Algebra

Munir Uz Zaman

Date: November 21, 2021

Contents

1 Polynomials

Definition 1.0.1. A Polynomial $P(x)$ is an one variable expression or function of the form

$$P(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0, a_1, \cdots, a_n$ are constants and $n \in \mathbb{N}$. The constants a_i are called the *coefficients* of the polynomial. We will denote $A[x]$ as the set of all polynomials with $a_i \in A$. If $n \neq 0$ then n is called the *degree* of the polynomial $P(x)$ and write $\deg P(x) = n$. If $a_n = 1$ then we say that the polynomial is *monic*.
r is called a *root* of the polynomial $P(x)$ if and only if $P(r) = 0$.

§1.1 Division Algorithm

Theorem 1.1.1 (The Division Algorithm)
Given two polynomial $A(x)$ and $B(x)$ there exists unique polynomials $Q(x)$ and $R(x)$ with $\deg R(x) < \deg B(x)$ such that,

$$A(x) = Q(x)B(x) + R(x)$$

The polynomials $Q(x)$ and $R(x)$ are known as the *quotient* and the *remainder*, respectively. If the remainder $R(x) = 0$ then we say that $B(x)$ divides $A(x)$ and write $B(x) \mid A(x)$.

For example, if $B(x) = x^2 - x + 1$ and $A(x) = x^5 + x^3 + 2x$ then,

$$x^5 + x^3 + 2x = \left(x^3 + x^2 + x\right)\left(x^2 - x + 1\right) + x$$

In this example, the remainder $R(x) = x$ and the quotient $Q(x) = x^3 + x^2 + x$.
Suppose $B(x)$ is a polynomial of degree $n \geq 1$ and let $A(x) = x - z$ be linear polynomial. Now from Theorem 1.1.1 we know that there exists polynomials $Q(x)$ and $R(x)$ with $\deg R(x) < 1$ such that,

$$B(x) = A(x)Q(x) + R(x)$$

Since $0 \leq \deg R(x) < 1$, $R(x)$ must be a constant polynomial, we can assume $R(x) = r$ where $r \in \mathbb{R}$. Therefore,

$$\begin{aligned} B(x) &= A(x)Q(x) + R(x) \\ &= (x - z)Q(x) + r \end{aligned}$$

Now if $r = 0$ then,

$$B(x) = (x - z)Q(x) \implies B(z) = 0$$

Now if $B(z) = 0$ that is if z is a root of the polynomial $B(x)$ then,

$$B(z) = (z - z)Q(x) + r \implies B(z) = r \implies r = 0$$

Therefore we have proved the following theorem.

Theorem 1.1.2 (Factor Theorem)
The real number z will be a root of the polynomial $P(x)$ if and only if $P(x)$ is divisible by $x - z$.

Corollary 1.1.2.1
The number $-\frac{b}{a}$ where $a, b \in \mathbb{R}$ will be a root of the polynomial $P(x)$ if and only if the polynomial $P(x)$ is divisible by $ax + b$.

If $P(x)$ has the root z then the Factor Theorem guarantees that there exists a polynomial $Q_0(x)$ such that,

$$P(x) = (x - z)\, Q_0(x)$$

Now if,

$$P(x) = (x - z)^m\, Q(x)$$

then we say that z is root of $P(x)$ of *multiplicity* m.

§1.2 The Fundamental Theorem of Algebra

Theorem 1.2.1 (The Fundamental Theorem of Algebra)
The Fundamental Theorem of Algebra states that, every polynomial $P(x)$ in $\mathbb{C}[x]$ has at least one root in $\mathbb{C}$

Corollary 1.2.1.1
If $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial of degree n then,

$$P(x) = k(x - z_1)(x - z_2)\cdots(x - z_n)$$

where, $k = a_n$ and $z_i \in \mathbb{C}$. The numbers $z_1, z_2 \cdots z_n$ are not necessarily distinct.

