# Factoring Polynomials

Thaqib Mo.

December 14, 2020

# 1 Complex Numbers

Using localization similar to the construction of $\mathbb{Q}$ we can construct elements of $\mathbb{C}$ in terms of ordered pairs $(a, b) \in \mathbb{R} \times \mathbb{R}$. The addition is defined component wise,

$$(a, b) + (c, d) = (a + c, b + d)$$

and multiplication similar to the Gaussian integers is defined as

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

The addition is the same as the addition in $\mathbb{R}$ so we can already conclude that $\mathbb{C}, +$ is an abelian group. $(1, 0)$ is clearly the multiplicative identity and it is easy to check that multiplication is associative.
To check that every non-zero element in $\mathbb{C}$ has an multiplicative inverse:

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

So we have $\left( \frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \right)$ this ordered pair is the inverse of $(a, b)$. We have $a^2 + b^2 \neq 0$ when $(a, b) \neq (0, 0)$. Now consider

$$\begin{aligned}
&(a, b) \cdot ((c, d) + (e, f)) = (a, b) \cdot (c + e, d + f) \\
&= (a(c + e) - b(d + f), a(d + f) + b(c + e)) \\
&= (ac - bd + ae - bf, ad + bc + af + be) \\
&= (a, c) \cdot (e, f) + (a, b) \cdot (e, f)
\end{aligned}$$

So we can now say $\mathbb{C}$ is a field.

## 1.1 Complex Number Constructions and Properties

**Definition 1**

Let $z \in \mathbb{C}$ and we write $z = a + bi$ for some $a, b \in \mathbb{R}$

- The form $a + bi$ is called the standard form of $z$
- The number $a$ is the *Real* part of $z$ denoted by $\mathrm{Re}(z)$
- The number $b$ is the *imaginary* part of $z$ denoted by $\mathrm{Im}(z)$
- $\bar{z} = a - bi$ is called the *complex conjugate*
- $|z| = \sqrt{a^2 + b^2}$ is called the *absolute value* of $z$

**Proposition 1**

$\phi : \mathbb{C} \to \mathbb{C}$ given by $\phi(z) = \bar{z}$ is a ring homomorphism.

*Proof.* Let $z = a + bi$ and $w = c + di$

Consider $\phi(z + w) = \overline{z + w} = a + c - (b + d)i = a - bi + c - di = \phi(z) + \phi(w)$.

$\phi(zw) = \bar{z}\bar{w} = \overline{ac - bd + (ad + bc)i} = ac - bd - (ad + bc)i = ac - bd - adi - bci = (a - bi)(c - di) = \phi(z)\phi(w)$.

For $\phi(1 + 0i) = 1 - 0i = 1$. So $\phi$ is a ring homomorphism. $\square$

**Proposition 2**

For all $z \in \mathbb{C}$ we have $|zw| = |z||w|$

*Proof.* Let $z = a + bi$ and $w = c + di$ we have $zw = ac - bd + (ad + bc)i$ so we have

$$
\begin{aligned}
|zw| &= \sqrt{(ac - bd)^2 (ad + bc)^2} \\
&= \sqrt{a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2} \\
&= \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} \\
&= \sqrt{a^2(c^2 + d^2) + b^2(c^2 + d^2)} \\
&= \sqrt{(a^2 + b^2)(c^2 + d^2)} \\
&= \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
&= |z||w|
\end{aligned}
$$

$\square$

The *triangle inequality* also holds in $\mathbb{C}$

**Theorem 1: Triangle inequality**

For all $z, w \in \mathbb{C}$ we have $|z + w| \leq |z| + |w|$

*Proof.*

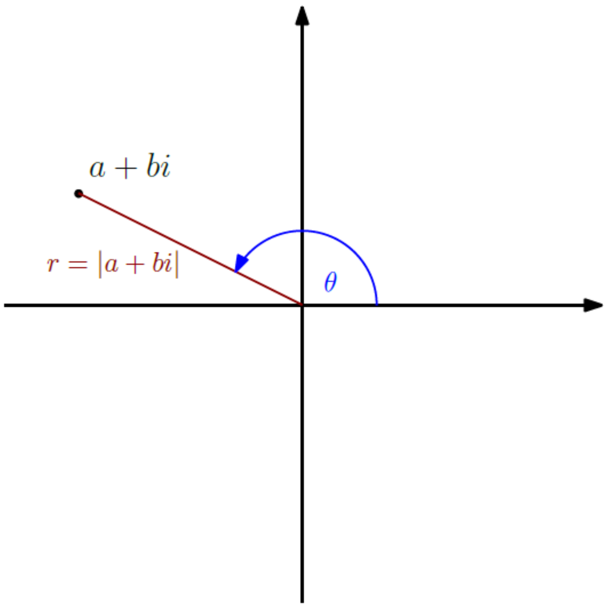
$$
\begin{aligned}
|z + w|^2 &= (z + w)\overline{(z + w)} \\
&= (z + w)(\bar{z} + \bar{w}) \\
&= z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\
&= |z|^2 + |w|^2 + (z\bar{w} + \overline{z\bar{w}}) \\
&= |z|^2 + |w|^2 + 2\,\mathrm{Re}(z\bar{w})
\end{aligned}
$$

