Algebra

Munir Uz Zaman

Date: December 18, 2021

Contents

1 Inequalities

§1.1 AM-GM Inequality

> **Theorem 1.1.1** (AM-GM Inequality)
>
> For all positive real numbers $a_1, a_2, \cdots, a_n$ where $n \in \mathbb{N}$ and $n \geq 2$ the following inequality holds,
> $$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}$$
> Equality occurs if and only if $a_1 = a_2 = \cdots = a_n$.

Proof: We will prove this theorem using a special type of induction know as *Cauchy Induction*. Here's how we'll prove it, (let P_n be the statement for n numbers.)

- We will first show that P_2 is true.

- We will show that $P_n \implies P_{2n}$

- Then we will show that $P_n \implies P_{n-1}$

When these are verified, all the assertions P_n with $n \geq 2$ are shown to be true.
First we need to prove that if a_1, a_2 are two positive reals then

$$\frac{a_1 + a_2}{2} \geq \sqrt[2]{a_1 a_2}$$

This can be easily shown from the fact that $(\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$.
Next we need show that $P_n \implies P_{2n}$. This is also very easy.

$$a_1 + a_2 + \cdots + a_{2n} \geq n\sqrt[n]{a_1 a_2 \cdots a_n} + n\sqrt[n]{a_{n+1}a_{n+2} \cdots a_{2n}} \geq 2n\sqrt[2n]{a_1 a_2 \cdots a_{2n}}$$

Now we just need to show that $P_n \implies P_{n-1}$. Let $g = \sqrt[n-1]{a_1 a_2 \cdots a_{n-1}}$. Now,

$$a_1 + \cdots + a_{n-1} + g \geq n\sqrt[n]{a_1 \cdots a_{n-1} \times g}$$
$$\implies a_1 + \cdots + a_{n-1} + g \geq n\sqrt[n]{g^{n-1}g}$$
$$\implies a_1 + \cdots + a_{n-1} + g \geq ng$$
$$\implies a_1 + \cdots + a_{n-1} \geq (n-1)g$$
$$\implies a_1 + \cdots + a_{n-1} \geq (n-1)\sqrt[n-1]{a_1 a_2 \cdots a_{n-1}}$$

By *Cauchy induction*, the inequality is true for every natural number $n \geq 2$. Equality occurs if and only if $a_1 = a_2 = \cdots = a_n$.

♣

> **Theorem 1.1.2** (Weighted AM-GM Inequality)
>
> If $a_1, a_2, \cdots, a_n$ are positive real numbers with $n \geq 2$ and $x_1, x_2, \cdots, x_n$ are n non-negative real numbers such that $\sum_{i=1}^{n} x_i = 1$ then
> $$a_1 x_1 + \cdots + a_n x_n \geq a_1^{x_1} \cdots a_n^{x_n}$$

Problem 1.1.1 (BDMO 2019)

Show that if a, b, c are positive real numbers then

$$\frac{a}{bc} + \frac{b}{ac} + \frac{c}{ab} \geq 2\left(\frac{1}{a} + \frac{1}{b} - \frac{1}{c}\right)$$

Solution:

$$(a + b - c)^2 \geq 0$$
$$\implies a^2 + b^2 + c^2 + 2(ab - bc - ca) \geq 0$$
$$\implies a^2 + b^2 + c^2 \geq 2(bc + ca - ab)$$
$$\implies \frac{a^2 + b^2 + c^2}{abc} \geq 2\left(\frac{bc + ca - ab}{abc}\right)$$
$$\implies \frac{a}{bc} + \frac{b}{ac} + \frac{c}{ab} \geq 2\left(\frac{1}{a} + \frac{1}{b} - \frac{1}{c}\right)$$

♣

2 Polynomials

Definition 2.0.1. 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 $P(r) = 0$.

§2.1 Division Algorithm

> **Theorem 2.1.1** (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 $B(x) \mid A(x)$.

