12-2021

Integers and Polynomials with Integer Coefficients for High School Students

Gabriella Nowobilski
Governors State University

Integers and Polynomials with Integer Coefficients for High School Students

by

Gabriella Nowobilski

B.A., Illinois State University, 2019

Thesis

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science with a Major in Mathematics

Governors State University

University Park, IL 60484

2021

Table of Contents

List of Figures

List of Symbols

$\mathbb{N}$	Set of Natural Numbers
$\mathbb{Z}$	Set of Integers
$\mathbb{Q}$	Set of Rational Numbers
$\mathbb{R}$	Set of Real Numbers
$\mathbb{C}$	Set of Complex Numbers
$\mathbb{Z}[x]$	Set of all polynomials with integer coefficients
$\mathbb{Q}[x]$	Set of all polynomials with rational coefficients
$\mathbb{R}[x]$	Set of all polynomials with rational coefficients
S	Any given set
(a, b)	The greatest common divisor of a and b
$a\|b$	a divides b

Abstract

Recently, many mathematics educators have tried to explore the potential for aspects of abstract algebra to improve the teaching of high school algebra. As a high school math teacher, I am specifically interested in how I can tie the ring theory in abstract algebra into a high school level algebra course. More precisely, this thesis concerns the possible application of the irreducibility of polynomials (with integer coefficients over rational field $\mathbb{Q}$) in high school algebra. We will explore the differences between a reducible polynomial and an irreducible polynomial. In detail, concepts such as the following will be explored and addressed: the comparison of the ring of integers and the rings of polynomials over $\mathbb{Q}$ (or $\mathbb{R}$), including the Division Theorem, Fundamental Theorem of Arithmetic, Factorization Theorem for Polynomials, and long division. Secondly, we will discuss how to verify a polynomial with integer coefficients is irreducible over $\mathbb{Q}$, such as Eisenstein's Criterion. In the final section, we will include several strategies and lesson proposals to introduce these topics at a secondary level tied in with appropriate common core state standards.

Chapter 1. The Division Theorem

1.1 The Division Theorem and its proof

It is not uncommon for a mathematics teacher to cope with uncertainty and reduce anxiety among many students in a high school classroom. Based on experience and outside conversation, I have built a beginning of an understanding of the fright students feel when they struggle to understand curriculum in their high school math classrooms. After several conversations with students, I have found that my desired goal with my thesis is to further explore several topics that involve higher level mathematics, and can be introduced to students in a classroom. According to a Scholastic article for parents entitled "Using the Rules of Divisibility Effectively", "3rd grade is when the concept of multiplication and division is taught, and 4th grade is when students learn about factors/multiples and prime/composite numbers. They will use this language through high school, so it's important they feel comfortable with them" (Scholastic, 2014). If topics of division and factors are discussed beginning at a 3rd or 4th grade level, why do we not work to introduce theorems such as the Division Theorem to students at a high school level, in such a way that could be useful to their understanding of division, factors, and remainders? Using several examples and representations of the division theorem, I will work to present it in a way that may be accessible to high school students.

Theorem 1.1.1 (Division Theorem). If n is any integer and d is a positive integer, then there exist unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.

Proof. There are two steps:

(1) Prove that there are integers q and r such that $n = dq + r$ and $0 \leq r < d$.

(2) Prove that q and r are unique.

Let $a, b \in \mathbb{Z}$ and $b \neq 0$. Then there is the set of numbers, $c \in \mathbb{N}$, defined to be $S = \{c = n - dx \geq 0, x \in \mathbb{Z}\}$. Now, we will show that there are elements in the set S.

There are three cases should be considered here: $n > 0, n < 0$, and $n = 0$.

(i) For $n > 0$ and $n = 0$, consider $n - d(0) = n \geq 0$. Therefore, for this case (when $n \geq 0$), $c = n - d(0) = n$ is an element in the set S.

(ii) Secondly, we need to show that when n is negative, the set also contains elements. With n being a negative integer and d being a positive integer, which means $d \geq 1$.

For $d \geq 1$, multiplying $-n$ on both sides yields $-nd \geq -n$. Adding n to both sides, $n - nd \geq 0$ and $n - nd$ is an element of set S.

Therefore, the set is non-empty for all cases.

The Well-Ordering Axiom will also need to be considered. The Well Ordering Axiom states: any nonempty subset of nonnegative integers has a least element.

Letting r represent the smallest element of the set S, where $r = n - dx$, such that, when $x = q$, $r = n - dq$, in other words, $n = dq + r$.

Since r is in the set we denoted above, $r \geq 0$. To prove the first part of the inequality, we must show that $r < d$.

This will be shown through a proof by contradiction. Assume the opposite, such that, $r \geq d$. Moving the d to the left by subtraction, $r - d \geq 0$.

Therefore, $r - d = n - dq - d = n - d(q + 1)$.

Considering the final equivalent statement, $n - d(q + 1)$, this is an element of the set S since $n - d(q + 1) = r - d \geq 0$. Since d is positive, it can be concluded that that $r - d < r$.

Therefore, $0 \leq r - d = (n - dq) - d = n - d(q + 1) < r$. This shows there exists another element that would be smaller than r, in the set S, which would contradict the assumption that r is the least element in S. By contradiction, $r < d$.

Lastly, a proof to show q and r are unique.

Let r_1, r_2, q_1, q_2 be integers, and $dq_1 + r_1 = n = dq_2 + r_2$, where the property proved above holds for r_1 and $r_{2,}$ such that $0 \leq r_1 < d$ and $0 \leq r_2 < d$.

Now, show that r_1 *and* r_2 are the same and q_1 *and* q_2 are the same.

Suppose that $r_2 \geq r_1$. As stated above $dq_1 + r_1 = n = dq_2 + r_2$, therefore, $0 = dq_1 + r_1 - dq_2 - r_2$.

Factoring out d and -1, yields $d(q_1 - q_2) - (r_2 - r_1) = 0$, or in other words, $d(q_1 - q_2) = r_2 - r_1$.

