2 Rings and Fields

2.7 The Complex Numbers

Let k be a field and $f(x)$ be a polynomial in $k[x]$ of degree $d > 0$. In section 2.5 we showed that $f(x)$ can have at most d roots in k. Consider the polynomial $f(x) = x^2 - 2$. As a polynomial in $\mathbb{Q}[x]$ it has no rational roots. But as a polynomial in $\mathbb{R}[x]$ it has two real roots, $+\sqrt{2}$ and $-\sqrt{2}$. What about the polynomial $x^2 + 2$ in $\mathbb{R}[x]$? If $x^2 + 2 = 0$ then $x^2 = -2$. But if x is real, then it's square cannot be negative. Thus in $\mathbb{R}[x]$, the polynomial $x^2 + 2$ has no roots.

One of the greatest discoveries in mathematics is the *complex numbers*. In the next section we will see that *every* polynomial in $\mathbb{R}[x]$ of degree $d > 0$ has d complex roots. That computing scientists have developed good algorithms to compute these complex roots has enabled many applications of mathematics in science and engineering. We begin by defining the complex numbers.

Let i be the number such that $i^2 = -1$. The number i is called the complex unit. We define the set of complex numbers to be

$$\mathbb{C} = \{a + bi \ : \ a \in \mathbb{R}, \ b \in \mathbb{R}, \text{ and } i^2 = -1.\}$$

If $z = a + bi$ is a complex number we call a the *real part* of z and b the *imaginary part* of z. If $b = 0$ then the complex number $z = a + 0i = a$ is a real number. It follows that $\mathbb{R} \subset \mathbb{C}$. If $b \neq 0$ we say z is non-real or imaginary.[1]

A natural way to define addition and multiplication of complex numbers is to think of $z = a + bi$ as a polynomial in i with real coefficients, that is, as an element of the ring $\mathbb{R}[i]$ with the property $i^2 = -1$ and to let i commute with real numbers. Thus if $a + bi \in \mathbb{C}$ and $c + di \in \mathbb{C}$ we have

$$(a + bi) + (c + di) = (a + b) + (c + d)i$$

and

$$\begin{aligned} (a + bi) \times (c + di) &= ac + adi + bic + bdi^2 \\ &= ac + (ad + bc)i - bd = (ac - bd) + (ad + bc)i. \end{aligned}$$

Example 2.7.1. *Let $x = 2 + 3i$ and $y = 3 - i$. Then $x + y = 5 + 2i$ and $x \times y = 6 + 9i - 2i - 3i^2 = 9 + 7i$.*

Our definition for $\mathbb{C}$ means that two wonderful things happen. The first is stated as Theorem 2.6.2 below. The second is the Fundamental Theorem of Algebra which is presented in the next section.

Theorem 2.7.2. *The set of complex numbers $\mathbb{C}$ is a field with $\mathbb{R}$ a proper subfield.*

[1] It is most unfortunate that the complex numbers $z = a + bi$ with b non-zero have been called "imaginary numbers". This suggests they are ficticious, inventions of mathematicians having no practical application. That is not true. The complex numbers i and $-i$ are, in fact, no less "real" than negative numbers.

Proof. The definitions for addition and multiplication in $\mathbb{C}$ imply that $\mathbb{C}$ is closed under addition and multiplication. Observe that if $x = 0 + 0i$ and $y = a + bi$ then $x + y = a + bi$ thus the complex number $0 + 0i$ is the additive identity. Observe also that if $x = 1 + 0i$ then $x \times y = (1 + 0i) \times (a + bi) = a + bi$ thus $1 + 0i = 1$ is the multiplicative identity. We leave it to the reader to check the remaining properties of a ring and to verify that the inverse of $a + bi$,

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

For example

$$(a + bi) + (c + di) = (a + c) + (b + d)i = (c + a) + (d + b)i = (c + di) + (a + bi)$$

shows that addition is commutative. □

To divide $x = a+bi$ by $y = c+di$ by hand, it is easiest to multiply x/y by $(c-di)/(c-di)$ as shown below.

$$\frac{(a + bi)}{(c + di)} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{(c^2 + d^2) + 0i} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

Example 2.7.3. *The inverse of* $3-i$ *is* $\frac{3}{10}+\frac{1}{10}i$ *and* $(2+3i)$ *divided by* $(3-i)$ *is* $\frac{6-3}{10}+\frac{9-(-2)}{10}i = \frac{3}{10} + \frac{11}{10}i$. *Also, since* $(-i)i = (0 - i)(0 + i) = -i^2 = -(-1) = 1$, *the inverse of* i *is* $-i$.

