8-2011

Counting Reducible Composites of Polynomials

Jacob Andrew Ogle
jogle6@utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Jacob Andrew Ogle entitled "Counting Reducible Composites of Polynomials." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Shashikant B. Mulay, Major Professor

We have read this dissertation and recommend its acceptance:

David F. Anderson, Richard M. Bennett, Luis Finotti, Pavlos Tzermias

Accepted for the Council:

Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:

I am submitting herewith a dissertation written by Jacob Ogle entitled "Counting Reducible Composites of Polynomials". I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Shashikant Mulay
Major Professor

We have read this dissertation
and recommend its acceptance:

David Anderson

Richard Bennett

Luis Finotti

Pavlos Tzermias

Accepted for the Council:

Carolyn R. Hodges
Vice Provost and Dean of
the Graduate School

(Original signatures are on file with offical student records.)

Counting Reducible Composites of Polynomials

A Dissertation
Presented for the
Doctor of Philosophy
Degree
The University of Tennessee, Knoxville

Jacob A. Ogle
August 2011

Dedication

This work is dedicated to Cassandra, as am I.

Acknowledgments

My appreciation goes to all of my professors, in mathematics and other subjects, both as an undergraduate and a graduate student, who enjoyed knowledge and made it clear that they did so.

Even tiny bits of mathematics, no matter how distant from the subject matter of this immediate work, can influence the way I think about, organize, and understand mathematics. So I must thank every professor, colloquium-giver, or just conversation-sharer who has taught me even a small fact.

A particular round of thanks should go to Justin and Jared for many fun and significant (even when off-topic) mathematical conversations, and for just general encouragement when it was needed.

The majority of my thanks certainly goes to Dr. Mulay, who gave me an amazing amount of freedom to explore on my own, while (more importantly) always answering my questions with insightful motivation, examples, and more than one repetition of "take it one step at a time." Because of the first, I can proudly say that this work is truly *mine*; but without the second, it would not exist at all.

Abstract

This research answers some open questions about the number of reducible translates of a fixed nonconstant polynomial over a field. The natural hypothesis to consider is that the base field is algebraically closed in the function field. Since two possible choices for the base field arise, this naturally yields two different hypotheses. In this work, we explicitly relate the two hypotheses arising from this choice. Using the theory of derivations, and specifically an explicit construction of a derivation with a well-understood ring of constants, we can relate the ranks of the two relative-unit-groups involved, both of which are free Abelian groups under our hypothesis. These results allow us to give a more natural (though not stronger) bound on the number of reducible translates than the bound that was previously known. Also, we extend this count of reducible translates to a count of reducible composites and find that a similar bound will hold in this more general setting.

Contents

Chapter 1

Introduction

Just as natural numbers are central to Arithmetic, polynomials are central to Algebra. The analogy between these two is astonishingly wide and unfathomably deep. Progress in Arithmetic is essentially tied to our understanding of various factorization properties of integers. Likewise, deciphering the mysteries of polynomial factorization is key to Algebra. This holds even more emphatically in the theory of polynomial equations. Study of polynomial equations in two or more unknowns constitutes the mathematical discipline known as Algebraic Geometry. Since the solutions of multivariate polynomial equations can be viewed as curves, surfaces, solids, etc., this leads to a naturally interesting interplay between the algebra of polynomials and the geometry of the corresponding loci. For example, a (nonconstant) polynomial $f(x, y)$ is irreducible precisely when the corresponding algebraic curve $C : f(x, y) = 0$ shares only finitely many points with any algebraic curve $D : g(x, y) = 0$, where $g(x, y)$ has strictly smaller degree than the degree of $f(x, y)$.

For more detailed discussion, consider polynomials in unknowns $X_1, \ldots, X_n$ (where n is tacitly assumed to be at least 2) having coefficients in the field of complex numbers. Given linearly independent polynomials $f_1, \ldots, f_r$, we aim to understand the factorization of the set of linear combinations $c_1 f_1 + \cdots + c_r f_r$ (where the coefficients c_i are constants) in terms of some intrinsic properties of the collection $\{f_1, \ldots, f_r\}$. More generally (and also more ambitiously), we can consider the set of all linear combinations of a fixed family of power-products in $f_1, \ldots, f_r$, *e.g.*, $c_1 f_1^3 + c_2(f_1 \cdots f_r)$. To distinguish between these two considerations, the first type of set is referred to as the "linear system" while the more general one is referred to as the "algebraic system." For our purposes here, we shall be content dealing with the case $r = 2$ and mostly

focus on the linear systems.

Historically speaking, the first celebrated result was in the linear case and it was due to the Italian algebraic-geometer Eugenio Bertini (1846-1933). In 1882 Bertini proved that under two necessary hypotheses on $\{f_1, \ldots, f_r\}$, a linear combination $c_1 f_1 + \cdots + c_r f_r$ is irreducible for "almost all" choices of constants $c_1, \ldots, c_r$. The first hypothesis is that $f_1, \ldots, f_r$ do not have a common factor and the second hypothesis is that the system is not "composite with a pencil." To be composite with a pencil means there is an integer $d \geq 2$ and polynomials g, h such that each f_i is a homogeneous polynomial of degree d in g, h. Here is an explicit simple example: $d = 2$, $f_1 = g^2$ and $f_2 = -h^2$. Observe that,

$$c_1 f_1 + c_2 f_2 = c_1 g^2 - c_2 h^2 = (\sqrt{c_1} g + \sqrt{c_2} h)(\sqrt{c_1} g - \sqrt{c_2} h)$$

for any choice of complex numbers c_1, c_2. This theorem of Bertini has now become classical, and has been greatly generalized by the prominent algebraic-geometers Enriques, Castelnuovo, Matsusaka, Zariski, Grothendieck, and others. The theorem is of great importance in the sense that it is constantly used in (researching) algebraic geometry ever since it was brought to light. But the glaring limitation of the theorem is summed up in the phrase "almost all." In particular, the exact set of all r-tuples $(c_1, \ldots, c_r)$ for which $c_1 f_1 + \cdots + c_r f_r$ is reducible remains virtually unknown even today. A useful qualitative / quantitative description of the set of reducibility is clearly very desirable.

The investigations and results of this thesis deal with the initial case of this problem; namely the case where $r = 2$, $f_1 = f$, and $f_2 = 1$. The factorization of a linear combination $c_1 f + c_2$ is of interest only when $c_1 \neq 0$. Thus (after dividing out by c_1) it suffices to consider the system of all translates $f + c$. This system will be composite with a pencil whenever f is composite with a univariate polynomial, *i.e.,* there are polynomials $g(X_1, \ldots, X_n)$ and $\phi(t)$, the second having degree ≥ 2, such that $f = \phi(g)$. One way to avoid this is to assume at the outset that f is irreducible. Such an assumption is not more restrictive than noncomposite-ness since most translates of any noncomposite f are assured to be irreducible by the Bertini theorem and the family of all translates of any $f + c$ is the same as the family of all translates of f. For convenience define $redset(f)$ to be the set of constants c such that $f + c$ is reducible. The main result of our investigation provides a useful upper bound on the size of

$redset(f)$. This bound is expressed as the rank of the relative group of units of the affine coordinate ring of the hypersurface $H : f = 0$. Our result holds not just for complex numbers but for all fields k of characteristic 0 provided f remains irreducible over the algebraic closure of k. Moreover, we can prove a similar bound even in the case of algebraic systems; this extension is essentially technical in nature. Our main theorems are in direct response to some questions raised by Abhyankar, Heinzer and Sathaye in their landmark paper of 2000. At present we do not know how to handle fields of positive characteristic. We hope to tackle this topic in our future research on this subject.

Chapter 2

Previous Results

Here, we will give an overview of the relevant work done in [6]. The main definitions and results in this chapter are from that paper.

2.1 The Redset Theorem

Let k be a field and $1 < n \in \mathbb{N}$. Let $X_1, ..., X_n$ be indeterminate over k and take $R := k[X_1, \ldots, X_n]$. Fix f, an irreducible element of $R \setminus k$.

Definition 2.1. Define the *reducible set* of f to be

$$\text{redset}(f) := \{c \in k \mid f - c \text{ is reducible in } R\}.$$

By reducible, we mean that $f - c = gh$ for some $g, h \in R \setminus k$. As further notation, let $A := R/fR$ denote the affine coordinate ring of f. We view k as a subfield of A via the canonical map $\pi : R \to A$. Let L denote the quotient field of A (where here we are using the fact that f is irreducible in R.) We seek to relate properties of k, A, and L with the size of redset(f). One particular subset of redset(f) will be important later.

Definition 2.2. The *primary set* of f is

$$\text{primset}(f) := \{c \in k \mid f - c = ah^\mu \text{ with } a \in k,\ h \in R,\ 2 \leq \mu \in \mathbb{N}\}.$$

The first result given here will be a finiteness result for the redset. First, we remind the reader of a few basic facts. Recall that, by an affine domain over a field

k', we mean a domain containing k' which is finitely generated as a ring extension of k'.

Theorem 2.3 (Noether Normalization)**.** *Let A be an affine domain over a field k. Then there are elements $y_1, ..., y_d \in A$ such that the family of y_i, $1 \leq i \leq d$, are algebraically independent over k and A is integral over $k[y_1, ..., y_d]$.*

Proof. See [28, section V.4, Theorem 8] or [4, Lecture 5, Theorem 46]. □

Theorem 2.4 (Hilbert Basis Theorem)**.** *Every finite ring extension, A, of a Noetherian ring R is also Noetherian.*

Proof. See [11, VIII.4.9] □

Lemma 2.5. *Let V be the subset of $k(X_1, ..., X_n)$ consisting of g/h with $deg(g) \leq deg(h)$. Then V is a discrete valuation ring of $k(X_1, ..., X_n)$ over k.*

Proof. This is a well-known example of a DVR. See, for example, [29, VI.5, Corollary 2]. □

Lemma 2.6. *Let A be an integral extension of a ring B. Then $dim(A) = dim(B)$.*

Proof. See [4, Lecture 5, Theorem 45.3] or [14, Theorem 48]. □

Lemma 2.7. *Let R be a normal local domain with maximal ideal M and quotient field K. Let L be a finite algebraic extension of K, and let S be the integral closure of R in L. Then there are only finitely many maximal ideals Q of S such that $Q \cap R = M$.*

Proof. Let G be the group of field automorphisms of L over K. Since L is a finite algebraic extension, G is a finite group; say $G = \{\sigma_1, ..., \sigma_d\}$ and assume σ_1 is the identity map. Note that each σ_i, when restricted to S, is a (ring) automorphism of S. Let Q be some maximal ideal of S such that $Q \cap R = M$. It is easy to check that, for $1 \leq i \leq d$, we have $\sigma_i(Q)$ is also a maximal ideal of S such that $\sigma_i(Q) \cap R = M$. Let $Q_i := \sigma_i(Q)$ for $1 \leq i \leq d$. We will show that $\{Q_1, ..., Q_d\}$ is the set of all ideals which satisfy the property under consideration. If possible, let P be a maximal ideal of S such that $P \cap R = M$, and such that $P \notin \{Q_1, ..., Q_d\}$. Then P cannot be contained in any Q_i, and hence is not contained in $Q_1 \cup \cdots \cup Q_d$ by prime avoidance. Let $a \in P \setminus \cup_{i=1}^{d} Q_i$, and let $b = \prod_{i=1}^{d} \sigma_i(a)$. Note that $b \in K \cap S$, and $K \cap S = R$ because R is normal. If $b \in M$ then $b \in Q_1$ and, since Q_1 is prime, we have some

$1 \leq j \leq d$ such that $\sigma_j(a) \in Q_1$. But then $a \in \sigma_j^{-1}(Q_1) \subseteq \cup_{i=1}^{d} Q_i$, contradicting our choice of a. Thus, we have that $b \notin M$. Then b is a unit in R, hence a unit in S, and hence a is a unit in S. But a was contained in P, a maximal ideal of S. This is a contradiction, so no such P can exist. So the set of maximal ideals under consideration is exactly $\{Q_1, ..., Q_d\}$. □

Then we have the following significant technical lemma, which is the key to much of what follows. For a ring R, we denote by $U(R)$ the multiplicative group of units of R, and for a domain R, we will use $\mathrm{qf}(R)$ to denote the quotient field of R.

Lemma 2.8 (Lemma from section 4 of [6])**.** *Let A' be an affine domain over a field k' such that k' is algebraically closed in $L' := qf(A')$. Then, there exists a finite number of DVRs $V_1, V_2, ..., V_t$ of L'/k' such that*

(i) $A' \cap V_1 \cap V_2 \cap \cdots \cap V_t = k'$

(ii) *$U(A')/U(k')$ is a free Abelian group of rank at most $max(0, t-1)$.*

Proof. First, we will prove the existence of $V_1, V_2, ..., V_t$. Using the Noether Normalization Theorem (2.3), choose $Y_1, Y_2, ..., Y_m \in A'$ which are algebraically independent over k', and such that A' is integral over $\widehat{A} := k'[Y_1, ..., Y_m]$. If $m = 0$, then $A' = L'$ is algebraic over k'; in this case, since k' is assumed to be algebraically closed in L', we have $A' = k'$. Obviously, $t = 0$ in this case, and our assertion holds trivially. So from now on, assume $m \geq 1$.

Let $\widehat{L} = k'(Y_1, ..., Y_m)$. Define

$$\widehat{V} = \{g/h \in \widehat{L} \mid deg(g) \leq deg(h)\}.$$

$\widehat{V}$ is known to be a DVR of L'/k' by lemma 2.5; moreover, clearly $\widehat{A} \cap \widehat{V} = k'$. Let V' denote the integral closure of $\widehat{V}$ in L'.

We want to note that V' is a 1-dimensional, semilocal domain. The fact that V' is 1-dimensional follows directly from lemma 2.6. Next, we want to see that V' must be Noetherian. Note that $\widehat{V}$ is Noetherian as a DVR. It suffices to show that V' is a finitely-generated ring extension of $\widehat{V}$. Since A' is a finite ring extension of k', it follows that L' is a finite extension of $\widehat{L}$. Since L' is also algebraic over $\widehat{L}$, we can pick a finite $\widehat{L}$-vector space basis, $\{a_1, ..., a_m\}$, for L'. Now given any set of elements

$b_1, ..., b_l \in V' \subseteq L'$, if $l > m$, we would have some nontrivial relation

$$c_1 b_1 + \cdots + c_l b_l = 0$$

with $c_i \in \widehat{L}$ for $1 \leq i \leq l$, not all $c_i = 0$. Since $\widehat{L}$ is the quotient field of $\widehat{V}$, we can multiply by a common denominator to assume that each $c_i \in \widehat{V}$. Let v be that valuation associated with $\widehat{V}$ as a valuation domain. Considering the values $\{v(c_i) \mid c_i \neq 0\}$, we can see that each has nonnegative value, and (reordering if necessary) we can assume $v(c_1) \leq v(c_i)$ for $2 \leq i \leq l$. Then notice that, for $2 \leq i \leq l$, the element c_i/c_1 has positive v-value, and hence is in $\widehat{V}$. So we have the relation

$$b_1 + \frac{c_2}{c_1} b_2 + \cdots + \frac{c_l}{c_1} b_l = 0.$$

This implies that $b_1 \in \widehat{V}[b_2, b_3, ..., b_l]$. Thus, considering V' as a module over $\widehat{V}$, we see that it can take at most m elements of V' to generate V' over $\widehat{V}$. Specifically, V' must be a finite ring extension of $\widehat{V}$. Hence, V' is Noetherian by the Hilbert Basis Theorem. To see that V' is quasilocal, note that any maximal ideal M in V' would have the property that $M \cap \widehat{V}$ would be maximal in $\widehat{V}$. Combining this with the fact that $\widehat{V}$ is normal and local as a DVR, the fact that V' is semilocal follows from Lemma 2.7.

