Polynomials, Their Roots, and Symmetric Polynomials

Abstract

This week, we shall explore properties of polynomials, beginning with polynomials in one variable of the form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where n is a nonnegative integer, and $a_0, a_1, \dots, a_n$ are coefficients. In particular, we consider properties of the set of *roots* (or *zeroes*) of such polynomials.

Using the Vieta's Formulas as motivation, we then consider multivariable polynomials and *symmetric polynomials* in particular. Building from some these results, we shall explore connections between symmetric polynomials and the roots of a polynomial in one variable.

0 Warmup Exercise

Let $p(x) := x^2 + 4x + 10$, and let r, s denote its respective roots. *Note:* r and s are nonreal complex numbers.

Determine a quadratic polynomial $q(x)$ such that the roots of q are precisely r^2 and s^2. Can you compute $q(x)$ *without* first computing the values r and s?

1 Review: Polynomials in One Variable

Definition 1.1. The *polynomials* in x with complex coefficients, denoted $\mathbb{C}[x]$, is the set

$$\left\{p(x) := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 : n \in \mathbb{Z}, n \geq 0, a_0, a_1, \dots, a_n \in \mathbb{C}\right\},$$

Addition and multiplication in $\mathbb{C}[x]$ are defined in the usual way.

Similarly, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, and $\mathbb{Z}[x]$ denote, respectively, the sets of polynomials in x with coefficients in the real numbers, the rational numbers, and the integers, respectively. If $m \in \mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ denotes the ring of integers modulo m, then $\mathbb{Z}/m\mathbb{Z}[x]$ is the set of polynomials whose coefficients are the integers modulo m.

Notation:. Where the context is clear, we shall use notation like $p(x)$ and p interchangeably.

Example 1.2.

- $5x^2 + 2x - 3 \in \mathbb{Z}[x]$
- $-\frac{17}{3}x^4 - 2x + \frac{81}{16} \in \mathbb{Q}[x]$
- $-\pi x^5 + 13x^3 - e^{\sqrt{2}}x + \frac{5}{21} \in \mathbb{R}[x]$
- $(1-2i)x^4 + \left(\frac{7}{22} + (\log 8)i\right)x^3 - 14x^2 + \frac{87}{13}ix + \left(\cos\frac{2\pi}{7} + \sin\frac{2\pi}{7}i\right) \in \mathbb{C}[x]$

Remark. Since $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, we likewise have the chain of inclusions $\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$. For example, a polynomial with rational coefficients also has complex coefficients. Conversely, given a polynomial $p(x) \in \mathbb{Z}[x]$, we can view the coefficents modulo m in order to obtain the associated polynomial in $\mathbb{Z}/m\mathbb{Z}[x]$.

1.1 How would you define polynomials in multiple variables? For example, if x and y are indeterminates, how might you define $\mathbb{C}[x, y]$, the set of polynomials over $\mathbb{C}$ in both x and y? What about $\mathbb{C}[x_1, x_2, \ldots, x_n]$?

1.2 What is the *degree* of a polynomial p (denoted $\deg p$)? (Ideally, you should be able to answer this for polynomials in one variable, as well as in multiple variables.)

1.3 Let $p(x) \in \mathbb{C}[x]$. What is a *root* or *zero* of p?

1.4 First, we explore a relationship between degree 1 factors of polynomials and their roots:

Theorem 1.3 (Polynomial Remainder Theorem)**.** *Let $p \in \mathbb{C}[x]$ and $c \in \mathbb{C}$. Then the remainder when dividing $p(x)$ by $x-a$ is the constant $p(c)$. (That is, p is expressible in the form $p(x) = (x-c)q(x) + p(c)$ for some polynomial q, and where $p(c)$ is the constant.)*

Note: Our priority is that you understand and can use this theorem later. Being able to prove it would be a bonus, but secondary.

1.5 Next, we present an important corollary to Theorem 1.3:

Corollary 1.3(a). *If $p \in \mathbb{C}[x]$ and $c \in \mathbb{C}$, then $x - c$ divides p if and only if $p(c) = 0$.*

Note: Again, the priority is being able to understand and apply this Corollary, not prove it.

