B KNOWLEDGE RECAP: COMPLEX ARITHMETICS

The set of complex numbers are denoted by the symbol $\mathbb{C}$.
An arbitrary complex number $z \in \mathbb{C}$ is of the following form:

$$z = a + b\,\mathbf{i}\,, \quad \text{with } a, b \in \mathbb{R}\,.$$

The imaginary unit $\mathbf{i}$, is defined such that:

$$\mathbf{i}^2 = \mathbf{i} \cdot \mathbf{i} = -1\,.$$

This complex number z has two parts:

- the real part $\Re(z) = a$;
- the imaginary part $\Im(z) = b$.

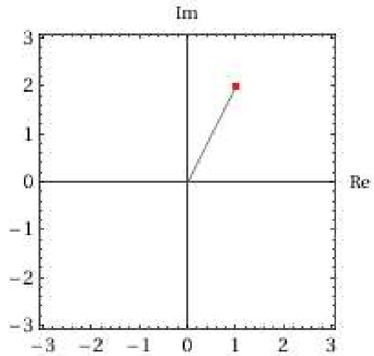

Figure B.1: A visualization of the complex number $1 + 2\,\mathbf{i}$ in the complex plane.

The **complex conjugate** of z is denoted as $\bar{z}$, and that:

$$\bar{z} = a - b\,\mathbf{i}, \quad \text{with } \Im(z) = -\Im(\bar{z})\,.$$

The **modulus** of z is denoted as $|z|$, and that:

$$|z| = \sqrt{a^2 + b^2}$$

The **argument** of z is denoted as $\arg(z)$

$$\arg(z) = \tan^{-1}(\frac{b}{a})\,, \quad \cos(\arg(z)) = \frac{a}{|z|}\,, \quad \sin(\arg(z)) = \frac{b}{|z|}\,.$$

The **principal argument** of z is denoted as $\mathrm{Arg}(z)$ such that $\mathrm{Arg}(z)$ still satisfy the relations above and $\mathrm{Arg}(z) \in (-\pi, \pi]$. We may say the following:

$$\arg(z) = \mathrm{Arg}(z) + 2k\pi, \text{ for } k \in \mathbb{Z}\,.$$

Do be aware that the argument of z is multi-valued by nature of the trigonometric functions. This might cause a bit of inconvenience during addition and multiplication, but will bring loads of trouble in power and logarithmic functions. We will briefly mention some in the following text, but the interested reader of this problem should refer to a textbook in complex analysis to actually (re)visit the related definition and solutions.

From now on, we let $\theta = \mathrm{Arg}(z)$ for our convenience.

We may derive the following for any complex number $z = a + b\,\mathbf{i}$:

$$z = a + b\,\mathbf{i} = |z|(\cos(\theta) + \mathbf{i}\sin(\theta))\,.$$

We introduce the notion $\hat{z}$ for our convenience, such that:

$$\hat{z} = \cos(\theta) + \mathbf{i}\sin(\theta)\,. \quad \text{with } \theta = \mathrm{Arg}(z)$$

© 2025 Hanshu Yu. This work is licensed under a
Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

We can find the following facts:

$$z = |z|\hat{z}\,, \quad |\hat{z}| = 1$$

The **Euler's formula** tells us:

$$e^{\mathbf{i}\,\theta} = \cos(\theta) + \mathbf{i}\sin(\theta)\,.$$

The **Euler's identity** tells us:

$$e^{\mathbf{i}\,\pi} + 1 = 0\,.$$

Thus, with the format of $z = |z|\hat{z}$, we arrive at the polar form of any complex number, where $\hat{z}$ only encodes the angular information(argument) of z with $|\hat{z}| = 1$ and the modulus $|z|$ encodes "how much" z stretches or shrinks in that direction.

Properties

Here we list some noteworthy properties of complex numbers. Given two complex numbers z and w, then:

- $|\mathfrak{R}(z)| \leqslant |z|\,, |\mathfrak{I}(z)| \leqslant |z|\,, |\bar{z}| = |z|$;
- $|zw| = |z||w|$;
- $|z+w| \leqslant |z| + |w|\,, |z-w| \geqslant ||z| - |w||$;
- $\bar{\bar{z}} = z\,, \overline{z+w} = \bar{z} + \bar{w}\,, \overline{zw} = \bar{z}\overline{(w)}$;
- $z + \bar{z} = 2\mathfrak{R}(z)\,, z - \bar{z} = 2\,\mathbf{i}\,\mathfrak{I}(z)$.

