia set originally arose from such considerations, as a consequence of Julia's result that two commuting polynomials (under composition) have the same Julia set. The methods of Fatou, Julia, and Ritt involved geometric

and analytic techniques, so it was something of a surprise that their results could be extended to polynomials over fields other than the complex numbers. This was achieved by suitably "algebraicizing" these complex techniques, and was done by Engstrom [Eng41], Levi [Lev42], Fried and MacRae [FM69], Fried [Fri74], Dorey and Whaples [DW74], Schinzel [Sch82, Sch00], Tortrat [Tor88], and Zannier [Zan93]. Their results have numerous applications to various areas of mathematics. These applications include:

1. Bilu and Tichy's classification [BT00] of $f, g \in \mathbb{Z}[t]$ for which the Diophantine equation $f(x) = g(y)$ has infinitely many integer solutions.

2. Ghioca, Tucker, and Zieve's classification [GTZ08, GTZ] of complex polynomials having orbits with infinite intersection

3. Medvedev-Scanlon's classification [MS09] of affine varieties having an endomorphism which acts as a nonlinear univariate polynomial on each coordinate.

4. Pakovich's classification [Pak08] of compact subsets $A, B \subset \mathbb{C}$ and $f, g \in \mathbb{C}[x]$ such that $f^{-1}(A) = g^{-1}(B)$.

5. Fried's classification [Fri70] of polynomials in $\mathbb{Z}[x]$ which induce a permutation on $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p (see also [Tur95]).

In order to generalize and refine the arithmetic applications 1 and 5 above, some authors have studied polynomial decomposition in case the coefficient ring is an integral domain (see, for example, [Tur95], [Gus88], [DG06]). This theory is in its infancy – for instance, prior to the present thesis, the extent of nonuniqueness of prime factorization in $\mathbb{Z}[x]$ under the operation of functional composition was a complete mystery. We will resolve this and develop the arithmetic of functional composition over arbitrary (even noncommutative!) rings. In the process, we introduce many

new techniques, and surprisingly, we find that several results remain true for quite general classes of rings. It turns out that, in order to obtain a rich theory, one must restrict to the semigroup of monic polynomials (with coefficients in a specified ring R) under the operation of functional composition; we call this semigroup $\mathbb{M}_R$. In $\mathbb{M}_R$, the identity is x. The units (invertible elements) are the linear polynomials, and the irreducible elements (which we will refer to as *indecomposable*) are those $F \in \mathbb{M}_R$ of degree at least 2 such that if $F = F_1 \circ F_2$ (with F_1 and F_2 in $\mathbb{M}_R$) then one of F_1 and F_2 is necessarily linear.

We show in Theorem V.8 that in many situations any two elements of $\mathbb{M}_R$ have a least common multiple:

Theorem. *If R is a ring with no $\mathbb{Z}$-torsion, then every pair $f, g \in \mathbb{M}_R$ has a least common $\mathbb{M}_R$-composite whose degree is either* 0 *or* $\operatorname{lcm}(\deg(f), \deg(g))$.

In Theorem VI.10, we show the existence of greatest common divisors in $\mathbb{M}_R$ for a slightly more restrictive class of rings R:

Theorem. *Suppose R is a commutative ring with no $\mathbb{Z}$-torsion and no nonzero nilpotents. Then if $f, g \in \mathbb{M}_R$ have a nonconstant common $\mathbb{M}_R$-composite, there exists a greatest common $\mathbb{M}_R$-divisor of f and g having degree* $\gcd(\deg(f), \deg(g))$.

Our two main results are analogous to the two theorems of Ritt, which characterized nonuniqueness of decomposition for polynomials in $\mathbb{C}[x]$. First, we show that if there are two "prime factorizations" of the same polynomial, then they have the same length and involve indecomposables of the same degrees, though possibly in different orders. Moreover, any two such decompositions are related to each other by a sequence of "swaps". More specifically, for rings R with no nonzero nilpotents,

if we write

$$h_1 \circ h_2 \circ ... \circ h_r = f = g_1 \circ g_2 \circ ... \circ g_s,$$

for indecomposables $h_i, g_j \in \mathbb{M}_R$, then $r = s$, and a decomposition related to (we will define an equivalence relation on decompositions in Chapter VII) $g_1 \circ g_2 \circ ... \circ g_r$ can be obtained from $h_1 \circ h_2 \circ ... \circ h_r$ by a sequence of steps, each of which involves replacing two adjacent indecomposables by two new indecomposables with the same composite and with the same degrees as the original indecomposables but in the reverse order. In other words, we apply the substitution

$$a \circ b = c \circ d$$

for some indecomposables $a, b, c, d \in \mathbb{M}_R$ with $\deg(a) = \deg(d)$ and $\deg(b) = \deg(c)$. These exchanges are often called "Ritt swaps" in the case of fields.

The precise statement below is given as Theorem VII.5, which holds over any ring with no nonzero nilpotents. The result is reminiscent of the Jordan-Hölder theorem.

Theorem. *Let R be a ring with no nonzero nilpotents. Then if $F = G_1 \circ G_2 \circ ... \circ G_r = H_1 \circ H_2 \circ ... \circ H_s$, where $F, G_i, H_i \in \mathbb{M}_R$ and where G_i, H_i are indecomposable over $\mathbb{M}_R$ and are of degree > 1, and where the degree of F in R (i.e., $1 + 1 + 1 + ... + 1$, $\deg(F)$ times) is neither 0 nor a zero divisor in R, it follows that $r = s$ and that the sequences $\langle \deg(G_i) \rangle_{i \leq r}, \langle \deg(H_i) \rangle_{i \leq r}$ are permutations of each other. Moreover, there exists a finite chain of decompositions $F = F_1^{(j)} \circ ... \circ F_r^{(j)} (1 \leq j \leq n)$ with $F_i^{(j)} \in \mathbb{M}_R$ indecomposable over $\mathbb{M}_R$ such that*

1. $\langle F_i^{(1)} \rangle_{i \leq r} = \langle G_i \rangle_{i \leq r}$,
2. *there exist invertible linear $L_1, ..., L_{r-1} \in \mathbb{M}_R$ such that*
   (a) $H_1 = F_1^{(n)} \circ L_1$

(b) $H_j = L_{j-1}^{-1} \circ F_j^{(n)} \circ L_j, \qquad$ *for* $1 < j < r$

(c) $H_r = L_{r-1}^{-1} \circ F_r^{(n)}$

3. for each $j < n$*, there exists* $k < r$ *such that*

$$F_k^{(j)} \circ F_{k+1}^{(j)} = F_k^{(j+1)} \circ F_{k+1}^{(j+1)},$$

with $\deg(F_k^{(j)}) = \deg(F_{k+1}^{(j+1)})$ *coprime to* $\deg(F_{k+1}^{(j)}) = \deg(F_k^{(j+1)})$*, and for each* $i \neq k, k+1$*, we have* $F_i^{(j)} = F_i^{(j+1)}$*. That is, the decompositions* $\langle F_i^{(j)} \rangle_{i \leq r}$ *and* $\langle F_i^{(j+1)} \rangle_{i \leq r}$ *differ only by having two consecutive terms with the same composition and reversed coprime degrees.*

We provide counterexamples to this theorem for rings with nonzero nilpotents, namely in $\mathbb{Z}[T]/\langle T^2 \rangle$ (Example VII.9). We also provide counterexamples in some rings where $\deg(F)$ in R is 0 or a zero divisor. For instance, we exhibit counterexamples in $\mathbb{Z}[T]/\langle 2T \rangle$ (Example VII.8) and in any ring of characteristic p prime (Example VII.7).

Our second main result characterizes Ritt swaps in integral domains. That is, we solve the functional equation $a \circ b = c \circ d$ where $\deg(a) = \deg(d)$ and $\deg(b) = \deg(c)$. When reduced to the case $\gcd(\deg(a), \deg(b)) = 1$, there is a surprisingly restrictive solution set to this functional equation when R is an integral domain. Namely, up to composing on both sides by linears, the only solutions are

$$\begin{aligned} x^n \circ x^r h(x^n) &= x^r (h(x))^n \circ x^n \\ D_n(x, t^m) \circ D_m(x, t) &= D_m(x, t^n) \circ D_n(x, t), \end{aligned}$$

where $n, m, r \in \mathbb{Z}_{>0}$ and $h \in \mathbb{M}_R$, and where $D_n(x, t)$ is the Dickson polynomial of degree n and parameter t (see Definition VII.10). Dickson polynomials are a generalization of Chebychev polynomials.

More precisely,

Theorem. *Let R be an integral domain, and let $A, B, G, H \in \mathbb{M}_R$ satisfy* $\deg(A) = \deg(H) = n > 1$ *and* $\deg(B) = \deg(G) = m > n$, *where* $\gcd(m, n) = 1$ *and* $G'H' \neq 0$. *Then $G \circ A = H \circ B$ if and only if there exist linear $L_1, L_2, L_3, L_4 \in \mathbb{M}_R$ such that either of the following holds:*

1. *For some $P \in \mathbb{M}_R$ and $r > 0$,*
   (a) $L_1 \circ G \circ L_2 = x^r P(x)^n$,
   (b) $L_2^{-1} \circ A \circ L_3 = x^n$,
   (c) $L_1 \circ H \circ L_4 = x^n$, *and*
   (d) $L_4^{-1} \circ B \circ L_3 = x^r P(x^n)$.
2. *For some $t \in R$ and $m, n > 0$,*
   (a) $L_1 \circ G \circ L_2 = D_m(x, t^n)$,
   (b) $L_2^{-1} \circ A \circ L_3 = D_n(x, t)$,
   (c) $L_1 \circ H \circ L_4 = D_n(x, t^m)$, *and*
   (d) $L_4^{-1} \circ B \circ L_3 = D_m(x, t)$.

We present an example showing that this result fails in a nondomain with few other notable properties - namely, in $\mathbb{Z}[a, b]/\langle ab \rangle$ (Example VII.23).

Over fields, the proofs of many of these results depend on a theorem of Lüroth, which states that for any field K, if a field L satisfies $K < L < K(x)$ where x is transcendental over K, then $L = K(y)$ for some y. In the language of algebraic geometry, Lüroth showed that unirational (dominated by projective space) curves are rational (birational to projective space). For any $f, g \in K[t]$, applying Lüroth's theorem to the subfields $K(f(t)) \cap K(g(t))$ and $K(f(t), g(t))$ of $K(t)$ shows (after

a short ramification argument) that f and g have a least common composite and a greatest common divisor (see, for example, [Sch00, Theorem 5]). Conversely, the existence of least common composites and greatest common divisors seems only slightly weaker than the full Lüroth theorem. In this thesis, we provide a Lüroth-free proof of several consequences (in the case R is a field) of Lüroth's theorem. We hope that this may point to an analog of Lüroth's theorem in a more general setting, namely to other one-dimensional schemes such as the affine line over certain rings.

In the following chapter, a guide to the definitions and notational conventions used throughout the thesis is provided. In Chapter III, several preliminary results regarding polynomial decomposition are presented. In Chapter IV, we consider decompositions and common composites over extension rings and their relationship to decompositions and common composites over a base ring. In Chapter V, we prove existence of least common composites in various settings, and we provide results about the degrees of common composites. Chapter VI gives a proof of the existence of greatest common divisors in certain classes of polynomial rings, and results are presented describing when the greatest common divisor has optimal degree. Lastly, results describing nonuniqueness of factorization in $\mathbb{M}_R$ are presented in Chapter VII.

CHAPTER II

Preliminaries

In this chapter, we introduce several definitions and establish notation that will be used throughout this thesis.

R is a ring, not necessarily commutative, with 1. Given R, we denote by $\mathbb{P}_R$ the monoid of polynomials in $R[x]$ under the operation of functional composition. We denote by $\mathbb{M}_R$ the submonoid of $\mathbb{P}_R$ consisting of monic polynomials. We do not consider 0 to be monic.

We denote the degree of a polynomial F by $|F|$. Let $S \in \{\mathbb{M}_R, \mathbb{P}_R\}$, and suppose $A, F \in S$. We refer to $H = A \circ F$ as a *left S-composite* of F and as a *right S-composite* of A. Similarly, we say that F is a *right S-divisor* of H and that A is a *left S-divisor* of H. In the following chapters, we present results about left composites and right divisors, but we do not give any results regarding right composites and left divisors. Therefore, we omit the left and right when discussing composites and divisors. Namely, $H = A \circ F$ is an *S-composite* of F, and F is an *S-divisor* of H.

We say that H is a *common S-composite* of polynomials $F, G \in R[x]$ if H is an S-composite of both F and G. Note that 1 is an S-composite of every polynomial in S, hence a common S-composite of all pairs of polynomials in S. For $F, G \in S$, we say that H is a *least common S-composite* of F and G if H is a common S-composite

of F and G and if every common S-composite H_0 of F and G is also an S-composite of H.

Similarly, we say that $F \in S$ is a *common S-divisor* of H and G if H and G are S-composites of F. If $F \in S$ is a common S-divisor of H and G such that all common S-divisors of H and G are also S-divisors of F, then we say F is a *greatest common S-divisor* of H and G. We note that when $S = \mathbb{M}_R$, the notions of least common S-composite and greatest common S-divisor coincide with those of the least common multiple and greatest common divisor in $\mathbb{M}_R$.

A polynomial $F \in S$ is *indecomposable over S* if $|F|$ is at least 2 and if $F = F_1 \circ F_2$ (with $F_1, F_2 \in S$) implies $|F_1| = 1$ or $|F_2| = 1$. If $|F| \geq 2$ and F is not indecomposable over S, we say that F is *decomposable over S*.

A *decomposition* of a polynomial F over S is a tuple $(F_1, F_2, ..., F_n)$ such that $F_i \in S$ and $F = F_1 \circ F_2 \circ ... \circ F_n$.

We denote by $O_R(x^n)$ the collection of polynomials in $R[x]$ whose degrees do not exceed n. Where the context is otherwise clear, we denote this collection of polynomials by $O(x^n)$. For brevity, we often write $f(x) = O(x^n)$, meaning that $f(x) \in O(x^n)$. This allows such sentences as "$f(x) = p(x) + O(x^n)$" as a convenient shorthand for "$f(x) = p(x) + q(x)$ for some polynomial $q(x) \in O(x^n)$".

We denote by $R\{x_1, x_2, ..., x_k\}$ the set of polynomials in the noncommuting variables $\{x_1, ..., x_k\}$ with coefficients in R. Though the indeterminates do not commute with each other, we require that they commute with all elements of R.

Let R be a commutative ring and M an R-module. An element $m \in M$ is an *R-torsion element* if there exists $r \in R$ that is neither 0 nor a zero divisor such that $rm = 0$. Then the *R-torsion submodule* $\mathrm{Tor}_R(M) = \{m \in M : rm = 0 \text{ for some nonzero } r \in R\}$. All rings may be considered as $\mathbb{Z}$-modules (by their abelian group

structure). We write $\mathrm{Tor}(R)$ as a shorthand for $\mathrm{Tor}_{\mathbb{Z}}(R)$. We say that a ring R has no $\mathbb{Z}$-torsion if $\mathrm{Tor}(R) = \{0\}$.

We say that a nonzero element $r \in R$ is a *zero divisor in* R if there exists a nonzero $s \in R$ such that $rs = 0$ or $sr = 0$. In particular, we do not regard 0 as a zero divisor.

For a nonnegative integer k, we refer to the element $1 + 1 + 1 + ... + 1$ (k times) of R as *the image of* k *in* R, and we denote this element by k_R.

CHAPTER III

Polynomial Decomposition

In this chapter, we begin our classification of decompositions of polynomials. The main result is Theorem III.3, which states that given a polynomial $H \in \mathbb{M}_R$ and $m, n \in \mathbb{Z}_{>0}$ such that $mn = |H|$ is neither 0 nor a zero divisor in R, there is at most one pair $F, G \in \mathbb{M}_R$ with $|F| = n$ and $|G| = m$ such that $H = F \circ G$.

To this end, we first describe a subset of the coefficients of $F \circ G$ in terms of the coefficients of F and G.