Note that $\mathrm{Re}(z\bar{w}) \leq |z\bar{w}| = |z||\bar{w}| = |z||w|$. So we have

$$|z+w|^2 = |z|^2 + |w|^2 + 2\,\mathrm{Re}(z\bar{w}) \leq |z|^2 + 2|z||w| + |w|^2 = (|z|+|w|)^2$$

Taking the positive square roots gives the triangle in equality. $\square$

## 1.2 Polar Form of a Complex Number




So we write $a + bi = re^{i\theta}$ where $r$ is the magnitude and $\theta$ is the argument. There are be many values for the argument for the same complex number, in particular any $\theta + 2k\pi$ for $k \in \mathbb{Z}$ would work.

**Theorem 2**

For complex numbers $z_1 = r_1 z^{\theta_1}$ and $z_2 = r_2 z^{\theta_2}$ we have

$$z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$$

*Proof.* We have $z_1 = r_1 e^{\theta_1} = r_1(\cos(\theta_1) + i\sin(\theta_1))$ and $z_2 = r_2(\cos(\theta_2) + i\sin(\theta_2))$ so we have

$$\begin{aligned}
z_1 z_2 &= r_1 r_2(\cos(\theta_1) + i\sin(\theta_1))(\cos(\theta_2) + i\sin(\theta_2)) \\
&= r_1 r_2(\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) + i(\cos(\theta_1)\sin(\theta_1) + \sin(\theta_2)\cos(\theta_2))) \\
&= r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1\theta_2)) \\
&= r_1 r_2 e^{i(\theta_1+\theta_2)}
\end{aligned}$$

$\square$

**Corollary 1: (de Moivre's Theorem)**

Let $z$ be a complex number with $z \neq 0$. Then we have

$$z^n = r^n e^{n\theta}$$

For $n \in \mathbb{Z}$

*Proof.* The base case is trivial we have $z^0 = 1$ and $r^0 e^{0\theta} = 1$. Now assume it holds true for some $n \in \mathbb{N}$. Now consider $n + 1$

$$\begin{aligned} z^{n+1} &= zz^n \\ &= re^{\theta} r^n e^{n\theta} \\ &= rr^n e^{n\theta+\theta} \\ &= r^{n+1} e^{(n+1)\theta} \end{aligned}$$

This completes the proof for $n \in \mathbb{N}$. Now consider $z^{-n}$ for $n \in \mathbb{N}$. By uniqueness of inverse since $\mathbb{C}$ is a field, we have $r^{-n} e^{-n\theta} z^n = 1$. □

# 2 The Fundamental Theorem of Algebra

## 2.1 Algebraically Closed Field

**Theorem 3: Fundamental Theorem of Algebra**

Let $f \in \mathbb{C}[x]$ be a non-constant polynomial. Then $f$ has a root in $\mathbb{C}$.

This leads to the definition of algebraically closed fields

**Definition 2: Algebraically Closed Field**

A field is algebraically closed if any non-constant polynomial $f \in F[x]$ has a root in $F$.

Another equivalent way of formulating algebraically closed field is in the following theorem:

**Theorem 4**

A field is algebraically closed if and only if every non-constant polynomial $f \in F[x]$ can be factored as a product of linear polynomials.

$$f = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

Where $n = \deg f$ and $c, a_1, a_2, \ldots, a_n \in F$.

*Proof.* ($\Rightarrow$) suppose that $F$ is algebraically closed. Consider the base case $n = 1$, it is already in linear form so we are done. Now assume the results holds true for $\deg f = n$ and consider $\deg f = n + 1$.
Since $F$ is algebraically closed $f$ has a root in $F$, and let $f(a_{n+1}) = 0$. Then by the factor theorem $(x - a_{n+1})$ divides $f$. So let

$$f = g(x - a_{n+1})$$

And since $\deg g = n$ by the inductive hypothesis it can be factored into linear factors and we have

$$f = c(x - a_{n+1})(x - a_1)(x - a_2) \cdots (x - a_n)$$

($\Leftarrow$) Suppose every non-constant polynomial in $F[x]$ can be factored into linear polynomials. Then

$$f = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

Now $f$ always has a root in $f$ since $a_1, a_2, \ldots, a_n$ are all roots. $\square$

## 3 Irreducible Polynomials

**Definition 3: Irreducible and Reducible Polynomials**

Let $F$ be a field. Then $f$ is reducible if $f$ has a proper factorization that is $f = gh$ where $g, h \in F[x]$ and $\deg(g), \deg(h) \geq 1$. Otherwise $f$ is irreducible.