Because $\mathbb{C}$ is a field and the rules for arithmetic in $\mathbb{C}$ involve only arithmetic with real numbers, this means we can do arithmetic with complex numbers and hence we can calculate in $\mathbb{C}[x]$ and do linear algebra over $\mathbb{C}$. Although the arithmetic with complex numbers can be tedious to do by hand, computers have no difficulty. For example, since $i^2 = -1$, i is a root of $x^2 + 1$. This means $(x - i)|(x^2 + 1)$ and hence we can find the other root of $x^2 + 1$ by dividing $x^2 + 1$ by $x - i$.

To visualize the complex numbers we draw them in $\mathbb{R}^2$. If $x = (a + bi) \in \mathbb{C}$ we locate x at the point $(a, b) \in \mathbb{R}^2$. We label the horizontal axis the *real axis* and the vertical axis the *imaginary axis* and call $\mathbb{R}^2$ the *complex plane*. Figure 2.7 below shows two complex numbers $x = 3 + 2i$ and $y = 1 - i$ and their sum $4 + i$.

Notice that the sum of $x + y$ corresponds to the sum of the two vectors $[3, 2]$ and $[1, -1]$. Notice also that if $c \in \mathbb{R}$, $(c+0i) \times (a+bi) = (ca)+(cb)i$, thus multiplication of the complex number $a + bi$ by c corresponds to multiplication of the vector $[a, b]$ by the scalar c in $\mathbb{R}^2$. Indeed we have the following

Theorem 2.7.4. *The set of complex numbers* $\mathbb{C}$ *is isomorphic to* $\mathbb{R}^2$ *as a vector space with isomorphism* $\varphi(a + bi) = [a, b]$.

In order to visualize what multiplication of one complex number by another means it is helpful to use a different representation of complex numbers. For a non-zero complex number

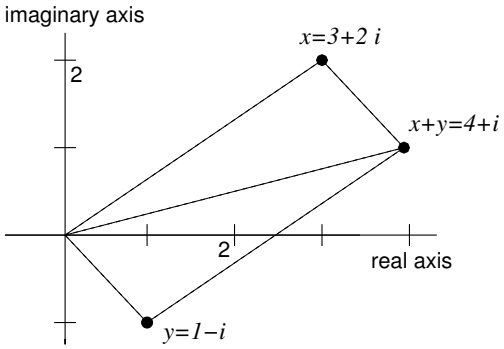

Figure 1: The complex plane

$z = a + bi$ we represent it in *polar co-ordinates* as $z = r(\cos\theta + i\sin\theta)$ where $r = \sqrt{a^2 + b^2}$ and $-\pi < \theta \leq \pi$. Figure 2.7 shows where this formula comes from.

The angle θ is called the argument of z, denoted $\arg(z)$. The quantity r is called the magnitude of z, denoted $|z|$. Notice that $|z|$ is the length of the vector $[a, b]$. For $z = 2 + 2i$ we obtain $r = \sqrt{8}$ and $\theta = \pi/4$ thus $2 + 2i = \sqrt{8}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$.

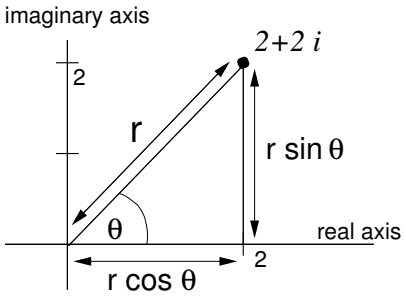

Figure 2: Polar co-ordinates for $2 + 2i$.

Lemma 2.7.5. *Let* $z_1 = r(\cos\theta + i\sin\theta)$ *and* $z_2 = s(\cos\omega + i\sin\omega)$.

(i) $z_1 z_2 = rs[\cos(\omega + \theta) + i\sin(\omega + \theta)]$.

