Similarities Between Integers and Polynomials

STUDENT NAME

DATE

Contents

Abstract

There are many analogies between the integers and polynomials. In this paper, we will prove several results in the integers and provide their analogous statements for polynomials. The topics we will cover include the Division Algorithm and the Euclidean Algorithm as well as how to construct fields using integers and polynomials. We will also discuss some algebraic properties of both structures.

1 Introduction

To understand a mathematical result or idea, it is often helpful to view that idea in an analogous setting. If we are able to understand a simpler analogous idea, we can apply this perspective to the original idea to help us understand the more complex analog. As an example of this methodology, to help work with results related to the integers, it can be helpful to work with analogous results related to polynomials.

During his UConn Math Club talk, Robert McDonald proved theorems for polynomials that are analogous to Fermat's Last Theorem and the abc Conjecture ([McD]), which are a very famous theorem and conjecture, respectively, for integers. The proofs of the polynomial analogs are relatively simple and can be completed in about a paragraph. Fermat's Last Theorem, which was originally conjectured by Pierre de Fermat in 1637, is stated as follows ([Wikb]).

Theorem 1.1 (Fermat's Last Theorem, as stated in [Wikb])**.** *There do not exist positive integer solutions a, b, and c of the equation $a^n + b^n = c^n$ for any integer $n > 2$.*

Surprisingly, it took over 350 years to find a correct proof of Fermat's Last Theorem ([Sin]). After over a year to correct a discovered error, Andrew Wiles presented the first correct proof of Fermat's Last Theorem in 1995 ([Wil95]).

The abc Conjecture, which was originally conjectured by David Masser in 1985 and William Osterlé in 1988 and whose potential proof is yet to be resoundingly confirmed, is stated as follows ([Wika]).

Conjecture 1.2 (The abc Conjecture, as stated in [Wika])**.** *For every $\epsilon > 0$, there exists only finitely many triples (a, b, c) of relatively prime positive integers a, b, and c such that $a + b = c$ and*

$$c > rad(abc)^{1+\epsilon},$$

where $rad(abc)$ is the product of distinct prime factors of abc.

It can also be helpful to adapt solution methods from one area to the other. For example, to find the greatest common divisor of two polynomials, we can adapt the method of finding the greatest common divisor of two integers to the polynomial case, which we will see in this paper. For these reasons, when dealing with problems in one area, it is often useful to keep the other in mind.

Our goal in this paper is to illustrate some of the similarities between the integers and polynomials with coefficients in a field by presenting results in the integers that have analogous statements for polynomials. In particular, we will discuss how to extend the Division Algorithm and the Euclidean Algorithm for integers to similar results for polynomials. We also discuss how to extend to polynomials the notion of extending the family of integers to a field, first through considering the family of integers modulo a prime and, second, the through constructing a field of fractions, which yields the family of irrational numbers in the case of integers. By highlighting connections between results for integers and results for polynomials, we hope to highlight the power of adapting results in one setting to another.

The remainder of this paper is organized as follows. In Section 2, we will cover results in the set of integers $\mathbb{Z}$ that have analogous statements in the set of polynomials $\mathbb{F}[T]$ in the variable T over a field $\mathbb{F}$. In Section 2.1, we will prove the Division Algorithm as well as provide the statement of the Euclidean Algorithm. Then, in Section 2.2, we will give examples of how to construct finite fields using integers as well as how to construct a familiar field of infinite order, namely $\mathbb{Q}$, using integers. Finally, in Section 2.3, we will discuss some of the algebraic properties of $\mathbb{Z}$. In Section 3, we will discuss statements in $\mathbb{F}[T]$ that are analogous to ones provided in Section 2.

2 The Integers

We begin by presenting various well known results about and constructions using integers. The main results of this section, which include both using the Division Algorithm and the Euclidean Algorithm to find the greatest common divisor of two integers and using the construction of the field of integers modulo a prime and the field of the rational numbers from the family of integers, will have analogous results for polynomials later in this paper.

2.1 The Division Algorithm and the Euclidean Algorithm

In this section, our goal is to present the Euclidean algorithm for finding the greatest common divisor of two integers. We will not prove that the Euclidean algorithm works, but we will provide proofs of the Division algorithm and another proposition which when combined, make it clear that the Euclidean algorithm is true.