B.A Complex Numbers Arithmetics

Given two arbitrary complex numbers:

$$z_1 = a + b\,\mathbf{i} \quad , \quad z_2 = c + d\,\mathbf{i}\,, \quad \text{with } z_1, z_2 \in \mathbb{C}\,, \text{ and } \; a, b, c, d \in \mathbb{R}\,,$$

we shall go through some basic complex number arithmetics.

Addition and subtraction

$$z_1 + z_2 = (a + c) + (b + d)\,\mathbf{i}$$
$$z_1 - z_2 = (a - c) + (b - d)\,\mathbf{i}$$

The geometrical interpretation of complex number addition appears to be the effect of a vector addition. Fig B.2 gives an example of two complex numbers adding together, similar to vectors addition in $\mathbb{R}^2$.

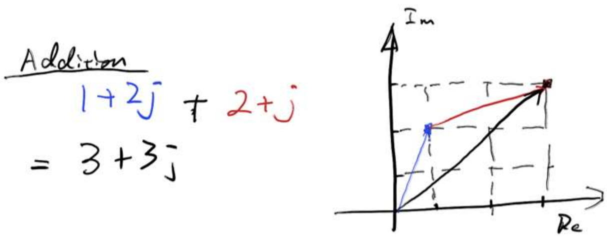

Figure B.2: A geometric visualization of complex number addition.

Multiplication

$$
\begin{aligned}
z_1 z_2 &= (a + b\,\mathbf{i})(c + d\,\mathbf{i}) \\
&= ac + ad\,\mathbf{i} + bc\,\mathbf{i} + bd\,\mathbf{i}^2 \\
&= ac - bd + (ad + bc)\,\mathbf{i}
\end{aligned}
$$

$$
\begin{aligned}
z_1 \bar{z}_1 &= (a + b\,\mathbf{i})(a - b\,\mathbf{i}) \\
&= a^2 - ab\,\mathbf{i} + ab\,\mathbf{i} - b^2\,\mathbf{i}^2 \\
&= a^2 + b^2
\end{aligned}
$$

Multiplication is a lot easier in polar form. We write $z_1 = |z_1|e^{\mathbf{i}\,\theta_1}, z_2 = |z_2|e^{\mathbf{i}\,\theta_2}$, then

$$z_1 z_2 = |z_1|e^{\mathbf{i}\,\theta_1}|z_2|e^{\mathbf{i}\,\theta_2} = |z_1||z_2|e^{\mathbf{i}(\theta_1+\theta_2)}\,.$$

The geometric interpretation is then much clearer, multiplying z_1 by a complex number $z_2 = |z_2|e^{\mathbf{i}\,\theta_2}$ indicates that the modulus of the original $|z_1|$ is multiplied by a factor $|z_2|$ and complete a rotation by θ_2.

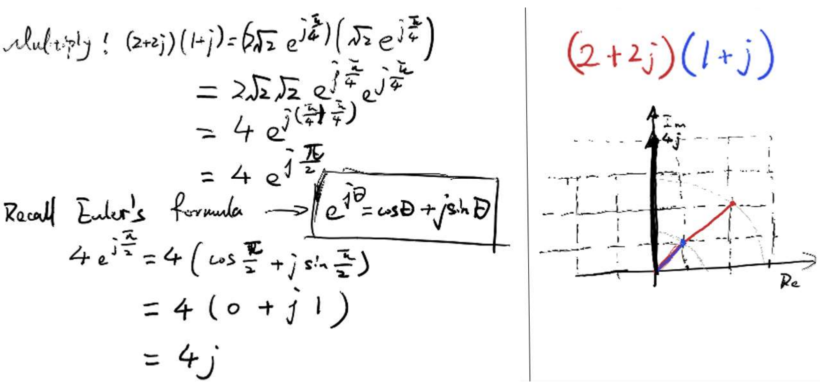

Figure B.3: A geometric visualization of complex number multiplication.