Now let $V_1, V_2, ..., V_t$ be the localizations of V' at its maximal ideals. Now V_i are DVRs of L'/k'. (They are 1-dimensional Noetherian as localizations of V' and local since they are each a localization of V' at a maximal ideal.) Also, $V' = V_1 \cap \cdots \cap V_t$. Now $A' \cap V_1 \cap \cdots \cap V_t = A' \cap V'$. Considering $\alpha \in A' \cap V'$, we see that α is integral over both $\widehat{A}$ and $\widehat{V}$. Let $T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$ be the minimal polynomial for α over $\widehat{A}$, and let $T^n + b_{n-1}T^{n-1} + \cdots + b_1 T + b_0$ be the minimal polynomial for α over $\widehat{L}$. (We can assume that the two polynomials have the same degree since $\mathrm{qf}(\widehat{A}) = \widehat{L}$.) Note that, then, α satisfies the polynomial

$$(a_{n-1} - b_{n-1})T^{n-1} + \cdots + (a_1 - b_1)T + (a_0 - b_0)$$

with coefficients in $\widehat{L}$. By minimality, then, we must have $a_i = b_i$ for each $1 \leq i \leq n-1$. So the minimal polynomial for α over $\widehat{L}$ actually has coefficients in $\widehat{A}$. Similarly, the minimal polynomial must have coefficients in $\widehat{V}$. Thus, α is integral over $\widehat{A} \cap \widehat{V} = k'$, and by the hypothesis that k' is algebraically closed in A', we see

that $\alpha \in k'$. Thus,

$$A' \cap V_1 \cap V_2 \cap \cdots \cap V_t = k'.$$

Next we show that $U(A')/U(k')$ is a free Abelian group of finite rank. Let W_i be the valuation associated with V_i (*i.e.*, W_i maps V_i onto $\mathbb{Z} \cup \{\infty\}$) for $i = 1, ..., t$. Define the map

$$W : U(L') \to \mathbb{Z}^t$$

by

$$W(z) = (W_1(z), ..., W_t(z)) \text{ for all } z \in U(L').$$

Since $ker(W) = U(V_1) \cap \cdots \cap U(V_t)$, we see $U(A') \cap ker(W) = U(k')$. Thus, we get the induced group monomorphism $W : U(A')/U(k') \to \mathbb{Z}^t$. Since subgroups of $\mathbb{Z}^t$ are free Abelian groups of rank at most t, the group $U(A')/U(k')$ is free Abelian, and the rank is at most t.

Finally, we show that the rank of $U(A')/U(k')$ is actually bounded by $t - 1$. Suppose the rank is t; then there exists $z_1, ..., z_t \in U(A')$ such that the matrix $[W_i(z_j)]$ has nonzero determinant. Hence, the columns of this matrix span the $\mathbb{Q}$-vector space $\mathbb{Q}^t$. Let $a_1, ..., a_t \in \mathbb{Q}$ be such that

$$\sum_j a_j W_i(z_j) = 1 \text{ when } i = 1$$

$$\sum_j a_j W_i(z_j) = 0 \text{ when } i \neq 1.$$

Let $a, b_j \in \mathbb{Z}$ be such that $a > 0$ and $aa_j = b_j$ for $j = 1, ..., t$. Define $z = z_1^{b_1} z_2^{b_2} \cdots z_t^{b_t} \in U(A')$ and note

$$W_1(z) = \sum_{j=1}^{t} b_j W_1(z_j) = a \sum_{j=1}^{t} a_j W_1(z_j) = a > 0$$

and, similarly, $W_j(z) = 0$ for $j = 2, 3, ..., t$. So we have $z \in A' \cap V_1 \cap \cdots \cap V_t = k'$. But this contradicts the assumption that the set $W(z_1), ..., W(z_t)$ was linearly independent. Thus the rank must be $\leq t - 1$. □

This allows us to move on to the Redset Theorem:

Theorem 2.9 (Redset Theorem)**.** *If k is algebraically closed in L, then* redset(f) *is finite.*

Proof. By the previous theorem, we know there are finitely many DVRs, $V_1, ..., V_t$ of L/k such that $A \cap V_1 \cap V_2 \cap \cdots \cap V_t = k$. Let $W(z) = (W_1(z), ..., W_t(z))$ for all $z \in U(L)$, as in Lemma 2.8. For $c \in \text{redset}(f)$, let

$$G(c) := \{g \in R \mid 1 \leq deg(g) < deg(f) \text{ and } g \text{ divides } f - c\}$$

and let $G := \cup G(c)$ where the union is taken over $c \in \text{redset}(f)$. G is contained in a finite-dimensional k-vector subspace, M, of $R = k[X_1, ..., X_n]$ because it is spanned by all monomials of degree at most $deg(f)$. Let $\{\beta_1, ..., \beta_d\}$ be an ordered k-basis of M, and let

$$\nu_i := \min\{W_i(\pi(\beta_1)), ..., W_i(\pi(\beta_d))\}$$

for $1 \leq i \leq t$. Observe that, for $g \in G$, $W_i(\pi(g)) \geq \nu_i$. Given $g \in G$, let $h \in G$, $c \in \text{redset}(f)$ be such that $gh = f - c$. Then $\pi(g)\pi(h) \in k$. Hence,

$$W_i(\pi(g)) = -W_i(\pi(h)) \leq -\nu_i.$$

Thus, the set of integers $\{W_i(\pi(g))\}$ is bounded below by ν_i and above by $-\nu_i$. It follows that $W_i(\pi(G))$, and hence $W(\pi(G))$, is a finite set. It suffices to show that each member of $W(\pi(G))$ corresponds to *at most one* element of redset(f).

Suppose that $g_1h_1 = f - c_1$, $g_2h_2 = f - c_2$, and

$$W(\pi(g_1)) = (W_1(\pi(g_1)), ..., W_t(\pi(g_1))) = (W_1(\pi(g_2)), ..., W_t(\pi(g_2))) = W(\pi(g_2)).$$

Since $W_i(\pi(g_1)) = W_i(\pi(g_2))$, we have that $\pi(g_1)/\pi(g_2) \in V_i$ for each $1 \leq i \leq t$. Since this holds for all V_i,

$$\frac{\pi(g_1)}{\pi(g_2)} \in V_1 \cap V_2 \cap \cdots \cap V_t.$$

Now we have that $g_2h_2 = f - c_2$, so $\pi(g_2)\pi(h_2) = -c_2$. Thus, $\pi(g_2)^{-1} = -c_2^{-1}\pi(h_2) \in A$, and we have

$$c := \frac{\pi(g_1)}{\pi(g_2)} \in A \cap V_1 \cap \cdots \cap V_t = k.$$

So $\pi(g_1) = c\pi(g_2)$ and consequently f divides $g_1 - cg_2$. But $\deg(g_1 - cg_2) < \deg(f)$, hence $g_1 = cg_2$. Note that $\deg(g_1) \geq 1$, and g_1 divides $\gcd(f - c_1, f - c_2)$. This is

possible only if $c_1 = c_2$, because otherwise $\gcd(f - c_1, f - c_2) = 1$. This proves the asserted finiteness. □

2.2 The Mixed Redset Theorem

Having said that redset(f) is finite, we can improve our understanding by getting a bound on redset(f) if we think about the problem more generally. Let Z be an indeterminate over $k(X_1, ..., X_n)$. By the *generic member* of the family $(f - c)_{c \in k}$ we mean the polynomial $f - Z \in R(Z)$. For notation, let

$$\begin{aligned} f^\sharp &:= f - Z \\ k^\sharp &:= k(Z) \\ R^\sharp &:= k(Z)[X_1, \ldots, X_n] \\ A^\sharp &:= R^\sharp / f^\sharp R^\sharp \\ L^\sharp &:= \mathrm{qf}(A^\sharp). \end{aligned}$$

Here we are thinking of $k^\sharp$ as the base field, $A^\sharp$ as the affine coordinate ring, and $L^\sharp$ as the function field, of $f^\sharp$. In this setting, we generalize the definition of the reducible set to:

$$\mathrm{redset}(f^\sharp) = \{c \in k(Z) \mid f^\sharp - c \text{ is reducible}\}.$$

Under the canonical epimorphism $\pi^\sharp : R^\sharp \to R^\sharp / f^\sharp R^\sharp$, we can make the following identifications, which will allow us to avoid the use of the extra variable Z, and simplify some work. Identify

$$\begin{aligned} k^\sharp &= k(f) \\ A^\sharp &= k(f)[X_1, \ldots, X_n] = k^\sharp[X_1, \ldots, X_n] \\ L^\sharp &= k(X_1, ..., X_n). \end{aligned}$$

Then, applying the Redset Theorem (2.9) in this setting, we get:

Theorem 2.10. *If $k^\sharp$ is algebraically closed in $L^\sharp$, then* redset$(f^\sharp)$ *is finite.*

We also have an obvious injection

$$\mathrm{redset}(f) \longrightarrow \mathrm{redset}(f^\sharp)$$

mapping

$$c \mapsto c - Z.$$

Hence, $|\text{redset}(f)| \leq |\text{redset}(f^\sharp)|$.

Under this new setup, we can do better than just saying the redset is finite and get an actual bound on its size. In particular, we have:

Theorem 2.11 (Mixed Redset Theorem)**.** *If $k^\sharp$ is algebraically closed in $L^\sharp$, then $U(A^\sharp)/U(k^\sharp)$ is a free Abelian group of finite rank r and $|\text{redset}(f)| \leq r$.*

Before the proof of this theorem, we will need the following lemma, which controls an interesting subset of redset(f).

Theorem 2.12 (Mixed Primset Theorem)**.** *If $k^\sharp$ is relatively algebraically closed in $L^\sharp$, then* primset$(f) = \varnothing$.

Proof. Recall the $c \in \text{primset}(f)$ means $f - c = ah^\mu$ with $a \in k$, $h \in R$, $2 \leq \mu \in \mathbb{N}$. In particular, notice that h is algebraic over $k^\sharp = k(f)$, hence $h \in k(f)$ by assumption. Then $h \in k(f) \cap R = k[f]$. But $k[f]$ is k-isomorphic to $k[T]$, where T is an indeterminate over k. Thus, $f - c$ is irreducible in $k[f]$ and, specifically, cannot be factored as ah^μ. □

We will see later that this proof actually yields a much stronger result (see Theorem 3.5 below). Also, note that our later Polyredset Theorem (3.6) will have the Mixed Redset Theorem as a corollary. But for now we can prove the Mixed Redset Theorem, as in [6].

Proof. (of the Mixed Redset Theorem.) By Lemma 2.8, $U(A^\sharp)/U(k^\sharp)$ is a free Abelian group of finite rank $r < \infty$. Assume $|\text{redset}(f)| = s > r$ and choose $c_1, ..., c_s \in \text{redset}(f)$. By the Mixed Primset Theorem, each $f - c_i$ can be written as a product $g_i h_i$ with $g_i, h_i \in R \backslash k$ and $\gcd(g_i, h_i) = 1$. Since $s > r$, there exist integers $a_1, ..., a_s$, not all zero, such that $g_1^{a_1} g_2^{a_2} \cdots g_s^{a_s} \in U(k^\sharp)$. Since $g_i h_i \in k^\sharp$ for $1 \leq i \leq s$, replacing g_i by the corresponding h_i, if needed, we may assume that $a_i \geq 0$ for $1 \leq i \leq s$. Now it follows that $g_1^{a_1} g_2^{a_2} \cdots g_s^{a_s} \in R \cap k(f) = k[f]$. For the same reason, $h_1^{a_1} h_2^{a_2} \cdots h_s^{a_s} \in k[f]$. Now, letting T be an indeterminate over L, there exists $g, h \in k[T]$ such that $g(f) = g_1^{a_1} g_2^{a_2} \cdots g_s^{a_s}$ and $h(f) = h_1^{a_1} h_2^{a_2} \cdots h_s^{a_s}$. Observe that

$$g(f)h(f) = \prod_{i=1}^{s} g_i^{a_i} \prod_{i=1}^{s} h_i^{a_i} = \prod_{i=1}^{s} (f - c_i)^{a_i}.$$

Again, $k[f]$ is k-isomorphic to $k[T]$, so by the unique factorization property,

$$g(f) = u\prod_{i=1}^{s}(f - c_i)^{b_i}$$

where $0 \leq b_i \leq a_i$ for $1 \leq i \leq s$, and $u \in U(k)$. If, for some i, $b_i \neq 0$, then for that i, h_i divides $g(f)$. Since $gcd(g_i, h_i) = 1$, h_i divides $g(f)$ if and only if h_i divides $\prod_{j\neq i}(f - c_j)^{b_j}$. On the other hand, $\gcd(f - c_i, f - c_j) = 1$ if $i \neq j$. Hence, we must have $b_i = 0$ for $1 \leq i \leq s$. Consequently, $g(f) \in U(k)$. But then $g_i \in U(k)$ for $1 \leq i \leq s$, contradicting our choice of g_i. Thus, $|\operatorname{redset}(f)| \leq r$. □

Example 2.13. In [6], they present examples to show that the Mixed Redset Theorem is best possible. That is, they provide examples of polynomials in $R = k[X, Y]$ such that $\operatorname{rank}(U(A^\sharp)/U(k^\sharp))$ has any arbitrary value, and for which $\operatorname{redset}(f)$ can have any value between 0 and $\operatorname{rank}(U(A^\sharp)/U(k^\sharp))$. See [6], examples 1-5, pages 59-67. Letting k^* be the algebraic closure of k and $R^* = k^*[X_1, ..., X_n]$. Then in each of these examples, $\operatorname{redset}(f) = \operatorname{redset}(f)^*$ where

$$\operatorname{redset}(f)^* := \{c \in k^* \mid f - c \text{ is reducible in } R^*\}.$$

The fact that $\operatorname{redset}(f) = \operatorname{redset}(f)^*$ in these examples will be significant later (see Remark 3.7.)

Having an understanding of the work on this topic that was done in [6], we can now present explicitly the questions to be answered in this paper.

Questions.

1. *A natural generalization of* $\operatorname{redset}(f)$ *would be the set of monic irreducible polynomials* $\Gamma \in k[T]$ *such that* $\Gamma(f)$ *is reducible in* $k[X_1, ..., X_n]$. *What can be said about the size of this set?*

2. *What is the exact relationship between the hypothesis of the Redset Theorem and that of the Mixed Redset Theorem? That is, is there a relationship between* k *being algebraically closed in* L *and* $k(f)$ *being algebraically closed in* $k(X_1, ..., X_n)$*?*

3. *Is the analog of the Mixed Redset Theorem true in the original case, i.e. without passing to the generic member and introducting $k^\sharp$, etc. Specifically, assuming k to be algebraically closed in L, is it true that* $|\mathrm{redset}(f)| \leq \mathrm{rank}(U(A)/U(k))$*?*

The rest of this paper will attempt to answer these three questions. Chapter 3 will be devoted to generalizing the definition of $\mathrm{redset}(f)$ to what we will call $\mathrm{polyredset}(f)$. Chapter 4 will answer Question 2. Finally, Chapter 5 will answer Question 3 for fields of characteristic 0.