Since $r_2 \geq r_1$, the quantity $d(q_1 - q_2)$ is not negative. But, since $0 \leq r_1 \leq r_2 < d$, if $r_1 < r_2$, then $d > r_2 - r_1 > 0$, so $d(q_1 - q_2) > 0$. But $d(q_1 - q_2) \geq d$, and $d(q_1 - q_2) = r_2 - r_1$ cannot be true, which is a contradiction. So $r_2 = r_1$ or $r_2 - r_1 = 0$.

Knowing that $0 = d(q_1 - q_2) - (r_2 - r_1)$, and $(r_2 - r_1)$ is equal to 0, by substitution we have $0 = d(q_1 - q_2) - 0$, then the quantity $q_1 - q_2$ must also be equal to 0.

In conclusion, we have proved both statements as desired: (1) There are integers q and r such that $n = dq + r$ and $0 \leq r < d$. (2) q and r are unique.

Now the proof is complete. I would like to discuss its conceptual understanding in a way that could be graspable for students in a high school classroom.

There are several steps and details from the proof we would address to students without overwhelming them with the tedious steps that may be too difficult for them.

1.2 Conceptual Understanding of the Division Theorem

Although a proof provides a detailed outline of the reasoning for a mathematical finding, this type of approach to a high school classroom probably would not fit as most effective. An approach involving arguments and examples that students can understand would be beneficial for teachers to introduce in high school classrooms. This method of examples and various representations to give a friendly and approachable introduction for students.

To introduce the Division Theorem in a high school classroom, the concept of greatest common divisor (gcd) could be considered. The gcd is one of the topics covered in a middle school and high school curriculum. The following examples are direct applications of the gcd using the Division Theorem.

Definition. A positive integer, d, is the greatest common divisor of integers a and b if d is a common divisor of a and b and not less than any other common divisor of a and b.

Euclid's Algorithm. Let $a, b \in \mathbb{N}, a > b$. By division theorem, there are unique integers q and r such that $a = bq + r$, where $0 \leq r < b$. If $r = 0$, we stop. If r is not zero, we apply the division theorem to b and r. We repeatedly use division theorem until we receive the remainder 0. This method to find the great common divisor is called the Euclid's Algorithm.

Example 1.2.1. Find the gcd between 58 and 16

Using the Division Theorem, 58 can be written as: $58 = 16 \cdot q + r$, where $0 \leq r < 16$. Dividing 58 by 16, the quotient is 3 and the remainder 10, such that $58 = 16 \cdot 3 + 10$, where $0 \leq 10 < 16$. Notice, by subtracting $16 \cdot 3$ on both sides, $58 - 16 \cdot 3 = 10$. Therefore, the gcd divides $58{,}16$ and 10. It implies that the gcd is a common divisor of 16 and 10. Not only is it a common divisor, but it is the great common divisor because if there were a divisor greater than d, then this number would also divide 58 and then d would not have been the gcd between 58 and 16. Therefore, since any number that divides 16 and 10, also divides 58, we can say $\gcd(58{,}16) = \gcd(16{,}10)$. Applying the division algorithm again for 16, there is a unique q and r such that $16 = 10 \cdot 1 + 6$. Similarly, as above, any number that divides 10 and 16 must also divide 6 because it can be rewritten as $16 - 10 \cdot 1 = 6$. Therefore, $\gcd(16{,}10) = \gcd(10{,}6)$. Applying the division algorithm again, $10 = 6 \cdot 1 + 4$, such that $\gcd(10{,}6) = \gcd(6{,}4)$. Applying the division algorithm one last time, $6 = 4 \cdot 1 + 2$. Thus, the $\gcd(6{,}4) = \gcd(4{,}2)$. Applying the theorem again, 2 is prime so it will not have any other greatest common divisor. Therefore, $\gcd(4{,}2) = 2$.

The concept of gcd will be addressed in the chapters to follow, applying it to polynomials rather than integers, which will build upon the extension of these division theorems, as possible applications in a high school curriculum.

1.3 Applying the Division Theorem to Even and Odd Integers

Another application of the division theorem could be to discuss the difference between even and odd integers. One can show that every integer is either even or odd but never both.

Before the proof, it is important to discuss the relevance of this topic in a high school mathematics classroom. I have found that students have an instilled fear of explanation in math classes. Some of the fear comes from the following types of questions: “Can you explain your work, how did you get your solution, describe your steps and why you took them”. Students freeze up oftentimes because they have a fear of approaching questions that require problem solving and do not have a clear solving approach. Additionally, their approach may be to guess the answer without analyzing, reasoning or deducting logically. (Not all students of course, I am speaking from previous experience as a student for 18 years and a teacher for 2). I want to take this example and focus more on reaction and thoughts of a student working through it, then focusing on the heavy mathematical content that can come behind it. To recall, we use this Division Theorem to prove the following statement, “every integer is even or odd, but not both”. We consider this problem from the lens of a freshman in high school. There are no strange expressions or complicated derivations of numbers that could look intimidating to students aged 14-years-old. One could recognize and understand the word integer, even, and odd. Now, we will use the Division Theorem to prove the claim.

Lemma 1.3.1. Let i represent this integer. Then, $i = 2q + r$, where q and r are integers and $0 \leq r < 2$.

Even: The set of even numbers, $S = \{2k, k \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of integers.

Odd: The set of odd numbers, $T = \{2k + 1, k \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of integers.

When the least nonnegative remainder of an integer divided by 2 is zero, the number is even, and it will follow that $i = 2q$ from the Division Theorem. By the Division Theorem, for any integer n, there are two unique integers q and r such that $n = 2q + r$, where $0 \leq r < 2$. So r is either 0 or 1. If r is not 0, then $r = 1$ and $n = 2q + 1$ is odd. This shows that an integer is either odd or even.

Now, the only part students might struggle with more as a teenage is finishing up by explaining why it is not possible for it to be both. Since we want to prove it cannot be both, we may assume it can be both and see what happens. Consider integer q_1 and q_2, where $i = 2q_1$ and $i = 2q_2 + 1$. Then $i = 2q_1 = 2q_2 + 1$ or $2(q_1 - q_2) = 1$.We know that this is not possible, because in the equation $2(q_1 - q_2) = 1$ the absolute value of the left side is either 0 when $q_1 = q_2$ or greater than 2 if $q_1 \neq q_2$, but the right side is 1. Therefore, an integer cannot be both even and odd.