We will assume that the reader is familiar with the concept of the greatest common divisor of two integers.

Theorem 2.1 (Division Algorithm from [GV05])**.** *If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique integers q and r such that*

$$a = bq + r \quad \textit{where} \quad 0 \leq r < b.$$

Proof. ([GV05]) Let $a, b \in \mathbb{Z}$ such that $b > 0$. Consider the set $S = \{\dots, a - 2b, a - b, a, a + b, \dots\}$. Note that S must contain non-negative integers. If $a \geq 0$, this is clear because $a \in S$. If $a < 0$, then $a - ab = (-a)(b - 1) \geq 0$ because $-a > 0$ and $b > 0$ implies $b - 1 \geq 0$. Hence, $a - ab \in S$ is non-negative and we have that S contains non-negative integers. Let S' be the subset of S containing only non-negative integers. By the Well-Ordering Principle, there is a smallest element of S'. Call this smallest element r and let $q \in \mathbb{Z}$ be the integer such that $a - qb = r$. We must now show $r < b$. Suppose $r \geq b$. Then since $a - qb = r$, we would have $r - b = a - qb - b = a - (q + 1)b$. Hence, $r - b$ is a non-negative integer of the form $a - nb$ where $n \in \mathbb{Z}$, so $r - b \in S'$. However, since $b > 0$, $r - b < r$, which contradicts the fact that r is the smallest non-negative integer in S'. Therefore, there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$. To prove q and r are unique, suppose we have $a = q_1 b + r_1 = q_2 b + r_2$ with $0 \leq r_1, r_2 < b$. Suppose for the sake of contradiction that $r_1 \neq r_2$. Then without loss of generality, suppose $r_2 > r_1$. It follows that $0 < r_2 - r_1 < b$. Since we have $q_1 b + r_1 = q_2 b + r_2$, we get $r_2 - r_1 = (q_1 - q_2)b$. Thus, $b | (r_2 - r_1)$ and we have $b \leq r_2 - r_1$. This contradicts the fact that $r_2 - r_1 < b$. Therefore, $r_2 = r_1$. It follows that $(q_1 - q_2)b = 0$. Since $b > 0$ by assumption, we have $q_1 - q_2 = 0$ and so $q_1 = q_2$. Hence, the integers q and r are unique. □

Our next proposition is very helpful in understanding why the Euclidean Algorithm works.

Proposition 2.2. (Proposition 2.21 from [GV05]) *If $a = qb + r$ where $a, b, q, r \in \mathbb{Z}$, then* $\gcd(a, b) = \gcd(b, r)$.

Proof. ([GV05]) Suppose $d = \gcd(a, b)$. Then since $a = qb+r$, we have $r = a-qb$. Therefore, $d|r$ because $d|a$ and $d|b$. It follows that d is a common divisor of b and r. Now suppose $c = \gcd(b, r)$. Then $d \leq c$ as d is a common divisor of b and r. Also, we have $c|a$ from the equation $a = qb + r$. Thus, c is a common divisor of both a and b. It follows that $c \leq d$ as $d = \gcd(a, b)$. Since $d \leq c \leq d$, we have $\gcd(a, b) = d = c = \gcd(b, r)$. □

Repeatedly using Theorem 2.1 and Proposition 2.2, we come to the Euclidean algorithm.

Theorem 2.3 (Euclidean Algorithm from [GV05])**.** *Let $a, b \in \mathbb{Z}$ such that $b \neq 0$. If $b|a$, then* $\gcd(a, b) = |b|$. If b does not divide a, then $\gcd(a, b) = r_n$, the last non-zero remainder in the following list of equations obtained from Theorem 2.1.

$$\begin{aligned}
a &= q_1 b + r_1 \quad \text{where} \quad 0 < r_1 < |b| \\
b &= q_2 r_1 + r_2 \quad \text{where} \quad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 \quad \text{where} \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \quad \text{where} \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Instead of providing a proof of the Euclidean algorithm, we will give an example of how one would go about computing the greatest common divisor of two integers using the algorithm.