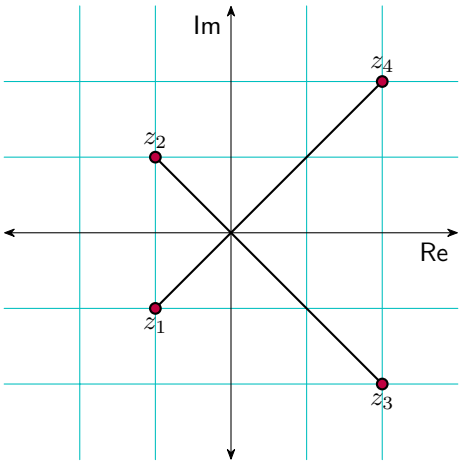

Figure 1.1: The 4 complex roots of the polynomial $x^4 - 2x^3 + 2x^2 + 8x + 16$

Theorem 1.2.2 (Complex Conjugate Root Theorem)
If $P(x) \in \mathbb{R}[x]$ and $z = a + bi$ where $a, b \in \mathbb{R}$ and $b \neq 0$ is a complex root of the polynomial $P(x)$ then $\overline{z} = a - bi$ is also a root of the polynomial $P(x)$.

Proof 1: We have to show that, $P(z) = 0 \implies P(\overline{z}) = 0$. Let $\mathbb{C}' = \{ki : k \in \mathbb{R}\}$ and let $\mathbb{R}$ be the set of real numbers. Now,

$$\begin{aligned} z^k + \overline{z}^k &= (a+bi)^k + (a-bi)^k \\ &= a^k \left[\left(\frac{b}{a} i + 1 \right)^k + \left(-\frac{b}{a} i + 1 \right)^k \right] \\ &= a^k \left[\left(\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a} \right)^j i^j \right) + \left(\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a} \right)^j (-1)^j i^j \right) \right] \\ &= a^k \left[\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a} \right)^j \left\{ i^j + (-i)^j \right\} \right] \end{aligned}$$

Notice, $i^j + (-i)^j$ will be zero if j is odd. If j is even then $i^j + (-i)^j = 2i^j = 2(-1)^{\frac{j}{2}}$. Therefore,

$$\begin{aligned} z^k + \overline{z}^k &= a^k \left[\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a} \right)^j \left\{ i^j + (-i)^j \right\} \right] \\ &= a^k \left[\sum_{l=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2l} \left(\frac{b}{a} \right)^{2l} \left\{ 2(-1)^l \right\} \right] \\ &= \sum_{l=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2l} \left(\frac{b}{a} \right)^{2l} 2a^k (-1)^l \end{aligned}$$

Remark. The set, $\left\{2l : 0 \leq l \leq \lfloor \frac{k}{2} \rfloor \right\}$, contains all even integers (including zero) less than or equal to k.

Therefore, $z^k + \overline{z}^k \in \mathbb{R}$ for all $0 \leq k \in \mathbb{Z}$. This implies that,

$$P(z) + P(\overline{z}) = \sum_{i=0}^{n} a_i \left(z^i + \overline{z}^i \right) \in \mathbb{R}$$

But since $P(z) = 0$, $P(z) + P(\overline{z}) \in \mathbb{R}$ implies $P(\overline{z}) \in \mathbb{R}$. Now,

$$\begin{aligned} z^k - \overline{z}^k &= (a+bi)^k - (a-bi)^k \\ &= a^k \left[\left(\frac{b}{a} i + 1 \right)^k - \left(-\frac{b}{a} i + 1 \right)^k \right] \\ &= a^k \left[\left(\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a} \right)^j i^j \right) - \left(\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a} \right)^j (-1)^j i^j \right) \right] \\ &= a^k \left[\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a} \right)^j \left\{ i^j - (-i)^j \right\} \right] \end{aligned}$$

If j is even then $i^j - (-i)^j$ will be equal to zero. If j is odd that is $j = 2l-1$ for some $l \in \mathbb{N}$ then $i^j - (-i)^j = i^{2l-1}\left(1-(-1)^{2l-1}\right) = 2i^{2l-1} = 2(-1)^l i^{-1} = 2(-1)^l i^3 = 2(-1)^{l+1}i$.
Therefore,

$$\begin{aligned} z^k - \overline{z}^k &= a^k \left[\sum_{j=0}^{k} \binom{k}{j} \left(\frac{b}{a}\right)^j \left\{i^j - (-i)^j\right\}\right] \\ &= a^k \left[\sum_{l=1}^{\lfloor \frac{k+1}{2} \rfloor} \binom{k}{2l-1} \left(\frac{b}{a}\right)^{2l-1} 2(-1)^{l+1} i\right] \\ &= \left[\sum_{l=1}^{\lfloor \frac{k+1}{2} \rfloor} \binom{k}{2l-1} \left(\frac{b}{a}\right)^{2l-1} 2a^k(-1)^{l+1}\right] i \end{aligned}$$

Remark. The set $\left\{2l-1 : 1 \le l \le \lfloor \frac{k+1}{2} \rfloor\right\}$ contains all odd positive integers less than or equal to k.