(ii) $z_1/z_2 = rs^{-1}[\cos(\omega - \theta) + i\sin(\omega - \theta)]$.

Proof. (i) $z_1 z_2 = rs[(\cos\omega\cos\theta + \sin\omega\sin\theta) + i(\cos\theta\sin\omega + \cos\omega\sin\theta)]$. Now apply trigonometric identities to obtain the result. (ii) Exercise. □

Notice that $|z_1 z_2| = rs$ because $\sin^2 A + \cos^2 A = 1$. Also the argument of $z_1 z_2$ is $\theta + \omega$, the sum of the angles. This means when we multiply two complex numbers $z_1 \times z_2$ we *multiply their magnitudes and add their arguments.* And when we divide we divide magnitudes and subtract arguments.

Example 2.7.6. *Let* $x = 2+2i$ *and* $y = -1+i$. *Converting to polar co-ordinates we have* $x = \sqrt{8}[\cos(\pi/4)+i\sin(\pi/4)]$ *and* $y = \sqrt{2}[\cos(\frac{3}{4}\pi)+i\sin(\frac{3}{4}\pi)]$. *Thus* $x \times y = 4[\cos\pi + i\sin\pi] = -4$ *and* $x/y = 2[\cos(-\pi/2) + i\sin(-\pi/2)] = -2i$.

Theorem 2.7.7. (De Moivre's formula) *Let $z = r(\cos\theta + i\sin\theta)$ be a complex number in polar co-ordinates and let $n \in \mathbb{N}$. Then $z^n = r^n(\cos n\theta + i\sin n\theta)$.*

Proof. Apply Lemma 2.6.6 $n-1$ times. □

Exercises 2.7

1. Let $y = 2+3i$ and $z = 4+5i$. Calculate $y+z$, $y-z$, $y\times z$, $|z|$, z^{-1} and y/z.

2. For complex numbers $x = a+bi$ and $y = c+di$ show that multiplication is commutative and the formula given for the inverse of x is correct.

3. Let $y = 1+i$ and $z = 2i$. Express y and z in polar co-ordinates, multiply and divide them in polar co-ordinates, then draw $y, z, y\times z$ and y/z in the complex plane.

4. Let $y = -1+\sqrt{3}i$. Determine $|y|$ and $\arg(y)$.
   Using De Moivre's formula, determine y^3 and sketch y, y^2, y^3 in the complex plane.

5. Let $z_1 = r(\cos\theta + i\sin\theta)$ and $z_2 = s(\cos\omega + i\sin\omega)$ be complex numbers in polar co-ordinates. Show that $z_1 z_2^{-1} = rs^{-1}[\cos(\theta-\omega) + i\sin(\theta-\omega)]$.

6. Let $f(x) = ix^2 - x + (1-i)$ and $h(x) = x^2 + 3x + (3+i)$ be two polynomials in $\mathbb{C}[x]$. Using the Euclidean algorithm, find the monic greatest common divisor of $f(x)$ and $g(x)$. You should get a linear polynomial of the form $x-\alpha$ for $\alpha \in \mathbb{C}$ hence you know one root of $h(x)$. Find the other root.

7. Calculate the inverse of the 2 by 2 matrix $A = \begin{bmatrix} i & 1 \\ -1 & 1+i \end{bmatrix}$. One way to do this is to apply elementary row operations to reduce the bookkeeping matrix $[A|I]$ to $[I|A^{-1}]$.

8. Let $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z} \text{ and } i^2 = -1\}$ and let addition and multiplication in $\mathbb{Z}[i]$ be defined as for $\mathbb{C}$. The set $\mathbb{Z}[i]$ is called the Gaussian integers. Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. See Lemma 2.2.4.

2.8 The Fundamental Theorem of Algebra

Consider the polynomial $f(x) = x^2 + 4$ in $\mathbb{C}[x]$ where $\mathbb{C}$ is the field of complex numbers. The polynomial x^2+4 has no real roots but, because $(2i)^2 = 4i^2 = 4(-1) = -4$ and $(-2i)^2 = (-2)^2 i^2 = (4)(-1) = -4$, $2i$ and $-2i$ are roots of x^2+4. And they must be the only roots because $\mathbb{C}$ is a field. Thus we have the factorization $x^2+4 = (x-2i)(x+2i)$. The Fundamental Theorem of Algebra states that not only do polynomials of the form x^2+a have complex roots, but every polynomial in $\mathbb{C}[x]$ which, since $\mathbb{R} \subset \mathbb{C}$, includes every polynomial in $\mathbb{R}[x]$, has complex roots.