2 The Fundamental Theorem of Algebra and Vieta's Formulas

We begin with the following, whose proof is beyond the scope of this session:

Theorem 2.1 (The Fundamental Theorem of Algebra)**.** *Let $p(x) := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with coefficients $a_0, a_1, \ldots, a_n$ lying in $\mathbb{C}$. If p is not a constant polynomial, then p has at least one root in $\mathbb{C}$.*

Remark. To better appreciate the value of The Fundamental Theorem of Algebra, we note that it uses *in an essential way* that the coefficients and roots of our polynomial both lie in $\mathbb{C}$, the field of complex numbers. For example:

- $3x - 2 \in \mathbb{Z}[x]$ has the unique root $r := \frac{2}{3}$, and this roots is not *an integer*
- $x^2 - 2 \in \mathbb{Q}[x]$ has the roots $\pm\sqrt{2}$, which are not rational
- $x^2 + 1 \in \mathbb{R}[x]$ has the roots $\pm i$, which are not real numbers
- $x^2 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x]$ has no roots lying in $\mathbb{Z}/2\mathbb{Z}$

Corollary 2.1(a). *Let $p(x) := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree $n \geq 1$. Then there exist $r_1, r_2, \ldots, r_n \in \mathbb{C}$, not necessarily distinct, such that*

$$p(x) = a_n (x - r_1)(x - r_2) \cdots (x - r_n).$$

That is, a nonconstant complex polynomial of degree n has precisely n complex roots, including multiplicity.[1]

The Fundamental Theorem and its corollary tell us that every nonconstant complex polynomial "splits linearly", meaning it is expressible as product of one nonzero constant and n monic[2] polynomials of degree 1. Now that we know every nonconstant polynomial over $\mathbb{C}$, let us use this to explore the relationship between the roots and coefficients of a polynomial:

2.1 Consider the polynomial $p(x) := 2x^2 + 3x - 5$. By The Fundamental Theorem of Algebra, p has precisely two roots, which we shall denote by r and s. Compute $r + s$ and rs. Can you do so *without* first computing r and s?

2.2 Let $p(x) := 5x^3 - 14x^2 - 2x + 8$, and denote its roots (including possible repetitions) by r_1, r_2, r_3. Compute the values

$$r_1 + r_2 + r_3$$
$$r_1 r_2 + r_1 r_3 + r_2 r_3$$
$$r_1 r_2 r_3.$$

2.3 Let $p(x) := 3x^5 + 17x^4 - 12x^3 - 68x^2 + 12x + 68$, and denote its roots (including possible repetitions) by r_1, r_2, r_3, r_4, r_5. Compute the values

$$r_1 + r_2 + r_3 + r_4 + r_5 \text{ and } r_1 r_2 r_3 r_4 r_5.$$

In the context of Exercise#2.2, what other expressions in the r_j can we also compute?

[1] The *multiplicity* of a root r_j of the nonzero polynomial p is the largest positive integer n_j such that $(x - r_j)^{n_j}$ divides p. This corollary therefore counts not just how many distinct roots p has, but also their multiplicity.

[2] If $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial, we say p is *monic* if and only if $a_n = 1$, where $n := \deg p$.

2.4 Let $p(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial over $\mathbb{C}$ with degree $n \geq 1$. Further, let $r_1, r_2, \ldots, r_n$ be the roots of p, including possible repetitions. Compute the values

$$\begin{gathered} r_1 + r_2 + \cdots + r_n \\ r_1 r_2 + \cdots r_1 r_n + r_2 r_3 + \cdots r_2 r_n + \cdots + r_{n-1} r_n \\ r_1 r_2 r_3 + \cdots + r_{n-2} r_{n-1} r_n \\ \vdots \\ r_1 r_2 \cdots r_{n-1} + \cdots + r_2 r_3 \cdots r_n \\ r_1 r_2 \cdots r_n \end{gathered}$$

in terms of the coefficients $a_0, a_1, \ldots, a_n$. The resulting equations are called *Vieta's Formulas.*

2.5 Let r, s be the roots of the polynomial $p(x) := x^2 + 4x + 7$.

What is the value of

$$r^3 + s^3?$$

Can you compute the value of

$$r^2 s + r s^2 + 11 r s,$$

as well?

3 Polynomials in Multiple Variables and Symmetric Polynomials

Vieta's Formulas help us connect the coefficients of a polynomial p in one variable to the relevant expressions in the roots $r_1, r_2, ..., r_n$ of p. Note that these expressions are multivariable polynomial expressions in the r_j, too. For example, if $e_n(x_1, x_2, \ldots, x_n) := x_1 x_2 \cdots x_n$, then evaluating at the point $(r_1, r_2, \cdots, r_n) \in \mathbb{C}^n$, we have

$$e_n(r_1, r_2, \cdots, r_n) = (-1)^n \cdot \frac{a_0}{a_n}.$$

Further, e_1 is such that any permutation of the variables $x_1, x_2, \dots, x_n$ does not change the polynomial e_1. (For example, $e_1(x_1, x_2, x_3) = e_1(x_3, x_1, x_2) = e_1(x_2, x_1, x_3)$, etc.) The form of the identites in Vieta's Formulas therefore motivates us to properties of certain classes of multivariable polynomial functions.