Lemma III.1. *Given $m, n \geq 1$, there are polynomials $r_i \in \mathbb{Z}\{x_{i+1}, x_{i+2}, ..., x_{m-1}\}$ for $0 \leq i \leq m-1$ and $s_j \in \mathbb{Z}\{y_{n-1}, y_{n-2}, ..., y_{j+1}, x_0, x_1, ..., x_{m-1}\}$ for $1 \leq j \leq n-1$ with the property that: for any ring R and any $a_0, ..., a_{n-1}, b_0, ..., b_{m-1}$ in R, the coefficient of $x^{nm-\ell}$ in $\left(x^n + \sum_{i=0}^{n-1} a_i x^i\right) \circ \left(x^m + \sum_{j=0}^{m-1} b_j x^j\right)$ equals*

1. *$nb_{m-\ell} + r_{m-\ell}(b_{m-\ell+1}, b_{m-\ell+2}, ..., b_{m-1})$ if $1 \leq \ell \leq m-1$,*
2. *$a_{n-k} + s_{n-k}(a_{n-1}, a_{n-2}, ..., a_{n-k+1}, b_0, b_1, ..., b_{m-1})$ if $\ell = km$ with $2 \leq k \leq n$, and*
3. *$nb_0 + a_{n-1} + r_0(b_1, b_2, ..., b_{m-1})$ if $\ell = m$.*

Proof. Let $a_n = b_m = 1$, and let $f = \sum_{i=0}^{n-1} a_i x^i$, and let $g = \sum_{j=0}^{m} b_j x^j$. Note that $f \circ g = x^n \circ g + O(x^{nm-m})$, so that for each $k < m$, the coefficient of x^{nm-k} contains no terms dependent on $a_0, a_1, ..., a_{n-1}$. Consider the highest degree term of $x^n \circ g$

with coefficient depending on b_{m-k}. It is clear that the degree of this term is $(m-k)+(n-1)m = nm-k$. This observation implies that the coefficient of x^{nm-k} in $f \circ g$ contains no terms dependent on $b_{m-k-1}, ..., b_0$. Moreover, the term of this coefficient dependent on b_{m-k} is $\binom{n}{1} b_{m-k} = nb_{m-k}$, and it follows that for $1 \leq k \leq m-1$, the coefficient of x^{nm-k} in $f \circ g$ is $nb_{m-k} + r_{m-k}($, where $r_{m-k}(b_{m-k+1}, b_{m-k+2}, ..., b_{m-1})$ for some $r_{m-k} \in \mathbb{Z}\{x_{m-k+1}, x_{m-k+2}, ..., x_{m-1}\}$.

For $2 \leq k \leq n$, to consider the coefficient of x^{nm-km} in $f \circ g$, notice that

$$\begin{aligned} f \circ g &= \left(\sum_{i=n-k+1}^{n} a_i x^i \right) \circ g + a_{n-k} x^{n-k} \circ g + O(x^{nm-(k+1)m}) \\ &= \left(\sum_{i=n-k+1}^{n} a_i x^i \right) \circ g + \left(a_{n-k} x^{nm-km} + O(x^{nm-km-1}) \right) + O(x^{nm-(k+1)m}). \end{aligned}$$

It follows that the coefficient of x^{nm-km} in $f \circ g$ is

$a_{n-k} + s_{n-k}(a_{n-k+1}, a_{n-k+2}, ..., a_{n-1}, b_0, b_1, ..., b_{m-1})$ for some

s_{n-k} in $\mathbb{Z}\{x_1, x_2, ..., x_{k-1}, y_0, y_1, ..., y_{m-1}\}$ whose coefficients depend only on m and n.

Lastly, we compute the coefficient of x^{nm-m} in $f \circ g$.

$$\begin{aligned} f \circ g &= x^n \circ g + a_{n-1} x^{n-1} \circ g + O(x^{nm-2m}) \\ &= x^n \circ g + (a_{n-1} x^{nm-m} + O(x^{nm-m-1})) + O(x^{nm-(k+1)m}) \\ &= (nb_0 + q(b_1, ..., b_{m-1}) + a_{n-1}) x^{nm-m} + O(x^{nm-m-1}), \end{aligned}$$

for some polynomial $q \in \mathbb{Z}\{y_1, ..., y_{m-1}\}$ whose coefficients depend only on m and n. The lemma follows directly. □

A corollary of Lemma III.1 is that we can find approximate decompositions. Given polynomials A and f with the degree of f dividing the degree of A, we can obtain a polynomial g so that $f \circ g$ agrees with A in the high-order terms.

Corollary III.2. *Let $A \in \mathbb{M}_R$ have degree nm, where n_R is a unit in R. If $f \in \mathbb{M}_R$ is of degree n, then there exists a unique $g \in \mathbb{M}_R$ such that $|g| = m$ and $|A - f \circ g| <$*

$m(n-1)$. *Also, for any element* $r \in R$ *there exists a unique monic* $g \in \mathbb{M}_R$ *such that* $|g| = m$, $g(0) = r$, *and* $|A - f \circ g| \leq m(n-1)$.

Proof. Write $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$, and $A(x) = \sum_{i=0}^{nm} c_i x^i$. The b_j's are undetermined, except that $b_m = 1$. By Lemma III.1, for $1 \leq l \leq m-1$, the coefficient of x^{nm-l} in $f \circ g$ is $nb_{m-l} + r_{m-l}$ for some element $r_{m-l} \in \mathbb{Z}\{b_{m-k+1}, b_{m-k+2}, ..., b_{m-1}\}$. The unique solution to $c_{nm-l} = nb_{m-l} + r_{m-l}$ is $b_{m-l} = \frac{1}{n}(c_{nm-l} - r_{m-l}) \in R$, since n_R is a unit. Solving for $b_1, ..., b_{n-1}$ in this manner, we ensure that A and $f \circ g$ agree in all terms of degree greater than $nm - m$. Again by Lemma III.1, we have $c_{nm-m} = nb_0 + a_{n-1} + r_0$ for some element $r_0 \in \mathbb{Z}\{b_1, b_2, ..., b_{m-1}\}$. We may solve, obtaining $b_0 = \frac{1}{n}(c_{nm-m} - a_{n-1} - r_0)$ to obtain $g(x)$ such that $|A - f \circ g| < m(n-1)$. If instead, we assert that $b_0 = g(0) = r$, we obtain $g(x)$ such that $|A - f \circ g| \leq m(n-1)$. □

It is crucial that n_R be neither 0 nor a zero divisor. For example, if $\mathrm{char}(R) = p$ prime, the for every $g \in \mathbb{P}_R$, we see that $x^p \circ g$ only has terms of degree divisible by p. Therefore for every g, we have that

$$|(x^{2p} + x^{2p-1}) - x^p \circ g| \geq 2p - 1.$$

Though Corollary III.2 requires n to be a unit in R, we can often work around this issue by passing to an extension ring in which n is invertible. For example, we do exactly this when proving the following theorem, which states that given a polynomial $H \in \mathbb{M}_R$ and degrees m and n such that $mn = |H|$, there is only one ordered pair of monic polynomials of degrees m and n respectively (up to a constant shift) whose composite agrees with H in the coefficients described by Lemma III.1.

Theorem III.3. *Let* $H \in \mathbb{M}_R$, *and let* m, n *be positive integers such that* $mn = |H|$ *and* n_R *is neither* 0 *nor a zero divisor. Then for any* $r \in R$, *there exist unique* $F, G \in \mathbb{M}_{R\left[\frac{1}{n}\right]}$ *such that*

1. $|F| = n$,
2. $|G| = m$,
3. $G(0) = r$, *and*
4. H *and* $F \circ G$ *agree in the coefficients of* x^{mn-k} *for* $1 \leq k \leq m-1$ *and in the coefficients of* x^{mn-km} *for* $1 \leq k \leq n$.

Remark III.4. $R\left[\frac{1}{n}\right]$ makes sense whenever n_R is neither 0 nor a zero divisor.

Proof. By Lemma III.1, we may use the coefficients of x^{mn-k} in H (for $1 \leq k \leq m-1$) to solve uniquely for the coefficients of x^{m-k} in G. Then we use the coefficients of x^{mn-km} in H (for $1 \leq k \leq n$) to solve uniquely for the coefficients of x^{n-k} in F. □

Note that $F \circ G$ may not equal H, but this theorem suggests an (efficient) algorithm for finding decompositions of a polynomial $H \in R[x]$. Namely, find all pairs of positive integers m, n such that $mn = |H|$. Then for each pair m, n, find the unique F and G guaranteed by Corollary III.3. Finally, compute $F \circ G$ to see if it agrees with H in all coefficients. This algorithm was presented in a 1989 paper of Kozen and Landau [KL89]. Of course, given a pair m, n, if n_R is 0 or a zero divisor, an alternate approach is required. See, for example, papers of Barton and Zippel [BZ85] and von zur Gathen [vzG91]. Finding a practical, efficient decomposition algorithm when H_R is 0 or a zero divisor remains an open problem.

CHAPTER IV

Decomposition and Common Composites over Extension Rings

In this chapter, we study the relationship between polynomial decomposition over a ring and polynomial decomposition over an extension ring. In Section 4.1, the general theme is that in many instances, when polynomials are related by some composition, we can show that the coefficients of one polynomial are elements of a subring S of R if the coefficients of one or more of the other polynomials also lie in S. In Section 4.2, we consider the relationship between common composites over an extension ring and common composites over a base ring.

4.1 Decomposition over Extension Rings

In our first such result, we prove that if g is nonconstant and both $f \circ g$ and g have coefficients in some subring S of R, then the coefficients of f are also in S.

Lemma IV.1. *Suppose S is a subring of a ring R. If $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{M}_R$ has degree n and $g = \sum_{j=0}^{m} b_j x^j \in \mathbb{M}_S$ has degree $m > 0$, and if $f \circ g \in \mathbb{M}_S$, then $f \in \mathbb{M}_S$.*

Proof. If $n = 0$, the result is clear, so assume $n > 0$. We show by induction on k that $a_{n-k} \in S$ for $0 \leq k \leq n$. The base case $k = 0$ is clear; since f is monic, $a_n = 1 \in S$. Now assume that $1 \leq k \leq n$ and that $a_n, a_{n-1}, a_{n-2}, ..., a_{n-k+1} \in S$.

By Lemma III.1, the coefficient of x^{nm-km} in $f \circ g$ is $a_{n-k} + s_{n-k}$, where $s_{n-k} \in Z\{a_{n-k+1}, ..., a_{n-1}, b_0, b_1, ..., b_{m-1}\}$. Since $\{a_{n-k+1}, ..., a_{n-1}, b_0, b_1, ..., b_{m-1}\} \subset S$, it follows that $s_{n-k} \in S$, and hence $a_{n-k} \in S$. □

Remark IV.2. The condition $m > 0$ is necessary, since otherwise for any subring S of R and any $r \in S \setminus R$, the polynomials $f(x) = x^2 + rx - r \in \mathbb{M}_R \setminus \mathbb{M}_S$ and $g(x) = 1 \in \mathbb{M}_S$, we have $f \circ g = 1 \in \mathbb{M}_S$.

We also note that if both $f \circ g$ and f have coefficients in some subring S of R, it does not follow that the coefficients of g are in S, as illustrated by the following example.

Example IV.3. Let $R = \mathbb{Z}[t]/\langle t^2 \rangle$, and let S be the subring of R generated by $\{1, 2t\}$. Now

$$x^2 \circ (x^2 + tx) = x^4 + 2tx^3.$$

Both x^2 and $x^4 + 2tx^3$ are elements of $\mathbb{M}_S$, but $t \notin S$, so $x^2 + tx \in \mathbb{M}_R \setminus \mathbb{M}_S$.

We now show that, under certain conditions, if a composite $H = F \circ G \in \mathbb{M}_S$ and $F, G \in \mathbb{M}_R$, then the coefficients of F and G, while not necessarily in S, are integral over S.

We first remind the reader of the notion of ring elements integral over a subring.

Definition IV.4. Let S be a subring of R. An element $r \in R$ is *integral over* S if r is the root of a polynomial in $\mathbb{M}_S$.

The elements of a commutative ring R that are integral over S form a subring of R. This proof can be found in a number of algebra textbooks, e.g. [DF99, p.666, Cor. 19]. We include the proof for the reader's convenience.

Proposition IV.5. *Let S be a subring of a commutative ring R. The set I_S of elements of R integral over S is a subring of R containing S.*

Proof. An element $r \in R$ is integral over S if and only if $S[r]$ is a finitely generated S-module. If $r, s \in R$ are both integral over S, then $S[r]$ and $S[s]$ are both finitely generated S-modules; hence, so is $S[r, s]$. Since $r - s$ and rs are both elements of $S[r, s]$, it follows that $S[r - s]$ and $S[rs]$ are finitely generated S-modules, so $r - s$ and rs are integral over S. Hence I_S is a subring of S. The result follows, since all elements of S are clearly integral over R. □

The set I_S is called the *integral closure* of S in R.

We now present the main result of this section.

Theorem IV.6. *Let S be a subring of R. If $F = G \circ H$ with $G, H \in \mathbb{M}_R$ and $F \in \mathbb{M}_S$, and if for some root α of G we have $F(x) = A(x) \cdot (H(x) - \alpha)$ where A and $H(x) - \alpha$ factor into monic linears in $\mathbb{M}_R$, then the coefficients of H are integral over S. If $|G|_S$ is neither 0 nor a zero divisor, then the coefficients of G are elements of $S\left[b_0, b_1, ..., b_{|H|-1}\right]\left[|G|_S^{-1}\right]$, where b_j is the coefficient of x^j in H.*

Proof. Let $G(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{M}_R$ and $H(x) = \sum_{j=0}^{m} b_j x^j \in \mathbb{M}_R$. Now let I_S be the integral closure of S in R, and suppose that $F(x) = G(H(x))$ and that $G(\alpha) = 0$. Suppose further that $F(x) = A(x) \cdot (H(x) - \alpha)$ for some $A \in \mathbb{M}_R$ and that both $A(x)$ and $H(x) - \alpha$ factor into linears in $\mathbb{M}_R$. Now, $H(x) - \alpha$ is the product of monic linear factors of the form $(x - r)$. Each such r is integral over S, since $F(r) = 0$. Since the elements of R that are integral over S form a subring, it follows that the coefficients of $H(x) - \alpha$ are integral over S; hence both α and the coefficients of $H(x)$ are in I_S. Since the coefficients of F are contained in $S \subset I_S$, Lemma IV.1 implies that the coefficients of g are also in I_S, proving the result.

Now, suppose that n_S is neither 0 nor a zero divisor. By Lemma III.1, there are integer polynomials s_i (for $0 \leq i \leq n - 2$) and r_0 depending only on m and n such

that the coefficient of $x^{nm-\ell}$ in $g(h(x))$ equals

- $a_{n-k} + s_{n-k}(a_{n-1}, ..., a_{n-k+1}, b_0, b_1, ..., b_{m-1})$ if $\ell = km$ with $2 \leq k \leq n$, and
- $nb_0 + a_{n-1} + r_0(b_1, b_2, ..., b_{m-1})$ if $\ell = m$.

It follows that for $0 \leq i \leq n-1$, we have $a_i \in S\left[b_0, b_1, ..., b_{m-1}\right]\left[n_S^{-1}\right]$, as desired. $\square$

When S is an integral domain and R is a field containing S, the above result is due to Turnwald [Tur95, Proposition 2.2.(ii)].

4.2 Common Composites and Extension Rings

We now consider the relationship between common composites over an extension ring and common composites over a base ring. Let S be a ring, and let R be an extension of S.

We use Lemma IV.1 to show that if F and G are monic polynomials with coefficients in S, then if F and G have a common $\mathbb{M}_R$-composite of degree $\text{lcm}(|F|, |G|)$, then they have a common $\mathbb{M}_S$-composite of the same degree.

Proposition IV.7. *Let S be a subring of R, and suppose that $F, G \in \mathbb{M}_S$ have a common $\mathbb{M}_R$-composite of degree $\text{lcm}(|F|, |G|)$. Then F and G have a common $\mathbb{M}_S$-composite of degree $\text{lcm}(|F|, |G|)$.*

Proof. Suppose $H = A \circ F = B \circ G$ is a degree-$\text{lcm}(|F|, |G|)$ common $\mathbb{M}_R$-composite of F and G. First, we show that $H \in \mathbb{M}_S + R$. Suppose not, and let $c_k x^k$ be the lowest degree nonconstant term of H which is not in $S[x]$. This term has degree divisible by $|F|$; in particular k will be $|F|$ times the degree of the highest degree term in A with coefficient in $R \backslash S$. By symmetry we see that k is divisible by $|G|$, hence by $\text{lcm}(|F|, |G|)$. But since $\gcd(|A|, |B|) = 1$, the degree of $A \circ F$ equals $\text{lcm}(|F|, |G|)$.

Hence $k = |A \circ F|$, but since $A \circ F$ is monic, it follows that $c_k = 1 \in R \setminus S$, which is a contradiction. Thus, $H \in \mathbb{M}_S + R$. Now

$$H - H(0) = (A - H(0)) \circ F = (B - H(0)) \circ G$$

is a common composite of F and G which has all coefficients in S. By Lemma IV.1, we conclude that $A - H(0)$ and $B - H(0)$ are also elements of $\mathbb{M}_S$, hence that $H - H(0)$ is a common $\mathbb{M}_S$-composite of F and G of degree $\operatorname{lcm}(|F|, |G|)$. □

The conclusion of Proposition IV.7 need not hold, however, if the condition $\gcd(|A|, |B|) = 1$ is not satisfied.