Theorem 2.8.1. The Fundamental Theorem of Algebra (FTA)[2]
Let $f(x) \in \mathbb{C}[x]$ have degree $n > 0$. Then $f(x)$ has a root $\alpha \in \mathbb{C}$.

Although the proof of this theorem is too difficult for us here, we will state and prove the following corollary which is equivalent to the FTA.

Corollary 2.8.2. *Every polynomial $f(x) \in \mathbb{C}[x]$ with degree $n > 0$ factors over $\mathbb{C}$ into linear factors, that is, there exist $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{C}$ and $a \in \mathbb{C}$ such that $f(x) = a(x-\alpha_1)(x-\alpha_2) \times ... \times (x-\alpha_n)$.*

Proof. (by induction on n) If $n = 1$ then $f(x) = ax + b$ for some non-zero $a \in \mathbb{C}$ and $b \in \mathbb{C}$. Since $\mathbb{C}$ is a field, a^{-1} exists and $\alpha = -ba^{-1}$ is a root of $f(x)$ and we have $f(x) = a(x - \alpha)$ as required.

If $n > 1$ then the FTA says $\exists \alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. Thus $(x - \alpha)|f(x)$ so $f(x) = g(x)(x - \alpha)$ for some polynomial $g(x) \in \mathbb{C}[x]$ with degree $n - 1$. By induction on n,

$$g(x) = a(x - \alpha_1)(x - \alpha_2) \times ... \times (x - \alpha_{n-1})$$

for some a and $\alpha_i \in \mathbb{C}$ and hence we have factored $f(x)$ into the required form. □

The FTA tells us that every polynomial in $f(x) \in \mathbb{R}[x]$ of degree $n > 0$ has n complex roots. How can we calculate them? For $a > 0$ the roots of $x^2 + a$ are $\pm\sqrt{a}i$ because $(\pm\sqrt{a}i)^2 = ai^2 = -a$. It turns out that for polynomials of the form $x^n - z$ where $z \in \mathbb{C}$ there is also a formula for the roots but beyond this, the problem of computing the complex roots of a polynomials is not simple.

Theorem 2.8.3. *Let $z \in \mathbb{C}$ and $z = r(\cos\theta + i\sin\theta)$. The n complex roots of $x^n - z$ are*

$$r^{\frac{1}{n}}\left[\cos\frac{\theta + 2j\pi}{n} + i\sin\frac{\theta + 2j\pi}{n}\right] \quad \text{for } j = 0, 1, 2, ..., n-1.$$

Proof. Letting $A = \frac{\theta+2j\pi}{n}$

$$\begin{aligned}
[r^{\frac{1}{n}}(\cos A + i\sin A))^n &= r(\cos nA + i\sin nA) \quad \text{(by De Moivre)} \\
&= r[\cos(\theta + 2\pi j) + i\sin(\theta + 2\pi j)] \\
&= r[\cos\theta + i\sin\theta] \\
&= z.
\end{aligned}$$

□

[2]The FTA was first proven by Carl Friederich Gauss in his Ph.D. thesis in 1799. Gauss (1777−1855) is considered one of the greatest mathematicians of all time. He made major contributions to algebra and many other areas of mathematics. The Gaussian integers $\mathbb{Z}[i]$ are named in honor of him.

Example 2.8.4. *Find the complex roots of $x^3 - 8$ and hence solve the equation $x^3 = 8$. We can see that 2 is one root of $x^3 - 8$. In polar co-ordinates $8 = 8(\cos 0 + i \sin 0)$ hence $r = 8$ and $\theta = 0$. Thus $r^{1/3} = 2$ and the roots are*

$$2[\cos 0 + i \sin 0/3], \quad 2[\cos 2\pi/3 + i \sin 2\pi/3], \quad 2[\cos 4\pi/3 + i \sin 4\pi/3]$$

which simplify to $2, -1 + \sqrt{3}i, -1 - \sqrt{3}i$.

