# The Fundamental Theorem of Algebra

### 2.1 Gauss's Dissertation

The most important functions in algebra and analysis are the polynomial functions. In general, a polynomial function is represented by the formula $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where the *coefficients* $a_n,\ a_{n-1},\ \ldots, a_1,\ a_0$ are members of an algebraic system called a *ring*. The Fundamental Theorem of Algebra asserts that every non-constant polynomial function with complex (including real) coefficients admits at least one *root* in the field of complex numbers. The first proof of this theorem appears in the doctoral dissertation of C. F. Gauss, which he defended in 1799 at the age of twenty-two.

### 2.2 If Polynomials Are All That Important, Then Why Are There No Rock Songs Written About Them?

Polynomials are a big topic in high school algebra. Starting as early as grade 9, we are called upon to explore their inherent mysteries. As we progress through grades 10, 11 and 12, vast swaths of our precious teenage years are brutally sacrificed to them. Through an endless succession of worksheets, we are prevailed upon to probe and massage them in every way imaginable. We evaluate them, manipulate them, analyze them, compute their sums, differences, products, quotients and remainders, to say nothing of all that dreadful business about factoring them, extracting their roots and sketching their graphs.

"What is all this for?!", the poor student might be heard protesting.

"Trust me," the poor teacher might be heard imploring, "this is very important!".

But, had your teacher succeeded in capturing your attention long enough to explain to you in some detail why polynomials are important, chances are the explanation would not have made much of an impression on you anyway, especially in light of your more urgent teenage aspirations, like seeking romance, making a fashion statement, or projecting a cool facade. Even at the college level, some students of mathematics still cannot find reason to make peace with polynomials.

Why are polynomials accorded so much importance in the mathematics curriculum, you ask? For one thing, they are an essential part of the "chemistry of mathematics". In just about every branch of mathematics, a solid understanding of them is essential if progress beyond the high school level is to be attained. For instance, in the context of building a theory of analytic functions, the polynomial functions serve as the fundamental building blocks, playing a role very much analogous to the role played by the integers in the context of building the system of real numbers. More generally, polynomials provide a crucial two-way connection between algebra and analysis, by means of which the discrete methods of algebra can be brought to bear upon the continuous problems of analysis, and vice versa.

## 2.3 Polynomials in $\mathcal{R}[x]$

Much of the material covered in this and later sections relates directly to our knowledge of polynomials acquired through high school algebra. Let $\mathcal{R}$ denote a commutative ring with identity, such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}_n$ (see Section 1.5 for details). By definition, a *polynomial with coefficients in* $\mathcal{R}$ is an expression of the form $P = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where the coefficients $a_n,\ a_{n-1},\ \ldots, a_1,\ a_0$ belong to $\mathcal{R}$. In a polynomial, the special symbol $x$, called an *indeterminate*, serves only as a formal place holder. It obeys the same formal rules (ring axioms) as a typical member of $\mathcal{R}$, but need not be a member of $\mathcal{R}$. The set of all polynomials in $x$ with coefficients in $\mathcal{R}$ is denoted by the symbol $\mathcal{R}[x]$.

$$\boxed{\mathcal{R}[x] = \left\{ P \;\middle|\; P = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,\ \text{where } a_n,\ a_{n-1},\ \ldots, a_1,\ a_0 \in \mathcal{R} \right\}}$$

Let $P \in \mathcal{R}[x]$, and suppose the highest power of $x$ in $P$ appears in conjunction with the non-zero coefficient $a_n$. Then, according to standard terminology, the coefficient $a_n$ is called the *leading coefficient* of $P$, and the corresponding index $n$ is called the *degree* of $P$. The special coefficient $a_0$ is called the *constant coefficient* of $P$.

**Ex**: If $P = 3x^5 + 4x^3 - x^2 + 7x - 4 \in \mathbb{Z}[x]$, then the degree of $P$ is 5, the leading coefficient of $P$ is 3, and the constant coefficient of $P$ is -4.

As we might recall from high school algebra, two polynomials in $\mathbb{R}[x]$ are considered equal if and only if their corresponding coefficients are equal.