Using this definition every linear polynomial is automatically irreducible. For larger degrees we have:

**Proposition 3**

Let $F$ be a field and $f \in F[x]$ If $\deg f \geq 2$ be irreducible then $f$ has no roots. Conversely, if $\deg f = 2$ and $\deg f = 3$ has no roots then $f$ is irreducible.

*Proof.* Suppose we have $\deg f \geq 2$ is irreducible. Assume $f$ has a root in $F$. By the factor theorem we have $f = (x - c)h$ then we have $\deg h = \deg f - 1 \geq 1$ this means we have factored $f$ into 2 non-constant polynomials thus a contradiction.

Conversely suppose $\deg f = 2$ or $\deg 3 = f$ and that $f$ has no roots in $F$. Suppose $f$ is reducible in $F$ then we must have $f = gh$ and we must have $\deg f = \deg g + \deg h$ and this forces one of $\deg g, \deg h = 1$ either way $f$ has a linear factor and must have a root again a contradiction. Thus $f$ must be irreducible. □

Note the converse does not generalize to higher degrees there can be polynomials $f$ with $\deg f = 4$ with no roots and still be irreducible. The above theorem also shows that $x^2 + 1 \in \mathbb{R}[x]$ is irreducible.

**Corollary 2**

If $F$ is algebraically closed and a non-constant polynomial $f \in F[x]$ is irreducible if and only if $\deg f = 1$

*Proof.* We already know that a linear polynomial is irreducible. Conversely assume that $f \in F[x]$ is irreducible and $\deg f > 1$ then $f$ has no roots in $F$ by the above proposition, which is a contradiction to $F$ being algebraically closed. □

**Example 1.** The polynomial $f(x) = x^3 + x + [1] \in \mathbb{Z}/2\mathbb{Z}$ is irreducible. A simple exhaustive proof can show this we have $f([0]) = [1]$ and $f([1]) = [1]$ so $f$ has no roots therefore $f$ is irreducible.

### 3.1 Irreducible Polynomials in $\mathbb{R}[x]$

**Lemma 1: Conjugate Roots**

Suppose $f \in \mathbb{R}[x]$ and if $c \in \mathbb{C}$ is a root of $f$ then $\bar{c}$ is also a root.

*Proof.* We know that $f(c) = 0$ so

$$a_0 + a_1 c + a_2 c^2 + \ldots + a_n c^n = 0$$

Then we have

$$\begin{aligned} 0 &= \bar{0} \\ &= \overline{a_0 + a_1 c + a_2 c^2 + \ldots + a_n c^n} \\ &= \bar{a_0} + \bar{a_1}\bar{c} + \bar{a_2}\bar{c^2} + \ldots + \bar{a_n}\bar{c^n} \\ &= a_0 + a_1\bar{c} + a_2\bar{c^2} + \ldots + a_n\bar{c^n} \\ &= f(\bar{c}) \end{aligned}$$

$\square$

Using this lemma we can prove a very important result for polynomials in $\mathbb{R}[x]$

**Theorem 5**

Let $f \in \mathbb{R}[x]$ be a non-constant polynomial. Then $f$ is irreducible in $\mathbb{R}[x]$ if and only if $\deg f = 1$ and $\deg f = 2$

*Proof.* If $\deg f = 1$ or $\deg f = 2$ has no real roots then we know that $f$ is irreducible. Conversely if $f \in \mathbb{R}[x]$ is an irreducible polynomial then $f$ is also a polynomial in $\mathbb{C}[x]$. Since $\mathbb{C}$ is algebraically closed there is a $c \in \mathbb{C}$ such that $f(c) = 0$. If we have $c \in \mathbb{R}$ then since $f$ is irreducible it forces us to $\deg f = 1$.
If $c \notin \mathbb{R}$ then $c \in \mathbb{C}$ then by the conjugate roots theorem $\bar{c}$ is also a root. To we can write $f(x) = (x-c)(x-\bar{c})h(x)$ for $h \in \mathbb{C}[x]$. Then let $g = (x-c)(x-\bar{c})$ we have

$$\begin{aligned} (x-c)(x-\bar{c}) &= x^2 - (c+\bar{c})x + c\bar{c} \\ &= x^2 - (2\operatorname{Re} c)x + |c|^2 \in \mathbb{R}[x] \end{aligned}$$