Chapter 3

Polyredset

3.1 The Polyredset Theorem

Having gotten a bound on redset(f) via the Mixed Redset Theorem, a natural question would be Question 1, above. Explicitly, after noticing that $f - c$ corresponds to the composition of $T - c$ with f, and that the family $\{T - c \mid c \in k\}$ are the degree 1 irreducible monic polynomials, we wonder what happens if we consider composites with f of irreducible monic polynomials of degree larger than 1. So in this section we will generalize the definitions of redset and primset to polynomials of larger degree. We will see ultimately that we get the same result as given by the Redset Theorem, even in this more general case (see Theorem 3.6 below.)

Definition 3.1. As a generalization of redset(f), we define the *polynomial reducible set* of f, polyredset(f), to be the set

$$\{\Gamma \in k[T] \text{ monic irreducible} \mid \Gamma(f) \text{ is reducible in } k[X_1, \ldots, X_n] \}.$$

Further, we will write, for each $\Gamma_i \in$ polyredset(f),

$$\Gamma_i(f) = u_i g_{i1}^{e_{i1}} g_{i2}^{e_{i2}} \cdots g_{iN_i}^{e_{iN_i}}$$

for some nonzero $u_i \in k$, $g_{i1}, g_{i2}, \ldots, g_{iN_i}$ pairwise nonassociate irreducible elements of R, $e_{ij} \in \mathbb{N}$, and $N_i \in \mathbb{N}$.

Here, we are implicitly assuming the set polyredset(f) is countable to simplify the notation. There is no canonical choice of such g_{ij}, but by the unique factorization

property, such a factorization is unique up to multiplication by an element of k. So we are letting a choice of g_{ij} be fixed. Clearly, redset$(f) \subseteq$ polyredset(f) after we identify $c \in$ redset(f) with $T - c \in$ polyredset(f). Also, when k is an algebraically closed field, the two sets coincide. Note that each g_{ij} cannot be a factor of both $\Gamma_i(f)$ and $\Gamma_{i'}(f)$ for $i \neq i'$.

Two subsets of polyredset(f) will be of particular interest.

Definition 3.2. Let the *polynomial primary set* of f, polyprimset(f), be the set

$$\{\Gamma \in \text{polyredset}(f) \mid \Gamma(f) = gh^{\mu} \text{ for some } g \in k,\ h \in R,\ 1 < \mu \in \mathbb{N}\}.$$

This will be the exact analog of primset(f). Also, let the *polynomial unique component set* of f, polyuniset(f), be defined as

$$\{\Gamma_i \in \text{polyredset}(f) \mid\ N_i = 1\}.$$

That is, $\Gamma \in$ polyuniset(f) if $\Gamma(f)$ is, up to a unit in k, some power of an irreducible polynomial of R. Clearly, polyuniset$(f) \subseteq$ polyprimset(f).

We did not define uniset(f) because there was no particular need to do so, but it could be defined in the way one would imagine. In [6], uniset is defined for more general families of the form $f - cw$ for fixed $f, w \in R$. (See Question 4 in that paper.) So this notation is chosen to match.

We want to compare |polyredset(f)| with the rank of $U(A^{\sharp})/U(k^{\sharp})$, which is a finitely-generated free Abelian group when $k^{\sharp}$ is algebraically closed in $L^{\sharp}$. Without any such assumption of algebraic closure, define the following free Abelian groups:

$$G := \sum_{\substack{\Gamma_i \in \text{polyredset}(f) \\ 1 \leq j \leq N_i}} \mathbb{Z}$$

$$G' := \sum_{\substack{\Gamma_i \in \text{polyredset}(f) \\ 1 \leq j \leq N_i - 1}} \mathbb{Z}.$$

Then we have the following lemma relating these groups to $U(A^{\sharp})/U(k^{\sharp})$.

Lemma 3.3. *There is a group epimorphism*

$$G \xrightarrow{\Psi} U(A^{\sharp})/U(k^{\sharp})$$

and a group monomorphism

$$G' \xrightarrow{\Psi'} U(A^\sharp)/U(k^\sharp).$$

Proof. Let S denote the set of all g_{ij}, where g_{ij} is a divisor of some $\Gamma_i(f)$ for $\Gamma_i \in$ polyredset(f), as chosen above. Similarly, let S' denote the set of all g_{ij} where $j \neq N_i$. Note that G is indexed by S and G' by S'. In either group, we will let e_{ij} be the element which is 0 in every slot except for the slot corresponding to g_{ij}, where it is 1. It is clear that the family $\{e_{ij} \mid i, j \text{ are such that } g_{ij} \in S\}$ forms a basis for G, and that $\{e_{ij} \mid i, j \text{ are such that } g_{ij} \in S'\}$ similarly forms a basis for G'.

Notice that, since g_{ij} divides $\Gamma_i(f)$ in R, g_{ij} is in $U(A^\sharp)$. Define Ψ by mapping e_{ij} to $g_{ij}U(k^\sharp)$ in $U(A^\sharp)/U(k^\sharp)$. By the universal mapping property of sums, this defines a group homomorphism. We need only to show the map is an epimorphism. Note that any element of $A^\sharp$ can be written as $h/\alpha(f)$ for some $h \in R$, $\alpha \in k[T]$. This is a unit in $A^\sharp$ if and only if there is some $h'/\alpha'(f)$ with $h' \in R$, $\alpha' \in k[T]$ such that $hh' = \alpha(f)\alpha'(f)$, *i.e.*, h divides (in R) some element of $k[f]$. But since R is a UFD, this implies that h is, up to a unit, a product of elements of $k[f]$ and polynomials g_{ij} in S. Since elements of $k[f]$ are in $U(k^\sharp)$, they are trivial elements of the group $U(A^\sharp)/U(k^\sharp)$. So it suffices to show that each g_{ij} is in the image of Ψ. But this is clear from the definition of Ψ. So Ψ maps onto the group $U(A^\sharp)/U(k^\sharp)$.

Now we turn our attention to Ψ'. We define the map similarly, by $e_{ij} \mapsto g_{ij}U(k^\sharp)$, and get a homomorphism as above. In this case, we want to show that this map is a monomorphism. So let $a_{ij} \in \mathbb{Z}$ be such that $(a_{ij}) \in G'$ satisfies $\Psi'((a_{ij})) \in U(k^\sharp)$. We will show that each $a_{ij} = 0$. We have

$$\Psi'((a_{ij})) = \Pi\ g_{ij}^{a_{ij}} = \frac{\gamma(f)}{\gamma'(f)}$$

for some $\gamma, \gamma' \in k[T]$, with $\gcd(\gamma, \gamma') = 1$. Remembering that the family $\{g_{ij}\}$ are pairwise coprime, we can focus on the g_{ij} having positive exponent a_{ij} and see that the product of these is equal to the numerator on the right. That is, letting $b_{ij} = a_{ij}$ when $a_{ij} > 0$ and $b_{ij} = 0$ when $a_{ij} \leq 0$, we have the product $\Pi\ g_{ij}^{b_{ij}} = \gamma(f)$ in R. Assuming that $\gamma(f) \notin k$, let P be any monic irreducible factor of γ in $k[T]$. We see then that $P(f)$ divides $\Pi\ g_{ij}^{b_{ij}}$, and hence $P \in$ polyredset(f). Say $P = \Gamma_I$. Then g_{IN_I} divides $P(f)$, which divides $\Pi\ g_{ij}^{b_{ij}}$ in R, but by the construction of G', this cannot

be. So γ must be in k. Thus, each $b_{ij} = 0$. Similarly, $\gamma' \in k$, and we can see that each $a_{ij} = 0$. So the original product $\Psi'((a_{ij})) = \Pi\ g_{ij}^{a_{ij}} \in k$, and since the g_{ij} are pairwise coprime, we must have each $a_{ij} = 0$. So the map is a monomorphism. □

This leads us to consider the relationship between the rank of $U(A^\sharp)/U(k^\sharp)$ (when this is a finitely-generated free Abelian group) and the various N_i. This motivates the study of polyuniset(f), and we find the following theorem:

Theorem 3.4 (Polyprimset Theorem)**.** *Assume that $k^\sharp$ is algebraically closed in $L^\sharp$. Then* polyprimset$(f) = \varnothing$.

Proof. The proof is identical with that of the Mixed Primset Theorem (see Theorem 2.12 above.) If polyprimset$(f) \neq \varnothing$, then there is some irreducible monic $\Gamma \in k[T]$ such that $\Gamma(f) = gh^\mu$ with $g \in k$, $h \in R$, and $\mu > 1$. But then h is algebraic over $k(f)$, hence is in $k(f)$, implying that $\Gamma(f)$ factors in $k[f]$. This contradicts the irreducibility of Γ. □

As a corollary, we have:

Corollary 3.5 (Polyuniset Theorem)**.** *Assume that $k^\sharp$ is algebraically closed in $L^\sharp$. Then* polyuniset$(f) = \varnothing$.

Thus, when $k^\sharp$ is algebraically closed in $L^\sharp$, we have that each $N_i > 1$, and that $U(A^\sharp)/U(k^\sharp)$ is a finitely-generated free Abelian group. Combining this with the homomorphisms from Lemma 3.3, we have the following:

$$\begin{aligned}\sum_{\Gamma_i \in \text{polyredset}(f)} N_i &\geq \text{rank}(U(A^\sharp)/U(k^\sharp)) \\ &\geq \sum_{\Gamma_i \in \text{polyredset}(f)} (N_i - 1) \\ &\geq |\,\text{polyredset}(f)|.\end{aligned}$$

This gives us the following theorem:

Theorem 3.6 (Polyredset Theorem)**.** *When $k^\sharp$ is algebraically closed in $L^\sharp$,*

$$|\text{polyredset}(f)| \leq \text{rank}(U(A^\sharp)/U(k^\sharp)).$$

Remark 3.7. Compare this to The Mixed Redset Theorem (2.11) to see the improvement. (Under the same assumptions, we get a much stronger result.) Also note that the Mixed Redset Theorem follows as a corollary of this theorem. It was mentioned at the end of Chapter 2 that there are examples showing that the Mixed Redset Theorem is best possible, and that in the examples given, $\text{redset}(f) = \text{redset}(f)^*$. Note that, over k^*, the algebraic closure of k, all irreducible polynomials in one variable must have degree 1, so $\text{polyredset}(f) = \text{redset}(f)^*$ in this case. So we have that the Polyredset Theorem is best possible in the sense that there are examples where $\text{polyredset}(f) = \text{redset}(f)^*$ and $|\text{polyredset}(f)| = \text{rank}(U(A^\sharp)/U(k^\sharp))$. Also, in these examples where $\text{redset}(f) = \text{rank}(U(A^\sharp)/U(k^\sharp))$, we can conclude that there are no polynomials in $\text{polyredset}(f) \setminus \text{redset}(f)$.

Remark 3.8. Without assuming any condition of algebraic closure, we have

$$\sum_{\Gamma_i \in \text{polyredset}(f)} (N_i - 1) \geq |\,\text{polyredset}(f)| - |\,\text{polyuniset}(f)|$$

because, when $\Gamma_i \in \text{polyredset}(f) \setminus \text{polyuniset}(f)$, we have $N_i > 1$. Thus, comparing this to Theorem 3.6, we see that the assumption that $k^\sharp$ is algebraically closed in $L^\sharp$ is essentially ensuring two things: the finiteness of $\text{rank}(U(A^\sharp)/U(k^\sharp))$, by Lemma 2.8, and the finiteness (emptiness) of $\text{polyuniset}(f)$ by Corollary 3.5.

Finally, we have an equivalence.

Corollary 3.9. $|\,\text{polyredset}(f)| < \infty$ *if and only if both* $U(A^\sharp)/U(k^\sharp)$ *is finitely-generated and* $|\,\text{polyuniset}(f)| < \infty$.

Proof. By Lemma 3.3, $(U(A^\sharp)/U(k^\sharp))$ has a subgroup which is free of rank $\sum(N_i - 1)$. So if $U(A^\sharp)/U(k^\sharp)$ is finitely-generated, that sum is finite. Thus, if $\text{polyuniset}(f)$ is also finite, $\text{polyredset}(f)$ is finite by the previous remark. Conversely, if $\text{polyredset}(f)$ is finite, then $\text{polyuniset}(f)$ is finite as a subset, and $U(A^\sharp)/U(k^\sharp)$ is finitely-generated since it can be viewed as a subgroup of G by Lemma 3.3, which is finitely-generated. □

3.2 Other Results Concerning Polyredset(f)

In this section, we seek to deepen our understanding of polyredset(f). Recall that:

$$\text{polyredset}(f) = \{\Gamma \in k[T] \text{ monic irreducible} \mid \Gamma(f) \text{ is reducible in } k[X_1, \ldots, X_n]\ \}$$

and, where k^* is the algebraic closure of k,

$$\text{redset}(f)^* = \{c \in k^* \mid f - c \text{ is reducible in } R^*\}.$$

There is a natural relationship between monic irreducible polynomials in $k[T]$ and elements of k^*, because each element of k^* has a minimal polynomial which is monic and irreducible. We wish to see how this relates to reducible sets. We can relate polyredset(f) and redset$(f)^*$ by the following theorem.

Theorem 3.10. *For k a perfect field,*

$$\{c \in k^* \mid c \textit{ is a root of some } \Gamma \in \text{polyredset}(f)\} \subseteq \text{redset}(f)^*.$$

Proof. Let $\Gamma \in k[T]$ be monic and irreducible. If $deg(\Gamma) = 1$, then Γ has the form $T - c$, and saying $\Gamma \in$ polyredset(f) implies that $c \in$ redset(f) $\subseteq$ redset$(f)^*$. So we focus of the case where Γ has degree at least 2. Over k^*, we can factor $\Gamma = \Pi_{i=1}^{m}(T - c_i)$ for some $c_1, c_2, ..., c_m \in k^*$. If $\Gamma \in$ polyredset(f), we have that $\Gamma(f) = gh$ for some $g, h \in R \setminus k$. Let $\overline{k}$ be the splitting field of Γ over k. We denote by $Aut(\overline{k}/k)$ the set of field automorphisms of $\overline{k}$ fixing k. We have that $Aut(\overline{k}/k)$ acts transitively on the roots of Γ, so let $\sigma_i \in Aut(\overline{k}/k)$ be such that $\sigma_i(c_1) = c_i$. Extend each σ_i to a ring automorphism of $\overline{k}[X_1, ..., X_n]$ by $\sigma(X_i) = X_i$. Then clearly,

$$k[X_1, ..., X_n] = \{p \in \overline{k}[X_1, ..., X_n] \mid \sigma_i(p) = p \text{ for } 1 \leq i \leq m\}.$$

To show that each $c_i \in$ redset$(f)^*$, we assume not—that $f - c_i$ is absolutely irreducible for some $1 \leq i \leq m$. Then, because we have $gh = \Gamma(f) = \Pi_{j=1}^{m}(f - c_j)$, we can assume without loss of generality that $f - c_i$ divides g in $\overline{k}[X_1, ..., X_n]$. But, since $g \in R$, $\sigma_j(g) = g$ for each $1 \leq j \leq m$. So we have, for $1 \leq j \leq m$,

$$f - c_j = \sigma_j\sigma_i^{-1}(f - c_i) \Big| \sigma_j\sigma_i^{-1}(g) = g.$$

Now if each $f - c_j$ divides g, since the various $f - c_j$ are pairwise coprime, we must have $\Gamma(f)|g$. But this implies $h \in k^*$, contradicting our assumption that $deg(h) > 0$. So we must have that $f - c_i$ is reducible over k^* for each $1 \leq i \leq m$. The result follows. □

Specifically, we have:

Corollary 3.11. *When k is a perfect field, if* redset$(f)^*$ *is finite, then* polyredset(f) *is finite.*

Remark 3.12. Note that the converse is generally not true–if f is irreducible but not absolutely irreducible, then $0 \in$ redset$(f)^*$ but clearly this corresponds to no element in polyredset(f). See further questions in Chapter 6.

