A. Complex Numbers

The fact that the square of every real number is nonnegative shows that the equation $x^2+1=0$ has no real root; in other words, there is no real number u such that $u^2=-1$. So the set of real numbers is inadequate for finding all roots of all polynomials. This kind of problem arises with other number systems as well. The set of integers contains no solution of the equation $3x+2=0$, and the rational numbers had to be invented to solve such equations. But the set of rational numbers is also incomplete because, for example, it contains no root of the polynomial x^2-2. Hence the real numbers were invented. In the same way, the set of complex numbers was invented, which contains all real numbers together with a root of the equation $x^2+1=0$. However, the process ends here: the complex numbers have the property that *every* polynomial with complex coefficients has a (complex) root. This fact is known as the fundamental theorem of algebra.

One pleasant aspect of the complex numbers is that, whereas describing the real numbers in terms of the rationals is a rather complicated business, the complex numbers are quite easy to describe in terms of real numbers. Every **complex number** has the form

$$a+bi$$

where a and b are real numbers, and i is a root of the polynomial x^2+1. Here a and b are called the **real part** and the **imaginary part** of the complex number, respectively. The real numbers are now regarded as special complex numbers of the form $a+0i=a$, with zero imaginary part. The complex numbers of the form $0+bi=bi$ with zero real part are called **pure imaginary** numbers. The complex number i itself is called the **imaginary unit** and is distinguished by the fact that

$$i^2=-1$$

As the terms *complex* and *imaginary* suggest, these numbers met with some resistance when they were first used. This has changed; now they are essential in science and engineering as well as mathematics, and they are used extensively. The names persist, however, and continue to be a bit misleading: These numbers are no more "*complex*" than the real numbers, and the number i is no more "*imaginary*" than -1.

Much as for polynomials, two complex numbers are declared to be **equal** if and only if they have the same real parts and the same imaginary parts. In symbols,

$$a+bi=a'+b'i \quad \text{if and only if } a=a' \text{ and } b=b'$$

The addition and subtraction of complex numbers is accomplished by adding and subtracting real and imaginary parts:

$$\begin{aligned}(a+bi)+(a'+b'i)&=(a+a')+(b+b')i\\(a+bi)-(a'+b'i)&=(a-a')+(b-b')i\end{aligned}$$

This is analogous to these operations for linear polynomials $a+bx$ and $a'+b'x$, and the multiplication of complex numbers is also analogous with one difference: $i^2=-1$. The definition is

$$(a+bi)(a'+b'i)=(aa'-bb')+(ab'+ba')i$$

With these definitions of equality, addition, and multiplication, the complex numbers *satisfy all the basic arithmetical axioms adhered to by the real numbers* (the verifications are omitted). One consequence of this is that they can be manipulated in the obvious fashion, except that i^2 is replaced by -1 wherever it occurs, and the rule for equality must be observed.

Example A.1

If $z = 2-3i$ and $w = -1+i$, write each of the following in the form $a+bi$: $z+w$, $z-w$, zw, $\frac{1}{3}z$, and z^2.

Solution.

$$\begin{aligned}
z+w &= (2-3i)+(-1+i) = (2-1)+(-3+1)i = 1-2i \\
z-w &= (2-3i)-(-1+i) = (2+1)+(-3-1)i = 3-4i \\
zw &= (2-3i)(-1+i) = (-2-3i^2)+(2+3)i = 1+5i \\
\tfrac{1}{3}z &= \tfrac{1}{3}(2-3i) = \tfrac{2}{3}-i \\
z^2 &= (2-3i)(2-3i) = (4+9i^2)+(-6-6)i = -5-12i
\end{aligned}$$

Example A.2

Find all complex numbers z such as that $z^2 = i$.

Solution. Write $z = a+bi$; we must determine a and b. Now $z^2 = (a^2-b^2)+(2ab)i$, so the condition $z^2 = i$ becomes

$$(a^2-b^2)+(2ab)i = 0+i$$

Equating real and imaginary parts, we find that $a^2 = b^2$ and $2ab = 1$. The solution is $a = b = \pm\frac{1}{\sqrt{2}}$, so the complex numbers required are $z = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ and $z = -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$.

As for real numbers, it is possible to divide by every nonzero complex number z. That is, there exists a complex number w such that $wz = 1$. As in the real case, this number w is called the **inverse** of z and is denoted by z^{-1} or $\frac{1}{z}$. Moreover, if $z = a+bi$, the fact that $z \neq 0$ means that $a \neq 0$ or $b \neq 0$. Hence $a^2+b^2 \neq 0$, and an explicit formula for the inverse is

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

In actual calculations, the work is facilitated by two useful notions: the conjugate and the absolute value of a complex number. The next example illustrates the technique.

Example A.3

Write $\frac{3+2i}{2+5i}$ in the form $a+bi$.

Solution. Multiply top and bottom by the complex number $2-5i$ (obtained from the denominator by negating the imaginary part). The result is

$$\frac{3+2i}{2+5i} = \frac{(2-5i)(3+2i)}{(2-5i)(2+5i)} = \frac{(6+10)+(4-15)i}{2^2-(5i)^2} = \frac{16}{29} - \frac{11}{29}i$$

Hence the simplified form is $\frac{16}{29} - \frac{11}{29}i$, as required.

The key to this technique is that the product $(2-5i)(2+5i) = 29$ in the denominator turned out to be a *real* number. The situation in general leads to the following notation: If $z = a+bi$ is a complex number, the **conjugate** of z is the complex number, denoted $\overline{z}$, given by

$$\overline{z} = a - bi \quad \text{where } z = a+bi$$

Hence $\overline{z}$ is obtained from z by negating the imaginary part. Thus $\overline{(2+3i)} = 2-3i$ and $\overline{(1-i)} = 1+i$. If we multiply $z = a+bi$ by $\overline{z}$, we obtain

$$z\overline{z} = a^2+b^2 \quad \text{where } z = a+bi$$

The real number a^2+b^2 is always nonnegative, so we can state the following definition: The **absolute value** or **modulus** of a complex number $z = a+bi$, denoted by $|z|$, is the positive square root $\sqrt{a^2+b^2}$; that is,

$$|z| = \sqrt{a^2+b^2} \quad \text{where } z = a+bi$$

For example, $|2-3i| = \sqrt{2^2+(-3)^2} = \sqrt{13}$ and $|1+i| = \sqrt{1^2+1^2} = \sqrt{2}$.

Note that if a real number a is viewed as the complex number $a+0i$, its absolute value (as a complex number) is $|a| = \sqrt{a^2}$, which agrees with its absolute value as a *real* number.

With these notions in hand, we can describe the technique applied in Example A.3 as follows: When converting a quotient $\frac{z}{w}$ of complex numbers to the form $a+bi$, multiply top and bottom by the conjugate $\overline{w}$ of the denominator.

The following list contains the most important properties of conjugates and absolute values. Throughout, z and w denote complex numbers.

$C1.$ $\overline{z \pm w} = \overline{z} \pm \overline{w}$

$C2.$ $\overline{zw} = \overline{z}\,\overline{w}$

$C3.$ $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$

$C4.$ $\overline{(\overline{z})} = z$

$C5.$ z is real if and only if $\overline{z} = z$

$C6.$ $z\overline{z} = |z|^2$

$C7.$ $\frac{1}{z} = \frac{1}{|z|^2}\overline{z}$

$C8.$ $|z| \geq 0$ for all complex numbers z

$C9.$ $|z| = 0$ if and only if $z = 0$

$C10.$ $|zw| = |z||w|$

$C11.$ $|\frac{z}{w}| = \frac{|z|}{|w|}$

$C12.$ $|z+w| \leq |z|+|w|$ (**triangle inequality**)

All these properties (except property C12) can (and should) be verified by the reader for arbitrary complex numbers $z = a+bi$ and $w = c+di$. They are not independent; for example, property C10 follows from properties C2 and C6.

The triangle inequality, as its name suggests, comes from a geometric representation of the complex numbers analogous to identification of the real numbers with the points of a line. The representation is achieved as follows:

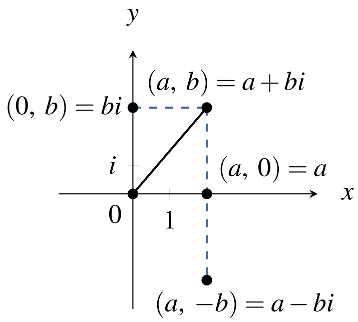


Figure A.1

Introduce a rectangular coordinate system in the plane (Figure A.1), and identify the complex number $a+bi$ with the point $(a,\ b)$. When this is done, the plane is called the **complex plane**. Note that the point $(a,\ 0)$ on the x axis now represents the *real* number $a = a+0i$, and for this reason, the x axis is called the **real axis**. Similarly, the y axis is called the **imaginary axis**. The identification $(a,\ b) = a+bi$ of the geometric point $(a,\ b)$ and the complex number $a+bi$ will be used in what follows without comment. For example, the origin will be referred to as 0.