Definition 2.8.5. *Let $z = a + bi \in \mathbb{C}$. The* complex conjugate *of z is $\bar{z} = a - bi$.*

Notice that $\bar{z}$ is the reflection of z about the real axis in the complex plane and thus $\bar{\bar{z}} = z$ and if $z = a + 0i$ then $\bar{z} = z$.

Lemma 2.8.6. *The mapping $\varphi : \mathbb{C} \to \mathbb{C}$ given by $\varphi = \bar{z}$ is an isomorphism of $\mathbb{C}$ onto itself.*

Proof. We need to prove the following three properties of φ.

(i) (φ is bijective)
This follows because φ reflects the complex plane about the real axis. Alternatively we have $\varphi(\varphi(z)) = \varphi(\bar{z}) = \bar{\bar{z}} = z$ which means $\varphi^{-1} = \varphi$ and hence φ is bijective.

(ii) ($\varphi(x + y) = \varphi(x) + \varphi(y)$). We have
$\varphi((a + bi) + (c + di)) = \varphi((a + c) + (b + d)i) = (a + c) - (b + d)i$ and
$\varphi(a + bi) + \varphi(c + di) = (a - bi) + (c - di) = (a + c) - (b + d)i$.

(iii) ($\varphi(x \times y) = \varphi(x) \times \varphi(y)$). We have
$\varphi((a + bi)(c + di)) = \varphi((ac - bd) + (ad + bc)i) = (ac - bd) - (ad + bc)i$
and $\varphi(a + bi) \times \varphi(c + di) = (a - bi)(c - di) = (ac - bd) - (ad + bc)i$.

□

An important result about the complex roots of a polynomial $f(x) \in \mathbb{R}[x]$ is that if z is a root then $\bar{z}$ is also a root, that is, the non-real roots of a polynomial with real coefficients come in pairs called conjugates. Observe that two complex roots in example 2.8.4 are $-1 \pm \sqrt{3}i$. This observation is stated in Theorem below. The proof is a beautiful application of the isomorphism $\varphi(z) = \bar{z}$.

Theorem 2.8.7. *Let $f(x) \in \mathbb{R}[x]$ and $z = a + bi \in \mathbb{C}$ be non-real, that is, $b \neq 0$.*
Then $f(z) = 0 \Longrightarrow f(\bar{z}) = 0$.

Proof. Let $f(x) = a_0 + a_1 x + ... + a_n x^n$ for $n > 0$ and $a_i \in \mathbb{R}$. Let $\varphi(z) = \bar{z}$. Applying isomorphism properties (ii) and (iii) we have

$$\begin{aligned}
\varphi(f(z)) &= \varphi(a_0 + a_1 z + ... + a_n z^n) \\
&= \varphi(a_0) + \varphi(a_1 + ... + a_n z^n) \\
&= \varphi(a_0) + \varphi(a_1 z) + ... + \varphi(a_n z^n) \\
&= \varphi(a_0) + \varphi(a_1)\varphi(z) + ... + \varphi(a_n)\varphi(z^n) \\
&= \varphi(a_0) + \varphi(a_1)\varphi(z) + ... + \varphi(a_n)\varphi(z)^n \\
&= a_0 + a_1 \bar{z} + ... + a_n \bar{z}^n \\
&= f(\bar{z}).
\end{aligned}$$

But $f(z) = 0$ hence $\varphi(f(z)) = \varphi(0) = 0$. Thus $f(\bar{z}) = 0$. □

A consequence of Theorem 2.8.7 is that if $f(x)$ is a polynomial of odd degree with real coefficients, it must have at least one real root. In particular

Corollary 2.8.8. *If $f(x) \in \mathbb{R}[x]$ has degree 3 then $f(x)$ has either 3 real roots or one real root and two complex roots.*

Exercises 2.8

1. Show that for all $y \in \mathbb{C}$, $|y|^2 = y\bar{y}$ and that for $x, y \in \mathbb{C}$ with $y \neq 0$, $x/y = (x\bar{y}) / |y|^2$.