Example IV.8. Let $R = \mathbb{Z}[t]/\langle t^2 \rangle$, and let S be the subring of R generated by $\{1, 2t\}$. Then

$$(x^2 + tx) \circ (x^4 + 2tx^2) = x^8 + 4tx^6 + tx^4 = (x^4 + 4tx^3 + tx^2) \circ x^2$$

is not an element of $\mathbb{M}_S$ but is a common $\mathbb{M}_R$-composite of $x^4 + 2tx^2$ and x^2.

Take $F, G \in \mathbb{P}_R$, and suppose F and G have a least common $\mathbb{P}_R$-composite of degree n. Do F and G necessarily have a least common $\mathbb{P}_S$-composite of degree n? The following theorem answers this question in the affirmative in case S and R are fields.

Theorem IV.9. *Let K be a field, and let $\bar{K}$ be the algebraic closure of K. Then if $f_1, f_2 \in \mathbb{P}_K$ have a nonconstant common $\mathbb{P}_{\bar{K}}$-composite, they have a nonconstant common $\mathbb{P}_K$-composite. Moreover, the minimal degree of any nonconstant common $\mathbb{P}_{\bar{K}}$-composite equals the minimal degree of any nonconstant common $\mathbb{P}_K$-composite.*

This was proved first by McConnell [McC74] in case K is infinite and by Bremner and Morton [BM78] in the general case. See also [BWZ09].

We provide a counterexample to the analogous statement for rings. More precisely, we exhibit a ring S, an extension $R \supset S$, and cubic polynomials $f, g \in S[x]$ such that f and g have no common $\mathbb{M}_S$-composite of degree 6 but have a common $\mathbb{M}_R$-composite of degree 6.

Example IV.10. Let $R = \mathbb{F}_2[a_1, f_1, f_2]/\langle f_2^2, f_1^3, a_1 f_1, a_1 f_2 + f_1^2, f_1^2 f_2, a_1^2 \rangle$, and $S = \mathbb{F}_2[f_1, f_2]/\langle f_2^2, f_1^3, f_1^2 f_2 \rangle$. That S embeds in R can be checked easily by noticing that $S = \{c_0 + c_1 f_1 + c_2 f_2 + c_3 f_1^2 + c_4 f_1 f_2 : c_i \in \mathbb{F}_2\}$, that $R = \{c_0 + c_1 f_1 + c_2 f_2 + c_3 f_1^2 + c_4 f_1 f_2 + c_5 a_1 : c_i \in \mathbb{F}_2\}$, and that inclusion is a ring map. Then $f(x) = x^3 + f_2 x^2 + f_1 x + 1$ and $g(x) = x^3$ have no common $\mathbb{M}_S$-composite of degree 6 but have a common $\mathbb{M}_R$-composite of degree 6. For $a, b, c, d \in R$, we have $(x^2 + bx + a) \circ (x^3 + f_2 x^2 + f_1 x + 1) = (x^2 + dx + c) \circ (x^3)$ if and only if $c = a + b + 1$, $d = b$, $bf_1 = 0$, and $bf_2 + f_1^2 = 0$. However, no element $b \in S$ satisfies both $bf_1 = 0$ and $bf_2 + f_1^2 = 0$ (this can be checked exhaustively, since S is finite). In R, though, $b = a_1$ simultaneously solves $bf_1 = 0$ and $bf_2 + f_1^2 = 0$. So, for example, we have $(x^2 + a_1 x + 1) \circ f = (x^2 + a_1 x + a_1) \circ g$.

However, f and g do have a degree-12 common $\mathbb{M}_S$-composite (namely, $x^2 \circ (x^2 + a_1 x + 1) \circ f$).

We do not know if it is possible for f and g to have a nonconstant common composite in an extension ring but no nonconstant common composite in the base ring.

CHAPTER V

Least Common Composites and Degrees of Common Composites

In this chapter, we study when two elements of $\mathbb{M}_R$ have a left least common $\mathbb{M}_R$-composite, and if so, what is the degree of this least common composite. The first part of this chapter leads us to the main result of the chapter (Theorem V.8). Namely, if R is a ring with no $\mathbb{Z}$-torsion, then F and G in $\mathbb{M}_R$ have a least common $\mathbb{M}_R$-composite whose degree is either 0 or $\text{lcm}(|F|, |G|)$.

In other words, in a (necessarily characteristic 0) ring with no $\mathbb{Z}$-torsion, if monic F and G have any nonconstant common composite, then they have a least common composite of degree $\text{lcm}(|F|, |G|)$. We also present similar results for rings with $\mathbb{Z}$-torsion, including those of positive characteristic (see, for example, Proposition V.1, Corollary V.2, and Corollary V.7).

We conclude the chapter with a discussion of common composites of monic quadratics.

Any common composite of monic F and G has degree a multiple of $\text{lcm}(|F|, |G|)$. The following result shows that if F and G have a nonconstant common composite, say of degree $d \cdot \text{lcm}(|F|, |G|)$, then we may remove the "coprime to the characteristic" part of d. That is, when $\text{char}(R) > 0$, there exists a common composite of degree $d' \cdot \text{lcm}(|F|, |G|)$, where d' is the largest divisor of d such that every prime factor of

d' also divides $\mathrm{char}(R)$. And if $\mathrm{char}(R) = 0$, there is a common composite of F and G of the lowest possible degree, namely $\mathrm{lcm}(|F|, |G|)$, provided that d_R is neither 0 nor a zero divisor.

Proposition V.1. *Suppose $A, F, B, G \in \mathbb{M}_R$ are such that $A \circ F = B \circ G$, and let d be any common divisor of $|A|$ and $|B|$ such that d_R is neither zero nor a zero divisor. Then there exist a, b in $\mathbb{M}_R$ such that $a \circ F = b \circ G$ and $|a| = \frac{|A|}{d}$.*

Proof. Let k be the largest common divisor of $|A|$ and $|B|$ such that k_R is neither 0 nor a zero divisor, and note that $d \mid k$. Also note that $R\left[\frac{1}{k}\right]$ makes sense since k_R is neither 0 nor a zero divisor. Let p be an arbitrary degree k polynomial in $\mathbb{M}_R$ (e.g., $p(x) = x^k$). By Corollary III.2, there are $\hat{a}, \hat{b}$ with no constant term in $\mathbb{M}_{R\left[\frac{1}{k}\right]}$ such that $|A - p \circ \hat{a}| \leq \frac{|A|}{k}(k-1)$ and $|B - p \circ \hat{b}| \leq \frac{|B|}{k}(k-1)$. Composing with F and G respectively yields

$$|A \circ F - p \circ \hat{a} \circ F| \leq \frac{|A \circ F|}{k}(k-1)$$

and

$$|B \circ G - p \circ \hat{b} \circ G| \leq \frac{|B \circ G|}{k}(k-1).$$

Since $A \circ F = B \circ G$, it follows that

$$|p \circ (\hat{a} \circ F) - p \circ (\hat{b} \circ G)| \leq \frac{|A \circ F|}{k}(k-1) = |\hat{a} \circ F|(k-1).$$

By Corollary III.2, there exists a unique $H \in \mathbb{M}_{R\left[\frac{1}{k}\right]}$ such that both $H(0) = 0$ and $|p \circ \hat{a} \circ F - p \circ H| \leq |\hat{a} \circ F|(k-1)$. Since $\hat{a} \circ F$ and $\hat{b} \circ G$ both satisfy the conditions for H, it follows that $\hat{a} \circ F = \hat{b} \circ G$. We now show that $\hat{a}, \hat{b} \in \mathbb{M}_R$ (and not just in $\mathbb{M}_{R\left[\frac{1}{k}\right]}$). If $\mathrm{char}(R) \neq 0$, then k is coprime to $\mathrm{char}(R)$, whence $\frac{1}{k} \in R$, so $\hat{a}$ and $\hat{b}$ are in $\mathbb{M}_R$, as desired. So suppose $\mathrm{char}(R) = 0$. Then $k = \gcd(|A|, |B|)$, so $\gcd(|\hat{a}|, |\hat{b}|) = 1$, it follows from Proposition IV.7 that $\hat{a}, \hat{b} \in R[x] + S$. Since $\hat{a}$ and $\hat{b}$ have constant term 0 by construction, $\hat{a}, \hat{b} \in \mathbb{M}_R$.

Now let d be any common divisor of A and B such that d_R is neither 0 nor a zero divisor. It follows that $d \mid k$, so say that $k = dn$. Now let $a = x^n \circ \hat{a}$ and $b = x^n \circ \hat{b}$, and notice that $|a| = \frac{n|A|}{k} = \frac{|A|}{d}$ and that $a \circ F = b \circ G$. □

Corollary V.2. *Suppose $A, B \in \mathbb{M}_R$ have a nonconstant common composite. If $\mathrm{char}(R) = 0$ and R has no $\mathbb{Z}$-torsion, then A and B have a common composite of degree $\mathrm{lcm}(|A|, |B|)$. If $\mathrm{char}(R) > 0$, then A and B have a common composite of degree $r \cdot \mathrm{lcm}(|A|, |B|)$, where r is a product of primes dividing $\mathrm{char}(R)$.*

In [BWZ09], the authors show that if F is a field of positive characteristic p, and if $A, B \in \mathbb{P}_F$ have a nonconstant common composite, then A and B have a common composite of degree $p^t \cdot \mathrm{lcm}(|A|, |B|)$. Their proof relies on Galois theory, but the authors ask for an elementary proof of this result. Our result is the first such.

Example V.3. When d_R is 0 or a zero divisor, the conclusion of Proposition V.1 may fail. Notice that $x^2 \circ (x^2 + Tx) = (x^2 + T^2x) \circ x^2$ in $\mathbb{Z}[T]/\langle 2T \rangle [x]$, but that $x^2 + Tx$ and x^2 do not have a monic common composite of degree 2. Here $d_R = 2$ is a zero divisor. If R were instead $\mathbb{F}_2$, then we construct a similar example with $d = 2$, whence $d_R = 0$. We see that $(x^2 + x) \circ x^2 = x^2 \circ (x^2 + x)$, but x^2 and $x^2 + x$ have no common composite of degree 2.

Proposition V.1 allowed us to find a new common composite $a \circ F = b \circ G$ given $A \circ F = B \circ G$. We now work toward showing that there is a P such that $A = P \circ a$ and $B = P \circ b$. The following lemma presents a kind of compositional division algorithm, which will be utilized toward this end.

Lemma V.4. *For $1 \neq a \in \mathbb{M}_R$ and $A \in \mathbb{P}_R \setminus R$, there exist unique polynomials $P, Q \in \mathbb{P}_R$ simultaneously satisfying:*

(1) $A = P \circ a + Q$, and

(2) no term of Q has degree divisible by $|a|$.

Proof. Let k be the largest integer such that $k|a| \leq |A|$. Then for $-1 \leq i \leq k$, we construct $P_i, Q_i \in \mathbb{P}_R$ such that $A = P_i \circ a + Q_i$ where Q_i has no terms of degree $j|a|$ for $j \geq k - i$. Then the lemma is established by taking $P = P_k$ and $Q = Q_k$. So take $P_{-1} = 0$ and $Q_{-1} = A$. Continue inductively, defining $P_i = P_{i-1} + r_i x^{k-i}$ and $Q_i = A - P_i \circ a$, where r_i is the coefficient of $x^{(k-i)|a|}$ in Q_{i-1}. From the definition of Q_i, it is clear that $(P_i \circ a) + Q_i = A$, and it remains to show that Q_i has no terms of degree $j|a|$ for $j \geq k - i$. This is immediate in the case $i = -1$, so we assume this for $i - 1$ and consider i. Then

$$\begin{aligned} Q_i &= A - (P_i \circ a) \\ &= A - ((P_{i-1} + r_i x^{k-i}) \circ a) \\ &= A - (A - Q_{i-1}) - (r_i x^{k-i} \circ a) \\ &= Q_{i-1} - (r_i x^{k-i} \circ a). \end{aligned}$$

Since a is monic, that $Q_{i-1} - (r_i x^{k-i} \circ a)$ has no terms of degree $j|a|$ for $j \geq k - i$ follows from the definition of r_i and from the inductive hypothesis, proving existence. For uniqueness, suppose that $A = P \circ a + Q = P' \circ a + Q'$. Then $0 = (P - P') \circ a + (Q - Q')$. First $Q - Q'$ must be 0, since otherwise $|Q - Q'|$ is divisible by $|a|$, contradicting (2). Then $(P - P') \circ a = 0$, which implies $P = P'$, since a is monic.

□

Remark V.5. We note that condition (2) implies that $Q(0) = 0$. Moreover, if we require that $|a|$ divides $|A|$, then if A is monic, P will also be monic. We also remark that the condition that $a \in \mathbb{M}_R$ is crucial. Indeed, if the leading coefficient of a is a zero divisor and we can write $A = P \circ a + Q$, the choice of P and Q are not unique.

For example, if $rs = 0$ in R, then $(rx) \circ (sx^k) = 0$ for every $k \geq 0$. Hence if s is the leading coefficient of a, we have that

$$\begin{aligned} A &= P \circ a + Q \\ &= (P + r(x - a(0))) \circ a + (Q - r(a - a(0))) \end{aligned}$$

We now show that, if F and G have a common composite H whose degree divides the degrees of all other common composites, then H is a least common composite. In other words, if the set of degrees of the common composites of F and G does not contradict the existence of a least common composite, then a least common composite of F and G exists.

Proposition V.6. *If H is a nonconstant common $\mathbb{M}_R$-composite of $F, G \in \mathbb{M}_R$, then the following are equivalent:*

1. *H is a least common $\mathbb{M}_R$-composite of F and G.*
2. *H is a least common $\mathbb{P}_R$-composite of F and G.*
3. *Each common $\mathbb{P}_R$-composite of F and G has degree divisible by $|H|$.*

Moreover, if these properties hold and we write $H = a \circ F = b \circ G$, then for any $A, B \in \mathbb{P}_R$ such that $A \circ F = B \circ G$, there exists $P \in \mathbb{P}_R$ such that $A = P \circ a$ and $B = P \circ b$.

Proof. Suppose that $H = a \circ F = b \circ G$.

(3 $\implies$ 1) Suppose that each common $\mathbb{P}_R$-composite of F and G has degree divisible by $|H|$, and let $A \circ F = B \circ G$ be a common $\mathbb{M}_R$-composite of F and G. If $|A| = |B| = 0$, then $A = B = 1$, and $H = F = G$. The result is clear. So suppose A is nonconstant. We use Lemma V.4 to write $A = P \circ a + Q$, where no term of Q has

degree divisible by $|a|$. Assume Q is nonzero. Composing with F gives

$$\begin{aligned} A \circ F &= P \circ a \circ F + Q \circ F, \quad \text{so} \\ Q \circ F &= A \circ F - P \circ a \circ F \\ &= B \circ G - P \circ b \circ G \\ &= (B - P \circ b) \circ G. \end{aligned}$$

Thus $Q \circ F$ is a common $\mathbb{P}_R$-composite of F and G, which implies $|Q||F|$ is a multiple of $k = |a||F|$. Hence $|Q|$ is a multiple of $|a|$, which is a contradiction. Thus, $Q = 0$, and it follows that $A = P \circ a$. Moreover, since $0 = Q \circ F = (B - P \circ b) \circ G$ with G monic, we have $B = P \circ b$. Hence H is a least common $\mathbb{M}_R$-composite of F and G.

(1 $\implies$ 2) Suppose H is a least common $\mathbb{M}_R$-composite of F and G. Let Q be any common $\mathbb{P}_R$-composite of F and G, and let P be a common $\mathbb{M}_R$-composite with $|P| > |Q|$ (take $P = x^N \circ H$ for sufficiently large N, for example). Then $P + Q$ is also a common $\mathbb{M}_R$-composite of F and G, so both P and $P + Q$ are $\mathbb{M}_R$-composites of H. It follows that $Q = (P + Q) - P$ is a $\mathbb{P}_R$-composite of H.

(2 $\implies$ 3) is clear, since H is monic.

Now if the above hold and $A, B \in \mathbb{P}_R$ are such that $A \circ F = B \circ G$, then since H is a least common $\mathbb{P}_R$-composite of F and G, there exists $P \in \mathbb{P}_R$ such that

$$A \circ F = P \circ (a \circ F) = P \circ (b \circ G),$$

whence $A = P \circ a$ and $B = P \circ b$. □

We can now combine the previous results to show that the existence of a monic common composite of F and G of degree $k \cdot \operatorname{lcm}(|F|, |G|)$, where k_R is neither 0 nor a zero divisor, implies the existence of a monic least common composite of the smallest degree possible: $\operatorname{lcm}(|F|, |G|)$. In particular, when R has no $\mathbb{Z}$-torsion, existence of a

nonconstant monic common composite implies the existence of a monic least common composite of degree $\operatorname{lcm}(|F|, |G|)$.