This representation of the complex numbers in the complex plane gives a useful way of describing the absolute value and conjugate of a complex number $z = a+bi$. The absolute value $|z| = \sqrt{a^2+b^2}$ is just the distance from z to the origin. This makes properties C8 and C9 quite obvious. The conjugate $\overline{z} = a-bi$ of z is just the reflection of z in the real axis (x axis), a fact that makes properties C4 and C5 clear.

Given two complex numbers $z_1 = a_1+b_1i = (a_1,\ b_1)$ and $z_2 = a_2+b_2i = (a_2,\ b_2)$, the absolute value of their difference

$$|z_1-z_2| = \sqrt{(a_1-a_2)^2+(b_1-b_2)^2}$$

is just the distance between them. This gives the **complex distance formula**:

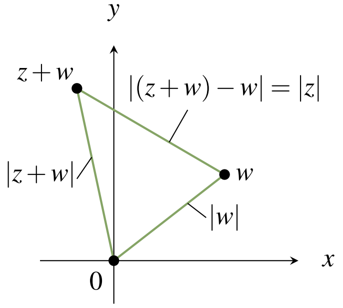


Figure A.2

$$|z_1-z_2| \text{ is the distance between } z_1 \text{ and } z_2$$

This useful fact yields a simple verification of the triangle inequality, property C12. Suppose z and w are given complex numbers. Consider the triangle in Figure A.2 whose vertices are 0, w, and $z+w$. The three sides have lengths $|z|$, $|w|$, and $|z+w|$ by the complex distance formula, so the inequality

$$|z+w| \le |z|+|w|$$

expresses the obvious geometric fact that the sum of the lengths of two sides of a triangle is at least as great as the length of the third side.

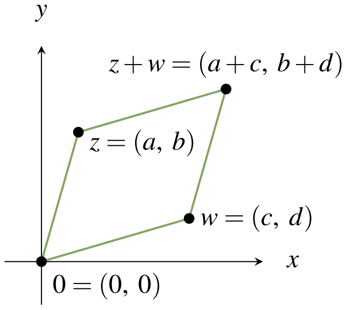


Figure A.3

The representation of complex numbers as points in the complex plane has another very useful property: It enables us to give a geometric description of the sum and product of two complex numbers. To obtain the description for the sum, let

$$z = a+bi = (a,\ b)$$
$$w = c+di = (c,\ d)$$

denote two complex numbers. We claim that the four points 0, z, w, and $z+w$ form the vertices of a parallelogram. In fact, in Figure A.3 the lines from 0 to z and from w to $z+w$ have slopes

$$\frac{b-0}{a-0} = \frac{b}{a} \quad \text{and} \quad \frac{(b+d)-d}{(a+c)-c} = \frac{b}{a}$$

respectively, so these lines are parallel. (If it happens that $a = 0$, then both these lines are vertical.) Similarly, the lines from z to $z+w$ and from 0 to w are also parallel, so the figure with vertices 0, z, w, and $z+w$ is indeed a parallelogram. Hence, the complex number $z+w$ can be obtained geometrically from z and w by *completing* the parallelogram. This is sometimes called the **parallelogram law** of complex addition. Readers who have studied mechanics will recall that velocities and accelerations add in the same way; in fact, these are all special cases of *vector* addition.

Polar Form

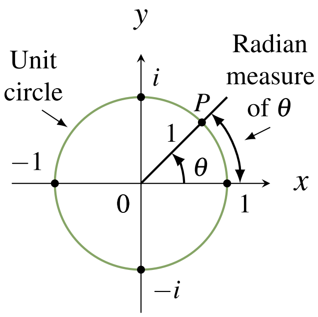


Figure A.4

The geometric description of what happens when two complex numbers are multiplied is at least as elegant as the parallelogram law of addition, but it requires that the complex numbers be represented in polar form. Before discussing this, we pause to recall the general definition of the trigonometric functions sine and cosine. An angle θ in the complex plane is in **standard position** if it is measured counterclockwise from the positive real axis as indicated in Figure A.4. Rather than using degrees to measure angles, it is more natural to use radian measure. This is defined as follows: The circle with its centre at the origin and radius 1 (called the **unit circle**) is drawn in Figure A.4. It has circumference 2π, and the **radian measure** of θ is the length of the arc on the unit circle counterclockwise from 1 to the point P on the unit circle determined by θ. Hence $90^\circ = \frac{\pi}{2}$, $45^\circ = \frac{\pi}{4}$, $180^\circ = \pi$, and a full circle has the angle $360^\circ = 2\pi$. Angles measured clockwise from 1 are negative; for example, $-i$ corresponds to $-\frac{\pi}{2}$ (or to $\frac{3\pi}{2}$).

Consider an angle θ in the range $0 \leq \theta \leq \frac{\pi}{2}$. If θ is plotted in standard position as in Figure A.4, it determines a unique point P on the unit circle, and P has coordinates $(\cos\theta,\ \sin\theta)$ by elementary trigonometry. However, *any* angle θ (acute or not) determines a unique point on the unit circle, so we *define* the **cosine** and **sine** of θ (written $\cos\theta$ and $\sin\theta$) to be the x and y coordinates of this point. For example, the points

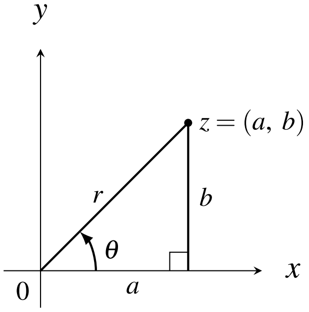
$$1 = (1,\ 0) \quad i = (0,\ 1) \quad -1 = (-1,\ 0) \quad -i = (0,\ -1)$$

plotted in Figure A.4 are determined by the angles 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$, respectively. Hence

$$\begin{array}{llll} \cos 0 = 1 & \cos\frac{\pi}{2} = 0 & \cos\pi = -1 & \cos\frac{3\pi}{2} = 0 \\ \sin 0 = 0 & \sin\frac{\pi}{2} = 1 & \sin\pi = 0 & \sin\frac{3\pi}{2} = -1 \end{array}$$

Now we can describe the polar form of a complex number. Let $z = a+bi$ be a complex number, and write the absolute value of z as

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



If $z \neq 0$, the angle θ shown in Figure A.5 is called an **argument** of z and is denoted

$$\theta = \arg z$$

This angle is not unique ($\theta + 2\pi k$ would do as well for any $k = 0,\ \pm 1,\ \pm 2,\ \dots$). However, there is only one argument θ in the range $-\pi < \theta \leq \pi$, and this is sometimes called the **principal argument** of z.

Returning to Figure A.5, we find that the real and imaginary parts a and b of z are related to r and θ by

$$a = r\cos\theta$$
$$b = r\sin\theta$$

Hence the complex number $z = a + bi$ has the form

$$z = r(\cos\theta + i\sin\theta) \qquad r = |z|,\ \theta = \arg(z)$$

The combination $\cos\theta + i\sin\theta$ is so important that a special notation is used:

$$e^{i\theta} = \cos\theta + i\sin\theta$$

is called **Euler's formula** after the great Swiss mathematician Leonhard Euler (1707–1783). With this notation, z is written

$$z = re^{i\theta} \qquad r = |z|,\ \theta = \arg(z)$$

This is a **polar form** of the complex number z. Of course it is not unique, because the argument can be changed by adding a multiple of 2π.

Example A.4

Write $z_1 = -2 + 2i$ and $z_2 = -i$ in polar form.

Solution.

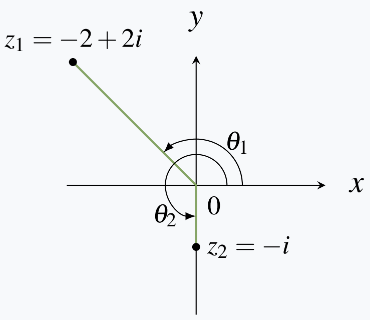


Figure A.6

The two numbers are plotted in the complex plane in Figure A.6. The absolute values are

$$r_1 = |-2 + 2i| = \sqrt{(-2)^2 + 2^2} = 2\sqrt{2}$$
$$r_2 = |-i| = \sqrt{0^2 + (-1)^2} = 1$$

By inspection of Figure A.6, arguments of z_1 and z_2 are

$$\theta_1 = \arg(-2 + 2i) = \tfrac{3\pi}{4}$$
$$\theta_2 = \arg(-i) = \tfrac{3\pi}{2}$$

The corresponding polar forms are $z_1 = -2 + 2i = 2\sqrt{2}e^{3\pi i/4}$ and $z_2 = -i = e^{3\pi i/2}$. Of course, we could have taken the argument $-\frac{\pi}{2}$ for z_2 and obtained the polar form $z_2 = e^{-\pi i/2}$.

In Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$, the number e is the familiar constant $e = 2.71828\dots$ from calculus. The reason for using e will not be given here; the reason why $\cos\theta + i\sin\theta$ is written as an *exponential* function of θ is that the **law of exponents** holds:

$$e^{i\theta} \cdot e^{i\phi} = e^{i(\theta+\phi)}$$

where θ and ϕ are any two angles. In fact, this is an immediate consequence of the addition identities for $\sin(\theta + \phi)$ and $\cos(\theta + \phi)$:

$$\begin{aligned}
e^{i\theta}e^{i\phi} &= (\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi)\\
&= (\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\cos\theta\sin\phi + \sin\theta\cos\phi)\\
&= \cos(\theta+\phi) + i\sin(\theta+\phi)\\
&= e^{i(\theta+\phi)}
\end{aligned}$$

This is analogous to the rule $e^a e^b = e^{a+b}$, which holds for real numbers a and b, so it is not unnatural to use the exponential notation $e^{i\theta}$ for the expression $\cos\theta + i\sin\theta$. In fact, a whole theory exists wherein functions such as e^z, $\sin z$, and $\cos z$ are studied, where z is a *complex* variable. Many deep and beautiful theorems can be proved in this theory, one of which is the so-called fundamental theorem of algebra mentioned later (Theorem A.4). We shall not pursue this here.

The geometric description of the multiplication of two complex numbers follows from the law of exponents.

Theorem A.1: Multiplication Rule

If $z_1 = r_1e^{i\theta_1}$ and $z_2 = r_2e^{i\theta_2}$ are complex numbers in polar form, then

$$z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}$$

In other words, to multiply two complex numbers, simply multiply the absolute values and add the arguments. This simplifies calculations considerably, particularly when we observe that it is valid for *any* arguments θ_1 and θ_2.

Example A.5

Multiply $(1-i)(1+\sqrt{3}i)$ in two ways.

Solution.

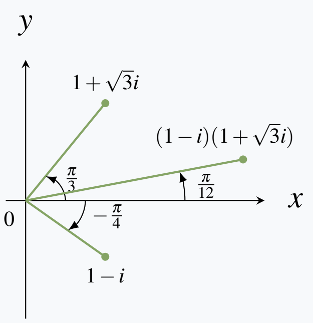


Figure A.7

We have $|1-i| = \sqrt{2}$ and $|1+\sqrt{3}i| = 2$ so, from Figure A.7,

$$\begin{aligned}
1-i &= \sqrt{2}e^{-i\pi/4}\\
1+\sqrt{3}i &= 2e^{i\pi/3}
\end{aligned}$$

Hence, by the multiplication rule,

$$\begin{aligned}
(1-i)(1+\sqrt{3}i) &= (\sqrt{2}e^{-i\pi/4})(2e^{i\pi/3})\\
&= 2\sqrt{2}e^{i(-\pi/4+\pi/3)}\\
&= 2\sqrt{2}e^{i\pi/12}
\end{aligned}$$

This gives the required product in polar form. Of course, direct multiplication gives $(1-i)(1+\sqrt{3}i) = (\sqrt{3}+1)+(\sqrt{3}-1)i$. Hence, equating real and imaginary parts gives the formulas $\cos(\frac{\pi}{12}) = \frac{\sqrt{3}+1}{2\sqrt{2}}$ and $\sin(\frac{\pi}{12}) = \frac{\sqrt{3}-1}{2\sqrt{2}}$.

Roots of Unity

If a complex number $z = re^{i\theta}$ is given in polar form, the powers assume a particularly simple form. In fact, $z^2 = (re^{i\theta})(re^{i\theta}) = r^2e^{2i\theta}$, $z^3 = z^2 \cdot z = (r^2e^{2i\theta})(re^{i\theta}) = r^3e^{3i\theta}$, and so on. Continuing in this way, it follows by induction that the following theorem holds for any positive integer n. The name honours Abraham De Moivre (1667–1754).

Theorem A.2: De Moivre's Theorem

If θ is any angle, then $(e^{i\theta})^n = e^{in\theta}$ holds for all integers n.

Proof. The case $n > 0$ has been discussed, and the reader can verify the result for $n = 0$. To derive it for $n < 0$, first observe that

$$\text{if} \quad z = re^{i\theta} \neq 0 \quad \text{then} \quad z^{-1} = \tfrac{1}{r}\, e^{-i\theta}$$

In fact, $(re^{i\theta})(\frac{1}{r}e^{-i\theta}) = 1e^{i0} = 1$ by the multiplication rule. Now assume that n is negative and write it as $n = -m$, $m > 0$. Then

$$(re^{i\theta})^n = [(re^{i\theta})^{-1}]^m = (\tfrac{1}{r}\, e^{-i\theta})^m = r^{-m}e^{i(-m\theta)} = r^ne^{in\theta}$$

If $r = 1$, this is De Moivre's theorem for negative n. □

Example A.6

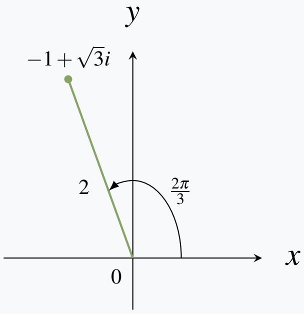


Figure A.8

Verify that $(-1+\sqrt{3}i)^3 = 8$.

Solution. We have $|-1+\sqrt{3}i| = 2$, so $-1+\sqrt{3}i = 2e^{2\pi i/3}$ (see Figure A.8). Hence De Moivre's theorem gives

$$(-1+\sqrt{3}i)^3 = (2e^{2\pi i/3})^3 = 8e^{3(2\pi i/3)} = 8e^{2\pi i} = 8$$

De Moivre's theorem can be used to find nth roots of complex numbers where n is positive. The next example illustrates this technique.

Example A.7

Find the cube roots of unity; that is, find all complex numbers z such that $z^3 = 1$.

Solution. First write $z = re^{i\theta}$ and $1 = 1e^{i0}$ in polar form. We must use the condition $z^3 = 1$ to determine r and θ. Because $z^3 = r^3e^{3i\theta}$ by De Moivre's theorem, this requirement becomes

$$r^3e^{3i\theta} = 1e^{0i}$$

These two complex numbers are equal, so their absolute values must be equal and the arguments must either be equal or differ by an integral multiple of 2π:

$$\begin{aligned} r^3 &= 1 \\ 3\theta &= 0 + 2k\pi, \quad k \text{ some integer} \end{aligned}$$

Because r is real and positive, the condition $r^3 = 1$ implies that $r = 1$. However,

$$\theta = \tfrac{2k\pi}{3}, \quad k \text{ some integer}$$

seems at first glance to yield infinitely many different angles for z. However, choosing $k = 0,\ 1,\ 2$ gives three possible arguments θ (where $0 \leq \theta < 2\pi$), and the corresponding roots are

$$\begin{aligned} 1e^{0i} &= 1 \\ 1e^{2\pi i/3} &= -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i \\ 1e^{4\pi i/3} &= -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i \end{aligned}$$

These are displayed in Figure A.9. All other values of k yield values of θ that differ from one of these by a multiple of 2π—and so do not give new roots. Hence we have found all the roots.

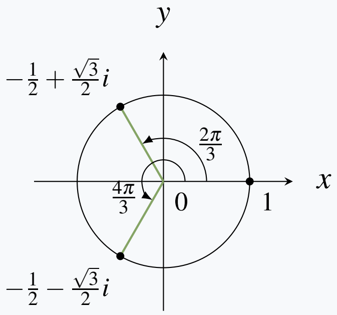

y
$-\frac{1}{2} + \frac{\sqrt{3}}{2}i$
$\frac{2\pi}{3}$
$\frac{4\pi}{3}$
0
1
x
$-\frac{1}{2} - \frac{\sqrt{3}}{2}i$

Figure A.9

The same type of calculation gives all complex n**th roots of unity**; that is, all complex numbers z such that $z^n = 1$. As before, write $1 = 1e^{0i}$ and

$$z = re^{i\theta}$$

in polar form. Then $z^n = 1$ takes the form

$$r^n e^{ni\theta} = 1e^{0i}$$

using De Moivre's theorem. Comparing absolute values and arguments yields

$$\begin{aligned} r^n &= 1 \\ n\theta &= 0 + 2k\pi, \quad k \text{ some integer} \end{aligned}$$

Hence $r = 1$, and the n values

$$\theta = \tfrac{2k\pi}{n}, \quad k = 0,\ 1,\ 2,\ \ldots,\ n-1$$

of θ all lie in the range $0 \leq \theta < 2\pi$. As in Example A.7, *every* choice of k yields a value of θ that differs from one of these by a multiple of 2π, so these give the arguments of *all* the possible roots.