Powers and roots

If we compute the powers of z_1 in a crude way, we see that it quickly becomes messy:

$$\begin{aligned}
z_1^2 &= (a + b\,\mathbf{i})^2 \\
&= a^2 - b^2 + 2ab\,\mathbf{i} \\
z_1^3 &= (a + b\,\mathbf{i})^3 \\
&= (a^2 - b^2 + 2ab\,\mathbf{i})(a + b\,\mathbf{i}) \\
&= a^3 + a^2 b\,\mathbf{i} - ab^2 - b^3\,\mathbf{i} + 2a^2 b\,\mathbf{i} + 2ab^2\,\mathbf{i}^2 \\
&= a^3 - 3ab^2 + (3a^2 b - b^3)\,\mathbf{i} \\
&\ldots\ldots
\end{aligned}$$

Luckily we still have the polar form, with $z = |z|\hat{z}$. We first take a look at $\hat{z} = e^{\mathbf{i}\,\theta} = \cos(\theta) + \mathbf{i}\sin(\theta)$ when we calculate the n-th power of $\hat{z}$:

$$\begin{aligned}
\hat{z}^n &= (e^{\mathbf{i}\,\theta})^n \\
&= e^{\mathbf{i}\,n\theta}
\end{aligned}$$

we make use of the Euler's formula,

$$\hat{z}^n = \cos(n\theta) + \mathbf{i}\sin(n\theta)$$

The Euler's formula also does not stop us from extending natural number powers to real number powers. Thus, when calculating the n-th root of a complex number, we can just take the $\frac{1}{n}$-th power and make use the of Euler's formula.

To summarize, the power of a complex number z can be conveniently calculated using its polar form:

$$z^x = |z|^x e^{x \cdot \mathrm{Arg}(z)}\,, \qquad \text{with } x \in \mathbb{R}$$

It becomes a bit obvious when we make use of the polar form for computation of integer powers for arbitrary complex number z:

$$\hat{z}^n = (\cos(\theta) + \mathbf{i}\sin(\theta))^n = \cos(n\theta) + \mathbf{i}\sin(n\theta)\,, \qquad \textit{with } n \in \mathbb{N}\,.$$

*This equation is also called **De Moivre's Theorem**.*

However, from a historical point of view, proving or even finding De Moivre's theorem from Euler's identity is basically cheating. De Moivre's theorem appeared earlier and it was Euler who provided the first proof. We shall quickly demonstrate how to prove De Moivre's theorem by mathematical induction.

Proof of De Moivre's Theorem by mathemtatical induction. When $n = 1$, the equation is trivially true. The inductive hypothesis is that the result holds for $n = k \in \mathbb{N}$, to prove the theorem we need to show that the result holds for $n = k + 1$.

$$\begin{aligned}
(\cos(\theta) + \mathbf{i}\sin(\theta))^{k+1} &= (\cos(\theta) + \mathbf{i}\sin(\theta))^k(\cos(\theta) + \mathbf{i}\sin(\theta)) \\
&= (\cos(k\theta) + \mathbf{i}\sin(k\theta))(\cos(\theta) + \mathbf{i}\sin(\theta)) \\
&= \cos(k\theta)\cos(\theta) - \sin(k\theta)\sin(\theta) + \mathbf{i}(\cos(k\theta)\sin(\theta) + \sin(k\theta)\cos(\theta))
\end{aligned}$$

From basic trigonometry relationship, we know:

$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta\,,$$

$$\sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha\,.$$

Then,

$$\begin{aligned}(\cos(\theta) + \mathbf{i}\sin(\theta))^{k+1} &= \cos(k\theta+\theta) + \mathbf{i}\sin(k\theta+\theta)\\ &= \cos(k+1)\theta + \mathbf{i}\sin(k+1)\theta\end{aligned}$$

Now our proof is complete by mathematical induction. □

We have been making use of the principal argument θ *in the calculations above, but recall that the argument of a complex number is multi-valued with a period of* 2π*. With integer's power of* $\hat{z}$*, we are safe because* $2\pi kn$ *are still integer multiples of* 2π*. When we are trying to extract* n*-th roots, then much care has to be taken.*

For $\gamma, z \in \mathbb{C}$*, we assume that* γ *is the* n*-th root of* z*. We have the following relationships:*

$$\gamma = z^{\frac{1}{n}}$$

Let $\mathrm{Arg}(z) = \theta$ *and* $\mathrm{Arg}(\gamma) = \phi$ *, we express the relationship above in polar form:*

$$|\gamma|e^{\mathbf{i}(\phi+2k\pi)} = |z|^{\frac{1}{n}}e^{\mathbf{i}\,\frac{\theta+2k\pi}{n}}$$