Being able to follow along a proof from the perspective of a high school student made me feel connected to a K-12 setting in this higher level of mathematics presented in this chapter. It opened the doors to being able to further explore division and factors in a high school setting using advanced theorems and corollaries. Moving forward, we will further make deeper connections to a high school classroom using the Fundamental Theorem of Arithmetic.

Chapter 2. The Fundamental Theorem of Arithmetic

After discussing the Division Theorem, Euclid's Algorithm, and properties of even and odd numbers, we will continue to build an understanding of what it means for a polynomial to be irreducible and reducible by diving into divisibility, prime and composite numbers, prime factorization, and the Fundamental Theorem of Arithmetic.

2.1 Divisibility

This section begins with discussing the divisibility of numbers, what it means for one number to be divisible by another, and how this allows us to determine the difference between prime and composite numbers and their applications.

Definition 2.1.1: An integer n is divisible by a nonzero integer m if there is an integer k such that $n = m \cdot k$.

The concept of divisibility is taught beginning in 4th and 5th grade, i.e., 15 is divisible by 5, 70 is divisible by 10, 35 is divisible by 7, and so forth, and builds the foundation of more complex corollaries and theorems they will learn later. Having been taught at a young age, students can quickly build an understanding of divisibility and the other applications that stem from it. Now, to introduce the concept of a divisor. m is a divisor of n if n is divisible by m. Another term to consider here is a factor. We will discuss the prime factorization in the following section. If m is a divisor of n, n is divisible by m, and m is a factor of n. Additionally, 1 divides any integer and any nonzero n divides itself.

Definition 2.1.2. An integer m is a proper divisor of n if m is a divsor of n, $m \neq 1, m \neq -1, m \neq n, and\ m \neq -n$.

Note: In this case it is stated that m is a proper factor of n.

Example 2.1.1. Consider the example for $3, 5, and$ 15. It is correct to say that 3 is a proper divisor of 15, 5 is a proper divisor of 15, and both 3 and 5 are proper divisors of 15.

Example 2.1.2. Asking students the following question: is it correct to say that every nonzero integer divides 0? Let us show it to be true. To build up the conceptual understanding, we first choose a number, say 3, to verify if it is correct. Because $3 \cdot 0 = 0$, we see that 3 divides 0 by definition. Similarly, for any nonzero integer n, $n \cdot 0 = 0$, therefore n divides 0.

Example 2.1.3. List all positive divisors of 52. The students will begin by listing all numbers that 52 can be divided by: $1, 2, 4, 13, 26, 52$. Those are all positive divisors of 52.

Lastly, to conclude the discussion on divisors and proper divisors, a connection between what we have been talking about with divisors to the definition of a prime number. One way to define a prime number is by saying that a prime number is an integer $p > 1$ that has no proper divisors. In Example 2.1.3, the prime divisors are 2 and 13.

2.2 Primes and Prime Factorization

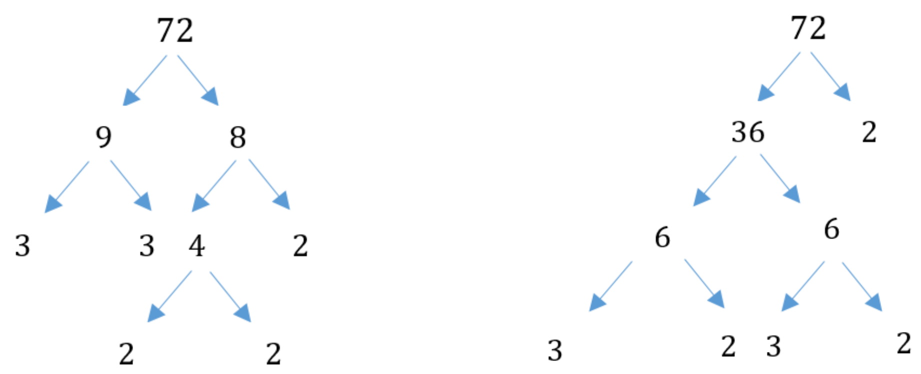
Drawing from the Division Theorem studied above, the Fundamental Theorem of Arithmetic and its connections and applications can be studied in a high school mathematics classroom.

The Fundamental Theorem of Arithmetic states that each positive integer (not including 1), can be represented as a product of one or more prime numbers. Furthermore, this factorization is unique, apart from the order in which the prime factors are listed.

Before the proof of the Fundamental Theorem of Arithmetic, one must describe primes, prime factorization, and show several examples. The topic of prime numbers is very applicable and reasonable to introduce in a high school classroom when teaching factoring strategies and several other algebra topics. Understanding the value of learning about prime numbers may encourage students to study the topic with excitement and an open mind. One main application of prime numbers that may draw relevance in the life of students is the study of cryptography and its application to the changing technology around us. The cyber world we live in highly relies on cryptographic algorithms for its security, including the execution of activities we perform on a daily basis: withdrawing cash safely from an ATM, paying TV programs, email security, secure web browsing, and so forth. Alongside cryptography, there are several other applications for students to explore. "Some applications are industrial – such as applications in numerical analysis, applied mathematics and other applied sciences – while some are of the 'conceptual feedback' variety, in which primes and their surrounding concepts are used in theoretical work outside of, say, pure number theory" (Crandall, 2001).

Dividing the set of positive integers that are greater than 1 into two distinct sets, the set of prime numbers that only contain factors 1 and itself, and the set of composite numbers that have proper factors. Consider the integer 72. We can break down 72 as $9 \cdot 8,$ then break down each of those numbers further having that there are both composite, such as: $9 = 3 \cdot 3$ and $8 = 4 \cdot 2$. Having that 4 is composite, it can break down further such that $4 = 2 \cdot 2$. This leaves the following factors: $72 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2$. Condensing the factors, the factorization of 72 is: $72 = 3^2 \cdot 2^3$. Consider two different factors of 72 to study the uniqueness of prime factorization, before it is proven to be true. We can break down 72 as $36 \cdot 2$. Breaking down 36 further, such that: $36 = 6 \cdot 6$. Finally break the $6's$ apart further such that $= 3 \cdot 2$. We are left with the following factors: $72 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2$. Condensing the factors, the factorization of 72 as follows: $7 = 3^2 \cdot 2^3$. There is another representation that can be used to show factorization, known as a factor tree, which can be very approachable to a high school student. A display of a factor is shown below for the example provided.