Theorem A.3: nth Roots of Unity

If $n \geq 1$ is an integer, the nth roots of unity (that is, the solutions to $z^n = 1$) are given by

$$z = e^{2\pi ki/n}, \quad k = 0,\ 1,\ 2,\ \ldots,\ n-1$$

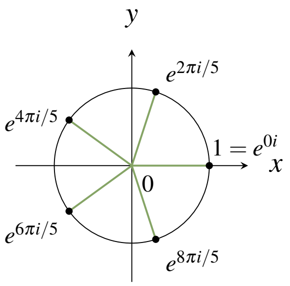


Figure A.10

The nth roots of unity can be found geometrically as the points on the unit circle that cut the circle into n equal sectors, starting at 1. The case $n = 5$ is shown in Figure A.10, where the five fifth roots of unity are plotted.

The method just used to find the nth roots of unity works equally well to find the nth roots of any complex number in polar form. We give one example.

Example A.8

Find the fourth roots of $\sqrt{2} + \sqrt{2}i$.

Solution. First write $\sqrt{2} + \sqrt{2}i = 2e^{\pi i/4}$ in polar form. If $z = re^{i\theta}$ satisfies $z^4 = \sqrt{2} + \sqrt{2}i$, then De Moivre's theorem gives

$$r^4 e^{i(4\theta)} = 2e^{\pi i/4}$$

Hence $r^4 = 2$ and $4\theta = \frac{\pi}{4} + 2k\pi$, k an integer. We obtain four distinct roots (and hence all) by

$$r = \sqrt[4]{2}, \qquad \theta = \frac{\pi}{16} = \frac{2k\pi}{16},\ k = 0,\ 1,\ 2,\ 3$$

Thus the four roots are

$$\sqrt[4]{2}e^{\pi i/16} \qquad \sqrt[4]{2}e^{9\pi i/16} \qquad \sqrt[4]{2}e^{17\pi i/16} \qquad \sqrt[4]{2}e^{25\pi i/16}$$

Of course, reducing these roots to the form $a + bi$ would require the computation of $\sqrt[4]{2}$ and the sine and cosine of the various angles.

An expression of the form $ax^2 + bx + c$, where the coefficients $a \neq 0$, b, and c are real numbers, is called a **real quadratic**. A complex number u is called a **root** of the quadratic if $au^2 + bu + c = 0$. The roots are given by the famous **quadratic formula**:

$$u = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The quantity $d = b^2 - 4ac$ is called the **discriminant** of the quadratic $ax^2 + bx + c$, and there is no real root if and only if $d < 0$. In this case the quadratic is said to be **irreducible**. Moreover, the fact that $d < 0$ means that $\sqrt{d} = i\sqrt{|d|}$, so the two (complex) roots are conjugates of each other:

$$u = \frac{1}{2a}(-b + i\sqrt{|d|}) \quad \text{and} \quad \overline{u} = \frac{1}{2a}(-b - i\sqrt{|d|})$$

The converse of this is true too: Given any nonreal complex number u, then u and $\overline{u}$ are the roots of some real irreducible quadratic. Indeed, the quadratic

$$x^2 - (u + \overline{u})x + u\overline{u} = (x - u)(x - \overline{u})$$

has real coefficients ($u\overline{u} = |u|^2$ and $u + \overline{u}$ is twice the real part of u) and so is irreducible because its roots u and $\overline{u}$ are not real.

Example A.9

Find a real irreducible quadratic with $u = 3 - 4i$ as a root.

Solution. We have $u + \overline{u} = 6$ and $|u|^2 = 25$, so $x^2 - 6x + 25$ is irreducible with u and $\overline{u} = 3 + 4i$ as roots.

Fundamental Theorem of Algebra

As we mentioned earlier, the complex numbers are the culmination of a long search by mathematicians to find a set of numbers large enough to contain a root of every polynomial. The fact that the complex numbers have this property was first proved by Gauss in 1797 when he was 20 years old. The proof is omitted.

Theorem A.4: Fundamental Theorem of Algebra

Every polynomial of positive degree with complex coefficients has a complex root.

If $f(x)$ is a polynomial with complex coefficients, and if u_1 is a root, then the factor theorem (Section 6.5) asserts that

$$f(x) = (x - u_1)g(x)$$

where $g(x)$ is a polynomial with complex coefficients and with degree one less than the degree of $f(x)$. Suppose that u_2 is a root of $g(x)$, again by the fundamental theorem. Then $g(x) = (x - u_2)h(x)$, so

$$f(x) = (x - u_1)(x - u_2)h(x)$$

This process continues until the last polynomial to appear is linear. Thus $f(x)$ has been expressed as a product of linear factors. The last of these factors can be written in the form $u(x - u_n)$, where u and u_n are complex (verify this), so the fundamental theorem takes the following form.

Theorem A.5

Every complex polynomial $f(x)$ of degree $n \geq 1$ has the form

$$f(x) = u(x - u_1)(x - u_2)\cdots(x - u_n)$$

where u, u_1, $\dots$, u_n are complex numbers and $u \neq 0$. The numbers u_1, u_2, $\dots$, u_n are the roots of $f(x)$ (and need not all be distinct), and u is the coefficient of x^n.

This form of the fundamental theorem, when applied to a polynomial $f(x)$ with *real* coefficients, can be used to deduce the following result.

Theorem A.6

Every polynomial $f(x)$ of positive degree with real coefficients can be factored as a product of linear and irreducible quadratic factors.

In fact, suppose $f(x)$ has the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where the coefficients a_i are real. If u is a complex root of $f(x)$, then we claim first that $\overline{u}$ is also a root. In fact, we have $f(u) = 0$, so

$$\begin{aligned} 0 = \overline{0} = \overline{f(u)} &= \overline{a_n u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0} \\ &= \overline{a_n u^n} + \overline{a_{n-1}u^{n-1}} + \cdots + \overline{a_1 u} + \overline{a_0} \\ &= \overline{a}_n \overline{u}^n + \overline{a}_{n-1}\overline{u}^{n-1} + \cdots + \overline{a}_1 \overline{u} + \overline{a}_0 \\ &= a_n \overline{u}^n + a_{n-1}\overline{u}^{n-1} + \cdots + a_1 \overline{u} + a_0 \\ &= f(\overline{u}) \end{aligned}$$

where $\overline{a}_i = a_i$ for each i because the coefficients a_i are real. Thus if u is a root of $f(x)$, so is its conjugate $\overline{u}$. Of course some of the roots of $f(x)$ may be real (and so equal their conjugates), but the nonreal roots come in pairs, u and $\overline{u}$. By Theorem A.6, we can thus write $f(x)$ as a product:

$$f(x) = a_n(x - r_1)\cdots(x - r_k)(x - u_1)(x - \overline{u}_1)\cdots(x - u_m)(x - \overline{u}_m) \tag{A.1}$$

where a_n is the coefficient of x^n in $f(x)$; $r_1, r_2, \dots, r_k$ are the real roots; and $u_1, \overline{u}_1, u_2, \overline{u}_2, \dots, u_m, \overline{u}_m$ are the nonreal roots. But the product

$$(x - u_j)(x - \overline{u}_j) = x^2 - (u_j + \overline{u}_j)x + (u_j \overline{u}_j)$$

is a real irreducible quadratic for each j (see the discussion preceding Example A.9). Hence (A.1) shows that $f(x)$ is a product of linear and irreducible quadratic factors, each with real coefficients. This is the conclusion in Theorem A.6.

Exercises for A

Exercise A.1 Solve each of the following for the real number x.

a. $x - 4i = (2 - i)^2$

b. $(2 + xi)(3 - 2i) = 12 + 5i$

c. $(2 + xi)^2 = 4$

d. $(2 + xi)(2 - xi) = 5$

Exercise A.2 Convert each of the following to the form $a + bi$.

a. $(2 - 3i) - 2(2 - 3i) + 9$

b. $(3 - 2i)(1 + i) + |3 + 4i|$

c. $\frac{1+i}{2-3i} + \frac{1-i}{-2+3i}$

d. $\frac{3-2i}{1-i} + \frac{3-7i}{2-3i}$

e. i^{131}

f. $(2 - i)^3$

g. $(1+i)^4$

h. $(1-i)^2(2+i)^2$

i. $\frac{3\sqrt{3}-i}{\sqrt{3}+i}+\frac{\sqrt{3}+7i}{\sqrt{3}-i}$

Exercise A.3 In each case, find the complex number z.

a. $iz-(1+i)^2=3-i$

b. $(i+z)-3i(2-z)=iz+1$

c. $z^2=-i$

d. $z^2=3-4i$

e. $z(1+i)=\overline{z}+(3+2i)$

f. $z(2-i)=(\overline{z}+1)(1+i)$

Exercise A.4 In each case, find the roots of the real quadratic equation.

a. $x^2-2x+3=0$

b. $x^2-x+1=0$

c. $3x^2-4x+2=0$

d. $2x^2-5x+2=0$

Exercise A.5 Find all numbers x in each case.

a. $x^3=8$

b. $x^3=-8$

c. $x^4=16$

d. $x^4=64$

Exercise A.6 In each case, find a real quadratic with u as a root, and find the other root.

a. $u=1+i$

b. $u=2-3i$

c. $u=-i$

d. $u=3-4i$

Exercise A.7 Find the roots of $x^2-2\cos\theta x+1=0$, θ any angle.