Example 2.4. Using Theorem 2.3, we will find the greatest common divisor of 484 and 451.

$$\begin{aligned}
484 &= 451 \cdot 1 + 33 \\
451 &= 33 \cdot 13 + 22 \\
33 &= 22 \cdot 1 + 11 \\
22 &= 11 \cdot 2 + 0
\end{aligned}$$

Therefore, $\gcd(484, 451) = 11$ by Theorem 2.3.

2.2 Constructing Fields Using Integers

We would now like to show that we can construct fields of different orders from the integers using modular arithmetic and equivalence classes. In order to show this, we will need the definition of a field. However, our definition of a field relies on knowing what a group is, so our first task is familiarizing ourself with the notion of a group.

Definition 2.5. (Definition 3.1.4 from [BB06]) Let G be a nonempty set with a single binary operation $*$. We say $(G, *)$ is a **group** if the followng hold:

- For all $a, b \in G$, $a * b \in G$.

- For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
- There exists $e \in G$ such that $a * e = e * a = a$ for every $a \in G$.
- For every $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

If $a * b = b * a$ for all $a, b \in G$, we say that $(G, *)$ is an **abelian group**.

We are now able to define the notion of a field in terms of groups.

Definition 2.6. (Definition 3.3.5 from [BB06]) Let F be a set with two binary operations $+$, $\cdot$, with respective identity elements 0 and 1. If $0 \neq 1$, then F is called a **field** if the following hold:

- The set F is an abelian group under $+$.
- The non-zero elements of F form an abelian group under $\cdot$.
- For all $a, b, c \in \mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Our next two sections deal with the actual constructions of both finite fields and the rational numbers.

2.2.1 Finite Fields

Using modular arithmetic, the equivalence classes of the integers modulo a prime number create a field of finite order. This is stated more formally in the following theorem.

Theorem 2.7. *Define $+$ and $\cdot$ to be ordinary addition and multiplication of equivalence classes. Then $\mathbb{Z}_m$ with binary operations $+$ and $\cdot$ is a field if and only if m is prime.*

Proof. ($\Longleftarrow$) It is easy to check that $\mathbb{Z}_m$ is an abelian group under $+$ for any $m \in \mathbb{N}$. Also, to check the non-zero elements of $\mathbb{Z}_m$ form an abelian group under $\cdot$, we will only show that for every $a \in \mathbb{Z}_m$, there exists $a^{-1} \in \mathbb{Z}_m$ such that $a \cdot a^{-1} = 1$. We know that $\cdot$ is associative, $\mathbb{Z}_m$ is closed under $\cdot$, and that the multiplicative identity, 1, is in $\mathbb{Z}_m$. Suppose $a \in \mathbb{Z}_m$. Then $a^{m-1} = 1$ by Fermat's Little Theorem. Thus, a^{m-2} is the multiplicative inverse of a in $\mathbb{Z}_m$. We know $a^{m-2} \in \mathbb{Z}_m$ since this set is closed under $\cdot$. Finally, we know that addition and subtraction obey the distributive laws.
($\Longrightarrow$) To show the forward direction, we will prove the contrapositive. Suppose $m \in \mathbb{Z}^+$ is composite. Then $m = nk$ for $n, k \in \mathbb{Z}^+$. Therefore, $n < m$ and $k < m$ where $n, k \neq 0$. Hence, n and k are non-zero elements in $\mathbb{Z}_m$. However, $nk = m = 0$ in $\mathbb{Z}_m$. Thus, the non-zero elements in $\mathbb{Z}_m$ are not closed under $\cdot$ if m is composite. Hence, the non-zero elements of $\mathbb{Z}_m$ do not form an abelian group under $\cdot$ and $\mathbb{Z}_m$ is not a field. □

Next, we will show how we can formally construct the rational numbers using equivalence classes.

2.2.2 Constructing the Rational Numbers

We want to define the rational numbers in terms of equivalence classes of a specific equivalence relation. To achieve this goal, we will first define a relation and then show it is in fact an equivalence relation.

Definition 2.8. ([GV05]) Define the relation $\sim$ on the set $\mathbb{Z} \times \mathbb{Z} - \{0\}$ by $(a, b) \sim (c, d)$ if and only if $ad = bc$.

We will want to show that the relation $\sim$ is an equivalence relation. We must show that $\sim$ is reflexive, transitive, and symmetric.