Corollary V.7. *If $F, G \in \mathbb{M}_R$ have a common $\mathbb{M}_R$-composite of degree $k \cdot \operatorname{lcm}(|F|, |G|)$ where k_R is neither 0 nor a zero-divisor, then F and G have a least common $\mathbb{M}_R$-composite of degree $\operatorname{lcm}(|F|, |G|)$.*

Proof. Let $F, G \in \mathbb{M}_R$, and suppose P is a common $\mathbb{M}_R$-composite of F and G of degree $k \cdot \operatorname{lcm}(|F|, |G|)$, where k_R is neither 0 nor a zero-divisor. Take $A, B \in \mathbb{M}_R$ such that $P = A \circ F = B \circ G$. Then by Proposition V.1 there exist monic $a, b \in \mathbb{M}_R$ such that $p = a \circ F = b \circ G$ has degree $\operatorname{lcm}(|F|, |G|)$. Since all common mr-composites of F and G have degree divisible by $\operatorname{lcm}(|F|, |G|)$, the hypotheses of Proposition V.6 are satisfied, and it follows that p is a least common $\mathbb{M}_R$-composite of F and G. □

This result enables us to exhibit a large class of rings in which any two monic polynomials have a monic least common composite.

Theorem V.8. *Suppose that R is a ring with no $\mathbb{Z}$-torsion, and let $F, G \in \mathbb{M}_R$. Then F and G have a least common $\mathbb{M}_R$-composite whose degree is either 0 or $\operatorname{lcm}(|F|, |G|)$.*

Proof. If all common $\mathbb{M}_R$-composites of F and G are degree 0, then 1 is a least common $\mathbb{M}_R$-composite of F and G. Otherwise, F and G have a nonconstant common $\mathbb{M}_R$-composite, and its degree must be $k \cdot \operatorname{lcm}(|F|, |G|)$ for some positive integer k. Since R has no $\mathbb{Z}$-torsion, k_R is neither 0 nor a zero divisor, so Corollary V.7 implies that F and G have a least common $\mathbb{M}_R$-composite of degree $\operatorname{lcm}(|F|, |G|)$. □

Sometimes, even if monic $F, G \in \mathbb{P}_R$ are such that the set of degrees of their common $\mathbb{P}_R$-composites is the set of nonnegative multiples of an integer k, a common $\mathbb{M}_R$-composite of degree k may not exist. Such is the case in the following example, where the hypotheses of Proposition V.6 cannot be satisfied.

Example V.9. Over $R = \mathbb{Z}/4\mathbb{Z}$, the polynomials $F = x^2$ and $G = x^2 + 2x$ have a monic degree-4 common composite, since $x^2 \circ F = x^4 = x^2 \circ G$. However, F and G also have a nonmonic degree-2 common composite, since $2x \circ F = 2x^2 = 2x \circ G$. This gives rise to a second degree-4 common $\mathbb{P}_R$-composite of F and G, namely

$$(x^2 + 2x) \circ F = x^4 + 2x^2 = (x^2 + 2x) \circ G.$$

Since F is monic, all common $\mathbb{P}_R$-composites of F and G have even degree. However, there is no degree-2 common $\mathbb{M}_R$-composite of F and G, so there is no least common $\mathbb{M}_R$-composite of F and G by Proposition V.6.

More generally, if $a - b$ is a zero divisor in a commutative ring R, then the polynomials $A = x^2 + ax$ and $B = x^2 + bx$ do not have a least common $\mathbb{M}_R$-composite. We will show in Proposition V.12 that A and B have a common $\mathbb{M}_R$-composite of degree $2k$ if and only if $k(a - b) = 0$. However, then

$$\begin{aligned} kx \circ (x^2 + ax) &= kx^2 + kax \\ &= kx^2 + kbx \\ &= kx \circ (x^2 + bx) \end{aligned}$$

is a degree-2 common $\mathbb{P}_R$-composite of A and B that cannot be a $\mathbb{P}_R$-composite of any common $\mathbb{M}_R$-composite of A and B, as any monic common composite of A and B has degree strictly greater than 2.

On the other hand, our results enable us to show the existence of least common composites over fields.

Theorem V.10. *Let K be a field, and let $F, G \in \mathbb{P}_K \setminus K$. Then F and G have a least common $\mathbb{P}_K$-composite.*

Proof. Without loss of generality, we assume F and G to be monic, since otherwise we may consider monic $ux \circ F$ and $vx \circ G$, where $u, v \in K$. If $a \circ ux \circ F = b \circ vx \circ G$ is a least common $\mathbb{P}_K$-composite of $ux \circ F$ and $vx \circ G$, then it is also a least common $\mathbb{P}_K$-composite of F and G, since $A \circ F = B \circ G$ implies

$$(A \circ u^{-1}x) \circ (ux \circ F) = (B \circ v^{-1}x) \circ (vx \circ G).$$

Since $a \circ ux \circ F = b \circ vx \circ G$ is a least common $\mathbb{P}_K$-composite of $ux \circ F$ and $vx \circ G$, we can rewrite the above as

$$P \circ (a \circ ux) \circ F = P \circ (b \circ vx) \circ G$$

for some $P \in \mathbb{P}_K$, whence we see that $a \circ ux \circ F = b \circ vx \circ G$ is also a least common $\mathbb{P}_K$-composite of F and G.

If $\mathrm{char}(K) = 0$, then K has no $\mathbb{Z}$-torsion, and the result follows from Theorem V.8. So assume that $\mathrm{char}(K) = p$. If F and G have no nonconstant common $\mathbb{P}_K$-composites, then 1 is a least common $\mathbb{P}_K$-composite, so choose a common $\mathbb{P}_K$-composite of F and G of degree $k \cdot \mathrm{lcm}(|F|, |G|)$ for some positive integer k. By Proposition V.1, F and G have a common $\mathbb{P}_K$-composite of degree $p^\beta \cdot \mathrm{lcm}(|F|, |G|)$. Let β_{min} be the smallest nonnegative integer β such that there exists a common $\mathbb{P}_K$-composite of F and G of degree $p^\beta \cdot \mathrm{lcm}(|F|, |G|)$. Call this common $\mathbb{P}_K$-composite H. It follows, again by Proposition V.1, that $p^{\beta_{min}} \mid k$, so every common K-composite of F and G has degree a multiple of $p^{\beta_{min}} \mathrm{lcm}(|F|, |G|)$. Moreover, by considering $x^n \circ H$, we see that there is a common $\mathbb{P}_K$-composite of F and G of degree $np^{\beta_{min}} \mathrm{lcm}(|F|, |G|)$ for each n, hence that the set of degrees of all common $\mathbb{P}_K$-composites of F and G is the set of nonnegative multiples of $p^{\beta_{min}} \mathrm{lcm}(|F|, |G|)$. Hence the hypotheses of Proposition V.6 are satisfied, and it follows that H is a least common $\mathbb{P}_K$-composite of F and G. □

Remark V.11. We point out that while Theorem V.10 was known previously, the above is the first proof that does not depend on Lüroth's theorem.

We now show that any two monic quadratic polynomials over a commutative ring R of positive characteristic have a nonconstant common $\mathbb{M}_R$-composite.

Proposition V.12. *Suppose R is a commutative ring. Fix $a, b \in R$ and $k \in \mathbb{Z}_{\geq 0}$. Then the polynomials $x^2 + ax$ and $x^2 + bx$ in $R[x]$ have a common $\mathbb{M}_R$-composite of degree $2k$ if and only if $k(a - b) = 0$.*

Proof. ($\Rightarrow$). Suppose $x^2 + ax$ and $x^2 + bx$ have a monic common $\mathbb{M}_R$-composite of degree $2k$. If $k = 0$, then $k(a - b) = 0$, so suppose $k > 0$. Then there exist monic degree-k polynomials p, q such that $p \circ (x^2 + ax) = q \circ (x^2 + bx)$. The coefficient of x^{2k-1} in $p \circ (x^2 + ax)$ is ka, and the coefficient of x^{2k-1} in $q \circ (x^2 + bx)$ is kb. Since these coefficients must be equal, it follows that $k(a - b) = 0$.

($\Leftarrow$). Suppose $\mathrm{char}(R) = 2$ and $k(a - b) = 0$. If k is odd, then $a - b = 0$. It follows that $x^2 + ax = x^2 + bx$, and the result holds. If k is even, then $(x^2 + b(a + b)x) \circ (x^2 + ax) = (x^2 + a(a + b)x) \circ (x^2 + bx)$, and the theorem follows. Hence we may assume that $\mathrm{char}(R) \neq 2$. Let r denote the additive order of $a - b$ in R. Note that $r \mid k$ and in particular r is finite since $k(a - b) = 0$.

For each $f \in R[x]$, define $\rho_f : R[x] \to R[x]$ by $h(x) \mapsto h(f(x))$. Note that ρ_f is a ring homomorphism and that $\rho_{f \circ g}(h) = \rho_g(\rho_f(h))$. Let $H = \langle \rho_{-x-a} \rangle$. Notice that H is a group of order two; i.e., ρ_{-x-a} is an involution. Let $G = \langle \rho_{-x-a}, \rho_{-x-b} \rangle$. Since $\rho_{-x-a} \circ \rho_{-x-b} = \rho_{x+a-b}$, it follows that G also equals $\langle \rho_{-x-a}, \rho_{x+a-b} \rangle$. Noting that

$$\rho_{-x-a} \circ \rho_{x+a-b} \circ \rho_{-x-a} = \rho_{x+b-a} = \rho_{x+a-b}^{-1},$$

we see that G is a dihedral group of order $2r$.

Let T be a set of representatives for the distinct right cosets of H in G. Then every element of G can be written in precisely one way as $\rho_h\rho_t$ with $\rho_h \in H, \rho_t \in T$ (where $h, t \in R[x]$).

Then, writing products to denote multiplication in $R[x]$, we have

$$\begin{aligned}\psi(x) &:= \prod_{\rho_g \in G} \rho_g(x) \\ &= \prod_{\rho_t \in T} \prod_{\rho_h \in H} \rho_h\rho_t(x) \\ &= \prod_{\rho_t \in T} \prod_{\rho_h \in H} t(h(x)) \\ &= \prod_{\rho_t \in T} t(x) \cdot t(-x-a).\end{aligned}$$

Writing $t(x) = \sum_{i\geq 0} t_i x^i$, we compute

$$\begin{aligned}t(x)\cdot t(-x-a) &= \left(\sum_{i\geq 0} t_i x^i\right)\left(\sum_{j\geq 0} t_j(-x-a)^j\right) \\ &= \sum_{i\geq 0} t_i^2(-x^2-ax)^i + \sum_{0\leq i<j} t_i t_j (x^i(-x-a)^j + x^j(-x-a)^i) \\ &= \sum_{i\geq 0} t_i^2(-x^2-ax)^i + \sum_{0\leq i<j} t_i t_j (-x^2-ax)^i((-x-a)^{j-i} + x^{j-i}).\end{aligned}$$

Since $(-x-a)^{j-i}+x^{j-i}$ is symmetric in x and $-x-a$, the Fundamental Theorem on Symmetric Functions implies that $(-x-a)^{j-i}+x^{j-i}$ may be written as a polynomial in the elementary symmetric functions on x and $-x-a$, namely $-a$ and $-x^2-ax$ [DF99, p. 589]. Thus $t(x)\cdot t(-x-a) \in R[-a, -x^2-ax] = R[x^2+ax]$, whence $\psi(x) \in R[x^2+ax]$. By symmetry, $\psi(x) \in R[x^2+bx]$, so $\psi(x)$ is a common R-composite of x^2+ax and x^2+bx. The leading coefficient of ψ is either 1 or -1, so either ψ or $-\psi$ is a monic common $\mathbb{M}_R$-composite of x^2+ax and x^2+bx of degree $|G| = 2r$, which divides $2k$. □

This result implies that any two quadratics in $\mathbb{M}_R$ have a nonconstant common composite in $\mathbb{M}_R$ whenever R has positive characteristic. The analogous statement

for cubics, however, is false, as shown in the following example.

Example V.13. The cubics $x^3 + x^2$ and $x^3 + 2x^2 + x$ have no nonconstant common composite, for suppose $F \circ (x^3 + x^2) = G \circ x^3 + 2x^2 + x$, and say that ax^n is the lowest degree nonconstant term of F. Then the lowest degree nonconstant term of G must be ax^{2n}. However, noting that $(x^3 + x^2) \circ (-1 - x) = -(x^3 + 2x^2 + x)$, we see that

$$\begin{aligned} F \circ -(x^3 + 2x^2 + x) &= F \circ (x^3 + x^2) \circ (-1 - x) \\ &= G \circ (x^3 + 2x^2 + x) \circ (-1 - x) \\ &= G \circ -(x^3 + x^2). \end{aligned}$$

Recalling that the lowest degree nonconstant term of G is ax^{2n} we now observe that the lowest degree nonconstant term of F must be ax^{4n}. Hence $n = 0$, a contradiction.

In light of Example V.9, we remark that the two quadratics need not have a least common $\mathbb{P}_R$-composite nor a least common $\mathbb{M}_R$-composite. In the case of commutative rings of prime characteristic p, however, we can show that $x^2 + ax$ and $x^2 + bx$ have a monic least common $\mathbb{P}_R$-composite of degree $2p$, so long as $a - b$ is neither 0 nor a zero divisor.

Corollary V.14. *If R is a commutative ring of prime characteristic p and $a, b \in R$ are such that $a - b$ is neither 0 nor a zero divisor, then $x^2 + ax$ and $x^2 + bx$ have a monic least common $\mathbb{P}_R$-composite of degree $2p$.*

Proof. By Proposition V.12, $x^2 + ax$ and $x^2 + bx$ have a monic common R-composite H of degree $2p$. Now take any common R-composite $F \circ (x^2 + ax) = G \circ (x^2 + bx)$ of degree $2s$. Let u be the coefficient of x^s in F. Clearly u is the leading coefficient of G as well. Notice that the coefficient of x^{2s-1} in $F \circ (x^2 + ax)$ is usa and that the

coefficient of x^{2s-1} in $G \circ (x^2+bx)$ is usb. These coefficients are equal, so $us(a-b) = 0$. If $p \nmid s$, then $s \in R^*$, and $u(a-b) = 0$, which is a contradiction. Hence $p \mid s$. But then the degrees of all common composites are the nonnegative multiples of $2p$, so H is a least common $\mathbb{P}_R$-composite of $x^2 + ax$ and $x^2 + bx$ by Proposition V.6. $\square$

Notice that this fails when $a - b$ is a zero divisor, though, since if $c(a-b) = 0$, then

$$cx \circ (x^2 + ax) = cx \circ (x^2 + bx).$$

This is a nonmonic common composite of degree 2, which violates the hypotheses of Proposition V.6. If $H = F \circ (x^2 + ax) = G \circ (x^2 + bx)$ is a monic common composite of degree $2p$, then it cannot be a least common composite, as $(F + cx) \circ (x^2 + ax) = (G + cx) \circ (x^2 + bx)$ is also a monic common composite of degree $2p$ that cannot be a composite of H.

We rely heavily on commutativity in the proof of Proposition V.12. In noncommutative rings, quadratics are not guaranteed to have nonconstant common composites as shown in the following example.

Example V.15. Let R' be a ring, and let $R = R'\{a, b\}$. Then $x^2 + ax$ and $x^2 + bx$ cannot have a nonconstant common R-composite. To the contrary, suppose that $F \circ (x^2 + ax) = G \circ (x^2 + bx)$ with $F, G \in \mathbb{P}_R \setminus R$. Let px^n be the lowest degree term of F, and let qx^m be the lowest degree term of G. Then the lowest degree term of $F \circ (x^2 + ax)$ is $pa^n x^n$ and the lowest degree term of $G \circ (x^2 + bx)$ is $qb^m x^m$. Therefore $n = m$ and $pa^n = qb^n$. However, a^n and b^n have no nonzero (left) common multiples in R, which is a contradiction.

CHAPTER VI

Greatest Common Divisors

In this chapter, we develop a theory of greatest common divisors in univariate polynomial rings under composition. In particular, our results lead us to the following theorem (Theorem VI.10) which, besides its intrinsic interest, is also integral in our study of unique factorization in $\mathbb{M}_R$ (Chapter VII): Suppose R is a commutative ring with no $\mathbb{Z}$-torsion and no nonzero nilpotents. Then if $f, g \in \mathbb{M}_R$ have a nonconstant common $\mathbb{M}_R$-composite, there exists a greatest common $\mathbb{M}_R$-divisor of f and g having degree $\gcd(|f|, |g|)$.

Engstrom [Eng41] proved, as a consequence of Lüroth's theorem, that polynomials $f, g \in F[x]$ with a non-constant common $\mathbb{P}_F$-composite have a greatest common $\mathbb{P}_F$-divisor of degree $\gcd(|f|, |g|)$ when F has characteristic 0. His argument extends to F having characteristic p (cf. [Sch00, Thm. 5]) so long as f and g have a nonconstant common $\mathbb{P}_F$-composite of degree coprime to p. We now show the analogous result for integral domains.

The following lemma will be useful in the proof.