Exercise A.8 Find a real polynomial of degree 4 with $2-i$ and $3-2i$ as roots.

Exercise A.9 Let re z and im z denote, respectively, the real and imaginary parts of z. Show that:

a. $\text{im}\,(iz)=\text{re}\,z$

b. $\text{re}\,(iz)=-\,\text{im}\,z$

c. $z+\overline{z}=2\,\text{re}\,z$

d. $z-\overline{z}=2i\,\text{im}\,z$

e. $\text{re}\,(z+w)=\text{re}\,z+\text{re}\,w$, and $\text{re}\,(tz)=t\cdot\text{re}\,z$ if t is real

f. $\text{im}\,(z+w)=\text{im}\,z+\text{im}\,w$, and $\text{im}\,(tz)=t\cdot\text{im}\,z$ if t is real

Exercise A.10 In each case, show that u is a root of the quadratic equation, and find the other root.

a. $x^2-3ix+(-3+i)=0$; $u=1+i$

b. $x^2+ix-(4-2i)=0$; $u=-2$

c. $x^2-(3-2i)x+(5-i)=0$; $u=2-3i$

d. $x^2+3(1-i)x-5i=0$; $u=-2+i$

Exercise A.11 Find the roots of each of the following complex quadratic equations.

a. $x^2+2x+(1+i)=0$

b. $x^2-x+(1-i)=0$

c. $x^2-(2-i)x+(3-i)=0$

d. $x^2-3(1-i)x-5i=0$

Exercise A.12 In each case, describe the graph of the equation (where z denotes a complex number).

a. $|z|=1$

b. $|z-1|=2$

c. $z=i\overline{z}$

d. $z=-\overline{z}$

e. $z=|z|$

f. $\text{im}\,z=m\cdot\text{re}\,z$, m a real number

Exercise A.13

a. Verify $|zw|=|z||w|$ directly for $z=a+bi$ and $w=c+di$.

b. Deduce (a) from properties C2 and C6.

Exercise A.14 Prove that $|z+w|=|z|^2+|w|^2+w\overline{z}+\overline{w}z$ for all complex numbers w and z.

Exercise A.15 If zw is real and $z\neq 0$, show that $w=a\overline{z}$ for some real number a.

Exercise A.16 If $zw=\overline{z}v$ and $z\neq 0$, show that $w=uv$ for some u in $\mathbb{C}$ with $|u|=1$.

Exercise A.17 Show that $(1+i)^n+(1-i)^n$ is real for all n, using property C5.

Exercise A.18 Express each of the following in polar form (use the principal argument).

a. $3-3i$

b. $-4i$

c. $-\sqrt{3}+i$

d. $-4+4\sqrt{3}i$

e. $-7i$

f. $-6+6i$

Exercise A.19 Express each of the following in the form $a+bi$.

a. $3e^{\pi i}$ b. $e^{7\pi i/3}$

c. $2e^{3\pi i/4}$ d. $\sqrt{2}e^{-\pi i/4}$

e. $e^{5\pi i/4}$ f. $2\sqrt{3}e^{-2\pi i/6}$

Exercise A.20 Express each of the following in the form $a+bi$.

a. $(-1+\sqrt{3}i)^2$ b. $(1+\sqrt{3}i)^{-4}$

c. $(1+i)^8$ d. $(1-i)^{10}$

e. $(1-i)^6(\sqrt{3}+i)^3$ f. $(\sqrt{3}-i)^9(2-2i)^5$

Exercise A.21 Use De Moivre's theorem to show that:

a. $\cos 2\theta = \cos^2\theta - \sin^2\theta$; $\sin 2\theta = 2\cos\theta\sin\theta$

b. $\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta$;
$\sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta$

Exercise A.22

a. Find the fourth roots of unity.

b. Find the sixth roots of unity.

Exercise A.23 Find all complex numbers z such that:

a. $z^4 = -1$ b. $z^4 = 2(\sqrt{3}i - 1)$

c. $z^3 = -27i$ d. $z^6 = -64$

Exercise A.24 If $z = re^{i\theta}$ in polar form, show that:

a. $\overline{z} = re^{-i\theta}$ b. $z^{-1} = \frac{1}{r}e^{-i\theta}$ if $z \neq 0$

Exercise A.25 Show that the sum of the nth roots of unity is zero.
[*Hint:* $1-z^n = (1-z)(1+z+z^2+\cdots+z^{n-1})$ for any complex number z.]

Exercise A.26

a. Let z_1, z_2, z_3, z_4, and z_5 be equally spaced around the unit circle. Show that $z_1+z_2+z_3+z_4+z_5=0$. [*Hint*: $(1-z)(1+z+z^2+z^3+z^4) = 1-z^5$ for any complex number z.]

b. Repeat (a) for any $n \geq 2$ points equally spaced around the unit circle.

c. If $|w| = 1$, show that the sum of the roots of $z^n = w$ is zero.

Exercise A.27 If z^n is real, $n \geq 1$, show that $(\overline{z})^n$ is real.

Exercise A.28 If $\overline{z}^2 = z^2$, show that z is real or pure imaginary.

Exercise A.29 If a and b are *rational* numbers, let p and q denote numbers of the form $a+b\sqrt{2}$. If $p = a+b\sqrt{2}$, define $\tilde{p} = a-b\sqrt{2}$ and $[p] = a^2-2b^2$. Show that each of the following holds.

a. $a+b\sqrt{2} = a_1+b_1\sqrt{2}$ only if $a = a_1$ and $b = b_1$

b. $\widetilde{p \pm q} = \tilde{p} \pm \tilde{q}$ c. $\widetilde{pq} = \tilde{p}\tilde{q}$

d. $[p] = p\tilde{p}$ e. $[pq] = [p][q]$

f. If $f(x)$ is a polynomial with rational coefficients and $p = a+b\sqrt{2}$ is a root of $f(x)$, then $\tilde{p}$ is also a root of $f(x)$.

B. Proofs

Logic plays a basic role in human affairs. Scientists use logic to draw conclusions from experiments, judges use it to deduce consequences of the law, and mathematicians use it to prove theorems. Logic arises in ordinary speech with assertions such as "If John studies hard, he will pass the course," or "If an integer n is divisible by 6, then n is divisible by 3."[1] In each case, the aim is to assert that if a certain statement is true, then another statement must also be true. In fact, if p and q denote statements, most theorems take the form of an **implication**: "If p is true, then q is true." We write this in symbols as

$$p \Rightarrow q$$

and read it as "p implies q." Here p is the **hypothesis** and q the **conclusion** of the implication. The verification that $p \Rightarrow q$ is valid is called the **proof** of the implication. In this section we examine the most common methods of proof[2] and illustrate each technique with some examples.

Method of Direct Proof

To prove that $p \Rightarrow q$, demonstrate directly that q is true whenever p is true.

Example B.1

If n is an odd integer, show that n^2 is odd.

Solution. If n is odd, it has the form $n = 2k+1$ for some integer k. Then $n^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ also is odd because $2k^2+2k$ is an integer.

Note that the computation $n^2 = 4k^2+4k+1$ in Example B.1 involves some simple properties of arithmetic that we did not prove. These properties, in turn, can be proved from certain more basic properties of numbers (called axioms)—more about that later. Actually, a whole body of mathematical information lies behind nearly every proof of any complexity, although this fact usually is not stated explicitly. Here is a geometrical example.

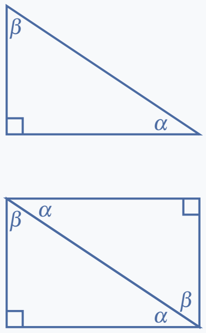
[1] By an *integer* we mean a "whole number"; that is, a number in the set $0, \pm1, \pm2, \pm3, \dots$

[2] For a more detailed look at proof techniques see D. Solow, How to Read and Do Proofs, 2nd ed. (New York: Wiley, 1990); or J. F. Lucas. *Introduction to Abstract Mathematics*, Chapter 2 (Belmont, CA: Wadsworth, 1986).

Example B.2

In a right triangle, show that the sum of the two acute angles is 90 degrees.

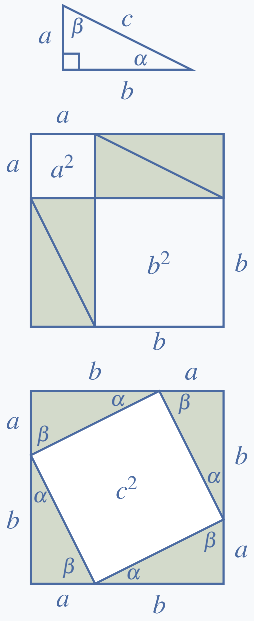
Solution.