Figure 2.1: Prime Factorization of 72



Let us now prove that every number is either prime or composite but not both. We will also prove that prime factorization is unique. This will allow students to build up to the understanding of the Fundamental Theorem of Arithmetic, its proof, and its applications to the world around us.

2.3 Fundamental Theorem of Arithmetic

Before the proof of the Fundamental Theorem of Arithmetic, for two integers a and b, we define (a, b) to be the greatest common divisor of a and b.

We say that a and b are relatively prime or coprime if $(a, b) = 1$, that is, they share no common positive divisors (or factors) except 1.

Theorem 2.3.2. (Bezout's Identity). Let $a, b \in \mathbb{Z}$. If d is the greatest common divisor of a and b, there are integers x and y, such that $ax + by = d$.

Example 2.2.1. Find the greatest common divisor d of $a = 9$ and $b = 12$, and show with Bezout's Identity that for some integers x and y, $d = ax + by$.

Applying the Division Theorem, $12 = 9 \cdot 1 + 3$. Therefore $\gcd(9,12) = \gcd(9,3)$ using Euclid's Algorithm. Since 3 is prime, the $\gcd(9,3) = 3$. Therefore, $d = 3$. Using Bezout's identity, for $d = ax + by$, where $d = 3, a = 9, b = 12$, $3 = 9 \cdot x + 12 \cdot y$. By the equation $12 = 9 \cdot 1 + 3, 3 = 12 - 9 = 9(-1) + 12(1)$. Therefore, $d = 3, x = -1$ and $y = 1$.

Theorem 2.3.4 (Fundamental Theorem of Arithmetic). Each positive integer greater than 1 can be represented as a product of one or more prime numbers.

There are two lemmas needed to prove the Fundamental Theorem of Arithmetic: If a and b are integers, we write $a|b$ if a divides b.

Lemma 2.3.1. $If\ a|bc$ and $(a, b) = 1$, then $a|c$.

Proof. Since$(a, b) = 1$, by Bezout's Identity, for some integers, d and e, $1 = da + eb$, so $c = dac + ebc$. From the given statement that $a|bc$, we can say that $a|dac$ and $a|ebc$, therefore, $a|(dac + ebc) = c$, as desired.

The following Lemma is known as Euclid's Lemma.

Lemma 2.3.2. If p is a prime and $p|a_1\ a_2 a_3 \ldots a_n$, then $p|a_i$ for some i.

Proof. The following is a proof by induction. Consider $n = 2$, for a_1 and a_2. Suppose that $p|a_1 a_2$. Therefore, either $p|a_1$ or $p \nmid a_1$. If $p|a_1$ then the claim holds true when $n = 2$. On the contrary, if $p \nmid a_1, p|a_2$. This is shown to be true by the lemma proved above. Assume $n = k$, if $p|a_1 a_2 a_3 \ldots a_k$, then $, p|a_i$ for some i. Now, consider the case $n = k + 1$, if $p|a_1 a_2 a_3 \ldots a_k a_{k+1}$, then $p|a_1(a_2 a_3 \ldots a_k a_{k+1)}$. If $p|a_1$, then the claim is true, if $p \nmid a_1$, then by Lemma 2.3.1,

$p|(a_2 a_3 \ldots a_k a_{k+1})$. Here $(a_2 a_3 \ldots a_k a_{k+1})$ is one integer, and there are k factors in its product. By inductive assumption, $p|a_i$ for some i between 2 and $k+1$. By mathematical induction, we have shown that this lemma holds true for all $n > 1$.

Proof of the Fundamental Theorem of Arithmetic. There are two parts to prove in the Fundamental Theorem of Arithmetic. First, show that each positive integer (not including 1), can be represented as a product of one or more prime numbers. Secondly, prove the uniqueness part of the theorem.

A proof by induction will be used to show that any integer that is greater than one can be written as a product of primes. Beginning with the case $n = 2$, 2 is prime, therefore the claim holds true. Now consider any case where $n > 2$, assuming that any other number less than n can be factored into a product of primes. There are two possibilities: n is either prime or composite. If n is prime, then we are done. If n is composite, it can be factored such that $n = ab$, under the conditions that $1 < a$ and $b < n$. By induction, we can make the claim that we can factor a and b into primes. This proves the existence of factorization.

Secondly, we will show the uniqueness of the Fundamental Theorem of Arithmetic. Let $a_1, \ldots, a_i$ be distinct primes and $b_1, \ldots, b_j$ be distinct primes, such that ${a_1}^{c_1} \ldots {a_i}^{c_i} = {b_1}^{d_1} \ldots {b_j}^{d_j}$, where all exponents c_1 to c_i and d_1 to $d_j$are natural numbers. Using the last lemma we proved: if p is a prime and $p|{a_1}^{c_1} \ldots {a_i}^{c_i}$ then $p|a_i$ for i. Since a_1 divides the product ${b_1}^{d_1} \ldots {b_j}^{d_j}$, by the same lemma stated above, a_1 divides b_k for some k between 1 and j. By arranging the order, we may assume $k = 1$ and $a_1|b_1$. Since both a_1 and b_1 are prime, a_1=b_1. Replacing b_1 by a_1 in the equation, it shows ${a_1}^{c_1} \ldots {a_i}^{c_i} = {a_1}^{d_1} \ldots {b_j}^{d_j}$. If $c_1 > d_1$, we can remove ${a_1}^{d_1}$ from the right, such that ${a_1}^{c_1 - d_1} \ldots {a_i}^{c_i} = {b_2}^{d_2} \ldots {b_j}^{d_j}$. We run into something unusual, something that is not possible.

This equation is absurd because a_1 divides the left side, but it would not divide the right. Similarly, $c_1 < d_1$ is not possible. Therefore, $c_1 = d_1$ holds true. We show $a_2^{c_2} \ldots a_i^{c_i} = b_2^{d_2} \ldots b_j^{d_j}$. We continue to follow the same steps for each additional power and the same argument holds. Therefore, we have shown that each positive integer (not including 1), can be represented as a product of one or more prime numbers, and that they are unique.