Proof: We will first prove the uniqueness of the polynomials $Q(x)$ and $R(x)$. Assume,

$$A(x) = Q_1(x)B(x) + R_1(x), \quad \deg R_1(x) < \deg B(x)$$
$$A(x) = Q_2(x)B(x) + R_2(x), \quad \deg R_2(x) < \deg B(x)$$

Now,

$$\left(Q_1(x) - Q_2(x)\right)B(x) + \left(R_1(x) - R_2(x)\right) = 0$$

Let $q(x) = Q_1(x) - Q_2(x)$ and $r(x) = R_1(x) - R_2(x)$. Now,

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

If $q(x) \neq 0$ then $\deg r(x) = \deg q(x) + \deg B(x) \geq \deg B(x)$. But that is impossible since $\deg R_2(x) < \deg B(x) \implies \deg (R_2(x) - R_1(x)) < \deg B(x)$. Thus $q(x)$ must be zero. Consequently $r(x)$ will also be zero. Therefore $R_1(x) = R_2(x)$ and $Q_1(x) = Q_2(x)$.

Now we will prove the existence of the polynomials $Q(x)$ and $R(x)$. Notice the following algorithm,

1: $A(x) \leftarrow a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$
2: $B(x) \leftarrow b_n x^n + b_{n-1} b^{n-1} + \cdots + b_0$
3: $R(x) \leftarrow A(x)$
4: **while** $\deg R(x) \geq \deg B(x)$ **do**
5:     $a \leftarrow$ leading coefficient of $R(x)$
6:     $b \leftarrow$ leading coefficient of $B(x)$

7:   $d \leftarrow \deg R(x) - \deg B(x)$
8:   $Q(x) = Q(x) + \left(\frac{a}{b}\right) x^d$
9:   $R(x) \leftarrow R(x) - \left(\frac{a}{b}\right) x^d B(x)$
  output $Q(x)$ and $R(x)$

In each iteration of the while loop, $\deg R(x)$ is decreasing (mono-variant) and the polynomial $Q(x)B(x) + R(x)$ always stays equal to $A(x)$ (invariant). At some point we will eventually get $\deg R(x) \leq \deg B(x)$ which proves the existence of $Q(x)$ and $R(x)$.

Remark. Notice that, if $A(x), B(x) \in \mathbb{R}[x]$ then $Q(x), R(x) \in \mathbb{R}[x]$. This implies that, if $A(x), B(x) \in \mathbb{R}[x]$ and $B(x) \mid A(x)$ then $\frac{A(x)}{B(x)} \in \mathbb{R}[x]$

♣

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 $Q(x) = x^3 + x^2 + x$.

Theorem 2.1.2 (Remainder Theorem)

If $P(x)$ is a polynomial and a is a constant then the remainder upon dividing $P(x)$ by the linear polynomial $x - a$ is equal to $P(a)$.

Proof: From the Division Algorithm we know that there exists polynomials $Q(x)$ and $R(x)$ such that,

$$P(x) = Q(x)(x - a) + R(x)$$

Since $\deg R(x) < \deg(x - a) = 1$, $R(x)$ must be a constant polynomial. Let us assume, $R(x) = r$. Now letting $x = a$ we get,

$$P(a) = Q(a) \times (a - a) + r \implies P(a) = r$$

Therefore $P(a)$ is the remainder upon dividing $P(x)$ by $x - a$. QED

♣

Theorem 2.1.3 (Factor Theorem)

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

Proof: We will first prove that, $P(z) = 0 \implies (x - z) \mid P(x)$. Let us assume that r is the remainder upon dividing $P(x)$ by $x - z$. Now we know from the Remainder Theorem that, $P(z) = r$. But since z is a root of $P(x)$, $P(z) = r = 0$. Therefore since $r = 0$, we must have $(x - z) \mid P(x)$. Using similar arguments one can also prove the converse.

♣

Corollary 2.1.3.1

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 $Q(x)$ such that,

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

Now if,

$$P(x) = (x - z)^m \, Q'(x), \quad Q'(z) \neq 0$$

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

For example, in the polynomial $P(x) = (x - 2)^2 \, (x - 3)$ the root 2 has multiplicity 2 and the root 3 has multiplicity 1.