To get some further understanding, we study the property of $k(f)$ being algebraically closed in $k(X_1, ..., X_n)$.

Lemma 3.13. *Given $f \in K[X_1, ..., X_n]$, $K(f) \cap K[X_1, ..., X_n] = K[f]$.*

Proof. It is clear that $K[f] \subseteq K(f) \cap K[X_1, ..., X_n]$. Conversely, let $g \in R$ and $\alpha(f), \beta(f) \in k[f]$ be such that

$$\frac{\alpha(f)}{\beta(f)} = g \neq 0,$$

where we can obviously assume that α and β have no common divisors in $k[T]$. Since $k[f]$ is k-isomorphic to $k[T]$, it is a PID. So, if we assume that $gcd(\alpha, \beta) = 1$, we would have $\alpha', \beta' \in k[T]$ such that $\alpha\alpha' + \beta\beta' = 1$. Then certainly $\alpha(f)\alpha'(f) + \beta(f)\beta'(f) = 1$, and hence $gcd(\alpha(f), \beta(f)) = 1$. Thus, we would conclude from $\alpha(f) = g\beta(f)$ that $\beta(f) \in k$. So $K(f) \cap K[X_1, ..., X_n] \subseteq K[f]$, and the equality has been proven. □

Lemma 3.14. *Let K be a field, and $K[X_1, ..., X_n]$ be a polynomial ring. Let $f \in K[X_1, ..., X_n]$. Then the ring $K[f]$ is integrally closed in $K[X_1, ..., X_n]$ if and only if $K(f)$ is algebraically closed in $K(X_1, ..., X_n)$.*

Proof. For the "if" part, assume $K(f)$ is algebraically closed in $K(X_1, ..., X_n)$ and let $g \in R = K[X_1, ..., X_n]$ be integral over $K[f]$. Then it is also algebraic over $K(f)$. Since $K(f)$ is algebraically closed in $K(X_1, ..., X_n)$, we would have that $g \in R \cap K(f) = K[f]$ by Lemma 3.13.

Conversely, say $a, b \in R$ are such that a/b is algebraic over $K(f)$. By the standard technique of clearing denominators, we can take a/b to be algebraic over $K[f]$. So we have an equation of the form

$$\alpha_n \left(\frac{a}{b}\right)^n + \alpha_{n-1} \left(\frac{a}{b}\right)^{n-1} + \cdots + \alpha_1 \left(\frac{a}{b}\right) + \alpha_0 = 0$$

with $\alpha_i \in K[f]$ for $1 \leq i \leq n$. Then we multiply this equation by α_n^{n-1} to get

$$\alpha_n^n \left(\frac{a}{b}\right)^n + \alpha_n^{n-1}\alpha_{n-1} \left(\frac{a}{b}\right)^{n-1} + \alpha_n^{n-1}\alpha_{n-2} \left(\frac{a}{b}\right)^{n-2} + \cdots + \alpha_n^{n-1}\alpha_1 \left(\frac{a}{b}\right) + \alpha_n^{n-1}\alpha_0 = 0$$
$$\left(\frac{\alpha_n a}{b}\right)^n + \alpha_{n-1} \left(\frac{\alpha_n a}{b}\right)^{n-1} + \alpha_n\alpha_{n-2} \left(\frac{\alpha_n a}{b}\right)^{n-2} + \cdots + \alpha_n^{n-2}\alpha_1 \left(\frac{\alpha_n a}{b}\right) + \alpha_n^{n-1}\alpha_0 = 0.$$

So we see that $\alpha_n a/b$ is integral over $K[f]$. Since R is a UFD, it is integrally closed in $K(X_1, ..., X_n)$, and hence $\alpha_n a/b$ must be in R. By hypothesis, $K[f]$ is integrally closed in R, hence $\alpha_n a/b$ must be in $K[f]$. Consequently $a/b \in K(f)$. □

Theorem 3.15. *If $k^\sharp$ is not algebraically closed in $L^\sharp$, then there is some $h \in R$ and $\Lambda \in k[T]$ with deg $\Lambda > 1$ such that $f = \Lambda(h)$.*

This theorem is given with more specifics in [6] as the Refined Lüroth Theorem. The proof we will give is from [5]–see particularly Theorems 2.5 and 2.11.

Proof. We will first prove the following statement: if A is a 1-dimensional subring of R, then there is a k-homomorphism Φ from R onto $k[T]$ such that Φ is an isomorphism on A. So, up to isomorphism, we can assume that $A \subseteq k[T]$.

To prove this, recall that $(X_1, ..., X_n)$ is a prime ideal in R, and consider the prime ideal P of A given by the intersection $(X_1, ..., X_n) \cap A$. Since A is 1-dimensional, $P = 0$ or P is maximal in A. If $P = 0$, the natural ring homomorphism $\Phi : R \to R/(X_1, ..., X_n) \cong k \subset k[T]$ is an isomorphism on A, since $ker(\Phi) = A \cap (X_1, ..., X_n) = 0$. Otherwise, assume $P \neq 0$ (and hence is maximal.) If $n = 1$, the statement follows from letting Φ be the identity map on $R = K[X_1]$. So assume that $n > 1$. Let Q_m be the prime ideal generated by $X_1^m - X_n$ in R, for $m \in \mathbb{N}$. Note that, for any m, $Q_m \subset (X_1, ..., X_n)$, so $Q_m \cap A$ is a prime ideal of A contained in P. But, for $\alpha \in P$, there is some $M > 1$ for which $X_1^M - X_n$ does not divide α, and hence $Q_M \cap A$ is properly contained in P. Thus, since A is 1-dimensional and P is maximal, $Q_M \cap A = 0$. So letting $\Phi_1 : R \to R/(X_1^M - X_n) \cong k[X_1, ..., X_{n-1}]$, we see that Φ_1

is a isomorphism on A. By iterating this procedure, we get the desired Φ. Note that the Φ defined by these procedures is actually an epimorphism.

Now we return to the main theorem. By Lemma 3.14, we see that our assumption that $k^\sharp$ is not algebraically closed in $L^\sharp$ tells us that $k[f]$ is not integrally closed in R. Let A denote the integral closure of $k[f]$ in R. Note that A is 1-dimensional, since it is integral over $k[f]$, by Lemma 2.6. From the previous paragraph, then, we can assume that there is a k-epimorphism $\Phi : R \to k[T]$ which is an isomorphism on A. So identify A with $\Phi(A)$ and consider the chain $k \subseteq A \subseteq k[T]$. Since $dim(A) = dim(k[T]) = 1$, we must have that $k[T]$ is integral over A. Specifically, we see that T is integral over A. Let $h \in R$ be an element of R such that $\Phi(h) = T$, and note that Φ maps $k[h]$ onto $k[T]$, so, since Φ is an isomorphism on A, $A \subseteq k[h]$. Let $\lambda \in A[Y]$ be the minimal polynomial for T over A, and note that $\Phi(\lambda(h)) = \lambda(T) = 0$. Since Φ is an isomorphism on A, we must have $\lambda(h) = 0$, *i.e.*, h is integral over A. But A is integrally closed in R, so $k[h] \subseteq A$. We now see that $A = k[h]$.

Since $A = k[h]$ and, specifically, $f \in A$, we have that f can be written as $f = \Lambda(h)$ for some $\Lambda \in k[T]$. If $k[f]$ is not integrally closed, then Λ must have degree greater than 1, because otherwise $A = k[h] = k[f]$. □

Remark 3.16. Note that the converse to this theorem is also obviously true–if $f = \Lambda(h)$ as described, then h is algebraic over $k^\sharp$, but is not in $k^\sharp$.

As a corollary of this, we have the following. (See the Composite Pencil Theorem in[6].)

Corollary 3.17. *If $k^\sharp$ is not relatively algebraically closed in $L^\sharp$, then* $\text{redset}(f)^* = k^*$.

Proof. By Theorem 3.15, in such a case, f would have the form $\Lambda(h)$. Over k^*, $\Lambda - c$ factors for every $c \in k^*$, and thus $f - c$ factors for every $c \in k^*$. □

Remark 3.18. If we have $f \in R = k[X_1, ..., X_n]$ such that $k^\sharp$ is not algebraically closed in $L^\sharp$, we know that we can write f as a composite $f = \Lambda(h)$, by Theorem 3.15. We can choose h of minimal degree, so that h cannot be further written as a composite $h = \Lambda'(h')$ with $\Lambda' \in k[T]$ and $h' \in k[X_1, ..., X_n]$. If we choose such an h, then $k(h)$ must be algebraically closed in $L^\sharp$, again by Theorem 3.15. Now for $\Gamma \in \text{polyredset}(f)$, we have that $(\Gamma(\Lambda(h))$ is reducible in R. We consider cases:

1 If $\Gamma(\Lambda)$ is a reducible element of $k[T]$, then $\Gamma \in \text{polyredset}(\Lambda)$.

2 If $\Gamma(\Lambda)$ is irreducible in $k[T]$, then there is some element $u \in k$ so that $u\Gamma(\Lambda)$ is monic irreducible. So $u\Gamma(\Lambda) \in \text{polyredset}(h)$. Since $k(h)$ is algebraically closed in L, the set $\text{polyredset}(h)$ is finite, so there can only be finitely many such Γ.

Conversely, every $\Gamma \in \text{polyredset}(\Lambda)$ certainly is in $\text{polyredset}(f)$. However, it is not expected that every $\Gamma' \in \text{polyredset}(h)$ corresponds to some $\Gamma \in \text{polyredset}(f)$. However, we can conclude the following:

$$\text{polyredset}(f) = \text{polyredset}(\Lambda) \cup S$$

where

$$S := \{\beta \in \text{polyredset}(h) \mid \ \beta = u\Gamma(\Lambda) \text{ for } u \in k, \Gamma \in \text{polyredset}(f)\}.$$

Specifically, since $S \subseteq \text{polyredset}(h)$ and $k(h)$ is algebraically closed in $L^\sharp$, S is finite. So we have the following.

Theorem 3.19. *When $k^\sharp$ is not algebraically closed in $L^\sharp$, then f can be decomposed as $f = \Lambda(h)$ with $\Lambda \in k[T]$ and $h \in k[X_1, ..., X_n]$. Then* $\text{polyredset}(f)$ *is finite if and only if* $\text{polyredset}(\Lambda)$ *is finite.*

We also have a correspondence between the finiteness of $\text{redset}(f)$ and the group $U(A^\sharp)/U(k^\sharp)$. (Compare the following to Corollary 3.9.)

Theorem 3.20. *When k is an infinite field, if $|\text{redset}(f)| < \infty$, we must have $U(A^\sharp)/U(k^\sharp)$ is finitely-generated.*

Proof. By Lemma 2.8, if $U(A^\sharp)/U(k^\sharp)$ is not finitely generated, we certainly cannot have that $k^\sharp$ is algebraically closed in $L^\sharp$. So, by Theorem 3.15, $f = \Lambda(h)$ for some $\Lambda \in k[T]$ with degree at least 2 and some $h \in R \setminus k$. Consider Λ as a function $k \to k$, and let

$$B := \{c \in k \mid c = \Lambda(\omega) \text{ for some } \omega \in k\}.$$

Note that, for $c \in k$, $\Lambda - c$ can have at most $deg(\Lambda)$ roots, so

$$B_c := \{x \in k \mid \Lambda(x) = c\}$$

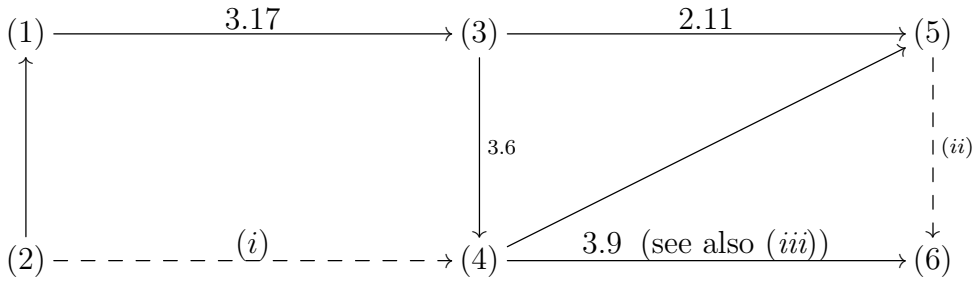
is finite for each c. Since every element of k is in some B_c, we have that $k = \cup_{c \in k} B_c$. So there must be infinitely many c for which $B_c \neq \emptyset$. So B is an infinite set. For any

$c \in B$, $\Lambda - c$ has a root in k, and hence is reducible. But for such c, $f - c = \Lambda(h) - c$ must be reducible, and so redset(f) is infinite. □

So consider the following conditions related to the polynomial f:

1. redset$(f)^* \neq k^*$.
2. redset$(f)^*$ is finite.
3. $k^\sharp$ is algebraically closed in $L^\sharp$.
4. polyredset(f) is finite.
5. redset(f) is finite.
6. $U(A^\sharp)/U(k^\sharp)$ is finitely-generated.

We can sum up the known relations between these thus:



Here, a solid arrow represents implication; a dashed arrow representations implication in certain cases, corresponding to the labels (i)-(iii) below. Unlabelled arrows are obvious implications.

(i) This implication is Corollary 3.11, when k is perfect, because in Theorem 3.10 we presented an explicit relationship between the sizes of the two sets. From this diagram, we can see that it is true more generally.

(ii) When k is infinite–see Theorem 3.20.

(iii) If we also know that polyuniset(f) is finite, this arrow is actually "if and only if"–see Corollary 3.9.

Specifically, if char$(k) = 0$, the implications (i) and (ii) also hold.

Chapter 4

Algebraic Closure Relations

Recall that k is field and $k^\sharp = k(f)$ where f is a fixed irreducible nonconstant polynomial in $R = k[X_1, ..., X_n]$. Also, $L = \text{qf}(R/fR)$ and $L^\sharp = k(X_1, ..., X_n)$. The hypotheses of the Redset Theorem (2.9) and the Mixed Redset Theorem (2.11) lead us to consider the following conditions:

(i) k is algebraically closed in L,

(ii) $k^\sharp$ is algebraically closed in $L^\sharp$.

Question 2 above asked us to relate these two conditions. The following theorem does this.

Theorem 4.1. *If k is algebraically closed in L, then $k^\sharp$ is relatively algebraically closed in $L^\sharp$.*

Proof. Assume k is algebraically closed in L, and let $g, h \in R = k[X_1, ..., X_n]$ be such that g/h is algebraic over $k(f)$. We take this fraction to be reduced, so that $gcd(g, h) = 1$, and define $D(g/h) = deg(g) + deg(h)$, where we always define D in terms of expressions with fully reduced fractions. We proceed by induction on $D(g/h)$.

Assume D(g/h)=0. Then $g/h \in k \subset k(f)$.

Assume that we have proven that every reduced element g/h of $L^\sharp$ which is algebraic over $k^\sharp$ with $D(g/h) \leq n-1$ is in $k(f)$ and take g/h algebraic over $k^\sharp$ with $D(g/h) = n$. If f divides g or h, we can consider the fraction g'/h' gotten by multiplying by a power of f so that $gcd(f, g) = gcd(f, h) = 1$. Since g'/h' is still algebraic over $k(f)$, and $D(g'/h') < D(g/h) = n$, we have that $g'/h' \in k(f)$ by the inductive

hypothesis. Thus, $g/h \in k(f)$, in this case. So, without loss of generality, we can assume $gcd(f,g) = gcd(f,h) = 1$.