Chapter 3. Factorization Theorem for Polynomials

3.1 Remainder and Factor Theorems

"Teaching that embraces productive struggle provides opportunities for students to delve deeply into relationships among mathematical ideas and to develop understanding that leads them to apply their learning to new problem solutions" (NCTM, 2014). In this main chapter of the paper, we will concentrate on the irreducibility of polynomials, using several factor theorems, and long division applications that one could introduce in a high school classroom. The first two chapters discussed the division theorem for integers and factorization of integers, which are topics that can be introduced at a high school level. In this section we will extend the concept of divisibility and factorization to polynomials over the rational field $\mathbb{Q}$. The first concept we will introduce is an irreducible polynomial, then the Division Theorems for polynomials with rational (or real) coefficients will be discussed.

Definition. (1) A polynomial is an expression of the form $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where the coefficients $a_0, a_1, a_2 \dots, a_n$ are rational (or real) numbers and x is called the indeterminate.

(2) If $a_n \neq 0$, we say the degree of $f(x)$ is n.

We define $f(x)$ and $g(x)$ to be equal if and only if the coefficients of each power of x are equal. In other words, for $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, $f(x) = g(x)$ if and only if $m = n$, $a_0 = b_0, a_1 = b_1, \dots, a_n = b_n, \dots, a_m = b_m$.

We can also add and multiply polynomials. Let us define the operations:

(1) Addition: If $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, then $f(x) + g(x) = (a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_mx^m)$. If $m > n$, we can combine the

terms such that $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_m x^m$.

(2) Multiplication: The multiplication of two polynomials is defined by the distributive law and addition formula as follows: $f(x) \cdot g(x) = (a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m}$. Additionally, if $a_n b_m \neq 0$, then the leading coefficient of $f(x) \cdot g(x)$ is the product of the leading coefficients of $f(x)$ and $g(x)$.

Definition. Let F be one of the sets $\mathbb{Z}, \mathbb{Q}, \text{and } \mathbb{R}$. We define $F[x]$ to be the set of all polynomials with coefficients in the set F.

Note: We will consider the set of polynomials with integer coefficients in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$.

Lemma 3.1.1. For all non-zero polynomials $f(x)$ and $g(x)$ with coefficients in $\mathbb{R}$, $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

Note: If a is not zero, then a has no zero divisors, which means if $b \neq 0$, then $ab \neq 0$. Additionally, the degree of a nonzero polynomial is greater than or equal to zero.

Proof. Suppose $f(x), g(x) \in \mathbb{R}[x]$, with degrees n and m, respectively. Let $a_n \neq 0$ be the leading coefficient of $f(x)$, and $b_m \neq 0$ the leading coefficient of $g(x)$. Then, by the product formula, $a_n b_m \neq 0$ is the leading coefficient of $f(x)g(x)$. Thus $f(x)g(x)$ has degree $n + m = \deg\ (f(x) + \deg\big(g(x)\big)$.

Note: By the product formula, if $f(x) = g(x)h(x)$ and $g(x)$ and $h(x)$ have positive degrees, then the degree of $f(x)$ is higher than the degrees of $g(x)$ and $h(x)$.

Definition. Let F be a subset in $\mathbb{Q}$ or $\mathbb{R}$ and $F[x]$ be the set of all polynomials with coefficients in F. A polynomial $f(x)$ in $F[x]$ is said to be irreducible over F if $f(x)$ is not a product of two polynomials $g(x)$ and $h(x)$ in $F[x]$ with positive degrees. Otherwise, $f(x)$ is called reducible.

Example 3.1.1. Consider the polynomial $x^2 - 2 \in \mathbb{Q}[x]$. (We will be revisiting this example using a different corollary later in this chapter). We know that $x^2 - 2$ has no roots over $\mathbb{Q}$. The goal is to show that $x^2 - 2$ is in fact irreducible. This can be done by showing that $f(x)$ is not a product of two polynomials $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$ with positive degrees. A proof by contradiction will be used. If $x^2 - 2$ is reducible, then the polynomial can be written as: $x^2 - 2 = g(x)h(x),$ where the degree of $g(x)$ and the degree of $h(x)$ are less than two and greater than zero. The degree of $x^2 - 2$ is two, therefore both $g(x)$ and $h(x)$ have degree one. In $\mathbb{Q}$, for this reason, $x^2 - 2$ will have a rational zero. This is a contradiction, so $x^2 - 2$ is irreducible.

Let us explore further theorems involving the irreducibility of polynomials. Once these theorems and irreducibility are discussed, they can be later applied to an example of long division.

Theorem 3.1.1. For any polynomial $f(x)$ of degree $n \geq 1$, there is a polynomial $g(x)$ of degree $n - 1$ and a constant r such that: $f(x) = (x - a)g(x) + r$, where $a \in \mathbb{Q}, f(x), g(x) \in \mathbb{Q}[x]$.

Proof: Consider $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. Then $(x - a)g(x) + r = (x - a)(b_0 + b_1x + \cdots + b_{n-1}x^{n-1}) + r$. Multiplying this out, gives $b_0x + b_1x^2 + \cdots + b_{n-2}x^{n-1} + b_{n-1}x^n + r - ab_0 - ab_1x - \cdots - ab_{n-1}x^{n-1}$. Simplifying, yields $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = r - ab_0 + (b_0 - ab_1)x + \cdots + (b_{n-2} - ab_{n-1})x^{n-1} + b_{n-1}x^n$. Therefore, $b_{n-1} = a_n,\ a_{n-1} = b_{n-2} - ab_{n-1},\ a_1 = b_0 - ab_1, a_0 = r - ab_0$. We receive n linear equations and n unknowns: $r, b_{0,} \dots, b_{n-1}$. By substitution, the linear system has a unique solution $r, b_{0,} \dots, b_{n-1}$.

In Theorem 3.1.1, $f(x)$ can be a polynomial of degree n with real coefficients and the number a could be a complex number. The linear equations may have complex coefficients and r can be a complex number when a is a complex number, and the proof still holds true.

We will prove a theorem about the greatest common divisor of polynomials and provide an example.

