ROSE-
HULMAN
UNDERGRADUATE
MATHEMATICS
JOURNAL

IRREDUCIBILITY AND FACTORS OF POLYNOMIALS IN NOETHERIAN INTEGRAL DOMAINS

Benjamin E. Anzis[a]

VOLUME 15, NO. 2, FALL 2014

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]University of Idaho

ROSE-HULMAN UNDERGRADUATE MATHEMATICS JOURNAL
VOLUME 15, NO. 2, FALL 2014

IRREDUCIBILITY AND FACTORS OF POLYNOMIALS IN NOETHERIAN INTEGRAL DOMAINS

Benjamin E. Anzis

Abstract. Let R be a Noetherian integral domain, and let f be a polynomial with coefficients in R. A question of great importance is whether f is irreducible. In this paper, we give a sufficient condition for f to be irreducible by looking at the content ideal of f. This result is then extended to show a connection between the height of a polynomial's (proper) content ideal and the maximal number of irreducible factors it can possess.

Acknowledgements: The author is grateful to the referees for their valuable input and corrections, which improved the exposition of the paper.

1 Introduction

When dealing with a polynomial, a question of great interest is whether it is irreducible over a certain ring. Recall that a polynomial f is irreducible over a ring R if, whenever f is written as a product

$$f = g \cdot h$$

with $g, h \in R[t]$, then either g or h is a unit. The notion of irreducibility is of great importance in several areas of mathematics, notably cryptography, since irreducible polynomials play a role in R analogous to that of primes in the integers, $\mathbb{Z}$. Because of that connection, cryptosystems (most notably RSA) based upon the difficulty of factoring large numbers have "cousin" cryptosystems based upon the difficulty of factoring complicated polynomials into irreducibles over a ring. As well, irreducible polynomials are used to build finite fields, which are essential for elliptic curve cryptography.

Gauss was the first to introduce irreducible polynomials as objects of study in connection with primitive polynomials. He subsequently proved a lemma bearing his name, which states that if a polynomial in $\mathbb{Z}[t]$ is irreducible over $\mathbb{Z}[t]$ then it is irreducible over $\mathbb{Q}[t]$. Since then, finding ways to test whether a polynomial is irreducible has garnered much attention from mathematicians. A notable example of such a test is Eisenstein's criterion, which establishes a test for irreducibility over $\mathbb{Q}[t]$, and uses Gauss' Lemma.

It is well-known that in a ring R a polynomial $a + bt \in R[t]$ is irreducible over R if and only if a and b do not share a common factor. This suggests a connection between "independence" of the coefficients of a polynomial (which we measure by taking the height of the content ideal of the polynomial) and the irreducibility of that polynomial. In this paper, we prove such a connection for polynomials of higher degree over an arbitrary Noetherian integral domain and then extend it to show an even larger link between this "independence" and the maximal possible number of irreducible factors in any factorization of the polynomial.

In section 2, we provide background from commutative algebra. In section 3, we prove a preliminary result concerning the irreducibility of a specific class of polynomials which we then extended in section 4 to provide an upper bound on the number of irreducible factors any polynomial possesses in any factorization. Finally, in section 5, we provide example uses of the main results in section 3 and 4.

2 Background

We assume the basics of abstract algebra. For the necessary background, we refer the reader to the text by Hungerford [2]. We also make use of the following concepts from commutative algebra. For more detail, we refer the reader to the text by Sharp [3].

Definition 2.1. *A ring R is said to be Noetherian if, for any chain of ideals*

$$J_1 \subseteq J_2 \subseteq \cdots$$

in R, there exists an $i \in \mathbb{N}$ so that $J_i = J_{i+n}$ for all $n \in \mathbb{N}$.

Definition 2.2. *The radical of an ideal I in a commutative ring R, denoted $\sqrt{I}$, is the set*

$$\sqrt{I} = \{a \in R : a^m \in I \text{ for some } m \in \mathbb{N}\}.$$

It is also an ideal of R.

Definition 2.3. *The variety of an ideal I in a ring R, denoted $Var(I)$, is the set*

$$Var(I) = \{P \text{ a prime ideal of } R \mid P \supset I\}.$$

Definition 2.4. *The height of an ideal I, denoted $ht(I)$, is defined to be*

$$ht(I) = \min_{P \in Var(I)} ht(P),$$

where $ht(P)$ for P prime is the maximum length n of a chain of prime ideals

$$P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n \subsetneq P.$$

Definition 2.5. *The content ideal of a polynomial $f = a_0 + \cdots + a_n t^n \in R[t]$, written $cont(f)$, is the ideal*

$$cont(f) = \langle a_0, \ldots, a_n \rangle \subseteq R.$$

Theorem 2.6 (Krull's Generalized Principal Ideal Theorem)**.** *(See [3, Theorem 15.4]) Let R be a commutative Noetherian ring and let I be a proper ideal of R which can be generated by n elements. Then $ht(I) \leq n$.*

3 Preliminary Result

In this section, we prove a preliminary result that shows a certain class of polynomials are irreducible.