We can also assume, without loss of generality, that $deg(h) \geq deg(g)$ because $D(g/h) = D(h/g)$ and g/h is algebraic over $k(f)$ iff h/g is algebraic over $k(f)$. Now we can take a polynomial over $k(f)$ satisfied by g/h and, multiplying by a common denominator, we can assume that this polynomial has coefficients in $k[f]$. So we have $a_{ij} \in k$ such that

$$\begin{aligned}
\sum_{\substack{0\leq i\leq M\\ 0\leq j\leq m}} a_{ij} f^i \Big(\frac{g}{h}\Big)^j &= 0 \\
\sum_{\substack{0\leq i\leq M\\ 0\leq j\leq m}} a_{ij} f^i g^j h^{m-j} &= 0 \\
\sum_{0\leq j\leq m} a_{0j} g^j h^{m-j} &= -f \sum_{\substack{1\leq i\leq M\\ 0\leq j\leq m}} a_{ij} f^{i-1} g^j h^{m-j}.
\end{aligned}$$

Now let $\pi : R \to R/fR$ be the canonical ring homomorphism. Applying π to this equation, we get

$$\sum_{0\leq j\leq m} a_{0j} \pi(g)^j \pi(h)^{m-j} = 0.$$

In $L = qf(A)$, this leads to the equation

$$\sum_{0\leq j\leq m} a_{0j} \pi\Big(\frac{g}{h}\Big)^j = 0.$$

But since we are assuming k is algebraically closed in L, this would mean $\pi(g/h) \in k$. That is, there is some $c \in k$ so that $f | g - ch$ in R. So there is some $\zeta \in R$ such that $\zeta f = g - ch$. Then $g = \zeta f + ch$ and note that $deg(\zeta f) \leq max\{deg(g), deg(h)\} = deg(h)$. So $deg(\zeta) < deg(h)$, since f has positive degree.

Now we can rewrite

$$\frac{g}{h} = \frac{\zeta f + ch}{h} = f\frac{\zeta}{h} + c,$$

which is algebraic over $k(f)$ if and only if ζ/h is. But $D(\zeta/h) < D(g/h) = n$, so $\zeta/h \in k(f)$ by the induction hypothesis. Thus, $g/h \in k(f)$. This completes the induction and hence the proof. $\square$

Example 4.2. We want to notice that the converse of this theorem is false. For instance, when k is an algebraically closed field, then k is always (regardless of f) algebraically closed in $\mathrm{qf}(R/fR)$, but we wouldn't expect every polynomial in R to satisfy the condition of $k(f)$ being algebraically closed in $L^\sharp$. For example, fix any irreducible polynomial f over k such that $k(f)$ is algebraically closed in $L^\sharp$. By the Polyredset Theorem (3.6), $\mathrm{polyredset}(f)$ is finite, so we can choose any $\Phi \in k[T] \setminus \mathrm{polyredset}(f)$. Then $\Phi(f)$ is irreducible, k is algebraically closed in $\mathrm{qf}(R/fR)$, but $k(\Phi(f))$ is not algebraically closed in $L^\sharp$.

Chapter 5

Comparison of Ranks

5.1 A homomorphism between groups

Throughout this chapter, let k be a field of characteristic 0.

Recalling some previous notation, we let $R = k[X_1, ..., X_n]$ and $A = R/P$, where $P = fR$ for f a fixed nonconstant irreducible polynomial in R. Let $\pi : R \to A$ be the canonical ring homomorphism and let $L = \mathrm{qf}(A)$. Also, let $A^\sharp = k(f)[X_1, ..., X_n]$ and let $L^\sharp = \mathrm{qf}(A^\sharp) = \mathrm{qf}(R)$.

We now turn our attention to Question 3 from Section 2.2. Recall these two facts, which follow from Lemma 2.8, and come from [6]:

1. If k is algebraically closed in L, then $U(A)/U(k)$ is a finitely-generated free Abelian group.

2. If $k^\sharp$ is algebraically closed in $L^\sharp$, then $U(A^\sharp)/U(k^\sharp)$ is a finitely-generated free Abelian group.

By the Mixed Redset Theorem, we know that $|\operatorname{redset}(f)|$ is bounded by the rank of the second group. From Theorem 4.1, we know that if k is algebraically closed in L, then both groups are finitely-generated free Abelian. We seek in this section to relate the ranks of these two groups. Our main strategy is as follows. In this section, we will set up an explicit group homomorphism between the two groups. In Section 2, we will introduce the concept of derivations. Section 3 will focus on constructing a derivation with a specific ring of constants; in Section 4, a further construction will give us the derivation we require. Finally, in Section 5, we will use this derivation to

argue that the mentioned homomorphism is in fact one-to-one. This will give us the relation we seek.

Before we go on, we should notice that the case where $n = 1$ is uninteresting because if we assume $k^\sharp$ is algebraically closed in $L^\sharp$, we see that f must have degree 1. Thus, certainly redset(f) is empty and, moreover, $A = R/fR \cong k$ and $A^\sharp = k(X_1) = k^\sharp$. So we see that $U(A)/U(k)$ and $U(A^\sharp)/U(k^\sharp)$ are both trivial groups. So from now on, we will consider only $n \geq 2$.

To relate the ranks of these two groups, we will need to study what elements of $U(A^\sharp)$ and $U(A)$ look like, and the relation between them. Let Y be an indeterminate over k and let

$$\begin{aligned}
&S := \{p(f) \mid 0 \neq p(Y) \in k[Y]\} = k[f] \setminus \{0\},\\
&T := \{a \in R \mid aR \cap S \neq \emptyset\},\\
&S_* := \{p(f) \mid p(Y) \in k[Y], \text{ with } p(0) \neq 0\} = k[f] \setminus fk[f], \quad \text{and}\\
&T_* := \{a \in R \mid aR \cap S_* \neq \emptyset\}.
\end{aligned}$$

Note that $S = U(k^\sharp) \cap R$ clearly. Similarly, a general element of $A^\sharp$ looks like $g/p(f)$ for some $g \in R$, $p \in k[Y]$. We previously noted that this element is a unit if there is some $g'/p'(f) \in A^\sharp$ such that $gg' = p(f)p'(f)$. Hence, $gR \cap k[f] \neq \{0\}$. So we see that T represents numerators of elements of $U(A^\sharp)$ (or, equivalently, $U(A^\sharp) \cap R$). Note that S_* and T_* restrict S and T respectively to elements which are not divisible by f.

Also note that S, T, S_*, and T_* are all multiplicative subsets of R and $A^\sharp = S^{-1}R = T^{-1}R$. The group $U(k)$ is a multiplicative subgroup of A. For $a \in R$, its $U(k)$-coset is denoted by $aU(k)$. Although $U(k)$ is not an additive subgroup, we let $U(k)+P$ denote the subset of R consisting of elements of the form $c+p$ with $c \in U(k)$ and $p \in P$.

We will soon define a multiplicative map $\Psi : A^\sharp \to A/U(k)$ by sending an element $g/p(f)$ of $A^\sharp$ to $\pi(g)$. Since we will ultimately be considering $U(A^\sharp)/U(k^\sharp)$, we will need to know when two elements are equivalent in this group. This motivates the following definition:

Definition 5.1. For $0 \neq v \in A^\sharp$, define $N(v)$ to be the set of all $\alpha \in R \setminus P$ such that $\alpha = svf^e$ for some $s \in S_*$ and $e \in \mathbb{Z}$.

Here, we have in $A^\sharp$ that $v = \alpha/sf^e$. Remembering that $s \in S_* \subseteq k(f)$, we see

that α is a numerator for some expression of v in $A^\sharp$, with any possible factors of f removed. Actually, $N(v)$ just collects all numerators of expressions of v where the denominator is in $k[f]$ and all powers of f have been factored out. The following technical lemma will clarify some of the properties of N.

Lemma 5.2. *Let v and w be nonzero elements of $A^\sharp$. Then, the following holds.*

(i) *$N(v)$ is nonempty.*

(ii) *For all $\alpha \in N(v)$ and $\beta \in N(w)$, we have $\alpha\beta \in N(vw)$.*

(iii) *$\pi(\alpha)U(k) = \pi(\beta)U(k)$ for all $\alpha, \beta \in N(v)$.*

(iv) *If $N(v) \cap (U(k) + P) \neq \emptyset$, then $N(v) \subset U(k) + P$.*

(v) *If $N(v) \cap T \neq \emptyset$, then $N(v) \subset T_*$.*

Before we delve into the proof, it might be helpful to give a quick idea what these actually mean. Part (i) is intuitively obvious–it just says that each $g \in A^\sharp$ can be written in the form α/sf^e, where $\alpha \in R$ and $sf^e \in k[f]$. Part (ii) tells us that N is a multiplicative map, and (iii) tells us that each element of $N(v)$ is going to be in the same coset of $U(A)/U(k)$. Parts (iv) and (v) will be useful when we want to study the behavior of the above-mentioned homomorphism. (See Theorem 5.3.)

Proof.

(i) Note that v is of the form $g/p(f)$ with $0 \neq g \in R$, $p(f) \in S$. Since f is irreducible in R and $g, p(f)$ are nonzero elements of R, we can write $g := f^i\alpha$, $p(f) := f^j s(f)$ where i, j are nonnegative integers, $\alpha \in R$ with $gcd(f, \alpha) = 1$, and $s \in k[Y]$ with $gcd(f, s(f)) = 1$. (So note $s(f) \in S_*$.) Letting $e := j - i$ it follows that $\alpha = svf^e$ and hence α is in $N(v)$.

(ii) This is clear from the definition of N, because if $\alpha = svf^d$ and $\beta = s'wf^e$, then $\alpha\beta = ss'vwf^{e+d}$.

(iii) Now suppose $\alpha, \beta \in N(v)$ and $(s, d), (\sigma, e) \in S_* \times \mathbb{Z}$ are such that $\alpha = svf^d$ and $\beta = \sigma vf^e$. Then we can see that $\alpha/sf^d = \beta/\sigma f^e$. Since $\alpha, \beta \in R\backslash P$ by definition of N and $s, \sigma \in S_*$, we can see that $d = e$ and, moreover, $\sigma\alpha = s\beta$. Applying the canonical epimorphism $\pi : R \to A$ to the last equation, we get $\pi(\sigma)\pi(\alpha) = \pi(s)\pi(\beta)$. Since s and σ were chosen from S_*, they satisfy $\pi(s), \pi(\sigma) \in U(k)$. Thus, we have (iii).

(iv) For $\alpha \in N(v)$, if $\alpha \in U(k)+P$, then $\pi(\alpha)$ is in $U(k)$. Thus, by (iii), if $\beta \in N(v)$, then $\pi(\beta) \in U(k)$, *i.e.*, $\beta \in U(k) + P$.

(v) Suppose $N(v) \cap T$ is nonempty and pick $t \in N(v) \cap T$. Since $tR \cap S \neq \emptyset$, we have $tr = h$ for some $r \in R$ and $h \in S$. Now for arbitrary $\alpha \in N(v)$, we have that $\alpha = svf^d$ and $t = \sigma v f^e$ for some $s, \sigma \in S_*$ and integers d, e. Thus, we have

$$\alpha\sigma f^e = tsf^d.$$

Since $s, \sigma \in S_*$, $gcd(s, f) = gcd(\sigma, f) = 1$. Similarly, since $\alpha, t \in N(v)$, $gcd(\alpha, f) = gcd(t, f) = 1$. So we have that $d = e$ and

$$\begin{aligned} \alpha\sigma &= ts \\ \alpha\sigma r &= tsr \\ \alpha\sigma r &= sh. \end{aligned}$$

Since s and h are in S, $sh \in S$. Thus, from this equation, we see that $\alpha R \cap S \neq \emptyset$, hence that $\alpha \in T$. Since also f does not divide α, we see that $\alpha \in T_*$. □

Now we can move on to the desired homomorphism. Let

$$G := \{v \mid v \in A^\sharp \text{ and } N(v) \subset U(k) + P\}.$$

Note that G is a multiplicative subset of $A^\sharp$.

Theorem 5.3. *Define $\Psi : U(A^\sharp) \to A/U(k)$ by setting $\Psi(v) := \pi(\alpha)U(k)$ for any $\alpha \in N(v)$. This map yields a group-homomorphism $U(A^\sharp) \to U(A)/U(k)$ with kernel $U(A^\sharp) \cap G$. Moreover, Ψ induces a group-homomorphism*

$$\psi : \frac{U(A^\sharp)}{U(k^\sharp)} \to \frac{U(A)}{U(k)}$$

with

$$Ker(\psi) = \frac{U(A^\sharp) \cap G}{U(k^\sharp)}.$$

Proof. By Lemma 5.2(i), $N(v) \neq \varnothing$, and so Ψ gives a definition for each $v \in U(A^\sharp)$. Part (iii) of the lemma tells us that the map is well-defined into $A/U(k)$, because

if $\alpha, \beta \in N(v)$, then, although $\pi(\alpha)$ need not be the same as $\pi(\beta)$, we do have that $\pi(\alpha)U(k) = \pi(\beta)U(k)$.

Now we need to see that Ψ actually maps into $U(A)/U(k)$. As previously noticed, $U(A^\sharp) = \{g/p(f) \mid g \in T \text{ and } p(f) \in S\}$. So for $v \in U(A^\sharp)$, we can write $v = f^d g/p(f)$ for $d \in \mathbb{Z}$, $g \in R \setminus P$, and $p \in k[T]$ as above. Then $g \in T \cap N(v)$. Thus, by Lemma 5.2(v), $N(v) \subset T_*$. So for any $t \in N(v)$, we have $t \in T_*$, and hence we have $r \in R$ and $\sigma \in S_*$ with $tr = \sigma$. Then $\pi(t)\pi(r) = \pi(\sigma) \in U(k) \subseteq U(A)$. So $\pi(t) \in U(A)$. Thus, we see that Ψ maps v to $\pi(t)U(k) \in U(A)/U(k)$, and hence maps $U(A^\sharp)$ into $U(A)/U(k)$. This tells us that Ψ does indeed map into $U(A)/U(k)$, not just into $A/U(k)$.

The fact that Ψ is a multiplicative homomorphism is just 5.2(ii). It is easy to check that $\Psi(U(k^\sharp)) = U(k)$, so that Ψ induces the map ψ.

It remains to describe $K := Ker(\psi)$. For $v \in U(A^\sharp)$ and $t \in N(v)$ we have $v \in K$ if and only if $\pi(t) \in U(k)$. This is if and only if $t \in U(k) + P$. Thus, $K = G \cap U(A^\sharp)$ by Lemma 5.2(iv). Note that $U(k^\sharp)$ is obviously a subset of $G \cap U(A^\sharp)$. □

Remark 5.4. It might be worth pointing out very explicitly the behavior of Ψ. Given an element $v = g/p(f)$ of $A^\sharp$, by factoring out all possible powers of f from g, we get a new polynomial $g' \in R$. This will be an element of $N(v)$, so we will have $\Psi(v) = \pi(g')$.

Now our long-term goal is to show that ψ is a monomorphism, and hence that it allows us to relate the ranks of the two groups in question. To do this, we need to show that $Ker(\psi)$ is trivial. To do this, we will show that $U(A^\sharp) \cap G \subseteq U(k^\sharp)$. Consider an element of R which is in $U(A^\sharp) \cap G$. It has two main properties: since it is in $U(A^\sharp)$, it divides a polynomial in f, and since it is in G, it has the form $c + f\lambda$ for some $c \in U(k)$ and $\lambda \in R$. We will show that any polynomial with those two properties is actually an element of k. To do this, we turn our attention to derivations.