Now, within the range of $(-\pi,\pi]$*, we have* n *candidates of "principal" arguments! Are these* n *complex numbers the roots of the complex number z? The answer is a clear yes! Think about the n-th root of real numbers, for example, the square root of* 4 *can be either* 2 *or* -2*. The fundamental theorem of algebra also tells you that a* n*-th degree polynomial should have* n *complex roots. To tie up the loose end, which one is the principal argument? It depends on your preference or the specific nature of the problem you are working on. Normally, when you are speaking of roots, you talk about* ***all*** *possible complex roots instead of just calling out one root as your "principal".*

Division

$$\begin{aligned}\frac{z_1}{z_2} &= \frac{a+b\,\mathbf{i}}{c+d\,\mathbf{i}}\\ &= \frac{(a+b\,\mathbf{i})(c-d\,\mathbf{i})}{(c+d\,\mathbf{i})(c-d\,\mathbf{i})}\\ &= \frac{ac+bd+(bc-ad)\,\mathbf{i}}{c^2+d^2}\\ &= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,\mathbf{i}\end{aligned}$$

In polar form:

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}e^{\mathbf{i}(\theta_1-\theta_2)}$$

B.B Quadratic Polynomials

We look at quadratic polynomials of the form:

$$f(x) = ax^2 + bx + c\,, \quad \text{with } a, b, c \in \mathbb{R}\,.$$

We may obtain a unique factorization with roots r_1 and r_2:

$$f(x) = ax^2 + bx + c = a(x-r_1)(x-r_2)\,.$$

In order to find the roots we solve the quadratic equation:

$$ax^2 + bx + c = 0\,.$$

If we obtain such a form:

$$(x - \beta)^2 = \alpha^2\,,$$

We may easily discover the roots:

$$\begin{aligned} x - \beta &= \pm\alpha \\ x &= \beta \pm \alpha \end{aligned}$$

We re-write $(x - \beta)^2 = \alpha^2$ into:

$$x - 2\beta + \beta^2 - \alpha^2 = 0\,.$$

And we re-write the quadratic formula $ax^2 + bx + c = 0$ into:

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0\,.$$

We may easily spot the correspondence of the coefficients:

$$-2\beta = \frac{b}{a}, \quad \beta^2 - \alpha^2 = \frac{c}{a}\,.$$

We can get:

$$\beta = -\frac{b}{2a}\,,$$

then

$$\begin{aligned} (-\frac{b}{2a})^2 - \alpha^2 &= \frac{c}{a} \\ \frac{b^2}{4a^2} - \frac{c}{a} &= \alpha^2 \\ \alpha &= \pm\frac{\sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

Thus we obtained the quadratic formula for the roots of our quadratic polynomial:

$$x = \beta \pm \alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Then we have the discriminant Δ:

$$\Delta = b^2 - 4ac\,.$$

- when $\Delta > 0$, the quadratic formula has 2 distinct real roots;
- when $\Delta = 0$, the quadratic formula has 1 real root with multiplicity 2;
- when $\Delta < 0$, the quadratic formula has 2 distinct complex roots and they form a complex conjugate pair.

B.C Exercise problems

1. For each of the following complex numbers:

   - calculate the modulus and argument and write the polar form;
   - find the complex conjugate;
   - visualize the given complex number and the complex conjugate you find in the complex plane.

   a) $3 + 4\,\mathbf{i}$

   b) $11\,\mathbf{i}$

   c) $-1 - \mathbf{i}$

   d) $-3 + \mathbf{i}$

2. Calculate:

   a) $(13 + 5\,\mathbf{i}) + (8 - 2\,\mathbf{i})$

   b) $(2\,\mathbf{i}) - (7 + 7\,\mathbf{i})$

   c) $(5 - 2\,\mathbf{i})(2 + 4\,\mathbf{i})$

   d) $\frac{3+2\,\mathbf{i}}{4-3\,\mathbf{i}}$

   e) $\frac{7-6\,\mathbf{i}}{2\,\mathbf{i}}$

   f) $\frac{1}{\mathbf{i}}$

B.D The fundamental theorem of algebra

A univariate complex polynomial P of degree $n \geqslant 0$ is of the following form:

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 z^0 \,,$$

in which $z \in \mathbb{C}$ and $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{C}$.