Thus, $z^k - \overline{z}^k \in \mathbb{C}'$ for all $k \in \mathbb{N}$. Now,

$$\begin{aligned} & P(z) - P(\overline{z}) = \sum_{i=0}^{n} a_i \left(z^i - \overline{z}^i\right) \\ \implies & P(z) - P(\overline{z}) = \sum_{i=1}^{n} a_i \left(z^i - \overline{z}^i\right) + a_0\left(z^0 - \overline{z}^0\right) \\ \implies & P(z) - P(\overline{z}) = \sum_{i=1}^{n} a_i \left(z^i - \overline{z}^i\right) \in \mathbb{C}' \end{aligned}$$

But since $P(z) = 0$, $P(z) - P(\overline{z}) \in \mathbb{C}'$ implies $P(\overline{z}) \in \mathbb{C}'$. And so, $P(\overline{z}) \in \mathbb{R} \cup \mathbb{C}' \implies P(\overline{z}) \in \{0\} \implies P(\overline{z}) = 0$. QED

♣

Proof 2(wiki): Since $P(z) = 0$,

$$P(z) = \sum_{k=0}^{n} a_k z^k = 0$$

Now using the properties of complex conjugates,

$$P(\overline{z}) = \sum_{k=0}^{n} a_k \overline{z}^k = \sum_{k=0}^{n} a_k \overline{z^k} = \sum_{k=0}^{n} \overline{a_k z^k} = \overline{\sum_{k=0}^{n} a_k z^k} = \overline{P(z)} = \overline{0} = 0$$

Therefore, $P(\overline{z}) = 0$.

♣

§1.3 Roots of Cubic Polynomials

Finding the roots of a cubic polynomial is quite hard. So, we are going to first try to solve the cubic polynomial,

$$f(x) = x^3 + px + q$$

where $p, q \in \mathbb{R}$. Setting $p = -3ab$ and $q = a^3 + b^3$ we get,

$$f(x) = x^3 + a^3 + b^3 - 3abx$$

Now using the formula,

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$$

we get,

$$f(x) = (x + a + b)(x^2 - (a + b)x + a^2 + b^2 - ab)$$

Therefore the 3 roots of f are,

$$\begin{aligned}
x_1 &= -a - b \\
x_2, x_3 &= \frac{a + b \pm \sqrt{a^2 + b^2 + 2ab - 4a^2 - 4b^2 + 4ab}}{2} \\
&= \frac{a + b \pm \sqrt{-3a^2 - 3b^2 + 6ab}}{2} \\
&= \frac{a + b \pm \sqrt{-3(a - b)^2}}{2} \\
&= \frac{a + b \pm \sqrt{3}i(a - b)}{2} \\
&= \frac{(1 + \sqrt{3}i)a \pm (1 - \sqrt{3}i)b}{2} \\
&= \frac{1 + \sqrt{3}i}{2}a \pm \frac{1 - \sqrt{3}i}{2}b
\end{aligned}$$

Now we have express the root in terms of p, q that is, we have to express a, b in terms of p, q. Now,

$$\begin{aligned}
q &= a^3 + b^3 \\
p &= -3ab \\
\implies a^3 b^3 &= -\frac{p^3}{27}
\end{aligned}$$

Let $u = a^3$ and $v = b^3$. Notice that u and v are the roots of the quadratic polynomial,

$$P(x) = x^2 - (u + v)x + uv = x^2 - q^3 x - \frac{p^3}{27}$$

Using the quadratic equation we get,

$$\begin{aligned}
u, v &= \frac{q^3 \pm \sqrt{q^6 + \frac{4}{27}p^3}}{2} \\
a, b &= \sqrt[3]{\frac{q^3}{2} \pm \frac{\sqrt{q^6 + \frac{4}{27}p^3}}{2}} \\
&= \sqrt[3]{\frac{q^3}{2} \pm \sqrt{\frac{q^6}{4} + \frac{p^3}{27}}}
\end{aligned}$$