§2.2 The Fundamental Theorem of Algebra

Theorem 2.2.1 (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 2.2.1.1

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.

Proof: This is an immediate consequence of The Fundamental Theorem of Algebra and Factor Theorem.
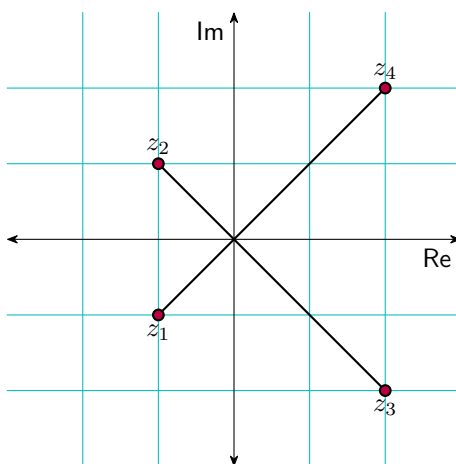
♣

Figure 2.1: The 4 complex roots of the polynomial $x^4 - 2x^3 + 2x^2 + 8x + 16$

Theorem 2.2.2 (Complex Conjugate Root Theorem)

If $P(x) \in \mathbb{R}[x]$ and $z = a + bi$ where $a, b \in \mathbb{R}$ 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,

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

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,

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

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,

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

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,

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

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

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

$$P(z) - P(\bar{z}) = \sum_{i=0}^{n} a_i \left(z^i - \bar{z}^i \right)$$

$$\implies P(z) - P(\bar{z}) = \sum_{i=1}^{n} a_i \left(z^i - \bar{z}^i \right) + a_0 \left(z^0 - \bar{z}^0 \right)$$

$$\implies P(z) - P(\bar{z}) = \sum_{i=1}^{n} a_i \left(z^i - \bar{z}^i \right) \in \mathbb{C}'$$

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

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

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

♣

> **Corollary 2.2.2.1**
>
> If z is a complex root of the polynomial $P(x)$ of multiplicity m then $\bar{z}$ is also a complex root of the polynomial $P(x)$ of multiplicity m. That is, complex conjugate roots have the same multiplicity.

Proof: If $z \in \mathbb{R}$ then obviously z and $\bar{z}$ will have the same multiplicity as $z = \bar{z}$. Let us assume $z \notin \mathbb{R}$ and let m and n be the multiplicity of z and $\bar{z}$ respectively. Without loss of generality, we can assume $n < m$. Now, let

$$P(x) = (x - z)^m (x - \bar{z})^n Q(x)$$

Now,

$$P(x) = (x - z)^n (x - \bar{z})^n (x - z)^{m-n} Q(x)$$

$$\implies \frac{P(x)}{(x - z)^n (x - \bar{z})^n} = (x - z)^{m-n} Q(x)$$

Let, $R(x) = \frac{P(x)}{(x-z)^n (x-\bar{z})^n}$. Since $P(x) \in \mathbb{R}[x]$ and $(x - z)^n (x - \bar{z})^n \in \mathbb{R}[x]$, $R(x) \in \mathbb{R}[x]$. Therefore, $R(x) = (x - z)^{m-n} Q(x) \in \mathbb{R}[x]$. As z is a root of $R(x)$ and $R(x) \in \mathbb{R}[x]$, $\bar{z}$ must also be a root of $R(x)$ which implies the multiplicity of $\bar{z} > n$. But that contradicts our assumption that $\bar{z}$ has multiplicity n. Therefore, m and n must be equal.