Theorem 2.9. *The relation $\sim$ from Definition 2.8 is an equivalence relation.*

Proof. Let $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{0\}$. Since integer multiplication is commutative, we know that $ab = ba$ and we have $(a, b) \sim (a, b)$. Now let $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z} - \{0\}$ and suppose $(a, b) \sim (c, d)$. Then we have $ad = bc$. Thus, $da = cb$ and we can conclude that $(c, d) \sim (a, b)$. Finally, suppose $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z} - \{0\}$ such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. We want to show that $(a, b) \sim (e, f)$. Since $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, we know that $ad = bc$ and $cf = de$. Therefore, we have $adf = bcf$ as well as $bcf = bde$. Thus, $adf = bde$. Since $d \neq 0$, we have $af = be$ and by definition, $(a, b) \sim (e, f)$. Since $\sim$ is reflexive, symmetric, and transitive, $\sim$ is an equivalence relation. □

Now that we know $\sim$ is an equivalence relation, we can define two operations, $+$ and $\cdot$, on the set of equivalence classes of $\sim$. For $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z} - \{0\}$, define $+$ by $(a, b) + (c, d) = (ad + bc, bd)$. Define $\cdot$ by $(a, b) \cdot (c, d) = (ac, bd)$. We now have a set on which two binary operations are defined. We will not check that $+$ and $\cdot$ are well-defined, but this is not difficult. We now have what is required to define $\mathbb{Q}$ as a field.

Definition 2.10. Define the rational numbers, denoted $\mathbb{Q}$, to be the set of equivalence classes of $\sim$ from Definition 2.8 with the binary operations $+$ and $\cdot$ defined above.

We will not prove that $\mathbb{Q}$ is a field. However, we will later see that there is an analogous construction in $\mathbb{F}[T]$ to the one outlined above.

2.3 Algebraic Properties of the Integers

Finally, we will discuss some of the algebraic properties of $\mathbb{Z}$. The integers are what is known as a ring. A ring is a field without the requirement that every non-zero element must have a multiplicative inverse. A more formal definition is given below.

Definition 2.11. (Definition 5.1.2 from [BB06]) Let R be a set on which two binary operations, $+, \cdot$, are defined. Then R is called a **commutative ring** if the following properties hold:

- The set R is an abelian group under $+$.

- The operation $\cdot$ is associative and commutative.
- The set R has an identity element under $\cdot$.
- For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

From this definition, it is clear that $\mathbb{Z}$ is a ring. We know that it cannot be a field because if it were, then an element such as $2 \in \mathbb{Z}$ would have a multiplicative inverse. So there would exist $a \in \mathbb{Z}$ such that $2 \cdot a = 1$, which we know is not possible. Thus, the non-zero elements of $\mathbb{Z}$ do not form an abelian group under $\cdot$ and $\mathbb{Z}$ cannot be a field. However, there is one more important algebraic property that $\mathbb{Z}$ has in common with fields.

Definition 2.12. (Definition 5.1.7 from [BB06]) A commutative ring R is said to be an **integral domain** if $1 \neq 0$ and for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

From experience, we know that if $ab = 0$ where $a, b \in \mathbb{Z}$, then $a = 0$ or $b = 0$. Thus, $\mathbb{Z}$ is an integral domain. However, not every ring is an integral domain. Consider the ring $\mathbb{Z}_4$. In $\mathbb{Z}_4$, $2 \neq 0$ but $2 \cdot 2 = 4 = 0$ in $\mathbb{Z}_4$. So $\mathbb{Z}_4$ is a ring that is not an integral domain.

We would like to prove one additional algebraic property that the integers have related to ideals. First, we will define the notion of an ideal.

Definition 2.13. (Definition 5.3.1 from [BB06]) Let R be a commutative ring. A nonempty subset $I \subset R$ is called an **ideal** of R if the following hold:

- For all $a, b \in I$, $a \pm b \in I$.
- If $a \in I$ and $r \in R$, then $ar \in I$.

For $a \in R$, define $(a) := \{ab | b \in R\}$. An ideal I is called **principal** if $I = (a)$ for some $a \in R$.

We now have all we need to prove our final algebraic property related to the integers.