Lemma VI.1. *Let R be an integral domain, and $F = \mathrm{Frac}(R)$. Then if $a, b \in \mathbb{M}_F$ and $h \in \mathbb{M}_F \setminus \{1\}$ satisfy*

1. $\gcd(|a|, |b|) = 1$,

2. $a \circ h$ *and* $b \circ h$ *are elements of* $R[x]$*, and*

3. $h(0) \in R$

then $a, b, h \in \mathbb{M}_R$*.*

Proof. Let $n = |a|$ and $m = |h|$. Write $h = r + \sum_{i=1}^{d} h_i x^i$. Then for $1 \leq k \leq d-1$, by Lemma III.1, the coefficient of x^{nd-k} in $a \circ h$ is $nh_{d-k} + r_{d-k}$, where $r_{d-k} \in \mathbb{Z}\{h_{d-k+1}, h_{d-k+2}, ..., h_{d-1}\}$, and the coefficient of x^{md-k} in $b \circ h$ is $mh_{d-k} + s_{d-k}$, where $s_{d-k} \in \mathbb{Z}\{h_{d-k+1}, h_{d-k+2}, ..., h_{d-1}\}$. Let j be the degree of the highest degree nonconstant term of h with coefficient in $F \setminus R$. Then $r_j, s_j \in R$, since $\{h_{j+1}, h_{j+2}, ..., h_{d-1}\} \subset R$. Since all coefficients of $a \circ h$ and $b \circ h$ are elements of R, it follows that $nh_j \in R$ and $mh_j \in R$. Since $\gcd(m, n) = 1$, there are integers p, q such that $pm + qn = 1$. Thus, $h_j = (pm + qn)h_j \in R$, which is a contradiction. Hence, $h \in \mathbb{M}_R$, as desired, and by Corollary IV.1, $a, b \in \mathbb{M}_R$ as well, completing the proof. □

Theorem VI.2. *Let* R *be an integral domain of characteristic* $p \geq 0$*. Let* $c, d, f, g \in \mathbb{M}_R \setminus \{1\}$ *be such that* $c \circ f = d \circ g$*, and let* $r \in R$*. Suppose that* p *does not divide* $|c| \cdot |f|$*. Then there exists* $h \in \mathbb{M}_R$ *with* $|h| = \gcd(|f|, |g|)$ *and* $h(0) = r$ *such that* h *is a greatest common* $\mathbb{M}_R$*-divisor of* f *and* g*. In other words, if* f, g *are* $\mathbb{M}_R$*-composites of* $H \in \mathbb{M}_R$*, then* h *is a* $\mathbb{M}_R$*-composite of* H*.*

Proof. Let $F = \mathrm{Frac}(R)$. Since f and g have a nonconstant common $\mathbb{P}_F$-composite of degree coprime to p, there exists a greatest common $\mathbb{P}_F$-divisor $\hat{h} \in \mathbb{P}_F$ of f and g such that $|\hat{h}| = \gcd(|f|, |g|)$ [Sch00, Theorem 5]. If e is the leading coefficient of $\hat{h}$, then $h := e^{-1}(\hat{h} - \hat{h}(0) + er)$ is also a greatest common $\mathbb{P}_F$-divisor. Note that h is monic, hence h is a greatest common $\mathbb{M}_F$-divisor of f and g, and note that $h(0) = r$.

Say $f = a \circ h$ and $g \circ h$ in $\mathbb{M}_F$, where $|a| = n$ and $|b| = m$ are coprime. Now, by Lemma VI.1, $a, b, h \in \mathbb{M}_R$. $\square$

Note that the above result does not imply that any two monic polynomials over a characteristic 0 integral domain have a greatest common divisor. Instead, under a stronger hypothesis (existence of a nonconstant common composite), the above implies a stronger conclusion (existence of a greatest common divisor of degree $\gcd(|f|, |g|)$.

We will prove next that there are much less restrictive settings where polynomials have greatest common divisors. Namely, over any ring R, if monic f and g have degrees coprime to $\text{char}(R)$, then f and g have a greatest common R-divisor. We do not require that f and g have a nonconstant common composite. However, it is not necessarily the case that the degree of the greatest common divisor is $\gcd(|f|, |g|)$.

Proposition VI.3. *If $f, g \in \mathbb{M}_R$ are such that $|f|_R$ and $|g|_R$ are neither 0 nor zero divisors, then f and g have a greatest common $\mathbb{M}_R$-divisor.*

Proof. To the contrary, choose some $f, g \in \mathbb{M}_R$ such that $|f|_R$ and $|g|_R$ are neither 0 nor zero divisors and such that f and g do not have a greatest common $\mathbb{M}_R$-divisor. Since x is a common $\mathbb{M}_R$-divisor of f and g, there must be common $\mathbb{M}_R$-divisors $c, d \in \mathbb{M}_R$ of f and g such that c and d have no common $\mathbb{M}_R$-composite that is a common $\mathbb{M}_R$-divisor of f and g. However, f is a common $\mathbb{M}_R$-composite of c and d, and $|f|_R$ is neither zero nor a zero divisor. So by Corollary V.7, c and d have a least common $\mathbb{M}_R$-composite - call it p - and since f and g are common $\mathbb{M}_R$-composites of c and d, we see that p is a common $\mathbb{M}_R$-divisor of f and g. This is a contradiction. $\square$

It is an immediate corollary that any two monic polynomials in rings with no $\mathbb{Z}$-torsion have a greatest common divisor.

Corollary VI.4. *Suppose that R has no $\mathbb{Z}$-torsion. Then any two elements of $\mathbb{M}_R$ have a greatest common $\mathbb{M}_R$-divisor.*

We remark here that even in the case $R = \mathbb{Q}$, this is the first proof of the existence of greatest common divisors that does not depend on Lüroth's theorem.

The following example illustrates that a greatest common divisor of f and g can have degree other than $\gcd(|f|, |g|)$, even when f and g have a nonconstant common $\mathbb{M}_R$-composite.

Example VI.5. Let $R = \mathbb{Z}[t]/\langle t^2 \rangle$. Then $f(x) = x^4 + 2tx$ and $g(x) = x^6 + 3tx^3$ have the common $\mathbb{M}_R$-composite

$$x^3 \circ f = x^{12} + 6tx^9 = x^2 \circ g.$$

However, we will show that f and g have no common $\mathbb{M}_R$-divisor of degree $\gcd(|f|, |g|) = 2$. In fact, f is indecomposable, since if f were $(x^2 + ax) \circ (x^2 + bx)$, then by comparing the coefficients of x^3 we obtain $2b = 0$ and thus $b = 0$. Hence, f would be a polynomial in x^2, which is a contradiction.

This example depends crucially on the fact that R contains nonzero nilpotent elements.

Definition VI.6. An element $r \in R$ is *nilpotent* if $r^n = 0$ for some positive integer n.

Definition VI.7. The *nilradical* of a ring R, denoted $\mathrm{Nil}(R)$ is the set of nilpotent elements of R.

All rings - even noncommutative - without nonzero nilpotents embed in a (possibly infinite) product of domains, which in many cases makes them easier to understand. In particular, by embedding commutative rings without nonzero nilpotents

in a product of integral domains, we will be able to invoke results about greatest common divisors in integral domains and apply them to commutative rings without nonzero nilpotents.

Theorem VI.8. $\mathrm{Nil}(R) = (0)$ *if and only if* R *embeds in a direct product of domains.*

Proof. This is Theorem 12.7 in [Lam01]. □

The following proposition allows us to embed commutative rings without nonzero nilpotents and with no $\mathbb{Z}$-torsion in a product of characteristic 0 integral domains, where we will be able to apply Theorem VI.2.

Proposition VI.9. *Let* R *be a commutative ring with no* $\mathbb{Z}$*-torsion and no nonzero nilpotents. Then* R *embeds in a product of characteristic 0 integral domains. In particular, let* $\mathcal{P}$ *be the set of prime ideals of* R *lying over the ideal* (0) *of* $\mathbb{Z}$*; that is,* $P \in \mathcal{P}$ *implies that* $P \cap \mathbb{Z} = 0$*. Then there is an injective ring homomorphism* $\phi : R \to \prod_{P \in \mathcal{P}} R/P$*.*

Proof. Let $\mathcal{P}$ be the set of prime ideals in R lying over the ideal (0) of $\mathbb{Z}$. We'll show that $R \hookrightarrow \prod_{P \in \mathcal{P}} R/P$. Notice that if P is a prime ideal in R lying over (0), then R/P is an integral domain of characteristic 0. There is a canonical homomorphism $\phi : R \to \prod R/P$, and it remains to show that the kernel of ϕ is 0.

Let $S = \mathbb{Z} - \{0\}$. Then S is closed under mutiplication, and since S contains no zero divisors in R it follows that R embeds in the localization of R at S ([DF99, p. 678]). That is, $\imath : R \to S^{-1}R$ is injective. We claim that the prime ideals in $S^{-1}R$ are of the form $S^{-1}P$ where $P \in \mathcal{P}$. To see this, first notice that if P is a prime ideal in R that contains a nonzero integer n, then $1 = n^{-1}n \in S^{-1}P$, so $S^{-1}P = S^{-1}R$. Second, let Q be a prime ideal in $S^{-1}R$, and let $P = Q \cap R$. It is clear that P is

a prime ideal in R, since $P = \imath^{-1}(Q)$, and the pullback of a prime ideal is prime. Lastly notice that $Q = S^{-1}P$.

Conversely, suppose that $P \in \mathcal{P}$. Then $S^{-1}P$ is an ideal in $S^{-1}R$ since P is an ideal in R. Moreover, $S^{-1}P$ is a prime ideal in $S^{-1}R$, since for any $r_1, r_2 \in R$ and $s_1, s_2 \in S$ such that $\frac{r_1}{s_1}\frac{r_2}{s_2} \in S^{-1}P$, there exists $s \in S$ and $p \in P$ such that $sr_1r_2 = s_1s_2p \in P$. Since P lies over (0), we see that $s \notin P$. However, P is prime, which implies either r_1 or r_2 is an element of P. It follows, then, that either $\frac{r_1}{s_1}$ or $\frac{r_2}{s_2}$ is an element of $S^{-1}P$. Hence $S^{-1}P$ is a prime ideal.

Notice that $S^{-1}R$ has no nonzero nilpotents, since $(\frac{r}{s})^n = 0$ implies $r^n = 0$, and R has no nonzero nilpotents. Since in any commutative ring R, we have that $\mathrm{Nil}(R)$ is the intersection of the prime ideals of R [DF99, p. 651, Prop. 9], and since the prime ideals of $S^{-1}R$ are of the form $S^{-1}P$, where P is a prime ideal in R lying over (0), it follows that $\cap_{P\in\mathcal{P}} S^{-1}P = \mathrm{Nil}(S^{-1}R) = 0$. Thus $\cap_{P\in\mathcal{P}} P = \ker(\phi) = 0$. □

We now use the embedding into a product of integral domains of characteristic 0 to show that when R is a commutative ring with no $\mathbb{Z}$-torsion and no nonzero nilpotents, then any two monic polynomials have a greatest common divisor of degree $\gcd(|f|, |g|)$.

Theorem VI.10. *Suppose R is a commutative ring with no $\mathbb{Z}$-torsion and no nonzero nilpotents. Then if $f, g \in \mathbb{M}_R$ have a nonconstant common $\mathbb{M}_R$-composite, there exists a greatest common $\mathbb{M}_R$-divisor of f and g having degree* $\gcd(|f|, |g|)$.

Proof. Let $\mathcal{P}$ be the set of prime ideals in R lying over (0). By Proposition VI.9, there exists an injective map $\phi : R \to \prod_{P\in\mathcal{P}} R/P$. For $P \in \mathcal{P}$, let ϕ_P be the natural map $R[x] \to (R/P)[x]$. Notice that each ϕ_P preserves the degree of monic polynomials; i.e., for any monic $a \in R[x]$, we have $|\phi_P(a)| = |a|$. For each $P \in \mathcal{P}$, the quotient

R/P is a characteristic 0 integral domain, so Theorem VI.2 implies that $\phi_P(f)$ and $\phi_P(g)$ have a monic greatest common (R/P)-divisor of degree $\gcd(|\phi_P(f)|, |\phi_P(g)|) = \gcd(|f|, |g|)$; call this polynomial d_P, and note that (again by Theorem VI.2) we may assume that $d_P(0) = 0$. Say $\phi_P(f) = a_P \circ d_P$ and $\phi_P(g) = b_P \circ d_P$.

For any monic polynomial $p \in R[x]$ and positive integers m, n such that $mn = |p|$, Corollary III.3 determines monic polynomials $p_1, p_2 \in R\left[\frac{1}{n}\right][x]$ that are unique subject to the conditions:

1. $|p_1| = n$,
2. $|p_2| = m$,
3. $p_2(0) = 0$, and
4. p and $p_1 \circ p_2$ agree in the coefficients of x^{mn-k} for $1 \leq k \leq m-1$ and in the coefficients of x^{mn-km} for $1 \leq k \leq n$.

Let $S = R\left[\frac{\gcd(|f|,|g|)}{|f|}\right]$, and take $f_1, f_2 \in S[x]$ to be the unique monics satisfying 1-4 above for $p = f$ and $m = \gcd(|f|, |g|)$. Similarly, let g_1, g_2 be the unique monics in $S[x]$ satisfying 1-4 above when $p = g$ and $m = \gcd(|f|, |g|)$. Notice that for each $P \in \mathcal{P}$, we have $\phi_P(f_1) \circ \phi_P(f_2)$ and $a_P \circ d_P$ satisfying properties 1-4 above for $p = \phi_P(f)$ (where the relevant rings are $(R/P)[x]$ and $(R/P)\left[\frac{\gcd(|f|,|g|)}{|f|}\right][x]$ respectively). Uniqueness implies $\phi_P(f_1) = a_P$ and $\phi_P(f_2) = d_P$. Likewise, we see that $\phi_P(g_1) = b_P$ and $\phi_P(g_2) = d_P$. But then injectivity of ϕ yields $f_2 = g_2$.

Moreover, $\phi_P(f) = a_P \circ d_P = \phi_P(f_1 \circ f_2)$, so again by the injectivity of ϕ, $f = f_1 \circ f_2$, and similarly, $g = g_1 \circ g_2 = g_1 \circ f_2$. We see that f and g have a greatest common $\mathbb{M}_R$-divisor by Proposition VI.3, and $f_2 = g_2$ is a common $\mathbb{M}_S$-divisor of f and g of the greatest possible degree. Hence f_2 is a greatest common $\mathbb{M}_S$-divisor of f, g, and it remains only to show that f_2 is an $\mathbb{M}_R$-divisor of f and g. However, since the

degrees of f_1 and g_1 are coprime, this is immediate by Lemma VI.1. Hence f_2 is a greatest common $\mathbb{M}_R$-divisor of f and g of degree $\gcd(|f|, |g|)$. □

Polynomials F and G with a nonconstant common $\mathbb{M}_R$-composite need not have a greatest common $\mathbb{M}_R$-divisor of degree $\gcd(|F|, |G|)$ if R has nonzero nilpotents or $\mathbb{Z}$-torsion.

Example VI.11. Suppose that $R = \mathbb{Z}[T]/\langle T^2 \rangle$. Then

$$x^3 \circ (x^4 + 2Tx) = x^12 + 6Tx^9 = x^2 \circ (x^6 + 3Tx^3),$$

so $x^4 + 2Tx$ and $x^6 + 3Tx^3$ have a nonconstant common $\mathbb{M}_R$-composite. However, $x^4 + 2Tx$ is indecomposable over $\mathbb{M}_R$, for if it decomposed into two quadratics, $f \circ g$, then by noting that the coefficients of x^3 and x^2 are 0, we see that g must be x^2, but this is impossible.

Example VI.12. Suppose that $R = \mathbb{Z}[T]/\langle 2T \rangle$. Then

$$x^2 \circ (x^2 + Tx) = x^4 + T^2x^2 = (x^2 + T^2x) \circ x^2.$$

So x^2 and $x^2 + Tx$ have a nonconstant common $\mathbb{M}_R$-composite. However, they have no degree-2 common $\mathbb{M}_R$-divisor.

CHAPTER VII

Nonuniqueness of Decomposition

In this chapter, we develop results describing the extent of nonuniqueness of decomposition of monic polynomials over rings. Recall that a polynomial F is indecomposable in $\mathbb{M}_R$ if $|F|$ is at least 2 and if $F = F_1 \circ F_2$ (with $F_1, F_2 \in \mathbb{M}_R$ implies $|F_1| = 1$ or $|F_2| = 1$. In Section 7.1, we describe a relationship between any two decompositions of a polynomial in $\mathbb{M}_R$ into indecomposables when R is a ring without nonzero nilpotent elements (Theorem VII.5). In particular, we show that the number of indecomposables in any two such decompositions is the same and that we can obtain a relationship among all such decompositions; namely, starting with any decomposition of F, by a sequence of "Ritt swaps" in which we replace polynomials $a \circ b$ in the decomposition by $c \circ d$, where $|a| = |d|$ and $|b| = |c|$, we can obtain any other decomposition, up to composition by linears and their inverses. We provide examples of rings with nonzero nilpotents where this conclusion does not hold. In section 7.2, we characterize solutions to $a \circ b = c \circ d$ for $a, b, c, d \in \mathbb{M}_R$ with R a domain. We also show that this characterization does not extend beyond domains.