Fundamental Theorem of Algebra . *Every non-constant univariate polynomial in $\mathbb{C}$ possesses at least 1 root in $\mathbb{C}$.*

We will not show the proof of this theorem as the proof requires some effort and would be a large deviation from our little piece of text.

Statement *The fundamental theorem of algebra tells us that in $\mathbb{C}$, we can finally state that a n-th order polynomial has exactly n roots!*

Proof. Consider a complex univariate polynomial

$$P(z) = \sum nk = 0 c_k z^k \,, \text{ where } \forall k = 0, 1, \ldots, n,\ c_k \in \mathbb{C} \,.$$

Based on the fundamental theorem of algebra, we know that $P(z)$ has at least 1 root, we denote this root as r_1. We can then factorize this polynomial:

$$P(z) = c_n(x - r_1) \sum n - 1k = 0\frac{c_k}{c_n} z^k .$$

In the meantime, the 'remainder polynomial' $\sum n - 1k = 0\frac{c_k}{c_n} z^k$ is also a complex univariate polynomial and based on the fundamental theorem of algebra also has at least 1 root. We can repeat this line of reasoning for a total of $n - 1$ times till the order of the 'remainder polynomial' becomes 1. Then we will find the last factor and completed the factorization of $P(z)$. Thus we have proved that P(z) is completely uniquely factorized with n (non-distinct) linear factors that corresponds to n (non-distinct) roots up to a permutation of these factors/roots. □

In fact, with the statement and proof above, we come to an equivalent statement of fundamental theorem of algebra below.

Fundamental Theorem of Algebra . *Every complex polynomial $P(z)$ of degree $n \geqslant 1$ has a unique factorization of distinct linear factors up to a permutation of these distinct factors.*

$$P(z) = c(z - r_1)^{m_1}(z - r_2)^{m_2}...(z - r_k)^{m_k} ,$$

where the roots $r_1, r_2, ..., r_k \in \mathbb{C}$ are distinct and the corresponding multiplicities $m_1, m_2, ..., m_k > 0$.

B.E Why complex numbers? (Just a tiny bit more than usual undergraduate engineering math...but fun!)

We quickly rush back to Section B.b and take a quick look back. When we are considering the polynomial

$$f(x) = ax^2 + bx + c , \quad \text{with } a, b, c, x \in \mathbb{R} ,$$

nothing is complex. We have all coefficients of $f(x)$ in $\mathbb{R}$, the function f is a map $\mathbb{R} \to \mathbb{R}$, we can graph it in $\mathbb{R}^2$. There is nothing in $\mathbb{C}$, or to be a bit more precise since many of you may know that $\mathbb{R} \subset \mathbb{C}$, the arithmetic 'party' $f(x) = ax^2 + bx + c$ did not really invite the imaginary part. But when we discuss about the roots, the imaginary parts just shows itself, otherwise we are forced to say that when $\Delta < 0$ the roots **do not exist** (in $\mathbb{R}$)!

Perhaps primary school students can happily live with this, but a mathematician, or even a concerned undergraduate student might feel deeply worried. This is just polynomials of order 2 and you need to discuss 3 different situations and even one of them tells you the root do not exist! What if you need to discover the roots of higher order polynomials? Things get ugly really fast, perhaps faster than you could imagine...

Going back to the quadratic polynomial case, if the discriminant $\Delta < 0$, we may write the quadratic formula in this form:

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

As long as we accept the existence of $\sqrt{-1}$ and extend the $\mathbb{R}$, we can tackle all possibly occurring roots for such kind of univariate polynomials.

Think about the arithmetics you have learned through out the years of school: addition, subtraction, multiplication, division. If you think about these in $\mathbb{R}$, there is (almost) nothing to worry about. When you add or subtract or multiply no matter how many real numbers, the result is always a real number. Division is a bit trickier due to the possible existence of 0 in the denominator but that is the only outlier and we may safely call it '*undefined*'. Of course it is possible to define some abstract algebraic structure such that division by 0 is defined. For those readers who are curious enough and ready to see some abstract algebra, I would like to point to a specific interesting example called 'wheel theory' and it has some interestingly weird properties that are totally different from real numbers. I would like to stop this discussion here before we really urge ourselves to dive deep into abstract algebra and comfortably claim the fact that division by zero is *undefined* in all circumstances that we may encounter.