So $f$ is divisible by $g \in \mathbb{R}[x]$

Thus we have a factorization $f = gh$ in $\mathbb{R}[x]$ where $\deg g = 2$. Again by irreducibility of $f$, $h$ must be a constant polynomial. Therefore $\deg f = 2$ $\square$

## 3.2 Irreducible Polynomials in $\mathbb{Q}[x]$

**Theorem 6: Rational Root Theorem**

Let $f \in \mathbb{Q}[x]$ be a non-constant polynomial and suppose $r \in \mathbb{Q}$ is a root of $f$, and let

$$f = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n$$

With $a_0, a_1, \ldots a_n \in \mathbb{Z}$ and $a_n \neq 0$ if we write $r = \frac{p}{q}$ with $\gcd(p, q) = 1$ (Simplest form). Then we must have

$$q \mid a_n \quad p \mid a_0 \text{ in } \mathbb{Z}$$

*Proof.* Since $\frac{p}{q}$ is a root we have

$$a_0 + a_1 \frac{p}{q} + \ldots + a_n \left(\frac{p}{q}\right) = 0$$

Multiplying by $q^n$ we have

$$\begin{aligned} a_0 q^n + a_1 p q^{n-1} + \ldots + a_n p = 0 \\ a_0 q^n = -(a_1 p q^{n-1} + \ldots + a_n p) = -p(a_1 q^{n-1} + \ldots a_n) \end{aligned}$$

This shows that we have $p \mid a_0 q^n$. Since $\gcd(p, q) = 1$ we have $\gcd(p, q^n) = 1$ and we get $p \mid a_0$ by the divisibility results.

Similarly we can isolate $a_n p^n$ to get $q \mid a_n p^n$ and again using $\gcd(p^n, q) = 1$ we have $q \mid a_n$ $\square$

**Example 2.** Let $f(x) = x^3 - 2x + 5 \in \mathbb{Q}[x]$ is irreducible. Since $\deg f = 3$ we know that it has no roots. We can also use the rational roots theorem. If $\frac{p}{q}$ is a root with $\gcd(p, q) = 1$ then we must have $q \mid 1$ and $p \mid 5$. This means we have $q \in \{-1, 1\}$ and $p \in \{-1, 1, -5, 5\}$. So the possibilities for $\frac{p}{q}$ are $1, -1, -5, 5$ and none of them are roots.

## 3.3 Showing a number is irrational

We can also use rational root theorem to show that some $\alpha \in \mathbb{R}$ is irrational.

**Algorithm 1**

#1 Find a non-zero polynomial for which $f$ with integer coefficients for which $\alpha$ is a root.

#2 Use RRT to show that $f$ has no rational roots.

These 2 steps combined should prove any $\alpha \in \mathbb{R}$ is irrational.

**Example 3.** $\alpha = \sqrt{2} + \sqrt{3}$ is irrational. We have $\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{5}$ so $\alpha^2 - 5 = 2\sqrt{6}$ and then $(\alpha^2 - 5)^2 = (2\sqrt{6})^2 = 24$. So we have $\alpha^4 - 10\alpha^2 + 1 = 0$. So all roots are integers and if $\alpha \in \mathbb{Q}$ then we must have $\alpha = \frac{p}{q}$ with $p \mid 1$ and $q \mid 1$ the only choices are $\frac{p}{q} = 1, -1$ and $f(1), f(-1) \neq 0$ so we cannot have $\alpha \in \mathbb{Q}$

**Example 4.** For any prime $p$ and $n \geq 2$ $\sqrt[n]{p}$ is irrational.

$$(\sqrt[n]{p})^n = p$$
$$(\sqrt[n]{p})^n - p = 0$$

So a polynomial with integer coefficients with root $\sqrt[n]{p}$ is $x^n - p$. Then if $\sqrt[n]{p} \in \mathbb{Q}$ then we have $\sqrt[n]{p} = \frac{r}{s}$. Then since it is a root of $x^n - p$ we must have $s \mid 1$ and $r \mid -p$ that means $s \in \{-1, 1\}$ and $r \in \{-1, 1, p, -p\}$ then the possibilities for $\frac{p}{q}$ are $1, -1, -p, p$. By simple computation we know that

$$(-1)^n - p \neq 0$$
$$(1)^n - p \neq 0$$

For the other possibility assume we have $p^n - p = 0$ then $p(p^{n-1} - 1) = 0$ so we must have $p = 0$ or $p^{n-1} - 1 = 0$ the first case directly leads to a contradiction and in the second case if we have $p^{n-1} - 1 = 0$ that means $p^{n-1} = 1$ which is not true for any prime $p$ so we have $\sqrt[n]{p} \notin \mathbb{Q}$