5.2 Derivations: basic notions

Definition 5.5. Let R be a ring and S an R-algebra. A *derivation of R into S* is an additive homomorphism $D : R \to S$ which also satisfies the product rule

$$D(xy) = xD(y) + yD(x)$$

for every $x, y \in R$.

Here, we will only be considering derivations of domains, and these have a nice extension property.

Lemma 5.6. *Let R be a domain, K be a field, and D be a derivation from R to K. Then D can be extended uniqely to a derivation D' from $\mathrm{qf}(R)$ to K.*

Proof. This is well-known. See [28], Section 17, Lemma 1. However, it is useful to note that the unique extension is given by the familiar quotient rule:

$$D'\left(\frac{x}{y}\right) = \frac{yD(x) - xD(y)}{y^2}. \qquad \square$$

We will be interested in studying the elements which are mapped to 0 by a derivation. So we have the following definitions:

Definitions 5.7. For a subring R' of R and a derivation $D : R \to S$, if $D(x) = 0$ for all $x \in R'$, we will say that D is an *R'-derivation*. Similarly, we will define $R^D := \{x \in R \mid D(x) = 0\}$. It is easy to check that R^D is a ring (see Lemma 5.8), called the *ring of constants of D in R*. If D is a derivation of a field K, the set K^D is a field, and will be called the *field of constants*.

Note that, given an R'-derivation D, we have that $R' \subseteq R^D$, but no equality is implied or, in general, true. The following very basic properties will be used without mention in what follows.

Lemma 5.8. *Let R be a domain and $D : R \to S$ be a derivation. Remember that any domain can be viewed as a $\mathbb{Z}$-module via the homomorphism sending $1_\mathbb{Z}$ to 1_R. Then*

1. *$1 \in R^D$, and hence $D(n) = 0$ for every $n \in \mathbb{Z}$.*
2. *If $g \in R^d$ and $g^{-1} \in R$, then $g^{-1} \in R^d$.*
3. *If $g \in R^d$, then for any $x \in R$, $D(gx) = gD(x)$.*
4. *If R is a field, the prime subfield of R is contained in R^D.*
5. *R^D is additively and multiplicatively closed.*

Proof. The proof of each of these statements follows directly from the basic definition. Note that (4) follows from (1), (2), and (3). Also, these provide the reasoning as to why R^D is a ring, and (3) explains why it is called the ring "of constants." □

We want to discuss further the existence and uniqueness of extensions of derivations of fields. To this end, for a field K and a transcendental extension $K(X_1, ..., X_n)$, we will denote by ∂_i the usual partial derivative $\frac{\partial}{\partial X_i}$.

Lemma 5.9. *Let K be a field of characteristic 0, $F = K(x)$ an extension field of K, and $D : K \to L$ be a derivation of K into a field L containing F. Then:*

(a) *If x is transcendental over K, then for any $g \in L$, there is a unique extension of D' of D to F such that $D'(x) = g$.*

(b) *If x is algebraic over K, then there is a unique extension of D to F.*

Proof.

(a) See [28], Section 17, Corollary 1 for proof, but it will be useful to understand the derivation D'. For any ax^i with $a \in K$ and $i \in \mathbb{N}$, the extension must follow the product rule, so we have $D'(ax^i) = D(a)x^i + aix^{i-1}g$. Then, D extends additively to polynomials in x.

(b) See [28], Section 17, Corollary 2 for a full proof. Again, we can see explicitly the behavior of such an extension. If we pick a minimal polynomial for x over k, say $x^e + a_{e-1}x^{e-1} + \cdots + a_1x + a_0 = 0$ with each $a_i \in K$, the product rule would require

$$d(x) = \frac{d(a_{e-1})x^{e-1} + \cdots + d(a_1)x + d(a_0)}{ex^{e-1} + (e-1)a_{e-1}x^{e-2} + \cdots + a_1}$$

and this is indeed how the extension is defined. □

This lemma extends further via the following, which can be thought of as iterating the previous lemma

Lemma 5.10. *Let K be a field of characteristic 0, F an extension field of K, and $D : K \to L$ be a derivation of K into a field L containing F. Then:*

(a) *If $F = K(X_1, ..., X_n)$ is purely transcendental over K, then for any $g_1, ..., g_l \in L$, there is a unique extension D' of D to F such that $D'(x_i) = g_i$ for each i.*

(b) *If F is algebraic over K, then there is a unique extension of D to F.*

Proof. See [28], Section 17, Corollary $1'$ and $2'$. □

Remark 5.11. Some of these statements regarding extensions of derivations will hold even when $\text{char}(K) \neq 0$, but our main results in the next two sections will require K to have characteristic 0.

As a consequence of 5.10 (a), we have a nice way to understand derivations on finite transcendental extensions of fields of characteristic 0.

Lemma 5.12. *Let K be a field of characteristic 0, $F = K[X_1, ..., X_n]$ a transcendental extension. Then the set of K-derivations of F into itself is a free F-module of degree n, with basis $\{\partial_1, \partial_2, ..., \partial_n\}$. Similarly, if $F = K(X_1, ..., X_n)$, then the set of K-derivations of F into itself is an n-dimensional F-vector space, with basis $\{\partial_1, \partial_2, ..., \partial_n\}$.*

As a quick explanation of this lemma, we see from Lemma 5.10 that it makes sense to extend the 0 derivation on K to the field $K(X_1, ..., X_n)$ simply by choosing an assignment $g_1, g_2, ..., g_n$ for each X_i. If each g_i is chosen in F, then the derivation maps into F, and any such choice of $\{g_i\}$ yields a valid, unique extension. This also gives us a nice way to represent such derivations. Given any derivation $D : K[X_1, ..., X_n] \to K[X_1, ..., X_n]$, by letting $D(X_i) = g_i$, we can write

$$D = g_1\partial_1 + g_2\partial_2 + \cdots + g_n\partial_n$$

as derivations from F to F.

Our major tool in this chapter will be the construction of derivations on $R = k[X_1, ..., X_n]$ with specified rings of constants. Remember that $g \in R$ is in the ring of constants R^D if $D(g) = 0$. However, it will be helpful for us to consider a more general notion, that of *Darboux polynomial*. Recall that, for two elements a, b in R, we say that a *divides* b and write $a|b$ if there is some $r \in R$ so that $ra = b$.

Definition 5.13. Given D, a k-derivation of R, we will say that $g \in R$ is a *Darboux polynomial* of D if $g|D(g)$.

Note each element g of R^D is a Darboux polynomial, because $g|0$. Then we have the following:

Lemma 5.14. *If K is a field of characteristic 0 and g, h are Darboux polynomials of a derivation D of $K[X_1, ..., X_n]$, then*

1. *gh is a Darboux polynomial.*

2. *Any factor of g is a Darboux polynomial.*

Proof.

1. Say $P_1 g = D(g)$ and $P_2 h = D(h)$ for some $P_1, P_2 \in R$. Then

$$D(gh) = gD(h) + D(g)h = gP_2 h + P_1 gh = (P_2 + P_1)gh.$$

   So $gh | D(gh)$.

2. If $g \in K$, this is trivially true, so assume $g \notin K$. By (1), it will suffice to show that each irreducible factor of g is a Darboux polynomial. Let α be such a factor, and write $g = \alpha^m \beta$ with $\beta \in R$, $m \in \mathbb{N}$, and $\gcd(\alpha, \beta) = 1$. Assuming g is a Darboux polynomial, $D(g) = Pg$ for some $P \in R$. Then:

$$\begin{aligned} Pg &= D(g) \\ Pg &= D(\alpha^m \beta) \\ P\alpha^m \beta &= m\alpha^{m-1} D(\alpha)\beta + D(\beta)\alpha^m \\ P\alpha\beta &= mD(\alpha)\beta + D(\beta)\alpha \\ mD(\alpha)\beta &= \alpha(P\beta - D(\beta)). \end{aligned}$$

   Since $\mathrm{char}(K) = 0$, $m \neq 0$, so since $g \notin K$, $\gcd(\alpha, m) = 1$. Then, from α dividing $mD(\alpha)\beta$, and the fact that $\gcd(\alpha, \beta) = 1$ (by assumption,) we can conclude $\alpha | D(\alpha)$. Thus, α is a Darboux polynomial. □

Remark 5.15. It is important here that $\mathrm{char}(K) = 0$. As a counterexample in general, let $K = \mathbb{F}_3$, the field with 3 elements, and consider the derivation $D = \partial_1$ on $K[X_1]$. Notice that X_1^3 is a Darboux polynomial of $K[X_1]$; in fact, $X_1^3 \in K[X_1]^D$ since $D(X_1^3) = 3X_1^2 = 0$. Note that X_1 is a factor of X_1^3, but $D(X_1) = 1$ and X_1 does not divide 1.

Given a nonzero $f \in K[X_1, ..., X_n]$, we wish to investigate the existence of a derivation $D : K[X_1, ..., X_n] \to K[X_1, ..., X_n]$ such that $K[X_1, ..., X_n]^D = K[f]$. The

next two sections are devoted to the construction of such a D provided f satisfies certain requirements. Before we continue, we should note some properties of such rings of constants in general. Let $R = K[X_1, ..., X_n]$. We have:

Theorem 5.16. *Let $D : R \to R$ be a derivation.*

1. $R \cap \mathrm{qf}(R^D) = R^D$.
2. *If* $\mathrm{char}(R) = 0$, *then R^D is integrally closed in R.*

Proof.

1. For $\alpha, \beta \in R^D$ with $\beta \neq 0$ and $\alpha/\beta \in R$, we can write $\beta\gamma = \alpha$ with $\gamma \in R$. Then, applying D, we see that $\beta D(\gamma) = 0$. Since R is a domain, $D(\gamma) = 0$. So $\gamma \in R^D$.

2. If $x \in R$ is integral over R^D, we can choose a monic polynomial $g \in R^D[T]$ of minimal degree such that $g(x) = 0$. Say

$$g(T) := T^e + a_{e-1}T^{e-1} + \cdots + a_1T + a_0$$

with $a_0, ..., a_{e-1} \in R^D$. Then we apply the derivation D to the equation $g(x) = 0$ to get

$$\begin{aligned} 0 &= ex^{e-1}D(x) + a_{e-1}(e-1)x^{e-2}D(x) + \cdots + a_1D(x) \\ &= eD(x)\left(x^{e-1} + a_{e-1}\frac{e-1}{e}x^{e-2} + \cdots + \frac{1}{e}a_1\right) \end{aligned}$$

where we have used the fact that, since $\mathrm{char}(R) = 0$, we have that $e \neq 0$. The parenthetical part is a monic polynomial in x with coefficients in R^D by Lemma 5.8, hence is nonzero since it has degree less than e. Thus, $D(x) = 0$ and $x \in R^D$. This tells us that R^D is integrally closed in R. □

Thus, for there to be a derivation with ring of constants $k[f]$, we must have the two properties from the previous lemma. (In fact, there exists such a derivation *if and only if* those two properties hold. See Theorem 5.4 in [18].) Luckily, the first property is always true for rings of the form $k[f]$–see Lemma 3.13.

However, Property 2 does not hold for arbitrary polynomials. For instance, if we consider the polynomial $g := (X + Y)^2 + 1$, it is easy to see that $X + Y$ is integral

over $k[g]$, but $X + Y \notin k[g]$. Nevertheless, in the case we are considering, we know that $k(f)$ is algebraically closed in $L^\sharp = k(X_1, ..., X_n)$, and we do indeed have that $k[f]$ is integrally closed in $K[X_1, ..., X_n]$, by Lemma 3.14.

5.3 A derivation with trivial field of constants

In this section, we will explicitly demonstrate a derivation with trivial field of constants.

Let k be a field of characteristic 0. Here we show that the derivation

$$d := \partial_1 + X_2\partial_2 + \cdots + X_2 \cdots X_n\partial_n = \sum_{1 \le i \le n} \left(\prod_{2 \le j \le i} X_j \right) \partial_i$$

acting on $k(X_1, ..., X_n)$ for $n \geq 2$ has trivial field of constants, *i.e.*, $k(X_1, ..., X_n)^d = k$. Ther derivation d appears in [8], where the proof uses complex analysis. Instead, we will present a suitable modification of Suzuki's proof of Theorem 1 of [23], where he shows that the derivation

$$d_1 := \partial_1 + \frac{1}{X_1}\partial_2 + \frac{1}{X_1X_2}\partial_3 + \cdots + \frac{1}{X_1X_2 \cdots X_{n-1}}\partial_n$$

has trivial field of constants. His derivation is closely related to the derivation d mentioned above. To elaborate, letting

$$d_2 \;\; = \;\; X_1X_2 \cdots X_{n-1}d_1,$$

it follows that d_1 has trivial field of constants if and only if d_2 has trivial field of constants. Note that d_2 has the added property of mapping $k[X_1, ..., X_n]$ to itself. This is true more generally:

Useful Fact 5.17. Given a derivation $D : k(X_1, ..., X_n) \to k(X_1, ..., X_n)$ having trivial field of constants, there is a polynomial $\alpha \in k[X_1, ..., X_n]$ (namely, a common denominator for the values $D(X_1), D(X_2), ..., D(X_n)$) such that αD is a derivation with trivial field of constants, and αD maps $k[X_1, ..., X_n]$ to itself.

Letting ρ be the field-isomorphism fixing k and mapping X_i to X_{n+1-i}, it is easy to see that $d = d_2\rho$. So, having shown that d_1 has trivial field of constants, the same will hold for d.

Lemma 5.18. *For d as defined, $\frac{1}{X_1} \neq d(f)$ for any $f \in k(X_1, ..., X_n)$.*

Proof. Set $K = k(X_2, ..., X_n)$ and let d_1 be the derivation of K such that $d = \partial_1 + X_2 \cdots X_n d_1$. Extend d_1 to $L = K(X_1)$ via $d_1(X_1) = 0$ and note that then d_1 and d are derivations mapping $K[X_1]$ to itself. Suppose $u \in L$ is such that $d(u) = \frac{1}{X_1}$ and let $h, g \in K[X_1]$ be coprime polynomials such that $u = h/g$ with g and h relatively prime in $K[X_1]$. Then,

$$\frac{1}{X_1} = \frac{gd(h) - hd(g)}{g^2}.$$

Specifically, we must have $X_1 | g$ in $K[X_1]$. Write $g = X_1^e g'$ with $e \geq 1$ and $g' \in K[X_1]$ is such that $g'(0) \neq 0$. Then

$$X_1^e (g')^2 = X_1 g' d(h) - ehg' - hX_1 d(g').$$

Comparing the X_1 - degrees of the two sides of this equation, it is clear that X_1 must divide heg' in $K[X_1]$. But, since k has characteristic 0, $ehg' \neq 0$, and X_1 does not divide g' by assumption. So $X_1 | h$. But we have assumed that $\gcd(g, h) = 1$ in $K[X_1]$ and we have seen already that $X_1 | g$, which is a contradiction. □

Lemma 5.19. *Let L be an algebraic field extension of a field K of characteristic 0 and let d be a derivation of K. Let d' be the unique extension of d to L. If $\lambda \in K$ but $\lambda \notin d(K)$, then $\lambda \notin d'(L)$.*

Proof. First, note first that d' exists, by Lemma 5.10. Assume that $y \in L$ is such that $d'(y) = \lambda$. Let Y be transcendental over K and $g \in K[Y]$ be a minimal polynomial of y over K. Say

$$g(Y) = Y^m + a_{m-1} Y^{m-1} + \cdots + a_1 Y + a_0$$

with $a_i \in K$ for $0 \leq i \leq m - 1$. Let $G \in K[Y]$ be defined by

$$\sum_{i=0}^{m-1} d'(a_i) Y^i + \lambda \sum_{i=1}^{m-1} i a_i Y^{i-1} + m\lambda Y^{m-1}.$$

Then apply d' to see that $0 = d'(g(y)) = G(y)$. This gives a polynomial for y over K of apparent degree less than m. Hence, it must be the zero polynomial. In particular,

its leading coefficient is 0, *i.e.*,

$$d(a_{m-1}) + m\lambda = 0.$$

Since $\text{char}(L) = 0$, $m \neq 0$ in L. But then

$$\lambda = \frac{-d(a_{m-1})}{m} = d\Big(\frac{-a_{m-1}}{m}\Big) \in d(K)$$

contradicting our hypothesis. □

Theorem 5.20. *Let d be the derivation $d = \partial_1 + X_2\partial_2 + \cdots + X_2 \cdots X_n\partial_n$. Then $k(X_1, ..., X_n)^d = k$.*

Proof. Let

$$d_n = \partial_n$$

$$d_{n-1} = \partial_{n-1} + X_n\partial_n$$

and, in general,

$$d_i = \partial_i + X_{i+1}d_{i+1}$$

where we are viewing d_i as a derivation of $k(X_i, ..., X_n)$ for each i. We will proceed by induction on d_i, but in the opposite to the usual order–from n to 1.