The right triangle is shown in the diagram. Construct a rectangle with sides of the same length as the short sides of the original triangle, and draw a diagonal as shown. The original triangle appears on the bottom of the rectangle, and the top triangle is identical to the original (but rotated). Now it is clear that $\alpha+\beta$ is a right angle.

Geometry was one of the first subjects in which formal proofs were used—Euclid's *Elements* was published about 300 B.C. The *Elements* is the most successful textbook ever written, and contains many of the basic geometrical theorems that are taught in school today. In particular, Euclid included a proof of an earlier theorem (about 500 B.C.) due to Pythagoras. Recall that, in a right triangle, the side opposite the right angle is called the *hypotenuse* of the triangle.

Example B.3: Pythagoras' Theorem



In a right-angled triangle, show that the square of the length of the hypotenuse equals the sum of the squares of the lengths of the other two sides.

Solution. Let the sides of the right triangle have lengths a, b, and c as shown. Consider two squares with sides of length $a+b$, and place four copies of the triangle in these squares as in the diagram. The central rectangle in the second square shown is itself a square because the angles α and β add to 90 degrees (using Example B.2), so its area is c^2 as shown. Comparing areas shows that both a^2+b^2 and c^2 each equal the area of the large square minus four times the area of the original triangle, and hence are equal.

Sometimes it is convenient (or even necessary) to break a proof into parts, and deal with each case separately. We formulate the general method as follows:

Method of Reduction to Cases

To prove that $p \Rightarrow q$, show that p implies at least one of a list $p_1, p_2, \dots, p_n$ of statements (the cases) and then show that $p_i \Rightarrow q$ for each i.

Example B.4

Show that $n^2 \geq 0$ for every integer n.

Solution. This statement can be expressed as an implication: If n is an integer, then $n^2 \geq 0$. To prove it, consider the following three cases:

$$(1)\ n > 0; \quad (2)\ n = 0; \quad (3)\ n < 0.$$

Then $n^2 > 0$ in Cases (1) and (3) because the product of two positive (or two negative) integers is positive. In Case (2) $n^2 = 0^2 = 0$, so $n^2 \geq 0$ in every case.

Example B.5

If n is an integer, show that $n^2 - n$ is even.

Solution. We consider two cases:

$$(1)\ n \text{ is even}; \quad (2)\ n \text{ is odd}.$$

We have $n^2 - n = n(n-1)$, so this is even in Case (1) because any multiple of an even number is again even. Similarly, $n - 1$ is even in Case (2) so $n(n-1)$ is again even for the same reason. Hence $n^2 - n$ is even in any case.

The statements used in mathematics are required to be either true or false. This leads to a proof technique which causes consternation in many beginning students. The method is a formal version of a debating strategy whereby the debater assumes the truth of an opponent's position and shows that it leads to an absurd conclusion.

Method of Proof by Contradiction

To prove that $p \Rightarrow q$, show that the assumption that both p is true and q is false leads to a contradiction. In other words, if p is true, then q must be true; that is, $p \Rightarrow q$.

Example B.6

If r is a rational number (fraction), show that $r^2 \neq 2$.

Solution. To argue by contradiction, we assume that r is a rational number and that $r^2 = 2$, and show that this assumption leads to a contradiction. Let m and n be integers such that $r = \frac{m}{n}$ is in lowest terms (so, in particular, m and n are not both even). Then $r^2 = 2$ gives $m^2 = 2n^2$, so m^2 is even. This means m is even (Example B.1), say $m = 2k$. But then $2n^2 = m^2 = 4k^2$, so $n^2 = 2k^2$ is even, and hence n is even. This shows that n and m are both even, contrary to the choice of these numbers.

Example B.7: Pigeonhole Principle

If $n+1$ pigeons are placed in n holes, then some hole contains at least 2 pigeons.

Solution. Assume the conclusion is false. Then each hole contains at most one pigeon and so, since there are n holes, there must be at most n pigeons, contrary to assumption.

The next example involves the notion of a *prime* number, that is an integer that is greater than 1 which cannot be factored as the product of two smaller positive integers both greater than 1. The first few primes are 2, 3, 5, 7, 11, ...

Example B.8

If $2^n - 1$ is a prime number, show that n is a prime number.

Solution. We must show that $p \Rightarrow q$ where p is the statement "$2^n - 1$ is a prime", and q is the statement "n is a prime." Suppose that p is true but q is false so that n is not a prime, say $n = ab$ where $a \geq 2$ and $b \geq 2$ are integers. If we write $2^a = x$, then $2^n = 2^{ab} = (2^a)^b = x^b$. Hence $2^n - 1$ factors:

$$2^n - 1 = x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \cdots + x^2 + x + 1)$$

As $x \geq 4$, this expression is a factorization of $2^n - 1$ into smaller positive integers, contradicting the assumption that $2^n - 1$ is prime.

The next example exhibits one way to show that an implication is *not* valid.

Example B.9

Show that the implication "n is a prime $\Rightarrow 2^n - 1$ is a prime" is false.

Solution. The first four primes are 2, 3, 5, and 7, and the corresponding values for $2^n - 1$ are 3, 7, 31, 127 (when $n = 2, 3, 5, 7$). These are all prime as the reader can verify. This result seems to be evidence that the implication is true. However, the next prime is 11 and $2^{11} - 1 = 2047 = 23 \cdot 89$, which is clearly *not* a prime.

We say that $n = 11$ is a **counterexample** to the (proposed) implication in Example B.9. Note that, if you can find even one example for which an implication is not valid, the implication is false. Thus disproving implications is in a sense easier than proving them.

The implications in Example B.8 and Example B.9 are closely related: They have the form $p \Rightarrow q$ and $q \Rightarrow p$, where p and q are statements. Each is called the **converse** of the other and, as these examples show, an implication can be valid even though its converse is not valid. If *both* $p \Rightarrow q$ and $q \Rightarrow p$ are valid, the statements p and q are called **logically equivalent**. This is written in symbols as

$$p \Leftrightarrow q$$

and is read "p if and only if q". Many of the most satisfying theorems make the assertion that two statements, ostensibly quite different, are in fact logically equivalent.

Example B.10

If n is an integer, show that "n is odd $\Leftrightarrow n^2$ is odd."

Solution. In Example B.1 we proved the implication "n is odd $\Rightarrow n^2$ is odd." Here we prove the converse by contradiction. If n^2 is odd, we assume that n is not odd. Then n is even, say $n = 2k$, so $n^2 = 4k^2$, which is also even, a contradiction.

Many more examples of proofs can be found in this book and, although they are often more complex, most are based on one of these methods. In fact, linear algebra is one of the best topics on which the reader can sharpen his or her skill at constructing proofs. Part of the reason for this is that much of linear algebra is developed using the **axiomatic method**. That is, in the course of studying various examples it is observed that they all have certain properties in common. Then a general, abstract system is studied in which these basic properties are *assumed* to hold (and are called **axioms**). In this system, statements (called **theorems**) are deduced from the axioms using the methods presented in this appendix. These theorems will then be true in *all* the concrete examples, because the axioms hold in each case. But this procedure is more than just an efficient method for finding theorems in the examples. By reducing the proof to its essentials, we gain a better understanding of why the theorem is true and how it relates to analogous theorems in other abstract systems.

The axiomatic method is not new. Euclid first used it in about 300 B.C. to derive all the propositions of (euclidean) geometry from a list of 10 axioms. The method lends itself well to linear algebra. The axioms are simple and easy to understand, and there are only a few of them. For example, the theory of vector spaces contains a large number of theorems derived from only ten simple axioms.

Exercises for B

Exercise B.1 In each case prove the result and either prove the converse or give a counterexample.

a. If n is an even integer, then n^2 is a multiple of 4.

b. If m is an even integer and n is an odd integer, then $m+n$ is odd.

c. If $x = 2$ or $x = 3$, then $x^3 - 6x^2 + 11x - 6 = 0$.

d. If $x^2 - 5x + 6 = 0$, then $x = 2$ or $x = 3$.

Exercise B.2 In each case either prove the result by splitting into cases, or give a counterexample.

a. If n is any integer, then $n^2 = 4k + 1$ for some integer k.

b. If n is any odd integer, then $n^2 = 8k + 1$ for some integer k.

c. If n is any integer, $n^3 - n = 3k$ for some integer k. [*Hint*: Use the fact that each integer has one of the forms $3k$, $3k+1$, or $3k+2$, where k is an integer.]

Exercise B.3 In each case prove the result by contradiction and either prove the converse or give a counterexample.

a. If $n>2$ is a prime integer, then n is odd.

b. If $n+m=25$ where n and m are integers, then one of n and m is greater than 12.

c. If a and b are positive numbers and $a \leq b$, then $\sqrt{a} \leq \sqrt{b}$.

d. If m and n are integers and mn is even, then m is even or n is even.