Definition 3.1. Let $p(x_1, x_2, \dots, x_n) \in \mathbb{C}[x_1, x_2, \dots, x_n]$. Then p is a *symmetric polynomial* if and only if for every permutation[3] τ on the set $\{1, 2, \dots, n\}$,

$$p(x_1, x_2, \dots, x_n) = p\left(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}\right).$$

Example 3.2. The following are examples—and nonexamples—of symmetric polynomials in $\mathbb{C}[x_1, x_2, \dots, x_n]$:

- $p(x, y) := x^2 + 5xy + y^2$ is symmetric in $\mathbb{C}[x, y]$
- $p(x, y) := x^2 + 5xy - 2y^2$ is not symmetric in $\mathbb{C}[x, y]$

  To see this, note that $p(y, x) = y^2 + 5xy - 2x^2$, and therefore $p(x, y) \neq p(y, x)$. Therefore, the permutation that transposes x and y shows that p is not symmetric.
- For every nonnegative integer k,

  $$\sigma_k(x_1, x_2, \dots, x_n) := x_1^k x_2^k + \cdots + x_n^k$$

  is symmetric in $\mathbb{C}[x_1, x_2, \dots, x_n]$. Each σ_k is called the *power sum polynomial of degree k*.
- If $a \in \mathbb{C}$ is a constant, and p, q are symmetric polynomials in $\mathbb{C}[x_1, x_2, \dots, x_n]$, then so are ap, $p + q$, and pq.
- Whether a polynomial is symmetric depends not just on the polynomial, but on the ambient space of polynomials.

  For example, $x^2 + 5xy + y^2$ is symmetric in $\mathbb{C}[x, y]$, but it is *not* symmetric in $\mathbb{C}[x, y, z]$. In the latter ring, $p(x, z, y) = x^2 + 5xz + z^2 \neq x^2 + 5xy + y^2 = p(x, y, z)$.

[3] *Question:* Do you understand what a permutation on a set S is? If not, please ask!

Definition 3.3. The *elementary symmetric polynomials* in $\mathbb{C}[x_1, x_2, \dots, x_n]$ are the following:

$$
\begin{aligned}
e_0(x_1, x_2, \dots, x_n) &:= 1 \\
e_1(x_1, x_2, \dots, x_n) &:= x_1 + x_2 + \cdots + x_n \\
e_2(x_1, x_2, \dots, x_n) &:= \sum_{1 \le j_1 < j_2 \le n} x_{j_1} x_{i_2} \\
e_3(x_1, x_2, \dots, x_n) &:= \sum_{1 \le j_1 < j_2 < j_3 \le n} x_{j_1} x_{j_2} \\
\vdots \quad & \quad \vdots \\
e_k(x_1, x_2, \cdots x_k) &:= \sum_{1 \le j_1 < j_2 < \cdots < j_k \le n} x_{j_1} x_{j_2} \cdots x_{j_k} \\
\vdots \quad & \quad \vdots \\
e_{n-1}(x_1, x_2, \dots, x_n) &:= \sum_{1 \le j_1 < j_2 < j_3 \le n} x_{j_1} x_{j_2} \cdots x_{j_{n-1}} \\
e_n(x_1, x_2, \dots, x_n) &:= x_1 x_2 \cdots x_n.
\end{aligned}
$$

That is, for each k with $1 \le k \le n$, each e_k is the sum over all distinct k-at-a-time products over $\{x_1, x_2, \dots, x_n\}$.

Example 3.4.