Definition. A polynomial $j(x)$ (of positive degree) divides a polynomial $f(x)$ if $f(x) = k(x)j(x)$ for some polynomial $k(x)$.

Definition. The greatest common divisor of two polynomials $f(x)$ and $g(x)$ is a polynomial $d(x)$ of highest degree that divides both $f(x)$ and $g(x)$. Usually, it is assumed that the highest degree term of $d(x)$ has coefficient 1 (called a monic polynomial).

Theorem 3.1.2. Let $f(x)$ and $g(x)$ be real polynomials with $\deg(g(x)) > 0$, and suppose $f(x) = q(x)g(x) + r(x)$. Then, $\gcd\big(f(x), g(x)\big) = \gcd\big(g(x), r(x)\big)$.

Proof. Suppose $\gcd\big(f(x), g(x)\big) = d(x)$. As defined above, the greatest common divisor divides both $f(x)$ and $g(x)$. Therefore, $d(x)|g(x)$ and $d(x)|f(x)$. Additionally, rearranging the polynomial equation such that $r(x) = f(x) - q(x)g(x)$, then $d(x)|r(x)$. Now, it remains to show that for some polynomial $h(x)$, if $h(x)|g(x)$ and $h(x)|r(x)$, then $h(x)|d(x)$, and the proof is complete. Since $f(x) = q(x)g(x) + r(x)$, and $h(x)$ divides both $g(x)$ and $r(x)$, then $h(x)|f(x)$. Lastly, since $h(x)|g(x)$ and $h(x)|f(x)$, and $\gcd\big(f(x), g(x)\big) = d(x)$, $h(x)|d(x)$, as desired.

We will illustrate Euclid's Algorithm for polynomials to determine $\gcd\big(f(x), g(x)\big)$.

Similar to the Division Theorem for integers, the Division Theorem for polynomials with rational (or real coefficients) is: Given two polynomials $f(x), g(x)$, with $g(x) \neq 0$, then $f(x) = q(x)g(x) + r(x)$, where $q(x), r(x) \in \mathbb{Q}[x]$ and $r(x) = 0$, or, $\deg r(x) < \deg g(x)$. We proved the special case when $g(x) = x - a$.

Applying the Division Algorithm for polynomials, such that $f(x) = q_1(x)g(x) + r_1(x)$ and $\deg\big(r_1(x)\big) < \deg\,(g(x))$, using the theorem above, $\gcd\big(f(x), g(x)\big) = \gcd\big(g(x), r_1(x)\big)$. When $r_1(x) = 0$, we stop. Otherwise, we continue to repeat the process with polynomials $g(x)$ and $r_1(x)$ instead of polynomials $f(x)$ and $g(x)$. Repeating the process, $g(x) = q_2(x)r_1(x) + r_2(x)$ and $\deg\big(r_2(x)\big) < \deg\,(r_1(x))$, then $\gcd\big(g(x), r_1(x)\big) = \gcd\,(r_1(x), r_2(x))$. If $r_2(x) = 0$, we stop. Otherwise, we continue the process in the same manner until we get a zero remainder.

Example 3.1.2. Determine the greatest common divisor of $f(x) = x^6 + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5$ and $g(x) = x^4 - x^2 - 2x - 1$.

First, we apply the Division Algorithm to $f(x)$ and $g(x)$, such that $f(x) = (x^2 + 2x + 3)g(x) + (x^3 - x^2 - x - 2)$. Continue the algorithm because the remainder is not 0. Now set $r_1(x) = x^3 - x^2 - x - 2$ and apply the Division Algorithm to $g(x)$ and $r_1(x)$, $g(x) = (x + 1)r_1(x) + (x^2 + x + 1)$. Now set $r_2(x) = x^2 + x + 1$ and apply the Division Algorithm to $r_1(x)$ and $r_2(x)$, $r_1(x) = (x - 2)r_2(x) + 0$. We get the zero remainder and stop. Therefore, using Euclid's Algorithm, we found that $\gcd(x^6 + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5, x^4 - x^2 - 2x - 1) = x^2 + x + 1$.

Theorem 3.1.3 (Remainder Theorem). For some polynomial $p(x)$ with degree at least 1 and real coefficients, and a some real number, when $p(x)$ is divided by $x - a$, $p(a)$ is the remainder.

Proof. By the remark after Theorem 3.1.1, $p(x) = (x - a)g(x) + r$, where $g(x)$ is a polynomial and r is a constant (real number), which is either 0 or a nonzero number. By substitution, $p(a) = (a - a)q(a) + r = 0 \cdot q(a) + r = r$. Therefore, $r = p(a)$.

Theorem 3.1.4 (Factor Theorem). A polynomial $f(x)$ in $F[x]$ has a zero c in F, that is, $f(c) = 0$, if and only if $f(x) = (x - c)g(x)$ for some polynomial $g(x)$ in $F[x]$, where F is $\mathbb{Q}$ or $\mathbb{R}$.

Proof. The Factor Theorem follows directly from the Remainder Theorem. If $f(x)$ has a factor $(x - c)$, $f(x) = (x - c)g(x)$ for a polynomial $g(x)$. Therefore, $f(c) = (c - c)g(c) = 0$. Hence, c is a zero of $f(x)$. Now, show that the converse holds true. That is, if $f(x) = 0$, then $f(x) = (x - c)g(x)$ for some polynomial $g(x)$. By the Remainder Theorem, when $f(x) = (x - c)g(x) + r$ is divided by $(x - a)$, $f(a) = r$ is the remainder. Since $0 = f(c) = (c - c)g(c) + r = r$, we see $f(x) = (x - c)g(x)$. Hence, $(x - c)$ is a factor of $f(x)$.

Example 3.1.2. Consider the function $f_1(x) = x^3 + 3x^2 - 3x - 5$.