7.1 A Characterization of Decompositions over Rings without Nonzero Nilpotents

Recall that a *decomposition* of a polynomial F over S is a tuple $(F_1, F_2, ..., F_n)$ such that $F_i \in S$ and $F = F_1 \circ F_2 \circ ... \circ F_n$.

Definition VII.1. A *complete* $\mathbb{M}_R$*-decomposition* is a decomposition into $\mathbb{M}_R$-indecomposables.

For a given F, there may be several complete $\mathbb{M}_R$-decompositions. Indeed, if $F = F_1 \circ F_2$ with F_1 and F_2 indecomposable in $\mathbb{M}_R$, and if L is a linear (which, in $\mathbb{M}_R$, is necessarily invertible), then $F = (F_1 \circ L) \circ (L^{-1} \circ F_2)$ is another complete $\mathbb{M}_R$-decomposition of F. To address this, we define an equivalence relation on decompositions that accounts for this type of nonuniqueness.

Definition VII.2. For $S \in \{\mathbb{M}_R, \mathbb{P}_R\}$, two decompositions of a polynomial F over S, say $F = F_1 \circ F_2 \circ ... \circ F_r$ and $F = G_1 \circ G_2 \circ ... \circ G_r$ (with $F_i, G_j \in S$) are S-equivalent, symbolically $\langle F_1, F_2, ..., F_r \rangle \sim_S \langle G_1, G_2, ..., G_r \rangle$ or $\langle F_i \rangle_{i \leq r} \sim_S \langle G_i \rangle_{i \leq r}$, if there exist invertible linear $L_1, ..., L_{r-1} \in S$ such that

$$\begin{aligned} G_1 &= F_1 \circ L_1, \\ G_j &= L_{j-1}^{-1} \circ F_j \circ L_j, \qquad \text{for } 1 < j < r, \text{ and} \\ G_r &= L_{r-1}^{-1} \circ F_r. \end{aligned}$$

Definition VII.3. A *Ritt quadruple* in $\mathbb{M}_R$ is a quadruple of indecomposable polynomials (a, b, c, d) such that $a \circ b = c \circ d$ with $|a| = |d|$ and $|b| = |c|$.

Definition VII.4. Given a Ritt quadruple (a, b, c, d), a *Ritt swap* is the replacing of $\langle ..., a, b, ... \rangle$ by $\langle ..., c, d, ... \rangle$ in a decomposition. That is, a Ritt swap replaces a pair of consecutive indecomposable polynomials in the decomposition with a new pair of indecomposables with the same composite and same degrees but in reversed order.

Even taking into account the nonuniqueness caused by linears, however, polynomial decomposition is not unique. For example

$$x^2 \circ (x^3 + x) = (x^3 + 2x^2 + x) \circ x^2.$$

But we now show that when R is a ring without nonzero nilpotents or $\mathbb{Z}$-torsion, then any two complete $\mathbb{M}_R$-decompositions of F are related to each other. In particular, the two decompositions involve the same number of indecomposables, and the multiset of degrees of the indecomposables is the same. Both the statement and proof of the following theorem bear similarities to the Jordan–Hölder theorem.

Theorem VII.5. *Let R be a commutative ring with no nonzero nilpotents. Suppose $F = G_1 \circ G_2 \circ ... \circ G_r = H_1 \circ H_2 \circ ... \circ H_s$, where $F, G_i, H_i \in \mathbb{M}_R$ and where G_i, H_i are indecomposable, and where $|F|_R$ is neither 0 nor a zero divisor. Then $r = s$ and the sequences $\langle |G_i| \rangle_{i \leq r}, \langle |H_i| \rangle_{i \leq r}$ are permutations of each other. Moreover, there exists a finite chain of decompositions $F = F_1^{(j)} \circ ... \circ F_r^{(j)} (1 \leq j \leq n)$ with $F_i^{(j)} \in \mathbb{M}_R$ indecomposable such that*

1. $\langle F_i^{(1)} \rangle_{i \leq r} = \langle G_i \rangle_{i \leq r}$,
2. $\langle F_i^{(n)} \rangle_{i \leq r} \sim_{\mathbb{M}_R} \langle H_i \rangle_{i \leq r}$, *and*
3. *for each $j < n$, there exists $k < r$ such that*

$$F_k^{(j)} \circ F_{k+1}^{(j)} = F_k^{(j+1)} \circ F_{k+1}^{(j+1)},$$

with $|F_k^{(j)}| = |F_{k+1}^{(j+1)}|$ coprime to $|F_{k+1}^{(j)}| = |F_k^{(j+1)}|$, and for each $i \neq k, k+1$, we have $F_i^{(j)} = F_i^{(j+1)}$. That is, the decomposition $\langle F_i^{(j+1)} \rangle_{i \leq r}$ is obtained from $\langle F_i^{(j)} \rangle_{i \leq r}$ by a Ritt swap.

Remark VII.6. For many rings, monics can be indecomposable over $\mathbb{M}_R$ but not indecomposable over $\mathbb{P}_R$. For instance, take $R = \mathbb{Z}/15\mathbb{Z}$, and notice that

$$(6x^2 - x) \circ (5x^2 + x) = x^2 - x.$$

That is, $x^2 - x$ decomposes into two (nonmonic) quadratics over $\mathbb{P}_R$; however, $x^2 - x$ is indecomposable over $\mathbb{M}_R$. Thus, there seems to be no hope of generalizing Theorem VII.5 to $\mathbb{P}_R$-decompositions, at least if R has zero divisors.

Proof. We proceed by induction on the degree of F. If $|F| \leq 3$, then $r = s = 1$ and we are done. So suppose not, and assume that $|G_r|$ and $|H_s|$ are not coprime. Then by Theorem VI.10, G_r and H_s have a common $\mathbb{M}_R$-divisor of degree at least 2. Indecomposability of G_r and H_s implies that $H_s = L \circ G_r$ for some linear $L \in \mathbb{M}_R$. Then

$$G_1 \circ G_2 \circ ... \circ G_{r-1} = H_1 \circ H_2 \circ ... \circ H_{s-2} \circ (H_{s-1} \circ L),$$

so by the inductive hypothesis, $r - 1 = s - 1$ (hence $r = s$), and there exists a finite chain of decompositions $F = F_1^{(j)} \circ ... \circ F_{r-1}^{(j)} (1 \leq j \leq n)$ with $F_i^{(j)} \in \mathbb{M}_R$ indecomposable such that

1. $\langle F_i^{(1)} \rangle_{i \leq r-1} = \langle G_1 \circ G_2 \circ ... \circ G_{r-1} \rangle$,
2. $\langle F_i^{(n)} \rangle_{i \leq r-1} \sim_{\mathbb{M}_R} \langle H_1 \circ H_2 \circ ... \circ H_{r-2} \circ (H_{r-1} \circ L) \rangle$, and
3. for each $j < n$, there exists $k < r - 1$ such that

$$F_k^{(j)} \circ F_{k+1}^{(j)} = F_k^{(j+1)} \circ F_{k+1}^{(j+1)},$$

with $|F_k^{(j)}| = |F_{k+1}^{(j+1)}|$ coprime to $|F_{k+1}^{(j)}| = |F_k^{(j+1)}|$, and for each $i \neq k, k+1$, we have $F_i^{(j)} = F_i^{(j+1)}$.

It is immediate that if

$$\langle A_1, A_2, ..., A_n\rangle \sim_{\mathbb{M}_R} \langle B_1, B_2, ..., B_n\rangle,$$

then for any $P \in \mathbb{M}_R$,

$$\langle A_1, A_2, ..., A_n, P\rangle \sim_{\mathbb{M}_R} \langle B_1, B_2, ..., B_n, P\rangle.$$

Therefore $\langle F_1^{(j)}, F_2^{(j)}, ..., F_{r-1}^{(j)}, G_r\rangle_j$ is a finite chain of decompositions satisfying

1. $\langle F_i^{(1)}\rangle_{i\leq r} = \langle G_1 \circ G_2 \circ ... \circ G_r\rangle$,

2. $\langle F_i^{(n)}\rangle_{i\leq r-1} \sim_{\mathbb{M}_R} \langle H_1 \circ H_2 \circ ... \circ H_{r-2} \circ (H_{r-1} \circ L) \circ G_r\rangle \sim_{\mathbb{M}_R} \langle H_1 \circ H_2 \circ ... \circ H_r\rangle$, and

3. for each $j < n$, there exists $k < r-1$ such that

$$F_k^{(j)} \circ F_{k+1}^{(j)} = F_k^{(j+1)} \circ F_{k+1}^{(j+1)},$$

with $|F_k^{(j)}| = |F_{k+1}^{(j+1)}|$ coprime to $|F_{k+1}^{(j)}| = |F_k^{(j+1)}|$, and for each $i \neq k, k+1$, we have $F_i^{(j)} = F_i^{(j+1)}$.

Hence we may assume that $|G_r|$ and $|H_s|$ are coprime. By Corollary V.7, G_r and H_s have a least common $\mathbb{M}_R$-composite P of degree $\text{lcm}(|G_r|, |H_s|)$. Thus there are $A, B \in \mathbb{M}_R$ such that $P = A \circ G_r = B \circ H_s$, where $|A| = |H_s|$ and $|B| = |G_r|$.

We show now that A and B are indecomposable. For, suppose to the contrary that, without loss of generality, $A = A_1 \circ A_2$, where $|A_1|, |A_2| > 1$. We then have

$$A_1 \circ A_2 \circ G_r = B \circ H_s.$$

Since H_s and $A_2 \circ G_r$ have a nonconstant common $\mathbb{M}_R$-composite, by Theorem VI.10 they have a nonconstant common $\mathbb{M}_R$-divisor (since $|A_2|$ divides $|H_s|$). Since H_s is indecomposable, it follows that H_s is a $\mathbb{M}_R$-divisor of $A_2 \circ G_r$, but then $A_2 \circ G_r$

is a common $\mathbb{M}_R$-composite of G_r and H_s of lesser degree than $A \circ G_r$, which is a contradiction. Hence A and B are indecomposable.

Since F is a common $\mathbb{M}_R$-composite of G_r and H_s, it is also an $\mathbb{M}_R$-composite of P, so we may write $F = C_1 \circ C_2 \circ ... \circ C_t \circ A \circ G_r$, where $C_i \in \mathbb{M}_R$ is indecomposable. It follows that $C_1 \circ C_2 \circ ... \circ C_t \circ A = G_1 \circ G_2 \circ ... \circ G_{r-1}$ is a polynomial of degree less than $|F|$. Hence by the inductive hypothesis, $r = t + 2$. Similarly,

$$F = C_1 \circ C_2 \circ ... \circ C_t \circ B \circ H_s = H_1 \circ H_2 \circ ... \circ H_{s-1} \circ H_s,$$

so $s = t + 2$, whence $r = s$.

Moreover, the inductive hypothesis provides a finite chain of decompositions $F = F_1^{(j)} \circ ... \circ F_{r-1}^{(j)} (1 \leq j \leq n)$ with $F_i^{(j)} \in \mathbb{M}_R$ indecomposable over $\mathbb{M}_R$ such that

1. $\langle F_i^{(1)} \rangle_{i \leq r-1} = \langle G_i \rangle_{i \leq r-1}$,
2. $\langle F_i^{(n)} \rangle_{i \leq r-1} \sim_{\mathbb{M}_R} \langle C_1, C_2, ..., C_{r-2}, A \rangle$, and
3. for each $j < n$, there exists $k < r - 1$ such that

$$F_k^{(j)} \circ F_{k+1}^{(j)} = F_k^{(j+1)} \circ F_{k+1}^{(j+1)},$$

with $|F_k^{(j)}| = |F_{k+1}^{(j+1)}|$ coprime to $|F_{k+1}^{(j)}| = |F_k^{(j+1)}|$, and for each $i \neq k, k+1$, we have $F_i^{(j)} = F_i^{(j+1)}$.

Note that $\langle F_i^{(n)} \rangle_{i \leq r-1} \sim_{\mathbb{M}_R} \langle C_1, C_2, ..., C_{r-2}, A \rangle$ implies that there exist linear $L_1, ..., L_{r-2} \in \mathbb{M}_R$ such that

1. $G_1 = C_1 \circ L_1$,
2. $G_{r-1} = L_{r-2}^{-1} \circ A$, and
3. for $2 \leq i \leq r - 2$, we have $G_i = L_{i-1}^{-1} \circ C_i \circ L_i$.

By appending G_r to each of these compositions, we get a chain

$$\mathcal{C}_j = \langle F_1^{(j)}, F_2^{(j)}, ..., F_{r-1}^{(j)}, G_r \rangle_j$$

such that

1. $\mathcal{C}_1 = \langle G_i \rangle_{1 \leq i \leq r}$,
2. $\mathcal{C}_n = \langle (C_1 \circ L_1), (L_1^{-1} \circ C_2 \circ L_2), ..., (L_{r-3}^{-1} \circ C_{r-2} \circ L_{r-2}), (L_{r-2}^{-1} \circ A), G_r \rangle$, and
3. for $1 \leq i \leq n-1$, we have that $\mathcal{C}_i$ differs from $\mathcal{C}_{i+1}$ by only a Ritt swap.

Since $A \circ G_r = B \circ H_s$, it follows that

$$(C_1 \circ L_1) \circ (L_1^{-1} \circ C_2 \circ L_2) \circ ... \circ (L_{r-3}^{-1} \circ C_{r-2} \circ L_{r-2}) \circ (L_{r-2}^{-1} \circ A) \circ G_r = C_1 \circ C_2 \circ ... \circ C_{r-2} \circ B \circ H_r.$$

Hence we may write

$$\mathcal{C}_{n+1} = \langle (C_1 \circ L_1), (L_1^{-1} \circ C_2 \circ L_2), ..., (L_{r-3}^{-1} \circ C_{r-2} \circ L_{r-2}), (L_{r-2}^{-1} \circ B), H_s \rangle,$$

and notice that $\mathcal{C}_{n+1}$ differs from $\mathcal{C}_n$ by only a Ritt swap, since (A, G_r, B, H_s), and hence $(L_{r-2}^{-1} \circ A, G_r, L_{r-2}^{-1} \circ B, H_s)$, is a Ritt quadruple.

Now, since

$$C_1 \circ C_2 \circ ... \circ C_{r-2} \circ B = H_1 \circ H_2 \circ ... \circ H_{r-1},$$

by the inductive hypothesis, there is a finite chain of decompositions

$$F = F_1^{(n+j+1)} \circ ... \circ F_{r-1}^{(n+j+1)} (1 \leq j \leq m)$$

with $F_i^{(n+j+1)} \in \mathbb{M}_R$ indecomposable such that

1. $\langle F_i^{(n+2)} \rangle_{i \leq r-1} = \langle C_1, C_2, ..., C_{r-2}, B \rangle$,
2. $\langle F_i^{(n+m+1)} \rangle_{i \leq r-1} \sim_{\mathbb{M}_R} \langle H_i \rangle_{i \leq r-1}$, and

3. for each $j < m$, there exists $k < r-1$ such that

$$F_k^{(n+j)} \circ F_{k+1}^{(n+j)} = F_k^{(n+j+1)} \circ F_{k+1}^{(n+j+1)},$$

with $|F_k^{(n+j)}| = |F_{k+1}^{(n+j+1)}|$ coprime to $|F_{k+1}^{(n+j)}| = |F_k^{(n+j+1)}|$, and for each $i \neq k, k+1$, we have $F_i^{(n+j)} = F_i^{(n+j+1)}$.

Hence, the chain of decompositions $\mathcal{D}_j = \langle F_1^{(n+j)}, F_2^{(n+j)}, ..., F_{r-1}^{(n+j)}, H_r \rangle_j$ is such that $\mathcal{D}_1 = \langle C_1, C_2, ..., C_{r-2}, B, H_r \rangle$, that $\mathcal{D}_m \sim_{\mathbb{M}_R} \langle H_i \rangle_{i \leq r}$, and that $\mathcal{D}_i$ only differs from $\mathcal{D}_{i+1}$ by a Ritt swap.

It follows that $\mathcal{C}_1, ..., \mathcal{C}_n, \mathcal{C}_{n+1} = \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, ..., \mathcal{D}_m$ is a finite chain of decompositions such that $\mathcal{C}_1 = \langle G_i \rangle_{i \leq r}$, that $\mathcal{D}_m \sim_{\mathbb{M}_R} \langle H_i \rangle_{i \leq r}$, and that consecutive decompositions in the chain differ only by a Ritt swap. □

When $|F|_R$ is 0 or a zero divisor, or when R contains nonzero nilpotents, F may decompose into chains of indecomposables of different lengths, as illustrated in the following examples.