Let $f = a_0 + \cdots + a_n t^n \in R[t]$ be a polynomial of degree $n \geq 1$, where R is a Noetherian integral domain. Let $cont(f) = \langle a_0, \ldots, a_n \rangle$ be the content ideal of f.

Proposition 3.1. *If $ht(cont(f)) = n + 1$, then f is irreducible over R.*

Remark 3.2. Note that $ht(cont(f)) = n + 1 \geq 2$ implies that $cont(f)$ is a proper ideal.

Proof. Assume that f is reducible over R. Then there exists $g = b_0 + b_1 t + \cdots + b_p t^p$ and $h = c_0 + c_1 t + \cdots + c_q t^q \in R[t]$ neither of which is a unit (with $b_q, c_p \neq 0$) such that

$$f = g \cdot h.$$

We will establish a contradiction after proving the following claims.

Claim 1: $p, q \leq n - 1$.

Assume without loss of generality that $q = n$. Then, since R is an integral domain, $p = 0$ and therefore

$$f = a_0 + a_1t + \cdots + a_nt^n = b_0(c_0 + c_1t + \cdots + c_nt^n).$$

Then, $cont(f) \subset \langle b_0 \rangle$ and hence $ht(cont(f)) \leq 1$ by Theorem 2.6. Therefore, $ht(cont(f)) = n + 1 \leq 1$, so $n = 0$, contradicting the assumption that $n \geq 1$.

Claim 2: $\sqrt{cont(f)}$ is a proper ideal of R.

If $\sqrt{cont(f)} = R$, then $1 \in \sqrt{cont(f)}$. Hence, for some $n_1 \in \mathbb{Z}_{\geq 1}$, $1^{n_1} = 1 \in cont(f)$, and so $cont(f)$ is not a proper ideal. This contradicts the assumption that $ht(cont(f)) = n + 1$.

Claim 3 (Gauss' Lemma [1, Exercise 3.4]): $cont(g) \cdot cont(h) \subseteq \sqrt{cont(f)}$.

By ([3, Lemma 3.48]),

$$\sqrt{I} = \bigcap_{P \in Var(I)} P.$$

For every prime ideal P of R, $P[t]$ is a prime ideal of $R[t]$. If $cont(f) \subseteq P$, then $f = g \cdot h \in P[t]$ and hence $g \in P[t]$ or $h \in P[t]$. Therefore $cont(g) \subseteq P$ or $cont(h) \subseteq P$, so $cont(g) \cdot cont(h) \subseteq P$. Since this is true for arbitrary $P \supseteq cont(f)$,

$$cont(g) \cdot cont(h) \subseteq \bigcap_{P \in Var(I)} P = \sqrt{I}.$$

Now, we return to the proof of the proposition. From Claims 2 and 3, we have that one of $cont(g)$ or $cont(h)$ is a proper ideal of R. For otherwise $1 \cdot 1 = 1 \in cont(g) \cdot cont(h) \subseteq \sqrt{cont(f)}$, contradicting Claim 2.

Assume without loss of generality that $cont(g) \subsetneq R$. Since $cont(f) \subseteq cont(g)$, we have $ht(cont(f)) \leq ht(cont(g))$. However, $ht(cont(g)) \leq p + 1$ by Krull's Generalized Principal Ideal Theorem. Therefore,

$$ht(cont(f)) = n + 1 > \deg(g) + 1 = p + 1 \geq ht(cont(g)) \geq ht(cont(f)),$$

a contradiction. Recall that the first equality is by hypothesis. Hence, there does not exist such g, and therefore f is irreducible over R. □

Remark 3.3. 1) If f were allowed to have degree $n = 0$ in the statement of the proposition, $f = a^2 \in R[t]$, for some non-unit $0 \neq a \in R$, would satisfy the conditions of this result, as $cont(f) = \langle a^2 \rangle \subset R$ has height equal to 1. Obviously f is reducible in $R[t]$, so the condition that $deg(f) \geq 1$ is necessary for f to be irreducible.

2) In the proposition, note that $cont(f)$ is required to be a complete intersection of full (maximum) height, that is, it is generated by $ht(cont(f))$ elements of R. This is maximal, since by Theorem 2.6, $ht(cont(f)) \leq \deg(f) + 1$, and Proposition 3.1 requires equality. Let $f = x^2 - y^2t^2 \in R[x, y][t]$. Note that $cont(f) = \langle x^2, y^2 \rangle$, which is a complete intersection of height 2. However, f is reducible over $R[x, y]$, since $f = (x + yt)(x - yt)$. Therefore, the condition that $cont(f)$ be a complete intersection of full height is necessary for f to be irreducible.

4 Main Result

The next result is an extension of Proposition 3.1.