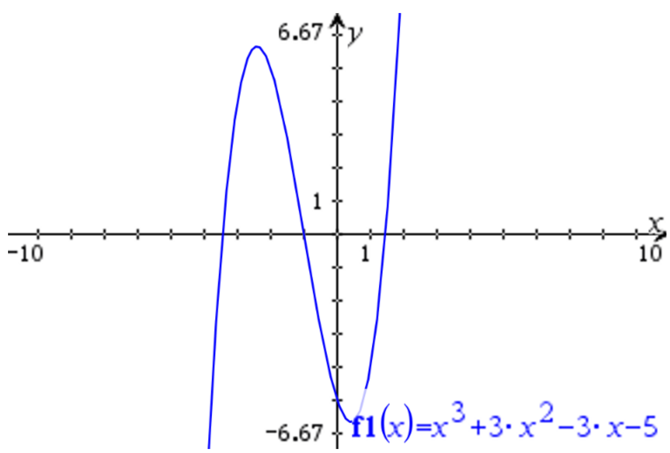


Figure 3.1. Graph of the polynomial $f(x) = x^3 + 3x^2 - 3x - 5$

Simply by examining the behavior of the graph, we see there are three zeros, one of them at $x = -1$. Although by using a command on a graphing calculator, one can approximate the real number that the zero is at, this is not so easy to do by hand. If $x = -1$ is a zero of this function, there is a factor $(x + 1)$ in the factorization of $f(x)$. Therefore, $f(x) = x^3 + 3x^2 - 3x - 5 = (x + 1)g(x)$ for some polynomial $g(x)$. One can perform standard long division, yielding $x^2 + 2x - 5$ as polynomial $g(x)$.

$$\begin{array}{r|rrrr} & x^2 & +2x & -5 & \\ \hline x+1 & x^3 & +3x^2 & -3x & -5 \\ - & x^3 & +x^2 & & \\ \hline & & 2x^2 & -3x & -5 \\ & - & 2x^2 & +2x & \\ \hline & & & -5x & -5 \\ & & - & -5x & -5 \\ \hline & & & & 0 \end{array}$$

Figure 3.2. Long Division of the polynomial $f(x) = x^3 + 3x^2 - 3x - 5$

Let us revisit long division from the lens of the Factor Theorem. All of the beginning terms of each step have the opposite term right above them. $-x^3$ is beneath x^3, $-2x^2$ is beneath $2x^2$, and $5x$ is beneath $-5x$. We omit these terms without missing any information. Let us shift everything up such that combining like terms from polynomial $g(x)$ such that $(x^3 + 3x^2 - 3x - 5) + (-x^2 - 2x + 5) = x^3 + 2x^2 - 5x + 0$. One can determine the quotient polynomial by dividing each one of the terms by x and combining the results. Therefore, dividing the polynomial $x^3 + 2x^2 - 5x + 0$ by x yields the quadratic function $x^2 + 2x - 5$, the quotient.

Now, after proving the Division and Factor Theorem and their applications, they can be used to prove Theorem 3.1.3.

Theorem 3.1.3. Let $f(x) \in F[x]$ be a polynomial over F of degree two or three. Then, $f(x)$ is irreducible if and only if it has no zeros in F, where F is $\mathbb{Q}$ or $\mathbb{R}$.

Proof. If $f(x)$ has a zero c in $\mathbb{Q}$, then by the Factor Theorem, there is a polynomial $g(x)$ such that $f(x) = (x - c)g(x)$ and the degree of $g(x)$ is lower than the degree of $f(x)$. This implies that if $f(x)$ is irreducible then it has no rational roots. If $f(x)$ is a reducible polynomial of degree two or three over $\mathbb{Q}$, then it has a factor of the form $(x - c)$ for some rational number c and $f(x) = (x - c)g(x)$. Then $f(x)$ has a zero $x = c$. We show that if $f(x)$ has no rational zeros, then $f(x)$ is irreducible. The proof remains valid for $F = \mathbb{R}$.

These fascinating theorems and corollaries bridge into some of the most significant findings of irreducibility over rationals contributed by Carl Gauss, a child prodigy and Prince of Mathematics.

Lemma 3.1.1. Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$. If $f(x)$ is reducible in $\mathbb{Z}[x]$, then it is also reducible in $\mathbb{Q}[x]$. More precisely, if $f(x) \in \mathbb{Z}[x]$, $f(x)$ can be factored into two polynomials of degree r and s in $\mathbb{Z}[x]$, then $f(x)$ can be factored into two polynomials with the same degrees r and s in $\mathbb{Q}[x]$.

Corollary 3.1.1. Let $(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $a_0 \neq 0.$ If $f(x)$ has a rational root, then it has a zero $c \in \mathbb{Z}$, and this zero divides a_0.

Proof. Let c be a rational zero of $f(x)$. Then $(x - c)$ is a linear factor of $f(x)$ over $\mathbb{Q}$. By Gauss' Lemma, $f(x)$ has a linear factor in $\mathbb{Z}[x]$ such that $f(x) = (dx + e)g(x)$, where $g(x)$ is a polynomial with integer coefficients and d and e are integers. The leading coefficient of $f(x)$ is 1, so d divides 1. In the equation $f(x) = (dx + e)g(x)$, d is either 1 or -1. This shows that $f(x)$ has an integer solution which is either e or $-e$.

3.2 Eisenstein's Criterion

Following Gauss' Lemma and several other lemmas we introduced involving the irreducibility of polynomials, we will prove Eisenstein's Criterion. Eisenstein's Criterion allows for the existence of irreducible polynomials of degree n over $\mathbb{Q}$, which are not always that easy to construct.

Theorem 3.2.1 (Eisenstein's Criterion). Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x], n \geq 1$. If there is a prime p such that $p|a_0, p|a_1, \ldots, p|a_{n-1}, p \nmid a_n,$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. The following is a proof by contradiction. Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x], n \geq 1$. By Gauss' Lemma, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$. Suppose $f(x) = g(x)h(x)$, such that $g(x) = b_dx^d + \cdots + b_0$ and $h(x) = c_ex^e + \cdots + c_0$, where $g(x)$ and $h(x)$ are polynomials with integer coefficients, and $d + e = n$. If $p|a_0$ and b_0c_0=a_0, $p|b_0c_0$. Since $p^2 \nmid a_0$, either $p|b_0$ or $p|c_0$, but not both. Let us assume $p|b_0$ and $p \nmid c_0$. Then, p divides $a_1 = b_1c_0 + b_0c_1$, and b_0, therefore, $p|b_1c_0$. Hence, $p|b_1$. Since p divides $a_2 = b_2c_0 + b_1c_1 + b_0c_2$, p divides $b_2c_0 = a_2 - b_1c_1 - b_0c_2$. So, p divides b_2 but not c_o. We continue this way for $a_3, \ldots, a_d$, and conclude by induction that p divides all $b_0, \ldots, b_d$.