Example VII.7. If R is a ring of characteristic p prime, then

$$\begin{aligned} x^{p+1} \circ (x^p + x) \circ (x^p - x) &= (x^{p^2} - x)^{p+1} \\ &= (x^{p^2} - x^{p^2-p+1} - x^p + x) \circ x^{p+1}. \end{aligned}$$

Certainly x^{p+1} will decompose into the same number of factors in both decompositions. It is clear that both $x^p + x$ and $x^p - x$ are indecomposable over $\mathbb{M}_R$, since they have prime degree. Moreover, $(x^{p^2} - x^{p^2-p+1} - x^p + x)$ is indecomposable over $\mathbb{M}_R$ since if it were decomposable over $\mathbb{M}_R$, it would necessarily decompose into two degree-p polynomials. So suppose that $f = \sum_{i=0}^{p} a_i x^i$ and $g = \sum_{j=0}^{p} b_j x^j$ are two monic

degree p polynomials. Then

$$\begin{aligned} f \circ g &= (x^p + O(x^{p-1})) \circ \left(\sum_{j=0}^{p} b_j x^j \right) \\ &= x^p \circ \left(\sum_{j=0}^{p} b_j x^j \right) + O(x^{p^2-p}) \\ &= \left(\sum_{j=0}^{p} b_j^p x^{pj} \right) + O(x^{p^2-p}) \\ &= x^p + O(x^{p^2-p}). \end{aligned}$$

Hence $(x^{p^2} - x^{p^2-p+1} - x^p + x)$ cannot decompose into two degree-p monics and is thus indecomposable over M_R. The two decompositions of $(x^{p^2} - x)^{p+1}$ into indecomposables, then, have different lengths.

This example, in the case of fields, is due to Dorey and Whaples [DW74]. This analog to Ritt's first theorem can fail due to $\mathbb{Z}$-torsion even in characteristic 0.

Example VII.8. Let $R = \mathbb{Z}[T]/\langle 2T \rangle$. Then

$$x^2 \circ (x^2+x) \circ (x^2+Tx) = x^8 + 2x^6 + (T^4+1)x^4 + T^2x^2 = (x^4 + 2x^3 + (T^4+1)x^2 + T^2x) \circ x^2.$$

We now show that $x^4 + 2x^3 + (T^4+1)x^2 + T^2x$ is indecomposable. So suppose to the contrary that

$$\begin{aligned} x^4 + 2x^3 + (T^4+1)x^2 + T^2x &= (x^2 + ax) \circ (x^2 + cx) \\ &= x^4 + 2cx^3 + (c^2 + a)x^2 + (ac)x. \end{aligned}$$

Note that we may always assume that the factors have no constant term, since otherwise we may compose with linears to eliminate them. Then, equating coefficients,

- $2c = 2$
- $c^2 + a = T^4 + 1$

- $ca = T^2$.

The first equation yields c $= \sum_{i=0}^{k} e_i T^i$ with $e_0 = e_k = 1$ and $e_i \in \{0, 1\}$. From the second equation, we see that $a = T^4 + 1 - c^2$, and substituting into the third equation, gives

$$c(T^4 + 1 - c^2) = T^2.$$

The only possibility is that $k = 2$, so $c = 1 + e_1 T + T^2$. Substituting into the previous equation gives

$$(1 + e_1 T + T^2) \cdot (e_1^2 T^2) = T^2,$$

a contradiction.

The following example shows that nonzero nilpotents can cause decompositions of different lengths, even if $|F|_R$ is neither 0 nor a zero divisor.

Example VII.9. If $R = \mathbb{Z}[T]/\langle T^2 \rangle$, then

$$x^3 \circ (x^4 + 2Tx) = x^{12} + 6Tx^9 = x^2 \circ (x^6 + 3Tx^3) = x^2 \circ (x^2 + 3Tx) \circ x^3.$$

But $x^4 + 2Tx$ is indecomposable (cf. Example VI.11), so $x^{12} + 6Tx^9$ has two complete $\mathbb{M}_R$-decompositions of different lengths.

7.2 A Characterization of "Ritt Swaps" over Domains

Theorem VII.5 describes the relationship between any two complete $\mathbb{M}_R$-decompositions of a polynomial, for certain rings R, in terms of the collections of indecomposables$A, B, G, H \in \mathbb{M}_R$ such that $G \circ A = H \circ B$ with $|G| = |B|$ and $\gcd(|G|, |A|) = 1$. In this section, we determine all such A, B, G, H in case R is an integral domain whose characteristic does not divide $|G \circ A|$. In fact, we do this without assuming the indecomposability or coprimality hypotheses above.

One example of such A, B, G, H is the commuting polynomials

$$x^n \circ x^m = x^m \circ x^n.$$

A more complicated example comes from the fact that the square of an odd polynomial is an even polynomial, or in other words,

$$x^2 \circ xP(x^2) = x(P(x))^2 \circ x^2.$$

These two examples are special cases of the more general example

$$x^n \circ x^r P(x^n) = x^r P(x)^n \circ x^n \tag{7.1}$$

where $P(x)$ is an arbitrary polynomial. We will prove that, if R is an integral domain, then all $A, B, G, H \in M_R$ which satisfy $G \circ A = H \circ B$ and $|G| = |B|$ can be obtained from the examples in (7.1) and certain variants of Chebychev polynomials, which we now define.

Definition VII.10. For fixed $t \in R$, the Dickson polynomials with parameter t, denoted $D_n(x,t)$, are the polynomials in $R[x]$ defined recursively by:

$$D_0(x,t) = 2, D_1(x,t) = x, D_n(x,t) = xD_{n-1}(x,t) - aD_{n-2}(x,t).$$

Lemma VII.11. *For $n \geq 1$, we have* $D_n(x,t) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-t)^i x^{n-2i}$.

Proof. By induction on n. □

Corollary VII.12. *Let $n \geq 0$ and $t \in R$. Then if n is even, $D_n(x,t) = g_n(x^2)$ for some monic polynomial $g_n \in R[x]$, and if n is odd, then $D_n(x,t) = xh_n(x^2)$ for some monic polynomial $h_n \in R[x]$.*

Proof. This is clear from Lemma VII.11. □

Remark VII.13. Many further properties of Dickson polynomials can be found in [ACZ00, LMT93].

It is well-known that Dickson polynomials commute under functional composition (see, for instance, [LMT93]). Namely,

$$D_n(x, t^m) \circ D_m(x, t) = D_m(x, t^n) \circ D_n(x, t),$$

providing a further example of polynomials $A, B, G, H \in \mathbb{M}_R$ satisfying $G \circ A = H \circ B$ and $|G| = |B|$. We now show that these examples, together with those in (7.1), are the source of all examples when R is an integral domain whose characteristic does not divide $|G \circ A|$.

Corollary VII.14. *Let R be an integral domain of characteristic $p \geq 0$. Suppose $A, F, B, G \in \mathbb{M}_R$ satisfy $|A| = |G|$ and $p \nmid |A| \cdot |F|$. Then $A \circ F = B \circ G$ if and only if there exist $U, V, A_0, F_0, B_0, G_0 \in \mathbb{M}_R$ such that*

1. $A = U \circ A_0$,
2. $F = F_0 \circ V$,
3. $B = U \circ B_0$,
4. $G = G_0 \circ V$, *and*
5. $\gcd(|A_0|, |B_0|) = 1 = \gcd(|F_0|, |G_0|)$,

and either

1. $\langle A_0, F_0 \rangle \sim_{\mathbb{M}_R} \langle x^r P(x)^n, x^n \rangle$,
   $\langle B_0, G_0 \rangle \sim_{\mathbb{M}_R} \langle x^n, x^r P(x^n) \rangle$, *where $P \in \mathbb{M}_R$ and $r > 0$, or*
2. $\langle A_0, F_0 \rangle \sim_{\mathbb{M}_R} \langle D_m(x, t^n), D_n(x, t) \rangle$,
   $\langle B_0, G_0 \rangle \sim_{\mathbb{M}_R} \langle D_n(x, t^m), D_m(x, t) \rangle$, *where $t \in R$.*

In view of Theorems V.8 and VI.10, it suffices to prove this result in case $|A|$ and $|F|$ are coprime. Thus, the result is a consequence of the following result.

Theorem VII.15. *Let R be an integral domain, and let $A, B, G, H \in \mathbb{M}_R$ satisfy $|A| = |H| = n > 1$ and $|B| = |G| = m > n$, where $\gcd(m, n) = 1$ and $G'H' \neq 0$. Then $G \circ A = H \circ B$ if and only if there exist linear $L_1, L_2 \in \mathbb{M}_R$ such that*

1. $\langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{M}_R} \langle x^r P(x)^n, x^n \rangle$,

   $\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{M}_R} \langle x^n, x^r P(x^n) \rangle$, *where $P \in \mathbb{M}_R$ and $r > 0$, or*

2. $\langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{M}_R} \langle D_m(x, t^n), D_n(x, t) \rangle$,

   $\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{M}_R} \langle D_n(x, t^m), D_m(x, t) \rangle$, *where $t \in R$.*

Note that in Theorem VII.15, we replace the condition $\operatorname{char}(R) \nmid |G| \cdot |H|$ by the much weaker condition $G'H' \neq 0$.

When R is a field, Theorem VII.15 is an easy consequence of the following result of Zannier (see [Sch00, Zan93]), which is an extension of previous work of Ritt, Levi, and Dorey and Whaples.

Theorem VII.16 (Zannier)**.** *Let K be a field, and let $A, B, G, H \in \mathbb{P}_K$ satisfy $|A| = |H| = n > 1$ and $|B| = |G| = m > n$, where $\gcd(m, n) = 1$ and $G'H' \neq 0$. Then $G \circ A = H \circ B$ if and only if there exist linear $L_1, L_2 \in \mathbb{P}_K$ such that either*

1. $\langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{P}_K} \langle x^r P(x)^n, x^n \rangle$,

   $\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{P}_K} \langle x^n, x^r P(x^n) \rangle$, *where $P \in K[x]$ and $r > 0$, or*

2. $\langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{P}_K} \langle D_m(x, t^n), D_n(x, t) \rangle$,

   $\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{P}_K} \langle D_n(x, t^m), D_m(x, t) \rangle$, *where $t \in K$.*

We prove Theorem VII.15 with the following 3 lemmas. The strategy will be to use Theorem VII.16 to write the (implicit and explicit) linears with coefficients in $\operatorname{Frac}(R)$ and then to show that we can choose all of the polynomials to be monic.

Lemma VII.17. *Let R be an integral domain, and let $A, B, G, H \in \mathbb{M}_R$ satisfy $|A| = |H| = n > 1$ and $|B| = |G| = m > n$, where $\gcd(m, n) = 1$ and $G'H' \neq 0$. Let $F = \mathrm{Frac}(R)$, and suppose that there exist linear $L_1, L_2 \in \mathbb{P}_F$ such that*

$$\langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle x^r P(x)^n, x^n \rangle$$

and

$$\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle x^n, x^r P(x^n) \rangle$$

for some $P \in \mathbb{P}_F$ and $r > 0$. Then there exist linear $M_1, M_2 \in \mathbb{M}_R$ such that

$$\langle M_1 \circ G, A \circ M_2 \rangle \sim_{\mathbb{M}_R} \langle x^r Q(x)^n, x^n \rangle$$

and

$$\langle M_1 \circ H, B \circ M_2 \rangle \sim_{\mathbb{M}_R} \langle x^n, x^r Q(x^n) \rangle,$$

for some $Q \in \mathbb{M}_R$.

Proof. Suppose that there exist linear $L_1, L_2 \in \mathbb{P}_F$ such that

$$\langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle x^r P(x)^n, x^n \rangle$$

and

$$\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle x^n, x^r P(x^n) \rangle$$

for some $P \in \mathbb{P}_F$ and $r > 0$. Then there are linears $L_3, L_4 \in \mathbb{P}_F$ such that

$$\begin{aligned} G &= L_1^{-1} \circ x^r P(x)^n \circ L_3^{-1} \\ A &= L_3 \circ x^n \circ L_2^{-1} \\ H &= L_1^{-1} \circ x^n \circ L_4^{-1} \\ B &= L_4 \circ x^r P(x^n) \circ L_2^{-1}, \end{aligned}$$

where $P \in \mathbb{P}_F$ and $r = m - n|P| > 0$. Notice that $\gcd(r, n) \mid r + n|P| = m$; hence, $\gcd(r, n) \mid \gcd(m, n) = 1$, which implies that $\gcd(r, n) = 1$.

We write

$$\begin{aligned} L_1^{-1} &= ax + b \\ L_2^{-1} &= \mu(x + \nu) \\ L_3 &= ex + f \\ L_4^{-1} &= c(x + d) \end{aligned}$$

with with $a, b, c, d, e, f, \mu, \nu \in F$, so that:

$$\begin{aligned} G &= (ax + b) \circ x^r P(x)^n \circ (\frac{x - f}{e}) \\ A &= (ex + f) \circ x^n \circ \mu(x + \nu) \\ H &= (ax + b) \circ x^n \circ c(x + d) \\ B &= (\frac{x}{c} - d) \circ x^r P(x^n) \circ \mu(x + \nu). \end{aligned}$$

Now, $A = f + e\mu^n(x+\nu)^n$, and since A is monic, $e\mu^n = 1$, whence $A = f + (x+\nu)^n$. Notice that the coefficient of x^{n-1} in A is $n\nu$. Since $A \in \mathbb{M}_R$, it follows that $n\nu \in R$.

Writing $P(x) = \sum_{j=0}^{|P|} p_j x^j$, we see that

$$B = -d + \frac{1}{c} \sum_{j=0}^{|P|} p_j \mu^{nj+r} (x + \nu)^{nj+r}.$$

By expanding $(x + \nu)^{nj+r}$, we observe that

$$B = \frac{p_{|P|}}{c} \mu^{n|P|+r} x^{n|P|+r} + \frac{p_{|P|}}{c} \mu^{n|P|+r} (n|P| + r) \nu x^{n|P|+r-1} + O(x^{n|P|+r-2}).$$

Again, since B is monic, we see that $\frac{p_{|P|}}{c} \mu^{n|P|+r} = 1$, so

$$B = x^{n|P|+r} + (n|P| + r) \nu x^{n|P|+r-1} + O(x^{n|P|+r-2}),$$

and since $B \in \mathbb{M}_R$, we have that $(n|P| + r)\nu \in R$. Since $n\nu \in R$ by the above analysis, $r\nu \in R$, and since $\gcd(r, n) = 1$, it follows that $\nu \in R$.

Since $\nu \in R$, we see that

$$-d + \frac{1}{c}\sum_{j=0}^{|P|} p_j \mu^{nj+r} x^{nj+r} = B \circ (x - \nu) \in \mathbb{M}_R,$$

whence $d \in R$ and for $0 \leq j \leq |P|$, we have $g_j := \frac{p_j}{c}\mu^{nj+r} \in R$. Then B has the desired form. That is,

$$B = (x - d) \circ (x^r \hat{p}(x^n)) \circ (x + \nu),$$

where $d, \nu, g_j \in R$ and where $\hat{p}(x) = \sum_{j=0}^{|P|} g_j x^j$).

Similarly, $f + x^n = A \circ (x - \nu) \in \mathbb{M}_R$, so $f \in R$, and A has the desired form. Namely,

$$A = (x + f) \circ x^n \circ (x + \nu),$$

where $f, \nu \in R$.