♣

> **Corollary 2.2.2.2**
> Every polynomial $P(x)$ in $\mathbb{R}[x]$ can be expressed in the form,
>
> $$P(x) = f_1^{e_1}(x) f_2^{e_2}(x) \cdots f_n^{e_n}(x)$$
>
> where the polynomials $f_i(x)$ are either linear or quadratic polynomials in $\mathbb{R}[x]$ and $e_i \in \mathbb{N}$

> **Corollary 2.2.2.3**
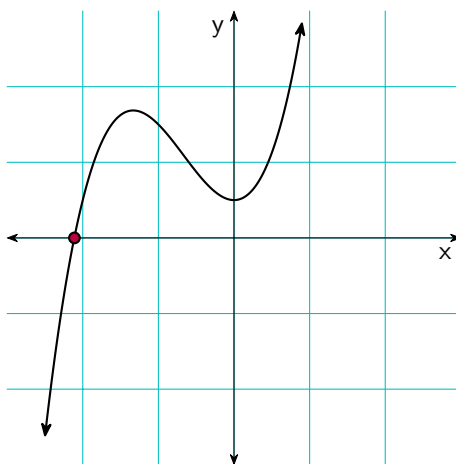> If $P(x) \in \mathbb{R}[x]$ and $\deg P(x)$ is odd then $P(x)$ has at least on real root.

Figure 2.2: The real root of the cubic polynomial $f(x) = x^3 + 2x^2 + 0.5$

§2.3 Quadratic Polynomials

Definition 2.3.1. A *quadratic polynomial* is a polynomial of the form,

$$P(x) = ax^2 + bx + c$$

where a, b, c are constants and $a \neq 0$.

One can find the roots of a quadratic polynomial using the well known *quadratic formula*,

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The value $\Delta = b^2 - 4ac$ is called the *discriminant* of the quadratic polynomial. The discriminant gives us the following informations about the roots of the quadratic polynomial,

- $\Delta > 0 \iff x_1, x_2 \in \mathbb{R}$ and $x_1 \neq x_2$

- $\Delta = 0 \iff x_1, x_2 \in \mathbb{R}$ and $x_1 = x_2$

- $\Delta < 0 \iff x_1, x_2 \in \mathbb{C}$ and $x_1 \neq x_2$

> **Theorem 2.3.1**
> The value $P\left(-\frac{b}{2a}\right)$ is either the maximum (if $a > 0$) or the minimum value (if $a < 0$) of the quadratic polynomial, $P(x) = ax^2 + bx + c$

Proof:

$$P(x) = ax^2 + bx + c$$

$$\implies P(x) = a\left(x^2 + 2\frac{b}{2a}x + \frac{b^2}{4a^2}\right) + c - \frac{b^2}{4a}$$

$$\implies P(x) = a\left(x + \frac{b}{2a}\right)^2 + \left(c - \frac{b^2}{4a}\right)$$
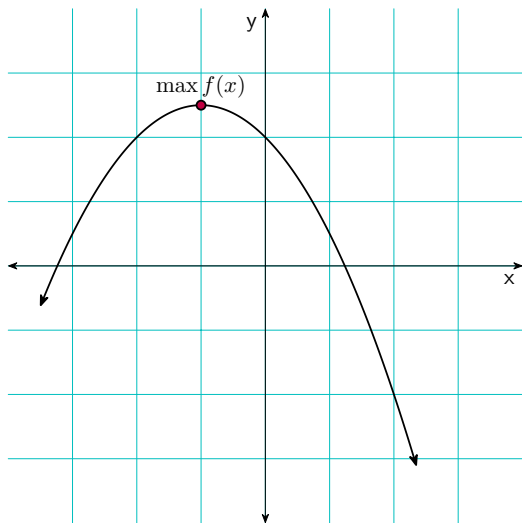
If $a < 0$ then,

$$P(x) = \left(c - \frac{b^2}{4a}\right) - |a|\left(x + \frac{b}{2a}\right)^2$$

$P(x)$ will reach its maximum when $x + \frac{b}{2a} = 0 \implies x = -\frac{b}{2a}$.
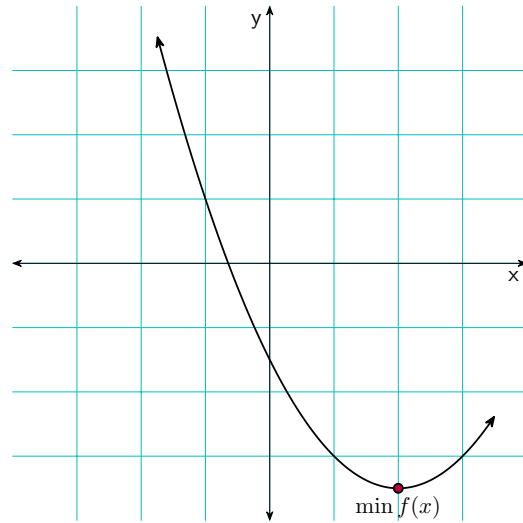If $a > 0$ then,