Exercise B.4 Prove each implication by contradiction.

a. If x and y are positive numbers, then $\sqrt{x+y} \neq \sqrt{x}+\sqrt{y}$.

b. If x is irrational and y is rational, then $x+y$ is irrational.

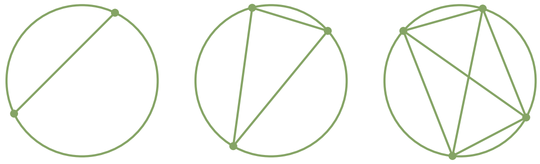
c. If 13 people are selected, at least 2 have birthdays in the same month.

Exercise B.5 Disprove each statement by giving a counterexample.

a. n^2+n+11 is a prime for all positive integers n.

b. $n^3 \geq 2^n$ for all integers $n \geq 2$.

c. If $n \geq 2$ points are arranged on a circle in such a way that no three of the lines joining them have a common point, then these lines divide the circle into 2^{n-1} regions. [The cases $n=2$, 3, and 4 are shown in the diagram.]



$n=2$ $\quad$ $n=3$ $\quad$ $n=4$

Exercise B.6 The number e from calculus has a series expansion

$$e=1+\tfrac{1}{1!}+\tfrac{1}{2!}+\tfrac{1}{3!}+\cdots$$

where $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$ for each integer $n \geq 1$. Prove that e is irrational by contradiction. [*Hint*: If $e=m/n$, consider

$$k=n!\left(e-1-\tfrac{1}{1!}-\tfrac{1}{2!}-\tfrac{1}{3!}-\cdots-\tfrac{1}{n!}\right).$$

Show that k is a positive integer and that

$$k=\tfrac{1}{n+1}+\tfrac{1}{(n+1)(n+2)}+\cdots<\tfrac{1}{n}.]$$

C. Mathematical Induction

Suppose one is presented with the following sequence of equations:

$$\begin{aligned} 1 &= 1 \\ 1+3 &= 4 \\ 1+3+5 &= 9 \\ 1+3+5+7 &= 16 \\ 1+3+5+7+9 &= 25 \end{aligned}$$

It is clear that there is a pattern. The numbers on the right side of the equations are the squares 1^2, 2^2, 3^2, 4^2, and 5^2 and, in the equation with n^2 on the right side, the left side is the sum of the first n odd numbers. The odd numbers are

$$\begin{aligned} 1 &= 2\cdot 1-1 \\ 3 &= 2\cdot 2-1 \\ 5 &= 2\cdot 3-1 \\ 7 &= 2\cdot 4-1 \\ 9 &= 2\cdot 5-1 \end{aligned}$$

and from this it is clear that the nth odd number is $2n-1$. Hence, at least for $n = 1$, 2, 3, 4, or 5, the following is true:

$$1+3+\cdots+(2n-1) = n^2 \tag{S_n}$$

The question arises whether the statement S_n is true for *every* n. There is no hope of separately verifying all these statements because there are infinitely many of them. A more subtle approach is required.

The idea is as follows: Suppose it is verified that the statement S_{n+1} will be true whenever S_n is true. That is, suppose we prove that, *if* S_n is true, then it necessarily follows that S_{n+1} is also true. Then, if we can show that S_1 is true, it follows that S_2 is true, and from this that S_3 is true, hence that S_4 is true, and so on and on. This is the principle of induction. To express it more compactly, it is useful to have a short way to express the assertion "If S_n is true, then S_{n+1} is true." As in Appendix B, we write this assertion as

$$S_n \Rightarrow S_{n+1}$$

and read it as " S_n implies S_{n+1}." We can now state the principle of mathematical induction.

The Principle of Mathematical Induction

Suppose S_n is a statement about the natural number n for each $n = 1, 2, 3, \dots$.
Suppose further that:

1. *S_1 is true.*
2. *$S_n \Rightarrow S_{n+1}$ for every $n \geq 1$.*

Then S_n is true for every $n \geq 1$.

This is one of the most useful techniques in all of mathematics. It applies in a wide variety of situations, as the following examples illustrate.

Example C.1

Show that $1+2+\cdots+n = \frac{1}{2}n(n+1)$ for $n \geq 1$.

Solution. Let S_n be the statement: $1+2+\cdots+n = \frac{1}{2}n(n+1)$ for $n \geq 1$. We apply induction.

1. S_1 is true. The statement S_1 is $1 = \frac{1}{2}1(1+1)$, which is true.
2. $S_n \Rightarrow S_{n+1}$. We *assume* that S_n is true for some $n \geq 1$—that is, that

$$1+2+\cdots+n = \frac{1}{2}n(n+1)$$

We must prove that the statement

$$S_{n+1} : 1+2+\cdots+(n+1) = \frac{1}{2}(n+1)(n+2)$$

is also true, and we are entitled to use S_n to do so. Now the left side of S_{n+1} is the sum of the first $n+1$ positive integers. Hence the second-to-last term is n, so we can write

$$\begin{aligned} 1+2+\cdots+(n+1) &= (1+2+\cdots+n)+(n+1) \\ &= \tfrac{1}{2}n(n+1)+(n+1) \quad \text{using } S_n \\ &= \tfrac{1}{2}(n+1)(n+2) \end{aligned}$$

This shows that S_{n+1} is true and so completes the induction.

In the verification that $S_n \Rightarrow S_{n+1}$, we *assume* that S_n is true and use it to deduce that S_{n+1} is true. The assumption that S_n is true is sometimes called the **induction hypothesis**.

Example C.2

If x is any number such that $x \neq 1$, show that $1+x+x^2+\cdots+x^n = \frac{x^{n+1}-1}{x-1}$ for $n \geq 1$.

Solution. Let S_n be the statement: $1+x+x^2+\cdots+x^n = \frac{x^{n+1}-1}{x-1}$.

1. S_1 is true. S_1 reads $1+x=\frac{x^2-1}{x-1}$, which is true because $x^2-1=(x-1)(x+1)$.

2. $S_n \Rightarrow S_{n+1}$. Assume the truth of $S_n : 1+x+x^2+\cdots+x^n=\frac{x^{n+1}-1}{x-1}$.

We must *deduce* from this the truth of S_{n+1}: $1+x+x^2+\cdot+x^{n+1}=\frac{x^{n+2}-1}{x-1}$. Starting with the left side of S_{n+1} and using the induction hypothesis, we find

$$\begin{aligned}1+x+x^2+\cdots+x^{n+1} &= (1+x+x^2+\cdots+x^n)+x^{n+1}\\ &= \tfrac{x^{n+1}-1}{x-1}+x^{n+1}\\ &= \tfrac{x^{n+1}-1+x^{n+1}(x-1)}{x-1}\\ &= \tfrac{x^{n+2}-1}{x-1}\end{aligned}$$

This shows that S_{n+1} is true and so completes the induction.

Both of these examples involve formulas for a certain sum, and it is often convenient to use summation notation. For example, $\sum_{k=1}^{n}(2k-1)$ means that in the expression $(2k-1)$, k is to be given the values $k=1,\ k=2,\ k=3,\ \dots,\ k=n$, and then the resulting n numbers are to be added. The same thing applies to other expressions involving k. For example,

$$\sum_{k=1}^{n} k^3 = 1^3+2^3+\cdots+n^3$$

$$\sum_{k=1}^{5}(3k-1) = (3\cdot 1-1)+(3\cdot 2-1)+(3\cdot 3-1)+(3\cdot 4-1)+(3\cdot 5-1)$$

The next example involves this notation.

Example C.3

Show that $\sum_{k=1}^{n}(3k^2-k)=n^2(n+1)$ for each $n\geq 1$.

Solution. Let S_n be the statement: $\sum_{k=1}^{n}(3k^2-k)=n^2(n+1)$.

1. S_1 is true. S_1 reads $(3\cdot 1^2-1)=1^2(1+1)$, which is true.

2. $S_n \Rightarrow S_{n+1}$. Assume that S_n is true. We must prove S_{n+1}:

$$\begin{aligned}\sum_{k=1}^{n+1}(3k^2-k) &= \sum_{k=1}^{n}(3k^2-k)+[3(n+1)^2-(n+1)]\\ &= n^2(n+1)+(n+1)[3(n+1)-1] && \text{(using } S_n\text{)}\\ &= (n+1)[n^2+3n+2]\\ &= (n+1)[(n+1)(n+2)]\\ &= (n+1)^2(n+2)\end{aligned}$$

This proves that S_{n+1} is true.

We now turn to examples wherein induction is used to prove propositions that do not involve sums.

Example C.4

Show that $7^n + 2$ is a multiple of 3 for all $n \geq 1$.

Solution.