- In $\mathbb{C}[x, y, z]$, we have

$$
\begin{aligned}
e_1(x, y, z) &:= x + y + z \\
e_2(x, y, z) &:= xy + xz + yz \\
e_3(x, y, z) &:= xyz.
\end{aligned}
$$

- For every positive integer $n \ge 2$, in $\mathbb{C}[x_1, x_2, \dots, x_n]$, we have

$$
\begin{aligned}
e_{n-1}(x_1, x_2, \dots, x_n) := x_1 x_2 \cdots x_{n-2} x_{n-1} \\
+ x_1 x_2 \cdots x_{n-2} x_n \\
+ x_1 x_2 \cdots x_{n-3} x_{n-1} x_n \\
+ \cdots \\
+ x_1 x_3 \cdots x_{n-1} x_n.
\end{aligned}
$$

- Let $p(x) \in \mathbb{C}[x]$ be a polynomial of degree n, and whose roots (including multiplicity) are $r_1, r_2, \dots, r_n$. Then we can express Vieta's Formulas (Exercise #2.4) in terms of elementary symmetric polynomials:

$$\begin{aligned} e_1(r_1, r_2, \ldots, r_n) &= -\frac{a_{n-1}}{a_n} \\ e_2(r_1, r_2, \ldots, r_n) &= \frac{a_{n-2}}{a_n} \\ \vdots &= \vdots \\ e_k(r_1, r_2, \ldots, r_n) &= (-1)^k \cdot \frac{a_{n-k}}{a_n} \\ \vdots &= \vdots \\ e_n(r_1, r_2, \ldots, r_n) &= (-1)^n \cdot \frac{a_0}{a_n}. \end{aligned}$$

3.1 Consider the symmetric polynomial $p(x, y) := x^3 + y^3 \in \mathbb{C}[x, y]$. Express p in terms of the elementary symmetric functions in $\mathbb{C}[x, y]$.

3.2 Consider the symmetric polynomial $p(x, y, z) := x^2 + y^2 + z^2 \in \mathbb{C}[x, y, z]$. Express p in terms of elementary symmetric functions.

3.3 Let $p(x, y, z) \in \mathbb{C}[z, y, z]$ be a symmetric polynomial containing the monomial xyz^2. What other terms must appear in p?

3.4 **[Challenging:]** Prove the following theorem.

Theorem 3.5 (The Fundamental Theorem of Symmetric Polynomials)**.** *Let p be any symmetric polynomial in $\mathbb{C}[x_1, x_2, \ldots, x_n]$. Prove that there exists some polynomial q—itself not necessarily symmetric!—such that $q \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ and*

$$p(x_1, x_2, \ldots, x_n) = q\left(e_1(x_1, x_2, \ldots, x_n), e_2(x_1, x_2, \ldots, x_n), \ldots, e_n(x_1, x_2, \ldots, x_n)\right).$$

Furthermore, q is uniquely determined by by p.

4 Playing with Polynomials

4.1 Let x be a number such that

$$x + \frac{1}{x} = 1.$$

What is the value of

$$x^2 + \frac{1}{x^2}?$$

Can you compute the value of

$$x^3 + \frac{1}{x^3}$$

as well? Can you further generalize?

4.2 Let $\alpha \in \mathbb{C}$. We say that α is an *algebraic number* if and only if there exists some nonconstant polynomial $p \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$. One can show that for every algebraic number, there exists a unique *minimal polynomial* $p \in \mathbb{Q}[x]$ such that (a) $p(\alpha) = 0$, (b) p is irreducible in $\mathbb{Q}[x]$, and (c) p has n *distinct* roots in $\mathbb{C}$, where $\deg p = n$.

Assume that α and β are algebraic numbers. Prove that $\alpha + \beta$ and $\alpha\beta$ are also algebraic numbers.

Hint: Say α and β have minimal polynomials p and q, respectively, where $n := \deg p$ and $m := \deg q$. Consider the *conjugates* $\{\alpha_i\}$ of α, the collection of all n complex roots of p, and $\{\beta_j\}$, the set of all m complex roots of q. Define polynomials

$$S(x) := \prod_{1 \le i \le n} \prod_{1 \le j \le m} \left(x - (\alpha_i + \beta_j)\right)$$

and

$$P(x) := \prod_{1 \le i \le n} \prod_{1 \le j \le m} \left(x - (\alpha_i \beta_j)\right).$$

What can we say about the coefficients of S and P?

4.3 Let $p \in \mathbb{Q}[x]$ be a monic polynomial of degree $n \geq 1$ such that the roots of p, including multiplicity, are $r_1, r_2, \ldots, r_n$. Define the *discriminant of p* to be the number

$$\operatorname{Disc} p := \prod_{1 \leq i < j \leq n} (r_i - r_j)^2.$$

- Prove that if $p \in \mathbb{Q}[x]$, then $\operatorname{Disc} p$ is a *rational* number.
- Consider $p(x) := x^2 + b + c$. Compute $\operatorname{Disc} p$.
- Show that in general, $\operatorname{Disc} p = 0$ if and only if p has a repeated root.