Moreover, $H = b + ac^n(x + d)^n$, and since H is monic, $ac^n = 1$, whence $H = b + (x + d)^n$. We showed $d \in R$ above, so by noting that $H \circ (x - d) \in \mathbb{M}_R$, we

conclude that $b \in R$ and that $H = (x+b) \circ x^n \circ (x+d); b, d \in R$. Lastly, we compute

$$\begin{aligned}
G &= b + a\frac{1}{e^r}(x-f)^r \left(\sum_{j=0}^{|P|} p_j \frac{(x-f)^j}{e^j} \right)^n \\
&= b + a\frac{1}{e^r}(x-f)^r \left(\sum_{j=0}^{|P|} (\frac{cg_j}{\mu^{nj+r}}) \frac{(x-f)^j}{e^j} \right)^n \\
&= b + \frac{1}{e^r}(x-f)^r \left(\sum_{j=0}^{|P|} (\frac{g_j}{\mu^{nj+r}}) \frac{(x-f)^j}{e^j} \right)^n \qquad (\text{since } ac^n = 1) \\
&= b + \frac{1}{e^r}(x-f)^r \left(\sum_{j=0}^{|P|} (\frac{g_j}{\mu^r})(x-f)^j \right)^n \qquad (\text{since } e\mu^n = 1) \\
&= b + (x-f)^r \left(\sum_{j=0}^{|P|} g_j (x-f)^j \right)^n \qquad (\text{since } e\mu^n = 1) \\
&= (x+b) \circ x^r \left(\sum_{j=0}^{|P|} g_j x^j \right)^n \circ (x-f),
\end{aligned}$$

where $b, f, g_j \in R$. This establishes the lemma. □

Lemma VII.18. *Let R be an integral domain, and let $A, B, G, H \in \mathbb{M}_R$ satisfy $|A| = |H| = n > 1$ and $|B| = |G| = m > n$, where $\gcd(m, n) = 1$ and $G'H' \neq 0$. Let $F = \mathrm{Frac}(R)$, and suppose that there exist linear $L_1, L_2 \in \mathbb{P}_F$ such that*

$$\langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle D_m(x, t^n), D_n(x, t) \rangle$$

and

$$\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle D_n(x, t^m), D_m(x, t) \rangle$$

for some $t \in F$. Then there exist $\nu \in R$ and $b, d, f, T \in F$ such that

$$\begin{aligned}
G &= (x+b) \circ D_m(x, T^n) \circ (x-f) \\
A &= (x+f) \circ D_n(x, T) \circ (x+\nu) \\
H &= (x+b) \circ D_n(x, T^m) \circ (x+d) \\
B &= (x-d) \circ D_m(x, T) \circ (x+\nu).
\end{aligned}$$

Proof. Suppose that there exist linear $L_1, L_2 \in \mathbb{P}_F$ such that

$$\langle \langle L_1 \circ G, A \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle D_m(x, t^n), D_n(x, t) \rangle$$

and

$$\langle L_1 \circ H, B \circ L_2 \rangle \sim_{\mathbb{P}_F} \langle D_n(x, t^m), D_m(x, t) \rangle$$

for some $t \in F$. Then there are linear $L_3, L_4 \in \mathbb{P}_F$ such that

$$\begin{aligned} G &= L_1^{-1} \circ D_m(x, t^n) \circ L_3^{-1} \\ A &= L_3 \circ D_n(x, t) \circ L_2^{-1} \\ H &= L_1^{-1} \circ D_n(x, t^m) \circ L_4^{-1} \\ B &= L_4 \circ D_m(x, t) \circ L_2^{-1}. \end{aligned}$$

We write

$$\begin{aligned} L_1^{-1} &= ax + b \\ L_2^{-1} &= \mu(x + \nu) \\ L_3 &= ex + f \\ L_4^{-1} &= c(x + d) \end{aligned}$$

with with $a, b, c, d, e, f, \mu, \nu \in F$, so that:

$$\begin{aligned} G &= (ax + b) \circ D_m(x, t^n) \circ (\frac{x - f}{e}) \\ A &= (ex + f) \circ D_n(x, t) \circ \mu(x + \nu) \\ H &= (ax + b) \circ D_n(x, t^m) \circ c(x + d) \\ B &= (\frac{x}{c} - d) \circ D_m(x, t) \circ \mu(x + \nu). \end{aligned}$$

with $a, b, c, d, e, f, \mu, \nu \in F$.

Notice that

$$\begin{aligned} B &= -d + \frac{1}{c}\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-i}\binom{m-i}{i}(-t)^i \mu^{m-2i}(x+\nu)^{m-2i} \\ &= \frac{1}{c}\mu^m x^m + \frac{1}{c}\mu^m m\nu x^{m-1} + O(x^{m-2}). \end{aligned}$$

Since B is monic, we see that $\frac{\mu^m}{c} = 1$ and that $B = x^m + m\nu x^{m-1} + O(x^{m-2})$. Hence $m\nu \in R$. Similarly,

$$\begin{aligned} A &= f + e\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-t)^i \mu^{n-2i}(x+\nu)^{n-2i} \\ &= e\mu^n x^n + e\mu^n n\nu x^{n-1} + O(x^{n-2}), \end{aligned}$$

and since A is in $\mathbb{M}_R$, we see that $e\mu^n = 1$. It follows that $n\nu \in R$, and coprimality of m and n yields $\nu \in R$.

Rewriting, we see that

$$\begin{aligned} B &= -d + \frac{1}{c}\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-i}\binom{m-i}{i}(-t)^i \mu^{m-2i}(x+\nu)^{m-2i} \\ &= -d + \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-i}\binom{m-i}{i}(\frac{-t}{\mu^2})^i (x+\nu)^{m-2i} \\ &= (x-d) \circ D_m(x, \frac{t}{\mu^2}) \circ (x+\nu) \end{aligned}$$

and

$$\begin{aligned} A &= f + e\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-t)^i \mu^{n-2i}(x+\nu)^{n-2i} \\ &= f + \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(\frac{-t}{\mu^2})^i (x+\nu)^{n-2i} \\ &= (x+f) \circ D_n(x, \frac{t}{\mu^2}) \circ (x+\nu). \end{aligned}$$

Considering G and H, we see that

$$\begin{aligned}
G &= b + a\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-i}\binom{m-i}{i}(-t^n)^i(\frac{1}{e})^{m-2i}(x-f)^{m-2i} \\
&= b + \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-i}\binom{m-i}{i}(-t^n)^i e^{2i}(x-f)^{m-2i} \qquad (\frac{a}{e^m} = 1 \text{ since } G \text{ is monic}) \\
&= b + \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-i}\binom{m-i}{i}(-(\frac{t}{\mu^2})^n)^i(e\mu^n)^{2i}(x-f)^{m-2i} \\
&= b + \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-i}\binom{m-i}{i}(-(\frac{t}{\mu^2})^n)^i(x-f)^{m-2i} \\
&= (x+b) \circ D_m(x, (\frac{t}{\mu^2})^n) \circ (x-f) \\
H &= b + a\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-t^m)^i c^{n-2i}(x+d)^{n-2i} \\
&= b + \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-t^m)^i c^{-2i}(x+d)^{n-2i} \qquad (ac^n = 1 \text{ since } H \text{ is monic}) \\
&= b + \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-(\frac{t}{\mu^2})^m)^i(\frac{\mu^m}{c})^{2i}(x+d)^{n-2i} \\
&= b + \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-(\frac{t}{\mu^2})^m)^i(x+d)^{n-2i} \\
&= (x+b) \circ D_n(x, (\frac{t}{\mu^2})^m) \circ (x+d).
\end{aligned}$$

Summarizing, we have that $\nu \in R$ and $b, d, f, \frac{t}{\mu^2} \in F$. Moreover,

$$\begin{aligned}
G &= (x+b) \circ D_m(x, (\frac{t}{\mu^2})^n) \circ (x-f) \\
A &= (x+f) \circ D_n(x, \frac{t}{\mu^2}) \circ (x+\nu) \\
H &= (x+b) \circ D_n(x, (\frac{t}{\mu^2})^m) \circ (x+d) \\
B &= (x-d) \circ D_m(x, \frac{t}{\mu^2}) \circ (x+\nu)
\end{aligned}$$

Taking $T = \frac{t}{\mu}$ proves lemma. □

Lemma VII.19. *Under the hypotheses of Lemma VII.18, if additionally $n > 2$, then there exist linear $M_1, M_2 \in \mathbb{M}_R$ such that*

$$\langle M_1 \circ G, A \circ M_2 \rangle \sim_{\mathbb{M}_R} \langle D_m(x, u^n), D_n(x, u) \rangle$$

and

$$\langle M_1 \circ H, B \circ M_2 \rangle \sim_{\mathbb{M}_R} \langle D_n(x, u^m), D_m(x, u) \rangle,$$

for some $u \in R$.

Proof. By Lemma VII.18, there exist $\nu \in R$ and $b, d, f, T \in F$ such that

$$\begin{aligned} G &= (x+b) \circ D_m(x, T^n) \circ (x-f) \\ A &= (x+f) \circ D_n(x, T) \circ (x+\nu) \\ H &= (x+b) \circ D_n(x, T^m) \circ (x+d) \\ B &= (x-d) \circ D_m(x, T) \circ (x+\nu). \end{aligned}$$

It suffices to show that $b, d, f, T \in R$. Since $\nu \in R$, the composites $B \circ (x-\nu)$ and $A \circ (x-\nu)$ lie in $\mathbb{M}_R$. Noting that $m > 2$, we see that $B \circ (x-\nu) = x^m - mTx^{m-2} + O(x^{m-3})$. So $mT \in R$, and likewise $nT \in R$. Since m and n are coprime, it follows that $T \in R$. Hence, $D_m(x, T) \in R[x]$, and it follows that $d \in R$. Since $n > 2$, similar analysis of $A \circ (x-\nu)$ yields that $f \in R$. But since f and T are in R, both $D_m(x, T^n)$ and $G \circ (x+f) = (x+b) \circ D_m(x, T^n)$ lie in $\mathbb{M}_R$. It follows that $b \in R$, proving the result. □

Note that Lemma VII.19 is not generally true when $\min(m, n) = 2$:

Example VII.20. Let $R = \mathbb{Z}$, and take $G = x^3 - x^2, A = x^2 + 1, B = x^3 + x, H = x^2$. Then $G \circ A = H \circ B$. It is straightforward to verify that there is only one solution

set $t, b, d, f, \nu \in \mathbb{Q}$ to

$$\begin{aligned} G &= b + D_m(x - f, t^n) \\ A &= f + D_n(x + \nu, t) \\ H &= b + D_n(x + d, t^m) \end{aligned}$$

$$B = -d + D_m(x + \nu, t),$$

and that the solution $(t = -\frac{1}{3}, b = -\frac{2}{27}, d = \nu = 0, f = \frac{1}{3})$ is not in $\mathbb{Z}$.

However, we handle the case of $\min(m, n) = 2$ (not covered by Lemma VII.19) by showing that any such A, B, G, H satisfy the hypotheses of Lemma VII.17.

Lemma VII.21. *Under the hypotheses of Lemma VII.18, if additionally $n = 2$, then there exist linear $M_1, M_2 \in \mathbb{M}_R$ such that*

$$\langle M_1 \circ G, A \circ M_2 \rangle \sim_{\mathbb{P}_F} \langle x^r P(x)^n, x^n \rangle$$

and

$$\langle M_1 \circ H, B \circ M_2 \rangle \sim_{\mathbb{P}_F} \langle x^n, x^r P(x^n) \rangle$$

for some $P \in \mathbb{P}_F$ and $r > 0$.

Proof. Coprimality of m and n implies that m is odd. It follows from the definitions

that $D_2(x,u) = x^2 - 2u$, so Lemma VII.18 yields:

$$\begin{aligned}
A &= (x+f) \circ D_2(x,T) \circ (x+\nu) \\
&= (x+f) \circ (x^2 - 2T) \circ (x+\nu) \\
&= (x+f-2T) \circ x^2 \circ (x+\nu) \\
H &= (x+b) \circ D_2(x,T^m) \circ (x+d) \\
&= (x+b) \circ (x^2 - 2T^m) \circ (x+d) \\
&= (x+b-2T^m) \circ x^2 \circ (x+d) \\
G &= (x+b) \circ D_m(x,T^2) \circ (x-f) \\
&= (x+b-2T^m) \circ \left(D_m(x-2T,T^2) + 2T^m\right) \circ (x-f+2T) \\
B &= (x-d) \circ D_m(x,T) \circ (x+\nu)
\end{aligned}$$

From $G \circ A = H \circ B$, we conclude that

$$(D_m(x-2T,T^2) + 2T^m) \circ x^2 = x^2 \circ D_m(x,T).$$

By Corollary VII.12, there exists a polynomial $h \in \mathbb{M}_F$ such that $D_m(x,T) = xh(x^2)$. But then

$$\begin{aligned}
(D_m(x-2T,T^2) + 2T^m) \circ x^2 &= x^2 \circ D_m(x,T) \\
&= x^2 \circ xh(x^2) \\
&= x^2 h(x^2)^2 \\
&= xh(x)^2 \circ x^2,
\end{aligned}$$

whence $D_m(x - 2T, T^2) + 2T^m = xh(x)^2$. But then, we have that

$$\begin{aligned} G &= (x + b - 2T^m) \circ xh(x)^2 \circ (x - f + 2T) \\ A &= (x + f - 2T) \circ x^2 \circ (x + \nu) \\ H &= (x + b - 2T^m) \circ x^2 \circ (x + d) \\ B &= (x - d) \circ xh(x^2) \circ (x + \nu), \end{aligned}$$

with $b - 2T^m, f + 2T, d \in F, \nu \in R$. Now notice, though, that

$$\langle (x - b + 2T^m) \circ G, A \circ (x - \nu) \rangle \sim_{\mathbb{P}_F} \langle xh(x)^2, x^2 \rangle$$

and

$$\langle (x - b + 2T^m) \circ H, B \circ (x - \nu) \rangle \sim_{\mathbb{P}_F} \langle x^2, xh(x^2) \rangle.$$

Lemma VII.17 now implies the result. □

Lemmas VII.17-VII.21 now directly yield Theorem VII.15, which in turn implies Corollary VII.14.

Remark VII.22. The hypothesis $G'H' \neq 0$ of Theorem VII.15 is certainly satisfied if $\mathrm{char}(R)$ does not divide $|G| \cdot |H|$.

We conclude with an example suggesting that we would have to add more items to the conclusion of Theorem VII.15 to find an analog in rings which are not integral domains. We exhibit polynomials in one of the simplest examples of a commutative ring with zero divisors, namely $\mathbb{Z}[a, b]/\langle ab \rangle$, that violate the conclusions of Theorem VII.15.

Example VII.23. Let $R = \mathbb{Z}[a, b]/\langle ab \rangle$. Then

$$(x^4 + 3bx^3 + (4a^3 + 3b^2)x^2 + b^3x) \circ (x^3 + 3ax) = (x^3 + 6a^2x^2 + 9a^4x) \circ (x^4 + 4ax^2 + bx).$$

are two different complete $\mathbb{M}_R$-decompositions that do not satisfy the conclusion of Theorem VII.15.

BIBLIOGRAPHY

BIBLIOGRAPHY

[ACZ00] S. S. Abhyankar, S. D. Cohen, and M. E. Zieve, *Bivariate factorizations connection Dickson polynomials and Galois theory*, Trans. Amer. Math. Soc. **352** (2000), 2871–2887.

[BM78] A. Bremner and P. Morton, *Polynomial relations in characteristic p*, Quart. J. Math. Oxford (2) **29** (1978), 335–347.

[BT00] Y. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

[BWZ09] R. Beals, J. Wetherell, and M. Zieve, *Polynomials with a common composite*, Israel J. Math. **174** (2009), 93–117.

[BZ85] D. R. Barton and R. E. Zippel, *Polynomial decomposition algorithms*, J. Symbolic Comput. **1** (1985), 159–168.

[DF99] D. Dummit and R. Foote, *Abstract Algebra*, second ed., John Wiley & Sons, Inc., Hoboken, NJ, 1999.

[DG06] A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Quart. J. Math. **57** (2006), 193–201.

[DW74] F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra **28** (1974), 88–101.

[Eng41] H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.

[FM69] M. D. Fried and R. E. MacRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171.

[Fri70] M. Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55.

[Fri74] ———, *On a theorem of Ritt and related Diophantine problems*, J. reine agnew. Math. **264** (1974), 40–55.

[GTZ] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Linear relations between polynomial orbits*, submitted for publication, arXiv:0807.3576.

[GTZ08] ———, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math. **171** (2008), 463–483.

[Gus88] I. Gusić, *On decomposition of polynomials over rings*, Colloq. Math. **55** (1988), 329–353.

[KL89] D. Kozen and S. Landau, *Polynomial decomposition algorithms*, J. Symbolic Comput. **9** (1989), 445–456.

[Lam01] T. Y. Lam, *A First Course in Noncommutative Rings*, 2nd ed., Springer-Verlag, New York, NY, 2001.

[Lev42] H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. **64** (1942), 389–400.

[LMT93] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, John Wiley & Sons, Inc., New York, 1993.

[McC74] A. McConnell, *Polynomial subfields of $k(x)$*, J. reine agnew. Math. **266** (1974), 136–139.

[MS09] A. Medvedev and T. Scanlon, *Polynomial dynamics*, `arXiv:0901.2352`.

[Pak08] F. Pakovich, *On polynomials sharing preimages of compact sets, and related questions*, Geom. Funct. Anal. **18** (2008), 163–183.

[Sch82] A. Schinzel, *Selected Topics on Polynomials*, Ann Arbor, MI, 1982.

[Sch00] ———, *Polynomials with Special Regard to Reducibility*, Cambridge University Press, Cambridge, UK, 2000.

[Tor88] P. Tortrat, *Sur la composition des polynômes*, Colloq. Math. **55** (1988), 329–353.

[Tur95] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. (Ser. A) **58** (1995), 312–357.

[vzG91] J. von zur Gathen, *Functional decomposition of polynomials: the wild case*, J. Symbolic Comput. **10** (1991), 437–452.

[Zan93] U. Zannier, *Ritt's Second Theorem in arbitrary characteristic*, J. reine agnew. Math. **445** (1993), 175–203.