Theorem 2.14 (Theorem 2.1 from [Conb])**.** *In $\mathbb{Z}$, all ideals are principal.*

Proof. ([Conb]) Let I be an ideal in $\mathbb{Z}$. If $I = \{0\}$ then $I = (0)$ is principal. Suppose $I \neq \{0\}$. Let $a \in I$ with $a \neq 0$ such that for all $b \in I$ with $b \neq 0$, $|a| \leq |b|$. Then clearly, $(a) \subset I$. We must show that $I \subset (a)$. Let $b \in I$. By Theorem 2.1, there exist $q, r \in \mathbb{Z}$ such that $b = aq + r$ and $0 \leq r < |a|$. Thus, $r = b - aq$. Since $a \in I$, we know that $aq \in I$. Therefore, since $b \in I$, we have $b - aq \in I$. So $r \in I$. We also have $|r| < |a|$. If $r \neq 0$, then this contradicts the assumption that $|a| \leq |x|$ for any $x \in I$ with $x \neq 0$. Thus, $r = 0$ and $b = aq$. Therefore, we have $b \in (a)$ and $I \subset (a)$. It follows that $I = (a)$ □

3 Polynomials

In this section, we will cover many results for polynomials that are analogous to the ones presented in Section 2. Many proofs of the results in this section are omitted as they often end up being very similar to the proof from the integer case, perhaps with a subtle difference. In order to begin talking about polynomials, however, we will need to introduce some notation.

Remark 3.1. Let $\mathbb{F}$ be a field. The set of all polynomials with coefficients in $\mathbb{F}$ is denoted $\mathbb{F}[T]$.

We are now ready to begin presenting results related to polynomials. We will begin with the Division Algorithm and the Euclidean Algorithm just as we did in the integer case.

3.1 The Division Algorithm and The Euclidean Algorithm

Just as in $\mathbb{Z}$, we have a division algorithm in $\mathbb{F}[T]$. This will be used to create an analog to the Euclidean algorithm in $\mathbb{Z}$.

Theorem 3.2 (Theorem 4.2.1 from [BB06])**.** *For two polynomials $f(x), g(x) \in \mathbb{F}[T]$ such that $g(T) \neq 0$, there exist unique $q(T), r(T) \in \mathbb{F}[T]$ such that $f(T) = g(T)q(T) + r(T)$ where $deg(r(T)) < deg(g(T))$ or $r(T) = 0$.*

Theorem 3.2 is almost identical to Theorem 2.1. In the integer case, we required that the remainder r be strictly less than the quotient b. In this case, we do the same thing by requiring the degree (the analog of the absolute value of an integer) of $r(T)$ is less than the degree of $g(T)$ or that $r(T) = 0$. By repeated uses of Theorem 3.2, we can find the greatest common divisor of two polynomials in the exact same way we found the greatest common divisor of two integers.

Example 3.3. Find the greatest common divisor of $f(x) = x^4 + x^3 + x + 1$ and $g(x) = x^3 + x^2 + x + 1$ over $\mathbb{Z}_2$. We will proceed by the Euclidean Algorithm, replacing our integers a and b by the polynomials $f(x)$ and $g(x)$.

$$\begin{aligned} x^4 + x^3 + x + 1 &= (x^3 + x^2 + x + 1)(x) + (x^2 + 1) \\ x^3 + x^2 + x + 1 &= (x^2 + 1)(x + 1) + 0 \end{aligned}$$

As in the Euclidean Algorithm for integers, our greatest common divisor is the last non-zero remainder. Thus, $\gcd(f(x), g(x)) = x^2 + 1$.

3.2 Constructing Fields Using Polynomials

Just as in $\mathbb{Z}$, we can create finite fields and infinite fields using very similar methods in $\mathbb{F}[T]$. We will use the polynomial analog to prime numbers, irreducible polynomials, to create finite fields. Using the same equivalence relation from Definition 2.8, we will also be able to create fields of infinite order.

3.2.1 Finite Fields

We would like to be able to create fields of finite order using polynomials. Ideally, we will do this in a similar way to the construction in Section 2.2. In order to do this, we will need to introduce what it means to view one polynomial modulo another. First, we will define irreducible polynomials, our polynomial analog to prime numbers.