**Ex**: Suppose $P,\ Q \in \mathbb{R}[x]$, where $P = 5x^3 + 2x - 7$ and $Q = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Then $P = Q$ if and only if $a_4 = 0$, $a_3 = 5$, $a_2 = 0$, $a_1 = 2$ and $a_0 = -7$.

It may comfort the reader to learn that this important principle is valid in general. That is, two polynomials in $\mathcal{R}[x]$ are considered equal iff their corresponding coefficients are equal.

In high school algebra we acquired a great deal of experience combining polynomials by way of the operations of addition, subtraction and multiplication.

**Ex**: If $P = 3x^2 + 4x - 1 \in \mathbb{R}[x]$ and $Q = x^3 + 2x \in \mathbb{R}[x]$ then:
$P + Q = x^3 + 3x^2 + 6x - 1$
$P - Q = -x^3 + 3x^2 + 2x - 1$
$PQ = 3x^5 + 4x^4 + 5x^3 + 8x^2 - 2x$

The same algebraic rules that we learned in high school for combining polynomials in $\mathbb{R}[x]$ are valid also for the polynomials in $\mathcal{R}[x]$, for any coefficient ring $\mathcal{R}$.

**Ex**: If $P = 3x^2 + 4x - 1 \in \mathbb{Z}_5[x]$ and $Q = x^3 + 2x \in \mathbb{Z}_5[x]$ then:
$P + Q = x^3 + 3x^2 + x + 4$
$P - Q = 4x^3 + 3x^2 + 2x + 4$
$PQ = 3x^5 + 4x^4 + 3x^2 + 3x$

Strange things can happen, however, if the coefficient ring $\mathcal{R}$ is not an *integral domain.* By an integral domain we mean a commutative ring with identity wherein the product of any two non-zero elements is not zero. In other words, the equation $ab = 0$ implies that either $a = 0$ or $b = 0$. For instance, the ring $\mathbb{Z}_6$ is not an integral domain, since $2 \times 3 = 0$. However, every field is an integral domain (simple exercise for the reader).

A familiar principle from high school algebra asserts that the degree of the product of two polynomials equals the sum of their individual degrees. That is, $\deg(PQ) = \deg(P) + \deg(Q)$. Upon some reflection, we see that this formula is equivalent to the assertion that the leading coefficient of the product $PQ$ equals the product of the leading coefficients of $P$ and $Q$. However, if the coefficient ring $\mathcal{R}$ is not an integral domain, then the product of the two leading coefficients of $P$ and $Q$ could be zero, resulting in a breakdown of this formula.

**Ex**: If $P = 3x^2 + 1 \in \mathbb{Z}_6[x]$ and $Q = 2x^3 + x^2 \in \mathbb{Z}_6[x]$ then $\deg(P) = 2$, $\deg(Q) = 3$, while $\deg(PQ) = \deg\left(3x^4 + 2x^3 + x^2\right) = 4 \neq 2 + 3$.

In high school algebra we also learned a method for dividing one polynomial by another. The method is analogous to the long division algorithm used in grade school arithmetic to divide one whole number by another.

**Ex**: Take $F = 4x^3 + 5x^2 + 2x - 1$ and $G = 2x + 1 \in \mathbb{R}[x]$. Dividing $F$ by $G$, we obtain the quotient $Q = 2x^2 + \frac{3}{2}x + \frac{1}{4}$ and the remainder $R = -\frac{5}{4}$. The calculation is displayed below.

$$
\begin{array}{r@{}l}
 & \;2x^2 + \tfrac{3}{2}x + \tfrac{1}{4} \\
2x+1 & \overline{\big)\,4x^3 + 5x^2 + 2x - 1} \\
 & \underline{-4x^3 - 2x^2} \\
 & \qquad\quad 3x^2 + 2x \\
 & \qquad \underline{-3x^2 - \tfrac{3}{2}x} \\
 & \qquad\qquad\quad \tfrac{1}{2}x - 1 \\
 & \qquad\qquad \underline{-\tfrac{1}{2}x - \tfrac{1}{4}} \\
 & \qquad\qquad\qquad\quad -\tfrac{5}{4}
\end{array}
$$

To perform the above calculation, we see that it was necessary to be able to divide by the elements of the coefficient ring. For instance, the coefficients $\frac{3}{2}$ and $\frac{1}{4}$ appearing in the quotient $Q$ were obtained as a result of dividing by the elements 2 and 4, respectively. In other words, we had to use the fact that $\mathbb{R}$ is a field. In general, the division algorithm for polynomials in $\mathcal{R}[x]$ is feasible when and only when the coefficient ring is a field.