So let's now try to solve the cubic equation using the results we've got so far,

$$f(x) = x^3 - x^2 - 2x + 1$$

First we have to use substitution to transform the polynomial into another polynomial of the form,

$$x^3 + px + q$$

Since every polynomial can be uniquely defined by its coefficients, we can associate or express a polynomial of degree n by a unique point in $n+1$ dimensional space. For example we can express the polynomial,

$$(1) \cdot x^3 + (-1) \cdot x^2 + (-2) \cdot x + (1)$$

as,

$$(1) \cdot x^3 + (-1) \cdot x^2 + (-2) \cdot x + (1) \to (1, -1, -2, 1)$$

Likewise, the point $(5, -1, 0, 1)$ can be used to represent the polynomial,

$$(5, -1, 0, 1) \to 5x^3 - x^2 + 1$$

Notice that,

$$(x_3, x_2, \cdots, x_0) + (y_3, y_2, \cdots, y_0) = (x_3 + y_3, x_2 + y_2, \cdots, x_0 + y_0)$$

Say that there exists a polynomial $u(x) = (x + n)$ where $n \in \mathbb{C}$ such that,

$$x^3 - x^2 - 2x + 1 = u(x)^3 + pu(x) + q$$

This equation can also be represented as,

$$(1, -1, -2, 1) = (1, 3n, 3n^2, n^3) + (0, 0, p, pn) + (0, 0, 0, q) \implies (1, -1, -2, 1) = (1, 3n, 3n^2 + p, n^3 + pn + q)$$

This gives us the system of equation,

$$\begin{aligned} 3n &= -1 \\ 3n^2 + p &= -2 \\ n^3 + pn + q &= 1 \end{aligned}$$

Therefore,

$$\begin{aligned} n &= -\frac{1}{3} \\ p &= -\frac{7}{3} \\ q &= \frac{7}{27} \end{aligned}$$

Thus,

$$x^3 - x^2 - 2x + 1 = \left(x - \frac{1}{3}\right)^3 - \frac{7}{3}\left(x - \frac{1}{3}\right) + \frac{7}{27} \implies f(x) = g\left(x - \frac{1}{3}\right)$$

where

$$g(x) = x^3 - \frac{7}{3}x + \frac{7}{27}$$

Now we can use the results we've proved earlier to solve the polynomial $g(x)$. After that we add $\frac{1}{3}$ to the 3 roots of $g(x)$. The 3 numbers we will get by adding $\frac{1}{3}$ are the 3 roots of $f(x)$.

§1.4 Lagrange Interpolation

Theorem 1.4.1 (Lagrange Interpolation)
Let $\alpha_0, \alpha_1, \cdots, \alpha_n$ be distinct real numbers and $\beta_0, \beta_1, \cdots, \beta_n$ be another set of $n+1$ real numbers. Then there exists a unique polynomial,

$$P(x) = \sum_{i=0}^{n} \left(\prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - \alpha_j}{\alpha_i - \alpha_j} \right) \beta_i$$

with $\deg P(x) \leq n$ such that $P(\alpha_k) = \beta_k$ for all $0 \leq k \leq n$.

Proof: Let,

$$D_k(x) = \prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{x - \alpha_j}{\alpha_k - \alpha_j} = \frac{(x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{k-1})(x-\alpha_{k+1})\cdots(x-\alpha_n)}{(\alpha_k-\alpha_0)(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_{k-1})(\alpha_k-\alpha_{k+1})\cdots(\alpha_k-\alpha_n)}$$