Definition 3.4. (Definition 4.2.6 from [BB06]) A polynomial $f(T) \in \mathbb{F}[T]$ is said to be **reducible over** $\mathbb{F}$ if there exist $g(T), h(T) \in \mathbb{F}[T]$ such that $f(T) = g(T)h(T)$ where $\deg(g(T)) < \deg(f(T))$ and $\deg(h(T)) < \deg(f(T))$. If a polynomial is not reducible over $\mathbb{F}$ then it is said to be **irreducible**.

Next, we would like to introduce what it means to look at a polynomial modulo another polynomial. This is done using division with remainder, just as it is done for the integers.

Definition 3.5. Let $f(T), g(T) \in \mathbb{F}[T]$ with $g(T) \neq 0$. By Theorem 3.2, we may write $f(T) = g(T)q(T) + r(T)$ where $\deg(r(T)) < \deg(g(T))$ or $r(T) = 0$. We define $f(T)$ **modulo** $g(T)$ to be $r(T)$.

Just as we may view the integers modulo a single integer, we would also like to be able to view the entire set of polynomials modulo a single polynomial.

Remark 3.6. Given a polynomial $f(T) \in \mathbb{F}[T]$ with $f(T) \neq 0$, we will denote the set $\{a(x) \text{ modulo } f(x) | a(x) \in \mathbb{F}[T]\}$, the set of all polynomials in $\mathbb{F}[T]$ modulo $f(T)$, by $\mathbb{F}[T]/(f(T))$.

Armed with this new notation, we are finally ready to construct fields of finite order. For this construction, we will take $\mathbb{F} = \mathbb{Z}_p$ where p is a prime integer. We will make a field of order p^n by "modding out" $\mathbb{Z}_p[T]$ by an irreducible polynomial in $\mathbb{Z}[T]$. This is analogous to the result that the integers modulo a prime p is a field of order p.

Theorem 3.7 (Theorem 1.1 from [Cona]). *For a prime p and irreducible polynomial $\pi(T) \in \mathbb{Z}_p[T]$ of degree n, the ring $\mathbb{Z}_p[T]/(\pi(T))$ is a field of order p^n.*

Proof. ([Cona]) By Definition 3.5, any polynomial $f(x) \in \mathbb{Z}_p[T]/(\pi(T))$ must have degree less than the degree of $\pi(T)$ since $f(T)$ modulo $\pi(T)$ is the remainder acquired from Theorem 3.2. Thus, $\mathbb{Z}_p[T]/(\pi(T)) = \{c_0 + c_1T + \cdots + c_{n-1}T^{n-1} | c_i \in \mathbb{Z}_p\}$. There are p choices for each coefficient since the coefficients are in $\mathbb{Z}_p$. Also, we must make this choice n times as there are n coefficients in the remainder. Hence, the set $\mathbb{Z}_p[T]/(\pi(T))$ has order p^n. Using a method similar to the proof that $\mathbb{Z}_p$ is a field, we can conclude that $\mathbb{Z}_p[T]/(\pi(T))$ is a field. □

These fields are analogous to $\mathbb{Z}_p$ for a prime number p. One difference is that we can construct fields of any prime power by finding an irreducible polynomial of a certain degree.

Example 3.8. $\mathbb{Z}_2[T]/(T^4 + T + 1)$ is a field of order $2^4 = 16$.

3.2.2 Fraction Fields

We can use almost the exact same equivalence relation from Definition 2.8 to define "fraction fields."

Definition 3.9. Define the relation $\sim$ on the set $\mathbb{F}[T] \times (\mathbb{F}[T] - \{0\})$ such that $(f(T), g(T)) \sim (h(T), k(T))$ if and only if $f(T)k(T) = g(T)h(T)$.

By a method similar to the proof of Theorem 2.9, $\sim$ from Definition 3.9 is an equivalence relation. Now, we must define our two operations and we will have a field analogous to the rational numbers. For $(f(T), g(T)), (h(T), k(T)) \in \mathbb{F}[T] \times (\mathbb{F}[T] - \{0\})$ define $+$ by $(f(T), g(T)) + (h(T), k(T)) = (f(T)k(T) + h(T)g(T), g(T)k(T))$. Define $\cdot$ by $(f(T), g(T)) \cdot (h(T), k(T)) = (f(T)h(T), g(T)k(T))$.