For the remainder of this module it will be assumed that the coefficient ring $\mathcal{R}$ is a field. It will turn out that virtually all of the familiar results about polynomials covered in high school algebra remain valid in $\mathcal{F}[x]$, for any field $\mathcal{F}$.

### 2.4 Polynomials and Polynomial Functions in $\mathcal{F}[x]$

Until now, we have not had occasion to distinguish between "polynomials" and "polynomial functions". Unless you have taken a course in abstract algebra, it is unlikely that you have ever encountered or given any thought to this distinction. It turns out to be a very important distinction, especially if you wish to understand polynomials from a perspective slightly more advanced than that of high school algebra.

In contrast to polynomials, which are completely identified by their coefficients, functions are completely indentified by their input and ouput values. That is, two polynomials are equal iff they have the same corresponding coefficients, while two functions are equal iff they return the same output values for the same input values. For instance, consider the two polynomials in $\mathbb{Z}_3[x]$ given by $P = x^3 + x^2 + x + 2$ and $Q = x^2 + 2x + 2$. Plainly these two polynomials are distinct because their corresponding coefficients are different. Now compare the corresponding functions $f(x) = x^3 + x^2 + x + 2$ and $g(x) = x^2 + 2x + 2$, whose input and output values we can easily tabulate as follows:

$f(0) = 2 = g(0)$
$f(1) = 2 = g(1)$
$f(2) = 1 = g(2)$

Thus $f(x) = g(x)$ for all $x \in \mathbb{Z}_3$, which means that $f$ and $g$ are equal as functions.

According to standard terminology, the polynomial $P = a_n x^n + \cdots + a_1 x + a_0 \in \mathcal{F}[x]$ is said to *induce* the polynomial function $f(x) = a_n x^n + \cdots + a_1 x + a_0$, whose input and output values lie in the field $\mathcal{F}$. As the above example shows, there are circumstances under which two different polynomials can induce the same polynomial function. It turns out that this phenomenon cannot occur except in finite fields. In infinite fields, such as $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, polynomials are basically indistinguishable from the polynomial functions they induce. In any event, provided we bear in mind the distinction between polynomials and polynomial functions when dealing with finite fields, there is never any ambiguity in denoting polynomials by the familiar functional symbolism $f(x) = a_n x^n + \cdots + a_1 x + a_0$ .

Let $f(x) \in \mathcal{F}[x]$. An element $r \in \mathcal{F}$ is called a *root* of the polynomial $f(x)$ iff $f(r) = 0$.

**Ex**: a) $r = \frac{2}{5}$ is a root of $f(x) = 5x^2 + 3x - 2 \in \mathbb{Q}[x]$, since $f\left(\frac{2}{5}\right) = 0$
b) $r = 3 + \sqrt{2}$ is a root of $f(x) = x^2 - 6x + 7 \in \mathbb{R}[x]$, since $f(3 + \sqrt{2}) = 0$
c) $r = 3 + i\sqrt{2}$ is a root of $f(x) = x^2 - 6x + 11 \in \mathbb{C}[x]$, since $f(3 + i\sqrt{2}) = 0$
d) $r = 2$ is a root of $f(x) = x^3 + x^2 + 3 \in \mathbb{Z}_5[x]$, since $f(2) = 0$

For any field $\mathcal{F}$, the polynomials in $\mathcal{F}[x]$ behave much like the familiar polynomials of high school algebra. Below we collect a number of classic propositions pertaining the behavior of polynomials and their roots in $\mathcal{F}[x]$. The proofs are omitted, but can be found in any one of a number of standard references such as Hungerford's *Absract Algebra, An Introduction*.