When $l = n$, $d_l = \partial_n$ has field of constants k as a derivation of $k(X_n)$. By the induction hypothesis, assume that $d_l = \partial_l + X_{l+1}\partial_{l+1} + \cdots + X_{l+1} \cdots X_n\partial_n$ satisfies $k(X_l, ..., X_n)^{d_l} = k$ for each $l = n, n-1, ..., m+1$. We prove the corresponding statement when $l = m$. Let $\overline{d_{m+1}}$ extend d_{m+1} to $k(X_m, ..., X_n)$ via $\overline{d_{m+1}}(X_m) = 0$. Fix a $\lambda \in k(X_m, ..., X_n) \setminus d_{m+1}(k(X_m, ..., X_n))$. (Note that λ exists by lemma 5.18.) Set $d' = \overline{d_{m+1}} + \lambda\partial_m$.

Let $K := k(X_{m+1}, ..., X_n)$. Assume that there is $u \in K(X_m)$ such that $d'(u) = 0$. That is, $0 = \overline{d_{m+1}}(u(X_m)) + \lambda u'(X_m)$ where $u'(X_m)$ denotes $\partial_m u(X_m)$. Set $u = h/g$ with $h, g \in K[X_m]$ and $\gcd(g, h) = 1$. If $u(X_m) \in K$, then $d'(u) = 0$ implies $\overline{d_{m+1}}(u(X_m)) = d_{m+1}(u(X_m)) = 0$, and hence $u \in k$ by hypothesis. Otherwise, letting $\overline{K}$ denote the algebraic closure of K, let $\alpha_1, .., \alpha_b$ be the zeroes of $u'(X_m)$ in $\overline{K}$ which are not roots of $g(X_m)$. Pick some $c \in k \setminus \{u(\alpha_1), ..., u(\alpha_b)\}$. Now $(h - cg)(X_m)$ has a root in $\overline{K}$, since $u(X_m) \notin K$. Let us denote such a root by ζ. If $g(\zeta) = 0$, then $h(\zeta) = 0$, contradicting that h and g are relatively prime in $K[X_m]$. Thus, $g(\zeta) \neq 0$.

Now $\overline{K}$ is a separable algebraic extension of K, and hence there is a unique extension d^* of d to $\overline{K}$ by Lemma 5.10. Then

$$d^*(u(\zeta)) = d^*\left(\frac{h(\zeta)}{g(\zeta)}\right) = d^*(c) = 0.$$

We will now show that

$$d^*(u(\zeta)) = \overline{d_{m+1}}(u(\zeta)) + u'(\zeta)d^*(\zeta).$$

For a monomial $\alpha\zeta^i \in K[\zeta]$, we have

$$d^*(a\zeta^i)\overline{d_{m+1}}(\alpha)\zeta^i + \left[\partial_n(\alpha X_n^i)\Big|_{X_n=\zeta}\right]d^*(\zeta).$$

This shows that the equation holds for monomials. Since d^*, $\overline{d_{m+1}}$, and ∂_n are each linear, this will extend to any polynomial in $K[\zeta]$. We have

$$\begin{aligned} g(\zeta)d^*(h(\zeta)) - h(\zeta)d^*(g(\zeta)) = \\ \left[g(\zeta)\overline{d_{m+1}}(h(\zeta)) - h(\zeta)\overline{d_{m+1}}(g(\zeta))\right] + \left[g(\zeta)h'(\zeta)d^*(\zeta) - h(\zeta)g'(\zeta)d^*(\zeta)\right]. \end{aligned}$$

The quotient rule gives

$$d^*\left(\frac{h(\zeta)}{g(\zeta)}\right) = \frac{g(\zeta)d^*(h(\zeta)) - h(\zeta)d^*(g(\zeta))}{(g(\zeta))^2}$$

and

$$\overline{d_{m+1}}\left(\frac{h(\zeta)}{g(\zeta)}\right) = \frac{g(\zeta)\overline{d_{m+1}}(h(\zeta)) - h(\zeta)\overline{d_{m+1}}(g(\zeta))}{(g(\zeta))^2}.$$

Finally, noting that

$$(g(\zeta))^2u'(\zeta)d^*(\zeta) = g(\zeta)h'(\zeta)d^*(\zeta) - h(\zeta)g'(\zeta)d^*(\zeta),$$

we get the desired equality.

Now we are assuming that

$$0 = \overline{d_{m+1}}(u(X_m)) + \lambda u'(X_m).$$

Substituting $X_m = \zeta$ in this equation and using the fact that $u'(\zeta) \neq 0$ by choice of ζ, we see that $d^*(\zeta) = \lambda$. Thus, $\lambda \in d^*(\overline{K})$. However, by Lemma 5.19, since λ was chosen to be in $K \setminus d(K)$, we have $\lambda \notin d^*(\overline{K})$. Hence, we have a contradiction, and no such u can exist.

So we know now that d' has a trivial field of constants. But notice that, taking $\lambda = \frac{1}{X_{m+1}}$ (which is a valid choice of λ by Lemma 5.18,) we have that $d' = \overline{d_{m+1}} + \frac{1}{X_{m+1}}\partial_m$, so $X_{m+1}d' = X_{m+1}\overline{d_{m+1}} + \partial_m = X_{m+1}d_{m+1} + \partial_m = d_m$. This establishes our assertion. □

5.4 A derivation with ring of constants $k[f]$

In this section our goal is to construct a derivation of $R = k[X_1, ..., X_n]$ having ring of constants $k[f]$. As was mentioned previously, the existence of such a derivation was established in Theorem 5.4 of [18]. It is necessary for us to have a constructive proof of existence; such a proof is given in [24], Theorem 3.1.

We are working under the assumption that $k(f)$ is algebrically closed in $L^\sharp = k(X_1, ..., X_n)$, so by Lemma 3.14, $k[f]$ is integrally closed in R. First we must fix some notation. Since $f \notin k$, we have some $\partial_i(f) \neq 0$. Without loss of generality, we assume $\partial_n(f) \neq 0$.

Although we are only considering redset(f) when $n \geq 2$, it is probably worth pointing out that, when $n = 1$, the existence of such a derivation is rather trivial: $k(f)$ can only be algebraically closed in $k(X_1)$ if $\deg f = 1$, and in this case, $k[f] = k[X_1]$. So the zero derivation suffices.

When $n = 2$, we can use the Jacobian derivation $\partial_1(f)\partial_2 - \partial_2(f)\partial_1$.

Theorem 5.21. *Let $R = k[X, Y]$, $f \in R \setminus k$ such that $k(f)$ is algebraically closed in $k(X, Y)$, and $d := \partial_X(f)\partial_Y - \partial_Y(f)\partial_X$. Then $R^d = k[f]$.*

Proof. Clearly, $k[f] \subseteq R^d$. If the two rings are not equal, we can choose some $h \in R^d \setminus k[f]$. Since $k(f)$ is algebraically closed in $k(X, Y)$, we have that h is transcendental over $k(f)$. Thus, by considering transcendence degree over k, we see that $k(X, Y)$ is an algebraic extension of $k(f, h)$. Then we have

$$k(f, h) \subseteq k(X, Y)^d \subseteq k(X, Y).$$

But, from Theorem 5.16, we know that $k(X,Y)^d$ is algebraically closed in $k(X,Y)$. Since every element of $k(X,Y)$ is known to be algebraic over $k(f,h)$, it is certainly algebraic over $k(X,Y)^d$. Thus, $k(X,Y)^d = k(X,Y)$. But it is simple to check that $d(X) = -\partial_Y(f)$ and $d(Y) = \partial_X(f)$. So if $X, Y \in R^d$, we would have $f \in k$, a contradiction. So no such h exists, and $R^d = k[f]$. □

To generalize this construction for $n > 2$, we use the following argument. Noticing that ∂_1 is a derivation of $k(X_1)$ with trivial field of constants, the above Jacobian derivation has the form $\partial_n(f)d - d(f)\partial_n$ with $d = \partial_1$. We proceed to present a generalization of this.

The line of argument (specifically the construction, Lemma 5.23, and Theorem 5.24) are from [24].

Let us denote by δ the derivation of $K(X_1, ..., X_{n-1})$ considered in the previous section:

$$\delta := \partial_1 + X_2\partial_2 + \cdots + X_2 \cdots X_{n-1}\partial_{n-1}.$$

Of course, δ is a derivation of $k[X_1, ..., X_{n-1}]$. By Theorem 5.20, we have proven that $k(X_1, ..., X_{n-1})^\delta = k$. Extend δ to a derivation Δ of $k[X_1, ..., X_n]$ by Lemma 5.9(a) by defining

$$\Delta(X_i) := \begin{cases} \delta(X_i) & \text{if } 1 \leq i \leq n-1 \\ 0 & \text{if } i = n \end{cases}.$$

Define $d : R \to R$ by

$$d := \partial_n(f)\Delta - \Delta(f)\partial_n \tag{5.1}$$

Then d is a derivation of R by Lemma 5.12. We proceed to show that $R^d = k[f]$.

Lemma 5.22. *Let D be a derivation of a domain R into itself, and let $\overline{D}$ be the extension of D to* $\mathrm{qf}(R)$. *Then* $\mathrm{qf}(R^D) \subseteq (qf(R))^{\overline{D}}$.

Proof. If $\alpha, \beta \in R^D$ with $\beta \neq 0$, then it is simple to check that $\overline{D}\,(\alpha/\beta) = 0$. Thus, $\alpha/\beta \in (\mathrm{qf}(R))^{\overline{D}}$. □

Lemma 5.23. *Let $M \subseteq K \subseteq L$ be fields of characteristic* 0, *with L algebraic over K. Let $d : K \to K$ be a derivation with $K^d = M$. Let $\overline{d} : L \to L$ be the unique extension of d to L. If M is algebraically closed in L, then $L^{\overline{d}} = M$.*

Proof. Fix $u \in L$ with $\overline{d}(u) = 0$. Now u is algebraic over K. Let $g(T) \in K[T]$ be the minimal polynomial of u over K; say $g(T) := T^m + a_{m-1}T^{m-1} + \cdots + a_1T + a_0$ with

$a_0, a_1, ..., a_{m-1} \in K$. Applying $\overline{d}$ to the equation $g(u) = 0$, we get

$$\overline{d}(a_{m-1})u^{m-1} + \cdots + \overline{d}(a_1)u + \overline{d}(a_0) = 0$$

Minimality of $g(T)$ implies $\overline{d}(a_i) = 0$ for $0 \leq i \leq m-1$, hence each $a_i \in K^d = M$. Thus, u is algebraic over M. Since M is algebraically closed in L, $u \in M$. It follow that $L^{\overline{d}} = M$. □

Theorem 5.24. *With d given by equation 5.1, $R^d = k[f]$.*

Proof. It is clear that $k[f] \subseteq R^d$, so we need only show the other inclusion. By Lemma 5.6, we can extend d uniquely to a derivation $\overline{d} : k(X_1, ..., X_n) \to k(X_1, ..., X_n)$. Since $\overline{d}$ extends d, we have

$$k(X_1, ..., X_n)^{\overline{d}} \cap k[X_1, ..., X_n] = (\mathrm{qf}(R))^{\overline{d}} \cap R \supseteq \mathrm{qf}(R^d) \cap R = R^d$$

where we used Lemmas 5.22 and 5.16, respectively. Let $D := \frac{\overline{d}}{\partial_n(f)}$. Then D is a $k(f)$-derivation since $k(X_1, ..., X_n)^D = k(X_1, ..., X_n)^{\overline{d}}$.

Now $X_1, X_2, ..., X_{n-1}, f$ are algebraically independent over k since $\partial_n(f) \neq 0$. So we have $k(X_1, ..., X_n)$ is an algebraic extension of $k(f)(X_1, ..., X_{n-1})$. Let D' denote the restriction of D to $k(f)(X_1, ..., X_{n-1})$. We have

$$D'(X_i) = \frac{\overline{d}(X_i)}{\partial_n(f)} = \frac{\partial_n(f)\Delta(X_i) - \Delta(f)\partial_n(X_i)}{\partial_n(f)} = \frac{\partial_n(f)\Delta(X_i)}{\partial_n(f)} = \delta(X_i)$$

for $1 \leq i \leq n-1$. Thus, D' is a $k(f)$-derivation mapping $k(f)[X_1, ..., X_{n-1}]$ to $k(f)[X_1, ..., X_{n-1}]$, and D' agrees with δ on the variables X_i. By Theorem 5.20, $k(f)[X_1, ..., X_{n-1}]^{D'} = k(f)$. We are assuming that $k(f)$ is algebraically closed in $k(X_1, ..., X_n)$, and hence by Lemma 5.23, $k(X_1, ..., X_n)^D = k(f)$. Since the field of constants of D and $\overline{d}$ are the same, we see that $k(X_1, ..., X_n)^{\overline{d}} = k(f)$. Then

$$\begin{aligned} R^d &\subseteq k(X_1, ..., X_n)^{\overline{d}} \cap R \\ &= k(f) \cap R \\ &= k[f] \end{aligned}$$

by Lemma 3.13. Having already proven the other inclusion, we have $k[f] = R^d$. □

Remarks.

1. The particular choice of derivation δ is not important. Any derivation δ' of $k(X_1, ..., X_{n-1})$ satisfying $k(X_1, ..., X_{n-1})^{\delta'} = k$ could have been used in this construction. See [24], Section 2, for some other such derivations.

2. In [24], a slightly stronger statement is proven: if we do not assume $k[f]$ to be integrally closed in R and use the same construction, we would have R^d is the integral closure of $k[f]$ in R.

3. This construction also generalizes. In [6], consideration of the more general system of the form $f - cw$ as c varies over k leads to the consideration of $k\left(\frac{f}{w}\right)$. In relation to this, the above construction can be suitably altered to yield a derivation of $k(X_1, ..., X_n)$ with field of constants exactly $k\left(\frac{f}{w}\right)$. Again, see [24].

5.5 A comparison between ranks

We are now ready to answer the main question of this chapter. Recall that we are working under the assumption that f is an irreducible element of $R \setminus k$ such that k is algebraically closed in $L = \mathrm{qf}(R/fR)$. Under this assumption, we know that both of the groups $U(A)/U(k)$ and $U(A^\sharp)/U(k^\sharp)$ are finitely-generated free Abelian groups. In Theorem 5.3, we presented a homomorphism

$$\psi : \frac{U(A^\sharp)}{U(k^\sharp)} \to \frac{U(A)}{U(k)}$$

with kernel

$$\frac{U(A^\sharp) \cap G}{U(k^\sharp)},$$

where $G = \{v \mid v \in A^\sharp \text{ and } N(v) \subset U(k) + P\}$. We now want to argue that this map ψ is a monomorphism.