Theorem 3.10. *The equivalence classes of $\sim$ from Definition 3.9 are a field under $+$ and $\cdot$ defined above.*

As in the integer case, we will not check that all of the conditions are met for this to be a field. However, there is one major difference between this construction and the construction of the rational numbers. This difference has to do with the characteristic of the resulting field.

Definition 3.11. (Definition 5.2.10 from [BB06]) Let R be a commutative ring. The **characteristic** of R is the smallest positive integer a such that $a \cdot 1 = 0$ in R. If no such a exists, R has characteristic 0.

The rational numbers have characteristic 0. Also, the only fields of non-zero characteristic that we have seen so far have been finite. But, we can create fields of infinite order with non-zero characteristic by using the above construction.

Example 3.12. Set $\mathbb{F} = \mathbb{Z}_5$. Then the equivalence classes of the relation $\sim$ from Definition 3.9 are a field of infinite order with characteristic 5.

3.3 Algebraic Properties of Polynomials

Lastly, we will discuss some algebraic properties of $\mathbb{F}[T]$ and compare these to the algebraic properties discussed in Section 2.3. Just like the integers, $\mathbb{F}[T]$ is a ring and integral domain. Also, ideals in $\mathbb{F}[T]$ are all principal, just as in $\mathbb{Z}$. We will provide the proof of this fact to illustrate how similar the proofs of these analogous results can be.

Theorem 3.13 (Theorem 2.1 from [Conb])**.** *All ideals in $\mathbb{F}[T]$ are principal.*

Proof. ([Conb]) Let I be an ideal in $\mathbb{F}[T]$. If $I = \{0\}$, then the ideal (0) is principal. Suppose $I \neq \{0\}$. Then there exists $f(T) \in I$ such that $\deg(f(T)) \leq \deg(g(T))$ for every $g(T) \in \mathbb{F}[T]$ such that $g(T) \neq 0$. It is clear that $(f(T)) \subset I$. We must show that $I \subset (f(T))$. Let $g(T) \in I$ be any polynomial in I. Using Theorem 3.2, we may write $g(T) = f(T)q(T) + r(T)$

where $\deg(r(T)) < \deg(f(T))$ or $r(T) = 0$. Thus, we have $g(T) - f(T)q(T) = r(T)$. Since $f(T), g(T) \in I$, we have that $r(T) \in I$. If $r(T) \neq 0$, we have that there is a non-zero element in I such that $\deg(r(T)) < \deg(f(T))$. This contradicts our assumption that for every $g(T) \in I$, $\deg(f(T)) \leq \deg(g(T))$. Hence, we must have $r(T) = 0$ and $g(T) = f(T)q(T)$. Thus, $g(T) \in (f(T))$ and $I \subset (f(T))$. Therefore, $I = (f(T))$ and I is principal. □

The above proof could have been written by taking the proof of Theorem 2.14 and replacing $\mathbb{Z}$ with $\mathbb{F}[T]$ and replacing instances of specific integers with polynomials. The only major difference is that this proof references the degree of polynomials while the proof of Theorem 2.14 uses the absolute value of integers. But these are analogous properties.

References

[BB06] John A. Beachy and William D. Blair. *Abstract Algebra*. Waveland Press, Inc., 2006.

[Cona] Keith Conrad. Finite fields. http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/finitefields.pdf. Accessed: April 29, 2017.

[Conb] Keith Conrad. Notes on ideals. http://www.math.uconn.edu/~kconrad/math3231s17/handouts/ideals.pdf. Accessed: April 29, 2017.

[GV05] William Gilbert and Scott Vanstone. *An Introduction to Mathematical Thinking*. Pearson Prentice Hall, 2005.

[McD] Robert McDonald. Fermat for polynomials. https://lms.uconn.edu/bbcswebdav/pid-1327518-dt-content-rid-6342789_1/courses/1173-UCONN-MATH-2794W-SEC001-14285/Math%20Club%20Talk%204%20Notes.pdf. Accessed: April 29, 2017.

[Sin] Simon Singh. The whole story. http://simonsingh.net/books/fermats-last-theorem/the-whole-story/. Accessed: April 29, 2017.

[Wika] Wikipedia. abc conjecture. https://en.wikipedia.org/wiki/Abc_conjecture. Accessed: January 2, 2018.

[Wikb] Wikipedia. Fermat's last theorem. https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem. Accessed: January 2, 2018.

[Wil95] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.