1) If $f(x)$ and $g(x) \in \mathcal{F}[x]$, then $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

2) Given $f(x)$ and $g(x) \in \mathcal{F}[x]$, and $g(x) \neq 0$, there exist unique $q(x)$ and $r(x) \in \mathcal{F}[x]$ (quotient and remainder), such that $\deg(r(x)) < \deg(g(x))$ and $f(x) = q(x)g(x) + r(x)$.

3) For any given $f(x) \in \mathcal{F}[x]$ and $a \in \mathcal{F}$, we can find a unique $q(x) \in \mathcal{F}[x]$ such that $f(x) = (x - a)q(x) + f(a)$.

4) Let $f(x) \in \mathcal{F}[x]$, then $x = a$ is a root of $f(x)$ iff $x - a$ is a factor of $f(x)$.

5) Let $f(x) \in \mathcal{F}[x]$. If $\deg(f(x)) = n$, then $f(x)$ possesses at most $n$ roots in $\mathcal{F}$.

As we saw in Section 1.4, it is not always possible to find a root in the coefficient field $\mathcal{F}$ for a given polynomial $f(x) \in \mathcal{F}[x]$.

**Ex**: a) $f(x) = x^2 - 5 \in \mathbb{Q}[x]$ possesses no roots in $\mathbb{Q}$.
b) $f(x) = x^2 + 5 \in \mathbb{R}[x]$ possesses no roots in $\mathbb{R}$.
c) $f(x) = x^2 + x + 1 \in \mathbb{Z}_5[x]$ possesses no roots in $\mathbb{Z}_5$.

On the other hand, if every non-constant polynomial $f(x) \in \mathcal{F}[x]$ possesses at least one root $r \in \mathcal{F}$, then the field $\mathcal{F}$ is worthy of a special name. It is said to be *algebraically complete*. Basically, what this means is that every polynomial equation can be solved without having to venture away from home. As the above examples show, none of the fields $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{Z}_5$ is algebraically complete. However, it turns out that every field $\mathcal{F}$ can be *embedded* as a subfield of larger field $\mathcal{K}$ which is algebraically complete. The smallest such field $\mathcal{K}$ is called the *algebraic completion* of $\mathcal{F}$. The area of mathematics that deals with issues of this kind, called extension theory, is generally not accessible at the undergraduate level.

### 2.5 Roots of Polynomial Functions

In this section, we examine some basic facts pertaining to the roots of polynomials with coefficients in the specific fields $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. Our discussion begins with the finite fields of type $\mathbb{Z}_p$ and ends with the algebraically complete field $\mathbb{C}$.

For a given prime number $p$, it can easily be shown, by the methods of elementary number theory, that the ring $\mathbb{Z}_p$ is actually a field. Moreover, it can be shown that the relation $x^p = x$ holds for every $x \in \mathbb{Z}_p$ (Fermat's Little Theorem). It follows that every polynomial in $\mathbb{Z}_p[x]$ induces a polynomial function whose degree is at most $p-1$.

**Ex**: For $p = 3$, the polynomial $P = x^7 + x^5 + 2x^4 + x^3 + x + 2 \in \mathbb{Z}_3[x]$ induces the polynomial function $f(x) = x^7 + x^5 + 2x^4 + x^3 + x + 2$ which, via the relation $x^3 = x$, reduces to $f(x) = 2x^2 + x + 2$.

Thus, the study of roots of polynomials in $\mathbb{Z}_p[x]$ reduces to the study of roots of polynomial functions $f(x) = a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$, whose degrees do not exceed $p-1$. Given such a polynomial function, we can determine all of its roots in a finite number of steps. All we have to do is test each of the elements of $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

**Ex**: Take $f(x) = x^3 + 4x^2 + 4x + 3 \in \mathbb{Z}_5[x]$. By direct computation we get:

$f(0) = 3$
$f(1) = 2$
$f(2) = 0$
$f(3) = 3$
$f(4) = 2$

Thus, the only root is $x = 2$.