2. Find the complex roots of $x^3 + 8$ first by using the formula in Theorem 2.8.3. Since -2 is one root, if you divide $x^3 + 8$ by the known factor $x + 2$ you will get a quadratic quotient $x^2 + bx + c$. Use the quadratic formula to find the other roots.

3. Find the roots of $x^3 - 1$ over $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

4. Find the roots of $x^3 - 1$ over $\mathbb{Z}_3$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

5. Calculate the real and complex eigenvalues of the matrix $A = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

6. Find the roots of $x^4 + 4$. You should get four complex numbers of the form $a \pm bi$ and $c \pm di$. Multiply out the polynomials $(x - a - bi)(x - a + bi)$ and $(x - c - di)(x - c + di)$ and hence find two real factors of $x^4 + 4$.

7. Using any method, find the two quadratic factors of $x^4 - 4\,x^2 - 8\,x - 4$ which are irreducible over $\mathbb{Q}$ and then, using the quadratic formula, find all four roots.

8. Using the `solve` and `fsolve` commands in Maple (`Solve` and `NSolve` in Mathematica), find formulae and numerical approximations for the roots of $x^4 - 4\,x^2 - 8\,x - 4$.

9. If $f(x)$ is a function of x, Newton's method finds a root z of $f(x)$ by starting with an initial approximation z_0 for z and computing the sequence $z_1, z_2, z_3 ...$ using

$$z_{k+1} = z_k - \frac{f(z_k)}{f'(z_k)}$$

and stopping when the sequence converges. Newton's method also works in $\mathbb{C}$. Try it for $f(x) = x^4 - 4\,x^2 - 8\,x - 4$ using $z_0 = -1.5 - i$ and $z_0 = 0.5 + i$.

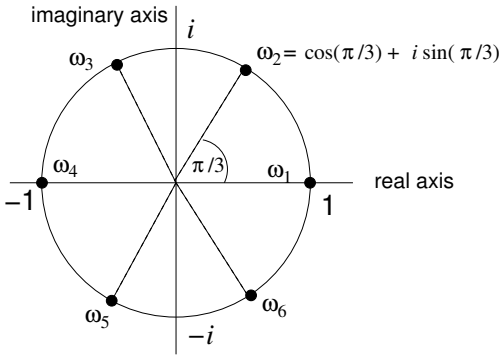

Figure 3: Sixth roots of unity.

2.9 Roots of Unity

Let $n \in \mathbb{N}$. The n'th roots of unity are the n complex roots of the polynomial $x^n - 1$. For example, factoring $x^6 - 1 = (x^3-1)(x^3+1) = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$, and using the quadratic formula, we find that the sixth roots of unity are $1, -1, \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ and $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Figure 2.9 shows that the roots are equally spaced around the unity circle.

Lemma 2.9.1. *The n complex roots ω_j of $x^n - 1$ are given by*

$$\omega_j = \cos\frac{2j\pi}{n} + i\sin\frac{2j\pi}{n} \quad \text{for} \quad j = 1, 2, ..., n.$$

Moreover, $|\omega_j| = 1$ and $\omega_j = \omega_1^j$.

Proof. Applying De Moivre's formula,

$$\omega_j^n = \left(\cos\frac{2j\pi}{n} + i\sin\frac{2j\pi}{n}\right)^n = \cos(2j\pi) + i\sin(2j\pi) = 1.$$

Now let $\theta = \frac{2j\pi}{n}$. We have $|\omega_j| = |\cos\theta + i\sin(\theta)| = \sqrt{\cos^2\theta + \sin^2\theta} = 1$. For the last part, again De Moivre's formula gives

$$\omega_1^j = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^j = \cos\frac{2j\pi}{n} + i\sin\frac{2j\pi}{n} = \omega_j.$$

□

Definition 2.9.2. *The roots of $x^n - 1$ in $\mathbb{C}$ which are not also roots of $x^m - 1$ for some $1 \leq m \leq n$ are called the* primitive n'th complex roots of unity*.*

Example 2.9.3. *We have $x^6-1 = (x-1)(x^5+x^4+x^3+x^2+x+1)$, $x^6-1 = (x^2-1)(x^4+x^2+1)$ and $x^6 - 1 = (x^3-1)(x^3+1)$. The roots of $x-1, x^2-1, x^3-1$ are $1, -1, -\frac{1/2}{\pm}\frac{\sqrt{3}}{2}i$. Thus the remaining two roots of $x^6 - 1$, namely, $\omega_1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\omega_5 = \frac{1}{2} - \frac{\sqrt{3}}{2}i$ are the primitive 6'th complex roots of unity.*

In the example there were two primitive sixth complex roots of unity. Letting $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. The following lemma tells us which of $\omega, \omega^2, \omega^3, \cdots, \omega^6 = 1$ are primitive.