Theorem 4.1. *$f = a_0 + \cdots + a_n t^n \in R[t]$ be a polynomial of degree $n \geq 1$, where R is a Noetherian integral domain. Suppose $ht(cont(f)) = \ell$ with $\ell \geq 2$. Then any factorization of f into irreducible factors has at most $n - \ell + 2$ terms.*

Proof. We will prove this theorem by proving that f possesses an irreducible factor of degree $\geq \ell - 1$.

If f is irreducible, then it is such a factor. Therefore, assume that f is reducible. Then, there exists $g_1, h_1 \in R[t]$ not units such that

$$f = g_1 \cdot h_1.$$

By the argument of Proposition 3.1, one of $cont(g_1)$ or $cont(h_1)$ is a proper ideal of R. Assume without loss of generality that $cont(g_1) \subsetneq R$. Then $ht(cont(f)) = \ell \leq ht(cont(g_1))$, since $cont(f) \subseteq cont(g_1)$.

If g_1 is irreducible, then it is an irreducible factor of f with $ht(cont(g_1)) \geq \ell$ so that by Theorem 2.6, $\deg(g_1) \geq \ell - 1$.

On the other hand, if g_1 is reducible, then applying the same argument used above to g_1 yields g_2 such that $g_1 = g_2 \cdot h_2$ with $cont(g_2) \subsetneq R$ and $ht(cont(g_2)) \geq ht(cont(g_1)) \geq \ell$. Again, assume that g_2 is reducible (for otherwise, it would be the irreducible factor of f we are looking for); then, repeatedly applying the same argument gives g_{j+1} where $g_j = g_{j+1} \cdot h_{j+1}$ with $cont(g_{j+1}) \subsetneq R$ and $ht(cont(g_{j+1})) \geq ht(cont(g_j))$.

Consider the sequence $\{\deg(g_1), \deg(g_2), \ldots\}$. Clearly, this is a monotonic decreasing sequence that it is bounded below by $\ell - 1$, i.e.

$$\deg(g_j) \geq \deg(g_{j+1}) \geq \cdots \geq \ell - 1.$$

By the Monotone Convergence Theorem, this sequence converges, say at the index k. Then, since R is an integral domain,

$$\deg(g_k) = \deg(g_{k+1}) + \deg(h_{k+1}),$$

so $\deg(h_{k+1}) = 0$. Hence, $h_{k+1} = r \in R$.

If r is not a unit, then $\ell = ht(cont(f)) \leq ht(\langle r \rangle) \leq 1$, contradicting the assumption $\ell \geq 2$. Therefore, h_{k+1} is a unit and g_k is not reducible. Hence g_k is an irreducible factor of f of degree $\geq \ell - 1$.

To conclude the proof, note that the condition $\ell \geq 2$ ensures that all irreducible factors of f have degree ≥ 1. Hence, the number of terms in any factorization of f into irreducibles is $\leq n - \deg(g_k) + 1$, which is $\leq n - \ell + 2$. □

5 Two Examples

Example 5.1. *Consider the polynomial*

$$f = (x + 1) + (y + 2)t + 2(x + y + 3)t^2 + 4zt^3 \in R[t]$$

where $R = \mathbb{Z}[x, y, z]$. *Then*

$$cont(f) = \langle x + 1, y + 2, 2(x + y + 3), 4z\rangle = \langle x + 1, y + 2, 4z\rangle.$$

Now, $\langle x+1, y+2, 4z\rangle \subsetneq \langle x+1, y+2, 2z\rangle \subsetneq \langle x+1, y+2, z\rangle$ *is a chain of ideals of maximum length, since* $\frac{\langle x+1,y+2,z\rangle}{\langle x+1,y+2,2z\rangle} \cong \frac{\langle x+1,y+2,2z\rangle}{\langle x+1,y+2,4z\rangle} \cong \mathbb{Z}/2\mathbb{Z}$*, a field. Hence,* $ht(cont(f)) = ht(\langle x + 1, y + 2, z\rangle) = 3$*, since* $\langle x + 1, y + 2, z\rangle$ *is the only prime ideal in the chain.*

Since $\mathbb{Z}$ *is a unique factorization domain and therefore every factorization of* f *into irreducibles is the same,* f *has at most* 2 *irreducible factors by Theorem 4.1.*

Example 5.2. *Consider the polynomial* $g = x + yt + zt^2$ *in the same integral domain as before. Then,* $ht(cont(g)) = 3$*, since* $\langle x, y, z\rangle$ *is a maximal (and therefore prime) ideal of height 3. Because* $\deg(g) + 1 = 3$*,* g *is irreducible by Proposition 3.1.*

References

[1] Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry*. New York, US: Springer-Verlag.

[2] Hungerford, T. (2003). *Algebra*. New York, US: Springer-Verlag.

[3] Sharp, R. Y. (2000). *Steps in commutative algebra (2nd ed.)*. Cambridge, UK: Cambridge University Press.