The above method of finding roots in $\mathbb{Z}_p$ is practical only if $p$ is small. If $p$ is large, say possessing several hundred digits, not even the most super-advanced technology could ever be fast enough to perform the calculation within the lifetime of the universe. This is not to say that efficient algorithms do not exist for finding the roots. However, a discussion of these algorithms would take us beyond the normal scope of undergraduate mathematics.

For polynomials in $\mathbb{Q}[x]$ the problem of finding the rational roots, if any, is completely answered by an elementary principle called the *Rational Roots Theorem.*

Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$. Without loss of generality, we are entitled to assume that each of the rational coefficients $a_j$ is a fraction in lowest terms. Let $d$ denote the lowest common denominator of all of the coefficients $a_j$. According to the Rational Roots Theorem, a rational number $\pm\frac{r}{s}$ (in lowest terms) might be a root of $f(x)$ only if $r$ is a positive divisor of $a_0 d$ and $s$ is a positive divisor of $a_n d$. We see that there are only finitely many possibilities to test, and every rational root, if any, must be among these possibilities.

**Ex**: Let $f(x) = 2x^3 + \frac{7}{3}x^2 + \frac{8}{3}x + \frac{5}{3}$. The lowest common denominator of the coefficients is $d = 3$. So, if $\pm\frac{r}{s}$ is a root, then $s$ must be a divisor of $2 \times 3 = 6$ and $r$ must be a divisor of $\frac{5}{3} \times 3 = 5$. Since the positive divisors of 6 are $\{1, 2, 3, 6\}$ and the positive divisors of 5 are $\{1, 5\}$, the only potential candidates for roots are:

$$\tfrac{r}{s} = \pm\tfrac{1}{1},\ \pm\tfrac{1}{2},\ \pm\tfrac{1}{3},\ \pm\tfrac{1}{6},\ \pm\tfrac{5}{1},\ \pm\tfrac{5}{2},\ \pm\tfrac{5}{3},\ \pm\tfrac{5}{6}$$

Testing each of these sixteen values in turn, we find $f(1) = 0$, $f\left(\frac{1}{3}\right) = 0$ and $f\left(-\frac{5}{2}\right) = 0$.

For a polynomial function $f(x) \in \mathbb{R}[x]$ the problem of finding its real roots, if any, is best understood in terms of the behavior of the graph of $y = f(x)$. Plainly $x_0$ is a root of $y = f(x)$ iff the graph of $y = f(x)$ intersects the $x$-axis at $x = x_0$. With the aid of a good graphing device, it is often possible to the determine the number of real roots of $y = f(x)$ and their approximate whereabouts. On the other hand, if $f(x)$ possesses no real roots, then its graph must be confined entirely and strictly to one side of the $x$-axis (either above or below). Equivalently, $f(x)$ possesses no real roots iff the absolute minimum value of $y = f(x)$ is a positive number or the absolute maximum value of $y = f(x)$ is a negative number.

A polynomial of even degree in $\mathbb{R}[x]$ may or may not possess a real root. For instance, $x^2 + 5$ possesses no real roots, while $x^2 - 5$ possesses two real roots. However, if $f(x) \in \mathbb{R}[x]$ is of odd degree, then it must possess at least one real root. To see why, consider the influence of the leading term $a_n x^n$ on the behavior of the graph of $y = f(x)$. As $x \to \pm\infty$, the leading term dominates the behavior of the graph. Since $n$ is odd, the graph either descends infinitely to the left and ascends infinitely to the right, or ascends infinitely to the left and descends infinitely to the right. Consequently, the graph, being continuous, must cross the $x$-axis at some point, at which we have a root of $f(x)$.

For polynomials in $\mathbb{C}[x]$, the question of existence of roots in $\mathbb{C}$ is completely answered by the following statement, known as the *Fundamental Theorem of Algebra*:

**Every polynomial in $\mathbb{C}[x]$ possesses at least one root in $\mathbb{C}$.**

Another way to express this theorem is to say that the field $\mathbb{C}$ is algebraically complete.

Among the more important consequences of this theorem is the fact that every polynomial with coefficients in $\mathbb{C}$ can be factored completely as a product of linear factors.