$$P(x) = \left(c - \frac{b^2}{4a}\right) + a\left(x + \frac{b}{2a}\right)^2$$

$P(x)$ will reach its minimum when $x + \frac{b}{2a} = 0 \implies x = -\frac{b}{2a}$.

♣

(a) Maximum of $f(x) = -0.5x^2 - x + 2$

(b) Minimum of $f(x) = 0.5x^2 - 2x - 1.5$

§2.4 **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,

$$x_1 = -a - b$$

$$x_2, x_3 = \frac{a + b \pm \sqrt{a^2 + b^2 + 2ab - 4a^2 - 4b^2 + 4ab}}{2}$$

$$= \frac{a + b \pm \sqrt{-3a^2 - 3b^2 + 6ab}}{2}$$

$$= \frac{a + b \pm \sqrt{-3(a-b)^2}}{2}$$

$$= \frac{a + b \pm \sqrt{3}i(a-b)}{2}$$

$$= \frac{(1 + \sqrt{3}i)a \pm (1 - \sqrt{3}i)b}{2}$$

$$= \frac{1 + \sqrt{3}i}{2}a \pm \frac{1 - \sqrt{3}i}{2}b$$

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,

$$q = a^3 + b^3$$

$$p = -3ab$$

$$\implies a^3 b^3 = -\frac{p^3}{27}$$

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,

$$u, v = \frac{q^3 \pm \sqrt{q^6 + \frac{4}{27}p^3}}{2}$$

$$a, b = \sqrt[3]{\frac{q^3}{2} \pm \frac{\sqrt{q^6 + \frac{4}{27}p^3}}{2}}$$

$$= \sqrt[3]{\frac{q^3}{2} \pm \sqrt{\frac{q^6}{4} + \frac{p^3}{27}}}$$

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,

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

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

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

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,

$$3n = -1$$
$$3n^2 + p = -2$$
$$n^3 + pn + q = 1$$

Therefore,

$$n = -\frac{1}{3}$$
$$p = -\frac{7}{3}$$
$$q = \frac{7}{27}$$

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 $f(x)$.

§2.5 Lagrange Interpolation

> **Theorem 2.5.1** (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 $0 \leq k \leq n$
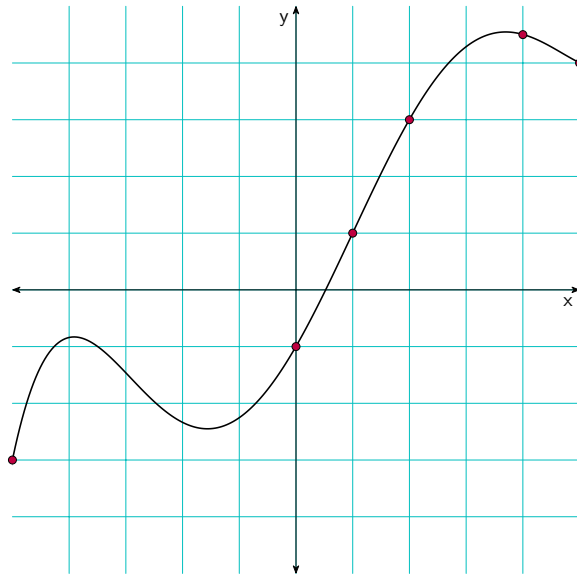
♣

Figure 2.4: Plot of a Lagrange Polynomial

[Figure 2.4]{.red} 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 2.5.1

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 2.5.1]{.red} 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,

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

♣