The implication is that p divides a_n. This contradicts the condition $p \nmid a_n$. The proof is completed.

This implies p divides a_n, which is a contradiction.

Example 3.2.1. Use Eisenstein's Criterion to show that $f(x) = -7x^4 + 25x^2 - 15x + 10$ is irreducible in $\mathbb{Q}[x]$.

Our goal is to find some prime p such that that $p|a_0, p|a_1, \dots, p|a_{n-1}, p \nmid a_n,$ and $p^2 \nmid a_0$. Consider the prime $p = 5$, $5|10, 5| - 15$, and $5|25$. Additionally, $5 \nmid -7$, and $5^2 \nmid 10$. Therefore, by Eisenstein's Criterion, $f(x) = -7x^4 + 25x^2 - 15x + 10$ is irreducible over $\mathbb{Q}$.

Example 3.2.2. Use Eisenstein's Criterion to show that $f(x) = 5x^{11} - 6x^4 + 12x^3 + 36x - 6$ is irreducible in $\mathbb{Q}$.

Let $p = 2$. Since, $2|-6$, $2|12$, $2|36$, $2 \nmid 5$, and $2^2 \nmid -6$, by Eisenstein's Criterion, $f(x) = 5x^{11} - 6x^4 + 12x^3 + 36x - 6$ is irreducible over $\mathbb{Q}$.

Conclusion

In this thesis, I tried to connect Division Algorithm for integers and the irreducibility and zeros of a polynomial with the following Common and Core Standards:

CCSS.Math.Content.HSA.APR.A.1: Understand that polynomials form a system analogous to the integers, namely, they are closed under the operations of addition, subtraction, and multiplication; add, subtract, and multiply polynomials. Understand the relationship between zeros and factors of polynomials.

CCSS.Math.Content.HSA.APR.B.2: Know and apply the Remainder Theorem: For a polynomial p(x) and a number a, the remainder on division by x - a is p(a), so p(a) = 0 if and only if (x - a) is a factor of p(x).

CCSS.Math.Content.HSA.APR.B.3: Identify zeros of polynomials when suitable factorizations are available, and use the zeros to construct a rough graph of the function defined by the polynomial.

The motivation to connect them is an attempt to adapt the IL Learning Standards. "The ILS for math are designed to help students acquire a deep, conceptual understanding of core math content by adding focus, coherence, and rigor to learning. Focus is the study of a few key concepts; shifting teaching/learning from a mile long and an inch deep model to deeper understanding of fewer concepts. Coherence is making math connections between grade levels logical building on progression. Rigor is the equal balance of conceptual understanding, application, and procedural skill and fluency. These key shifts in math teaching and learning will focus on concept mastery and will allow students to build upon previous skills, create opportunities for deeper conceptual mathematical understanding and application." (ISBE, 2003).

High school mathematics has been stained as fearful and challenging. A high school mathematics course is built upon several expectations that are demanding and can be overwhelming for a teenager. *Catalyzing Change* defines "mathematically demanding courses as those courses that require clarity precision in reasoning, have focused and significant mathematics learning standards, and approach the mathematics in an instructionally balanced way that includes attention to conceptual understanding, procedural fluency, problem solving, and mathematical reasoning and critical thinking practices" (NCTM, 2018). As educators, we should work to align our curriculum to these standards and bring our students up to these standards as well. This type of expectation can be met with hard work and dedication from both the teacher and students. Although there are students who enjoy mathematics at a high school level past algebra, the majority are intimated by its complexity and find difficulty in applying it to their studies. Through the various theorems we have introduced in our writing: Division Theorem, Gauss' Lemma, Eisenstein's Criterion, it is our hope that these are theorems we can introduce in conversation in high school classrooms. Moving forward, I hope that through our effort to engage and intrigue students to explore conceptual understanding of theorems of integers and polynomials, students can overcome the fear and anxiety so that the exploration of higher-level mathematics may open a door for creativity and a sense of accomplishment for them and prepare them for the challenge in the future.

References

Common Core State Standards for Mathematics [PDF]. (2018). Common Core State Standards Initiative.

Crandall, R., & Pomerance, C. (2001) The Uniquity of Prime Numbers. In: Prime Numbers. Springer, New York, NY. https://doi.org/10.1007/978-1-4684-9316-0_8

Herstein, I. N. (1996). *Abstract Algebra* (3rd Edition). New Jersey: Prentice-Hall.

Hogan, J. (2014, May 13). Using the Rules of Divisibility Effectively. Retrieved September 09, 2021, from scholastic.com/parents/school-success/learning-toolkit-blog/using-rules-divisibility-effectively.html

Illinois Learning Standards. Mathematics: Illinois State Board of Education 1997.

National Council of Teachers of Mathematics (NCTM). (2018). *Catalyzing Change in High School Mathematics*. Reston VA: Author.

National Council of Teachers of Mathematics (NCTM). (2014). *Principles to actions: Ensuring mathematical success for all*. Reston VA: Author.

National Council of Teachers of Mathematics (NCTM). (2020). *Standards for the preparation of secondary mathematics teachers*. Reston, VA: Author.

Nicholas H. Wasserman (2016), Abstract Algebra for Algebra Teaching: Influencing School Mathematics Instruction, *Canadian Journal of Science, Mathematics and Technology Education*, Vol 16, No1, 28-47.

Nicholas H. Wasserman (2018), Connecting *abstract algebra to secondary mathematics, for secondary mathematics teachers*. In J. Cai and J. A. Middleton (Eds.), Research in Mathematics Education Series. Cham, Switzerland: Springer.

Oklahoma State University. Lecture 7: The Division Algorithm. Retrieved September 15, 2021, from https://math.okstate.edu/people/binegar/3613/3613-l07.pdf

Peterson, Alvin, J., & Hashisaki. (1971). *Theory of Arithmetic* (Third Edition).