In keeping with tradition, we use the symbol $z$ to denote a complex variable. The complete factorization of a polynomial function $f(z) = c_n z^n + \cdots + c_1 z + c_0 \in \mathbb{C}[z]$ is accomplished in the following way. By the Fundamental Theorem of Algebra, there exists at least one root, say $\lambda_1 \in \mathbb{C}$. Hence $z - \lambda_1$ is a factor of $f(z)$. That is, $f(z) = (z - \lambda_1) f_1(z)$, where $f_1(z)$ is a polynomial of degree $n-1$. Applying the Fundamental Theorem of Algebra to $f_1(z)$, we get $f(z) = (z - \lambda_1)(z - \lambda_2) f_2(z)$. Continuing in this manner, we ultimately arrive at the complete factorization of $f(z)$:

$$f(z) = c_n (z - \lambda_1)(z - \lambda_2) \cdots (z - \lambda_n)$$

In the above factorization, some of the roots may appear more than once. The number of times that a root appears is called its *multiplicity.* Evidently, the sum of the multiplicities of the roots is exactly equal to the degree.

By the Fundamental Theorem of Algebra, every polynomial $f(x) \in \mathbb{R}[x]$ can be factored as a product of a mixture of linear and quadratic polynomials with real coefficients. This stems from the fact that the complex (non-real) roots of $f(x)$ occur always in conjugate pairs. In other words, if the non-real value $\lambda = a + bi$ is a root of $f(x) \in \mathbb{R}[x]$ then its complex conjugate $\bar{\lambda} = a - bi$ is a root also (exercise for the reader). Thus, given the complete factorization of $f(x)$ over $\mathbb{C}$, each pair of linear factors $x - \lambda$ and $x - \bar{\lambda}$ corresponding to complex conjugate pairs can be grouped together and multiplied, yielding a quadratic polynomial $x^2 - (\lambda + \bar{\lambda})x + \lambda\bar{\lambda}$, whose coefficients are real.

**Ex**: Take the polynomial $f(x) = x^4 - x^3 - x^2 + 7x - 6 \in \mathbb{R}[x]$, whose complete factorization over $\mathbb{C}$ is $f(x) = (x - (1 + i\sqrt{2}))\,(x - (1 - i\sqrt{2}))\,(x - 1)\,(x + 2)$. After some manipulation, this equates to $f(x) = (x^2 - 2x + 3)\,(x - 1)\,(x + 2)$.

Every known proof of the Fundamental Theorem of Algebra invokes, in some crucial way, the topological concept of continuity. This is viewed by many mathematicians as somewhat quaint, since the concept of continuity is more germane to analysis than to algebra.

Probably the most elegant proof of the Fundamental Theorem of Algebra is that based on a famous result in complex analysis known as Liouville's Theorem. According to Liouville's Theorem, the only *bounded entire* functions $g(z)$ (of a complex variable) are the constant functions. In this context, by "bounded" we mean that $|g(z)| < M$ for some fixed value $M > 0$ and for all $z \in \mathbb{C}$, and by "entire" we mean that $g(z)$ is expressible as a power series $g(z) = a_0 + a_1 z + a_2 z^2 + \cdots$ which converges for all $z \in \mathbb{C}$.

Now suppose $f(z) = c_n z^n + \cdots + c_1 z + c_0 \in \mathbb{C}[z]$ is a non-constant polynomial, and suppose it possesses no roots in $\mathbb{C}$. This implies that the function $g(z) = 1/f(z)$ is entire, since it possesses no singularities. On the other hand, since the polynomial $f(z)$ is dominated by its leading term $c_n z^n$, which grows rapidly in all directions in the complex plane, it follows that its reciprocal $g(z)$ is bounded. Therefore, by Liouville's Theorem, the function $g(z)$ is constant, which implies that $f(z)$ is constant, contradicting our assumption. Therefore $f(z)$ must possess at least one root in the complex number field $\mathbb{C}$.