If $x = \alpha_k$ then $D_k(x) = 1$ else if $x = \alpha_i$ where $i \neq k$ then $D_k(x) = 0$. Thus the polynomial,

$$P(x) = \sum_{k=0}^{n} D_k(x)\beta_k$$

will be equal to β_k for all $x = \alpha_k$. It is also clear that the polynomial $P(x)$ has degree at most n since $\deg D_k(x) = n$ for all $0 \leq k \leq n$.
Now suppose that there exists two polynomials $P_1(x)$ and $P_2(x)$, with degree at most n, such that,

$$P_1(\alpha_k) = P_2(\alpha_k) = \beta_k, \ 0 \leq k \leq n$$

Therefore the polynomial $Q(x) = P_1(x) - P_2(x)$ has $n+1$ distinct roots. But that is impossible since we know that $\deg Q(x) \leq n$ and a polynomial of degree n has at most n distinct roots. This proves that the polynomial $P(x)$ must be unique, that is, $P(x)$ is the only polynomial, with degree at most n, such that, $P(\alpha_k) = \beta_k$ for all $0 \leq k \leq n$

♣

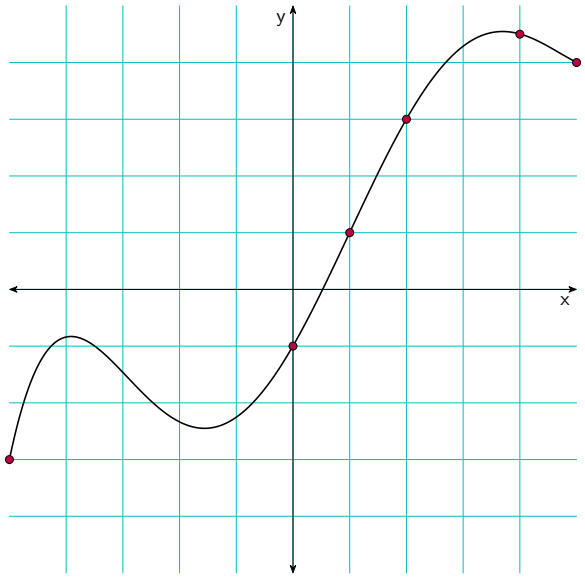

Figure 1.2: Plot of a Lagrange Polynomial

Figure 1.2 shows the Lagrange polynomial going through the points,

$$\{(1,1),(2,3),(0,-1),(5,4),(-5,-3),(4,4.5)\}$$

We can easily compute Lagrange polynomials in python using `sympy`.

```
>>> import sympy
>>> x = sympy.symbols('x')
>>> points = [(1,1), (2,3), (0, -1), (5, 4), (-5, -3), (4, 4.5)]
>>> expr = sympy.interpolate(points, x)
>>> print(expr)
0.00281746031746032*x**5 - 0.0129761904761905*x**4 -
↪  0.111944444444445*x**3 + 0.384404761904762*x**2 +
↪  1.73769841269841*x - 1
```

Problem 1.4.1

Let $P(x)$ be a polynomial of degree n such that, $P(k) = 2^k$ for all $0 \leq k \leq n$. Find $P(n+1)$.

Solution: From Theorem 1.4.1 we have,

$$P(x) = \sum_{k=0}^{n} 2^k D_k(x)$$

where,

$$\begin{aligned} D_k(x) &= \frac{x(x-1)\cdots(x-k+1)(x-k-1)(x-k-2)\cdots(x-n+1)(x-n)}{(k)(k-1)\cdots(1)(-1)(-2)\cdots(k-n+1)(k-n)} \\ &= (-1)^{n-k}\frac{x(x-1)\cdots(x-k+1)(x-k-1)(x-k-2)\cdots(x-n+1)(x-n)}{k!(n-k)!} \end{aligned}$$

Therefore,

$$\begin{aligned}
P(n+1) &= \sum_{k=0}^{n}(-1)^{n-k}2^k\frac{(n+1)n(n-1)\cdots(n-k+2)(n-k)(n-k-1)\cdots 1}{k!(n-k)!} \\
&= \sum_{k=0}^{n}(-1)^{n-k}2^k\frac{(n+1)!}{k!(n-k)!(n-k+1)} \\
&= \sum_{k=0}^{n}(-1)^{n-k}2^k\binom{n+1}{k} \\
&= (-1)\left(\sum_{k=0}^{n+1}\binom{n+1}{k}2^k(-1)^{n-k+1}\right)+2^{n+1} \\
&= (-1)\,(2-1)^{n+1}+2^{n+1} \\
&= 2^{n+1}-1
\end{aligned}$$

♣