When we think about power, it is still fine within $\mathbb{R}$. It would be nice if we know the roots as well because the roots are considered to be the 'inverse' of powers. But now the problem occurs with the inverse of even order powers, $f(x) = x^n$ when $n \in 2k \mid k \in \mathbb{N}$ is neither injective nor surjective in $\mathbb{R}$! In other words, multiple x could map to the same $f(x)$ value and there exist values in $\mathbb{R}$ that are not possible to obtain through $f(x), \forall x \in \mathbb{R}$.

Before we continue, I would like to first present the definition of a 'field'.

Definition 1 (Field)**.** A *field* is a set F together with two binary operations $+$ (addition) and $\cdot$ (multiplication) such that the following axioms hold for all $a, b, c \in F$:

1. **(Additive Associativity)** $a + (b + c) = (a + b) + c$
2. **(Additive Commutativity)** $a + b = b + a$
3. **(Additive Identity)** There exists an element $0 \in F$ such that $a + 0 = a$
4. **(Additive Inverse)** For each $a \in F$, there exists an element $-a \in F$ such that $a + (-a) = 0$
5. **(Multiplicative Associativity)** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
6. **(Multiplicative Commutativity)** $a \cdot b = b \cdot a$
7. **(Multiplicative Identity)** There exists an element $1 \in F$, $1 \neq 0$, such that $a \cdot 1 = a$
8. **(Multiplicative Inverse)** For each $a \in F$, $a \neq 0$, there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$
9. **(Distributivity)** $a \cdot (b + c) = a \cdot b + a \cdot c$

The set of rational numbers $\mathbb{Q}$, the set of real numbers $\mathbb{R}$, and the set of complex numbers $\mathbb{C}$ are all fields. You may spot in the definition that only addition and multiplication is defined but not really directly point to subtraction and division.

A quick-reacting reader might immediately claim that subtraction $a - b$ is basically defined by the addition between a and the additive inverse b: $a + (-b)$. The division $\frac{a}{b}$ with $b \neq 0$, can also be defined by multiplication between a and the multiplicative inverse of b: $a \cdot b^{-1}$. So we are safe to just stick to the two foundational operations: addition and multiplication.

Now we converge to our previously heavily discussed topic: polynomials. Polynomials are just the most natural function that combines addition and multiplication which are our two fundamental operations in a field. Polynomials are a generalization of numbers in any base and can be used to approximate any function. In many branches of mathematics, polynomials play a crucial role and if I'm allowed to continue there will be an endless list of the use of polynomials.

Polynomials are so fundamental yet so important such that mathematicians put much effort into researching properties of polynomials. There are lots of mathematical structures in manipulating polynomials such as factorization which leads to roots of polynomials. Now if we consider the field $\mathbb{R}$, we have already shown that there might be roots lying outside $\mathbb{R}$. To mathematicians, this is sub-optimal. Even if $\mathbb{R}$ is a complete field that allow us to do calculus and analysis which occur mostly in university level mathematics, it is still too weak to solve polynomials, a subject that pop-up in primary school math class.

We desire a field such that we may solve the most natural functions, polynomials, within the field. This field is the set of complex numbers $\mathbb{C}$ and such kind of field is called algebraically closed field. We wrap-up this section by formally stating the definition of an algebraically closed field.

Definition 2 (Algebraically Closed Field)**.** A field F is said to be **algebraically closed** if every non-constant polynomial with coefficients in F has at least one root in F. That is,

$$\forall f(x) \in F[x],\ \deg(f) \geqslant 1 \Rightarrow \exists \alpha \in F \text{ such that } f(\alpha) = 0.$$

Equivalently, every polynomial in $F[x]$ of degree $n \geqslant 1$ can be factored into linear factors over F:

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad \text{with } \alpha_i \in F.$$

There is much more to the matters we discussed in this short section, and hopefully my brief discussion has raised some interested eyebrows. We encourage the really enthusiastic readers to further explore in the field of abstract algebra, trust me there is tons of fun (and most-likely accompanied by tons of frustration).