### 2.6 Exercises

1. Let $P = x^3 - 3x^2 + 2x - 1 \in \mathbb{Z}[x]$ and $Q = x^2 - 2x + 1 \in \mathbb{Z}[x]$. Perform the indicated operations and simplify.
   (a) $P + Q$
   (b) $P - Q$
   (c) $PQ$
2. Let $P = x^3 + 4x^2 + 3x + 1 \in \mathbb{Z}_5[x]$ and $Q = x^2 + 3x + 4 \in \mathbb{Z}_5[x]$. Perform the indicated operations and simplify.
   (a) $P + Q$
   (b) $P - Q$
   (c) $PQ$
3. Find the quotient $Q$ and the remainder $R$ resulting from the polynomial division $F \div G$.
   (a) $F = 6x^3 - 3x^2 + 2x - 4$ and $G = 3x - 1$ in $\mathbb{Q}[x]$
   (b) $F = 5x^3 + 2x^2 + 3x + 1$ and $G = 2x + 3$ in $\mathbb{Z}_7[x]$
   (c) $F = x^6 + 2x - 4$ and $G = x^2 + x + 1$ in $\mathbb{Q}[x]$
4. Use Fermat's Little Theorem ( $x^p = x$ for all $x \in \mathbb{Z}_p$ ) to find a reduced polynomial function of degree at most $p - 1$ induced by the given polynomial $P \in \mathbb{Z}_p[x]$.
   (a) $P = x^8 + 2x^5 + x^4 + x^2 + 1 \in \mathbb{Z}_3[x]$
   (b) $P = x^{28} + x^{25} + 6x^4 + x + 1 \in \mathbb{Z}_5[x]$
5. Find all roots in $\mathbb{Z}_p$ of the polynomial function $f(x) \in \mathbb{Z}_p[x]$.
   (a) $f(x) = x^2 - 2 \in \mathbb{Z}_7[x]$
   (b) $f(x) = x^4 + 2x^3 - x - 2 \in \mathbb{Z}_7[x]$
   (c) $f(x) = x^4 - 1 \in \mathbb{Z}_5[x]$
6. Use the Rational Roots Theorem to find all roots in $\mathbb{Q}$ of the polynomial function $f(x) \in \mathbb{Q}[x]$.
   (a) $f(x) = 2x^2 - x - 3$
   (b) $f(x) = x^4 - \frac{1}{10}x^3 + \frac{4}{5}x^2 - \frac{1}{10}x - \frac{1}{5}$
   (c) $f(x) = 6x^3 - x^2 + 24x - 4$
7. Use a graphing device to help determine the number of real roots of the polynomial function $f(x) \in \mathbb{R}[x]$.
   (a) $f(x) = 6x^3 - x^2 + 24x + 1$
   (b) $f(x) = x^4 + x^3 - x + 5$
   (c) $f(x) = x^4 + x^3 - x - 5$

8. Factor $f(z)$ completely as a product of linear factors over $\mathbb{C}$.
   (a) $f(z) = z^4 + z^3 - z - 1$
   (b) $f(z) = z^5 - 4z^3 + z^2 - 4$
9. Factor $f(x)$ completely as a product of a mixture of linear and quadratic factors with real coefficients.
   (a) $f(x) = x^4 + x^3 - x - 1$
   (b) $f(x) = x^5 - 4x^3 + x^2 - 4$
10. Show that if $\lambda \in \mathbb{C}$ is a root of $f(x) \in \mathbb{R}[x]$, then so is $\bar{\lambda}$.
11. Given that $3 + i\sqrt{2}$ is a root of $f(x) = x^4 - 6x^3 + 20x^2 - 54x + 99$, find all the remaining roots of $f(x)$.
12. Find a polynomial function $f(x) \in \mathbb{Z}_5[x]$ satisfying the condition $f(x) = 2^x$ (in $\mathbb{Z}_5$) for all $x \in \mathbb{Z}_5$.
13. Show that no polynomial function $f(x) \in \mathbb{R}[x]$ exists satisfying the condition $f(x) = 2^x$ for all $x \in \mathbb{R}$. [Hint: Use Calculus.]
14. [Challenge: Honors Project] Show that every function $f(x)$ from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ is equal to a polynomial function in $\mathbb{Z}_p[x]$.