Lemma 2.9.4. *Let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Then ω^j is primitive $\Leftrightarrow$ gcd(j, n) = 1. It follows that the number of primitive complex n'th roots of unity is $\phi(n)$.*

Proof. We will prove that ω^j is not primitive $\Leftrightarrow \gcd(j,n) \neq 1$.

($\Rightarrow$) Suppose ω^j is not primitive. Then $(\omega^j)^d = 1$ for some $0 < d < n \implies \omega^{jd} = 1$. Dividing jd by n we have $jd = qn + r$ for some $0 \leq r < n$. Thus

$$1 = \omega^{jd} = \omega^{qn+r} = \omega^{qn} \cdot \omega^r = (\omega^n)^q \cdot \omega^r = 1^q\omega^r.$$

We have $\omega^r = 1$ and $0 \leq r < n$. Since ω is primitive r must be 0. Hence $n|jd$. But $0 < d < n$ hence $\gcd(n, j) > 1$.

($\Leftarrow$) Suppose $g = \gcd(j, n) > 1$. Then $n = qg$ and $j = pg$ for some $1 \leq q, p < n$. Consider $(\omega^j)^q = \omega^{jq}$. We have

$$\omega^{jq} = \omega^{p(gq)} = \omega^{pn} = (\omega^n)^p = 1.$$

So ω^j is a q'th root of unity with $0 \leq q < n$ hence ω^j is not primitive. □

The following figures shows the primitive third roots of unity and the 4'th roots of unity.

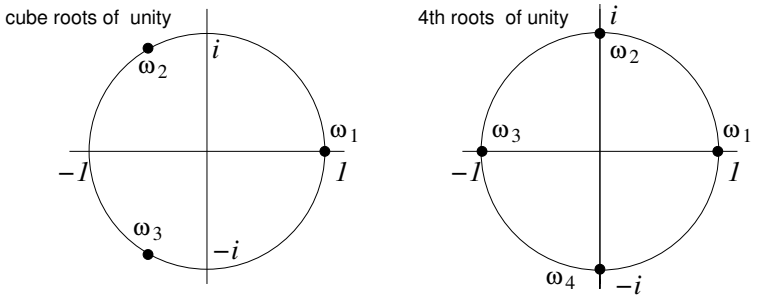

Figure 4: Third and fourth roots of unity.

The following lemma collects some facts about the roots of unity. For example the sum of the 4th roots of unity, $1, -1, i, -i$ is 0 and their product is -1.

Lemma 2.9.5. *Let ω be a primitive n'th root of unity. Then*

(i) If $S = \{\omega, \omega^2, \ldots, \omega^n = 1\}$ then $|S| = n$.

(ii) If n is even then $\omega^{n/2} = 1$ and $\omega^{j+n/2} = -\omega^j$.

(iii) If n is even then $\sum_{i=1}^{n} = 0$ and $\Pi_{i=1}^{n}\omega^j = -1$.

(iv) If n is odd then $\sum_{i=1}^{n} = 0$ and $\Pi_{i=1}^{n} = 1$.

Proof. We leave the proof of (ii) and (iv) as exercises.

(i) Suppose $\omega^j = \omega^k$ with $1 \leq j < k \leq n$. Then $\omega^k/\omega^j = 1 \implies \omega^{k-j} = 1$. But $0 < k - j < n \implies \omega$ is not primitive, a contradiction. Thus the powers of ω in S are distinct.

(iii) The sum $\sum_{j=1}^{n} \omega^j = 0$ follows from (iii). For the product notice that we can pair up the powers $\omega^1, \omega^2, ..., \omega^{n-1}, \omega^n$ so that

$$\Pi_{j=1}^{n} = (\omega^1\omega^n)(\omega^2\omega^{n-1}) \times ... \times (\omega^{n/2}\omega^{n/2+1}).$$

Thus $\Pi_{j=1}^{n}\omega^j = (\omega^{n+1})^{n/2} = (\omega^n)^{n/2} \cdot \omega^{n/2} = -1$ by (iii).