Since we are assuming $f \notin k$, we can assume without loss of generality that $\partial_n(f) \neq 0$. Let d be the derivation given by Equation 5.1. Specifically, we will use the fact that d has the form $d = \partial_n(f)\Delta - \Delta(f)\partial_n$ where Δ was a derivation of $k[X_1, ..., X_n]$ with $\Delta(X_n) = 0$, as well as the fact that $R^d = k[f]$ by Theorem 5.24.

So we seek to understand elements of $(U(A^\sharp) \cap G)/U(k^\sharp)$. Let v be in $U(A^\sharp) \cap G$, and write v as $f^e g/p(f)$ for some $e \in \mathbb{Z}$, $p \in k[Y]$, and $g \in R \setminus fR$. Since v is in $U(A^\sharp)$, we have that $g|\alpha(f)$ for some $\alpha \in k[Y]$. Since $v \in G$, we have that $N(v) \subset U(k) + P$. Specifically, $g \in U(k) + P$, and so g can be written as $g = c + f\lambda$ for some $0 \neq c \in k$ and $\lambda \in R$. To show that ψ is a monomorphism, we will show that $Ker(\psi) = (U(A^\sharp) \cap G)/U(k^\sharp)$ is trivial. Remembering that $\psi(v) = \pi(g)U(k)$, it suffices to show that $\pi(g) \in U(k)$. Thus our main goal here is to show that, given some $g \in R \setminus fR$ for which there is $g', \lambda \in R$, $\alpha \in k[Y]$, and $c \in U(k)$ such that $gg' = \alpha(f)$ and $g = c + f\lambda$, it must be the case that g is in $U(k^\sharp)$. (In fact, since $g \in R$, we will show that $g \in k[f] \setminus \{0\}$.)

Lemma 5.25. *If $g \in R$ is a polynomial which divides (in R) an element of $k[f]$, then g is a Darboux polynomial of g.*

Proof. Since any polynomial in $k[f]$ is in R^d, it is certainly a Darboux polynomial of d. Thus, by Lemma 5.14, g is also a Darboux polynomial. □

Lemma 5.26. *The homomorphism*

$$\psi : \frac{U(A^\sharp)}{U(k^\sharp)} \to \frac{U(A)}{U(k)}$$

is one-to-one.

Proof. Let us consider the result of applying d to g. From the previous lemma, g is a Darboux polynomial, so $g|d(g)$, *i.e.*, there exists a $P \in R$ such that $gP = d(g)$. On the other hand, since we have written $g = c + f\lambda$, we can apply d to get $d(g) = d(f\lambda) = fd(\lambda)$. Thus, since $gcd(g, f) = 1$, we have $fg|d(g)$. Write $d(g) = fg\zeta$ for some $\zeta \in R$. So letting $deg_n(\beta)$ denote the X_n-degree of an element of $\beta \in R$, we have that $\deg_n(d(g)) = \deg_n g + \deg_n f + \deg_n \zeta$.

On the other hand, we calculate from the definition of d that

$$d(g) = \partial_n(f)\Delta(g) - \Delta(f)\partial_n(g).$$

Now since $\Delta(X_n) = 0$, we have that $deg_n(\Delta(g)) \leq deg_n(g)$ and $deg_n(\Delta(f)) \leq deg_n(f)$. Thus, both of the terms in this difference have X_n-degree at most $deg_n(f)+deg_n(g)-1$. Thus, $deg_n(d(g)) \leq deg_n(f) + deg_n(g) - 1$. Comparing this with the above, we must

have that $deg_n(\zeta) < 0$. Hence, $\zeta = 0$. But then $d(g) = fg\zeta = 0$, and we have $g \in R^d = k[f]$.

Thus, we have shown that $\ker \psi = (U(A^\sharp) \cap G)/U(k^\sharp)$ is trivial. Hence ψ is a monomorphism. □

This gives us the following theorem:

Theorem 5.27. *If k is algebraically closed in L, then*

$$\operatorname{rank}(U(A^\sharp)/U(k^\sharp)) \leq \operatorname{rank}(U(A)/U(k)).$$

Proof. If k is algebraically closed in L, then $k^\sharp$ is algebraically closed in $L^\sharp$ by Theorem 4.1. Thus, by Lemma 2.8, the groups $U(A)/U(k)$ and $U(A^\sharp)/U(k^\sharp)$ are both finitely-generated free Abelian groups. By Theorem 5.3 and Theorem 5.26, $U(A^\sharp)/U(k^\sharp)$ is isomorphic to a subgroup of $U(A)/U(k)$. The result follows. □

Having related the ranks of these two groups, we can finally answer Question 3, by combining the previous theorem with the Mixed Redset Theorem (2.11.)

Theorem 5.28 (Strong Redset Theorem)**.** *When k has characteristic 0, f is irreducible in R, and k is algebraically closed in L, then*

$$|\operatorname{redset}(f)| \leq \operatorname{rank}(U(A)/U(k)).$$

And, similarly, by combining with the Polyredset Theorem (3.6), we get

Theorem 5.29 (Weak Polyredset Theorem)**.** *When k has characteristic 0, f is irreducible in R, and k is algebraically closed in L, then*

$$|\operatorname{polyredset}(f)| \leq \operatorname{rank}(U(A)/U(k)).$$

We have called Theorem 5.28 "strong" because it improves the Redset Theorem (2.9), which guarantees only finiteness, by providing an actual bound on the size of $\operatorname{redset}(f)$. Of course, because of the relationship given in Theorem 5.27, we can see that the bound from the Mixed Redset Theorem is actually a better bound. For the same reason, Theorem 5.29 provides a weaker bound than the one from the Polyredset Theorem (3.6).

Chapter 6

Summary and Future Questions

In the previous chapters, we did the following:

1. We generalized the concept of redset(f) by considering the set of monic irreducible polynomials $\Gamma \in k[T]$ such that $\Gamma(f)$ is reducible in $k[X_1, ..., X_n]$. We saw in Theorem 3.6 that this set is bounded above in the same manner as redset(f).

2. We related the hypothesis of the Redset Theorem and that of the Mixed Redset Theorem by showing that k being algebraically closed in L implies that $k(f)$ is algebraically closed in $k(X_1, ..., X_n)$.

3. We found that the analog of the Mixed Redset Theorem is true in the original case, without mention of $k^\sharp$, etc. Specifically, assuming k to be algebraically closed in L and $\operatorname{char} k = 0$, we showed that $|\text{redset(f)}| \leq \operatorname{rank}(U(A)/U(k))$.

Here we mention some further questions that arise.

In Chapter 3, we found some bounds on polyredset(f). But some natural extensions seem apparent:

1. In Theorem 3.10, we showed that, for k a perfect field,

$$\{c \in k^* \mid c \text{ is a root of some } \Gamma \in \text{polyredset}(f)\} \subseteq \text{redset}(f)^*.$$

It seems natural, due to the obvious relationship between $c \in k^*$ and irreducible monic polynomials, to ask if the other inclusion is true. That is, can we say

that

$$\text{redset}(f)^* = \{c \in k^* \mid c \text{ is a root of some } \Gamma \in \text{polyredset}(f)\}?$$

Or, can we say that

$$\text{polyredset}(f) = \{\Gamma \in k[T] \mid \Gamma \text{ is minimal for some } c \in \text{redset}(f)^*\}?$$

There is one obvious case where this fails to hold–if f is irreducible but not absolutely irreducible, then $0 \in \text{redset}(f)^*$, but clearly this corresponds to no element in polyredset(f). So, if we add the condition that f is absolutely irreducible, do we have the equality? In any case where this equality holds, we would have redset$(f)^*$ is finite if and only if polyredset(f) is finite, which would vastly simplify the list of equivalences at the end of Chapter 3.

2. Are there any conditions on f that ensure polyuniset(f) is finite, or even empty? We know it is empty when $k^\sharp$ is algebraically closed in $L^\sharp$, but can we get away with a weaker condition to ensure finiteness? Again, when we know that polyuniset(f) is finite, it simplifies our understanding of the equivalences in Chapter 3.

3. In Theorem 3.20, we saw that, when k was infinite, the finiteness of redset(f) ensured that $U(A^\sharp)/U(k^\sharp)$ must be finitely-generated. The immediate question would be: does the same thing hold even when k is a finite field?

4. Continuing from the previous question, consider the case where k is a finite field. Take $k = \mathbb{Z}/3\mathbb{Z}$ and let $f = (X+Y)^2 + 1$ in $k[X,Y]$. Clearly, we have that $|\text{redset}(f)| \leq 3$, but $k(f)$ is not algebraically closed in $L^\sharp$ (because $X+Y$ is algebraic over $k(f)$). So when k is finite, the finiteness of redset(f) does *not* imply $k^\sharp$ is algebraically closed in $L^\sharp$. But we might still wonder: when k is infinite, does redset(f) being finite imply that $k^\sharp$ is algebraically closed in $L^\sharp$?

In Chapter 4, we answered the second question for any k. The natural question in this case is about the converse:

5. What can be said about the converse of Theorem 4.1? We noted at the end of that section that the converse is, in general, false. But recall that $k(f) = k(f-c)$

for any $c \in k$, while $A = R/fR \neq R/(f-c)R$ when $c \neq 0$. In fact, it can even be the case that $R/fR \ncong R/(f-c)R$; for instance, one may be a domain while the other is not. Let $A_c := R/(f-c)R$. If we assume that $k^\sharp$ is algebraically closed in $L^\sharp$, is it possible to say something about the number of $c \in k$ for which k is algebraically closed in $\mathrm{qf}(A_c)$? For some c, $f-c$ will not be irreducible, and hence A_c will not be an integral domain, but by the Mixed Redset Theorem, we see that there are only finitely many such, so $\mathrm{qf}(A_c)$ usually exists. Also, k being algebraically closed in A_c is equivalent to $f-c$ being absolutely irreducible. So can we count the number of $f-c$ which fail to be absolutely irreducible if we work under the assumption that $k^\sharp$ is algebraically closed in $L^\sharp$?

The third question in our paper was effectively answered, but only when we assume $\mathrm{char}(k) = 0$. Answering the question when $\mathrm{char}(k) = p > 0$ is also an interesting question. So we raise the following:

6. Does the Strong Redset Theorem (5.28) hold even when $\mathrm{char}(k) \neq 0$?

To attempt to modify the argument used in this paper, there are essentially two issues:

7. Lemma 5.14 used the fact that $\mathrm{char}(k) = 0$. So for this same argument to work more generally, there either needs to be some restriction on what types of polynomials are under consideration, or a significantly different argument is needed to show that divisors of the Darboux polynomials we are interested in are still Darboux. Can such a thing be done?

8. The second part where $\mathrm{char}(k)$ needed to be 0 (in our argument) was in the construction of the derivation d with $R^d = k[f]$. When $\mathrm{char}(k) = p \neq 0$, no such derivation exists. However, is it possible to construct a *higher derivation* that gives the same sort of control supplied by d?

Bibliography

[1] Sheeram S. Abhyankar. *Ramification Theoretic Methods in Algebraic Geometry*. Princeton University Press, 1959.

[2] Sheeram S. Abhyankar. Historical ramblings in algebraic geometry and related algebra. *American Mathematical Monthly*, 83:409–448, 1976.

[3] Sheeram S. Abhyankar. *Algebraic Geometry for Scientists and Engineers*. American Mathematical Society, 2000.

[4] Sheeram S. Abhyankar. *Lectures on Algebra, Vol 1*. World Scientific Publishing Co, 2006.

[5] Sheeram S. Abhyankar, William Heinzer, and Paul Eakin. On the uniqueness of the coefficient ring in a polynomial ring. *Journal of Algebra*, 23:310–342, 1972.

[6] Sheeram S. Abhyankar, William J. Heinzer, and Avinash Sathaye. Translates of polynomials. In *A Tribute to Seshadri: Perspectives in Geometry and Representation Theory*, pages 51–124. Birkhauser-Verlag, Boston, 2000.

[7] David A. Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Springer, 2005.

[8] H. G. H. Derksen. The kernel of a derivation. *J. Pure Appl. Algebra*, 84:13–16, 1993.

[9] Gunter Harder. *Lectures on Algebraic Geometry 1: Sheaves, Cohomology of Sheaves, and Applications to Riemann Surfaces*. American Mathematical Society, 2008.

[10] Robin Hartshorne. *Algebraic Geometry*. Springer-Verlag, 1977.

[11] Thomas W. Hungerford. *Algebra*. Springer, 2000.

[12] Harry C. Hutchins. *Examples of Commutative Rings*. Polygonal Publishing House, 1981.

[13] Irving Kaplansky. *Fields and Rings*. University of Chicage Press, 1973.

[14] Irving Kaplansky. *Commutative Rings*. Polygonal Publishing House, 1974.

[15] Anthony W. Knapp. *Advanced Algebra*. Birkhauser Boston, 2007.

[16] Solomon Lefschetz. *Algebraic Geometry*. Dover Publications, 2005.

[17] Andrzej Nowicki. On the jacobian equation $j(f, g) = 0$ for polynomials in $k[x, y]$. *Nagoya Math Journal*, 109:151–157, 1988.

[18] Andrzej Nowicki. Rings and fields of constants for derivations in characteristic zero. *Journal of Pure and Applied Algebra*, 96:47–55, 1994.

[19] Andrzej Nowicki and Masayoshi Nagata. Rings of constants for k-derivations in $k[x_1, ..., x_n]$. *J. Math. Kyoto Univ.*, 28:111–118, 1988.

[20] Jean Moulin Ollagnier, Andrzej Nowicki, and Jean-Marie Strelcyn. On the non-existence of constants of derivations: The proof of a theorem of jouanolou and its development. *Bulletin des Sciences Mathematiques*, 119:195–233, 1995.

[21] Daniel Perrin. *Algebraic Geometry: An Introduction*. Springer, 2007.

[22] O.F.G. Schilling and Oscar Zariski. On the linearity of pencils of curves on algebraic surfaces. *American Journal of Mathematics*, 80:320–324, 1958.

[23] Satoshi Suzuki. Some types of derivations and their applications to field theory. *J. Math Kyoto U.*, 21-2:375–382, 1981.

[24] Arno van den Essen, Jean Moulin Ollagnier, and Andrzej Nowicki. Rings of constants of the form k[f]. *Communications in Algebra*, 34:3315–3321, 2006.

[25] Abraham Zaks. Dedekind subrings of $k[x_1, ..., x_n]$ are rings of polynomials. *Israel Journal of Math*, 9:285–289, 1971.

[26] Oscar Zariski. Pencils on an algebraic variety and a new proof of a theorem of bertini. *Transactions of the AMS*, 50:48–70, 1941.

[27] Oscar Zariski. *An Introduction to the Theory of Algebraic Surfaces, 2nd ed.* Springer-Verlag, 1972.

[28] Oscar Zariski and Pierre Samuel. *Commutative Algebra, Volume 1.* D. Van Nostrand Co., 1958.

[29] Oscar Zariski and Pierre Samuel. *Commutative Algebra, Volume 2.* D. Van Nostrand Co., 1958.

Vita

Jacob Andrew Ogle was born in Knoxville, Tennessee, on August 27, 1981. He started at Lee University in 1999. After changing his major many times, he ended up studying mathematics. He continued on to the University of Tennessee, where he graduated with a Ph.D. in mathematics in 2011. As of this writing, he has a lovely wife but no lovely children.