□

Definition 2.9.6. *The n'th cyclotomic polynomial*

$$\Phi_n(x) = \prod_{\substack{1 \leq j \leq n \\ \gcd(j,n)=1}} (x - \omega^j).$$

Example 2.9.7. *For $n = 4$, $\omega = i$ is a primitive 4'th root of unity since $i^1, i^2, i^3 = i, -1, -i$ are not 1. Since $\gcd(j, n) = 1$ for $j = 1, 3$, we have $\Phi_2(x) = (x - i)(x - (-i)) = x^2 + 1$.*

The first few cyclotomic polynomials are given in Table 2.9 below.

n	$\Phi_n(x)$	n	$\Phi_n(x)$
1	$x - 1$	6	$x^2 - x + 1$
2	$x + 1$	7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
3	$x^2 + x + 1$	8	$x^4 + 1$
4	$x^2 + 1$	9	$x^6 + x^3 + 1$
5	$x^4 + x^3 + x^2 + x + 1$	10	$x^4 - x^3 + x^2 - x + 1$

Table 1: Cyclotomic polynomials of orders 1 through 10.

Let n be a primitive n'th root of unity. One way to compute $\Phi_n(x)$ is to remove the factor $x - \omega^j$ with $\gcd(j, n) > 1$ by computing $g = \gcd(x^n - 1, x^j - 1)$ and dividing $x^n - 1$ by g. To remove all non-primitive factors we can use the following.

Lemma 2.9.8. *Let $\text{lcm}(f, g, h)$ denote the least common multiple of $f, g, h \in \mathbb{Q}[x]$. Then*

$$\Phi_n(x) = \frac{x^n - 1}{\text{lcm}(\gcd(x^n - 1, x^j - 1) \text{ for } 1 \leq j \leq n \text{ with } \gcd(j, n) > 1)}.$$

Thus to compute $\Phi_6(x)$, we need to remove $x - 1, x^2 - 1, x^3 - 1$. We divide $x^6 - 1$ by $\text{lcm}(x - 1, x^2 - 1, x^3 - 1) = x^4 + x^3 - x - 1$ to obtain $\Phi_6(x) = x^2 - x + 1$. Note, this is not the only way to compute $\Phi_n(x)$. It follows from the above that the coefficients of $\Phi_n(x)$ must be rational numbers. What is not obvious is that the coefficients are integers and $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. We will study the cyclotomic polynomials further in the exercises. They appear in many applications in science and engineering.

Exercises 2.9

1. Sketch the 8'th roots of unity in the complex plane and circle the primitive ones. Give formulae for the 8'th complex roots of unity.

2. Sketch the 12'th roots of unity in the complex plane and circle the primitive ones. The primitive 12'th roots of unity are roots of a factor of $x^{12} - 1$. Which factor?

3. Let p be a prime. How many primitive p'th roots of unity are there?

4. Let n be odd and let ω be a primitive n'th root of unity.
   Prove that $\sum_{j=1}^{n} \omega^j = 0$ and $\Pi_{j=1}^{n} \omega^j = 1$.

5. Consider $\mathbb{Z}_{13}$ the field of integers modulo 13. Find the roots of $x^6 - 1$ in $\mathbb{Z}_{13}$. Identify which roots are primitive. Which properties of $(i) - (v)$ in Lemma 2.9.5 hold?

6. Find $\Phi_{12}(x)$ the 12'th cyclotomic polynomial.

7. Develop an algorithm for computing the cyclotomic polynomials $\Phi_n(x)$. Using your algorithm compute $\Phi_n(x)$ for $1 < n < 31$. What do you observe for the cases n is prime and n is even?

8. Notice that the coefficients of the cyclotomic polynomials in Table 2.9 are all ± 1. This is not true for all n. Using your algorithm from exercise 7, find the first n for which $\Phi_n(x)$ has a coefficient greater than 1 in magnitude. Note, the answer is greater than 100 so you will need a computer to do this.