1. S_1 is true: $7^1 + 2 = 9$ is a multiple of 3.
2. $S_n \Rightarrow S_{n+1}$. Assume that $7^n + 2$ is a multiple of 3 for some $n \geq 1$; say, $7^n + 2 = 3m$ for some integer m. Then

$$7^{n+1} + 2 = 7(7^n) + 2 = 7(3m - 2) + 2 = 21m - 12 = 3(7m - 4)$$

so $7^{n+1} + 2$ is also a multiple of 3. This proves that S_{n+1} is true.

In all the foregoing examples, we have used the principle of induction starting at 1; that is, we have verified that S_1 is true and that $S_n \Rightarrow S_{n+1}$ for each $n \geq 1$, and then we have concluded that S_n is true for every $n \geq 1$. But there is nothing special about 1 here. If m is some fixed integer and we verify that

1. S_m is true.
2. $S_n \Rightarrow S_{n+1}$ for every $n \geq m$.

then it follows that S_n is true for every $n \geq m$. This “extended” induction principle is just as plausible as the induction principle and can, in fact, be proved by induction. The next example will illustrate it. Recall that if n is a positive integer, the number $n!$ (which is read “n-factorial”) is the product

$$n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$$

of all the numbers from n to 1. Thus $2! = 2$, $3! = 6$, and so on.

Example C.5

Show that $2^n < n!$ for all $n \geq 4$.

Solution. Observe that $2^n < n!$ is actually false if $n = 1,\ 2,\ 3$.

1. S_4 is true. $2^4 = 16 < 24 = 4!$.
2. $S_n \Rightarrow S_{n+1}$ if $n \geq 4$. Assume that S_n is true; that is, $2^n < n!$. Then

$$\begin{array}{rcll} 2^{n+1} & = & 2 \cdot 2^n & \\ & < & 2 \cdot n! & \text{because } 2^n < n! \\ & < & (n+1)n! & \text{because } 2 < n+1 \\ & = & (n+1)! & \end{array}$$

Hence S_{n+1} is true.

Exercises for C

In Exercises 1–19, prove the given statement by induction for all $n \geq 1$.

Exercise C.1 $1+3+5+7+\cdots+(2n-1)=n^2$

Exercise C.2 $1^2+2^2+\cdots+n^2=\frac{1}{6}n(n+1)(2n+1)$

Exercise C.3 $1^3+2^3+\cdots+n^3=(1+2+\cdots+n)^2$

Exercise C.4 $1\cdot 2+2\cdot 3+\cdots+n(n+1)$
$=\frac{1}{3}n(n+1)(n+2)$

Exercise C.5 $1\cdot 2^2+2\cdot 3^2+\cdots+n(n+1)^2$
$=\frac{1}{12}n(n+1)(n+2)(3n+5)$

Exercise C.6 $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$

Exercise C.7 $1^2+3^2+\cdots+(2n-1)^2=\frac{n}{3}(4n^2-1)$

Exercise C.8 $\frac{1}{1\cdot 2\cdot 3}+\frac{1}{2\cdot 3\cdot 4}+\cdots+\frac{1}{n(n+1)(n+2)}$
$=\frac{n(n+3)}{4(n+1)(n+2)}$

Exercise C.9 $1+2+2^2+\cdots+2^{n-1}=2^n-1$

Exercise C.10 $3+3^3+3^5+\cdots+3^{2n-1}=\frac{3}{8}(9^n-1)$

Exercise C.11 $\frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{n^2}\leq 2-\frac{1}{n}$

Exercise C.12 $n<2^n$

Exercise C.13 For any integer $m>0$, $m!n!<(m+n)!$

Exercise C.14 $\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\cdots+\frac{1}{\sqrt{n}}\leq 2\sqrt{n}-1$

Exercise C.15 $\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\cdots+\frac{1}{\sqrt{n}}\geq \sqrt{n}$

Exercise C.16 $n^3+(n+1)^3+(n+2)^3$ is a multiple of 9.

Exercise C.17 $5n+3$ is a multiple of 4.

Exercise C.18 n^3-n is a multiple of 3.

Exercise C.19 $3^{2n+1}+2^{n+2}$ is a multiple of 7.

Exercise C.20 Let $B_n=1\cdot 1!+2\cdot 2!+3\cdot 3!+\cdots+n\cdot n!$ Find a formula for B_n and prove it.

Exercise C.21 Let

$$A_n=(1-\tfrac{1}{2})(1-\tfrac{1}{3})(1-\tfrac{1}{4})\cdots(1-\tfrac{1}{n})$$

Find a formula for A_n and prove it.

Exercise C.22 Suppose S_n is a statement about n for each $n\geq 1$. Explain what must be done to prove that S_n is true for all $n\geq 1$ if it is known that:

a. $S_n \Rightarrow S_{n+2}$ for each $n\geq 1$.

b. $S_n \Rightarrow S_{n+8}$ for each $n\geq 1$.

c. $S_n \Rightarrow S_{n+1}$ for each $n\geq 10$.

d. Both S_n and $S_{n+1} \Rightarrow S_{n+2}$ for each $n\geq 1$.

Exercise C.23 If S_n is a statement for each $n\geq 1$, argue that S_n is true for all $n\geq 1$ if it is known that the following two conditions hold:

1. $S_n \Rightarrow S_{n-1}$ for each $n\geq 2$.
2. S_n is true for infinitely many values of n.

Exercise C.24 Suppose a sequence a_1, a_2, $\ldots$ of numbers is given that satisfies:

1. $a_1=2$.
2. $a_{n+1}=2a_n$ for each $n\geq 1$.

   Formulate a theorem giving a_n in terms of n, and prove your result by induction.

Exercise C.25 Suppose a sequence a_1, a_2, $\ldots$ of numbers is given that satisfies:

1. $a_1=b$.
2. $a_{n+1}=ca_n+b$ for $n=1$, 2, 3, $\ldots$.

   Formulate a theorem giving a_n in terms of n, and prove your result by induction.

Exercise C.26

a. Show that $n^2\leq 2^n$ for all $n\geq 4$.

b. Show that $n^3\leq 2^n$ for all $n\geq 10$.

D. Polynomials

Expressions like $3-5x$ and $1+3x-2x^2$ are examples of polynomials. In general, a **polynomial** is an expression of the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where the a_i are numbers, called the **coefficients** of the polynomial, and x is a variable called an **indeterminate**. The number a_0 is called the **constant** coefficient of the polynomial. The polynomial with every coefficient zero is called the **zero polynomial**, and is denoted simply as 0.

If $f(x) \neq 0$, the coefficient of the highest power of x appearing in $f(x)$ is called the **leading** coefficient of $f(x)$, and the highest power itself is called the **degree** of the polynomial and is denoted $\deg(f(x))$. Hence

$$\begin{array}{ll} -1+5x+3x^2 & \text{has constant coefficient } -1, \text{ leading coefficient } 3, \text{ and degree } 2, \\ 7 & \text{has constant coefficient } 7, \text{ leading coefficient } 7, \text{ and degree } 0, \\ 6x-3x^3+x^4-x^5 & \text{has constant coefficient } 0, \text{ leading coefficient } -1, \text{ and degree } 5. \end{array}$$

We do not define the degree of the zero polynomial.

Two polynomials $f(x)$ and $g(x)$ are called **equal** if every coefficient of $f(x)$ is the same as the corresponding coefficient of $g(x)$. More precisely, if

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots \quad \text{and} \quad g(x) = b_0 + b_1x + b_2x^2 + \cdots$$

are polynomials, then

$$f(x) = g(x) \quad \text{if and only if} \quad a_0 = b_0,\ a_1 = b_1,\ a_2 = b_2,\ \dots$$

In particular, this means that

$$f(x) = 0 \text{ is the zero polynomial if and only if } a_0 = 0,\ a_1 = 0,\ a_2 = 0,\ \dots$$

This is the reason for calling x an indeterminate.

Let $f(x)$ and $g(x)$ denote nonzero polynomials of degrees n and m respectively, say

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{and} \quad g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

where $a_n \neq 0$ and $b_m \neq 0$. If these expressions are multiplied, the result is

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_mx^{n+m}$$

Since a_n and b_m are nonzero numbers, their product $a_nb_m \neq 0$ and we have

Theorem D.1

If $f(x)$ and $g(x)$ are nonzero polynomials of degrees n and m respectively, their product $f(x)g(x)$ is also nonzero and

$$\deg [f(x)g(x)] = n + m$$

Example D.1

$(2 - x + 3x^2)(3 + x^2 - 5x^3) = 6 - 3x + 11x^2 - 11x^3 + 8x^4 - 15x^5$.

If $f(x)$ is any polynomial, the next theorem shows that $f(x) - f(a)$ is a multiple of the polynomial $x - a$. In fact we have

Theorem D.2: Remainder Theorem

If $f(x)$ is a polynomial of degree $n \geq 1$ and a is any number, then there exists a polynomial $q(x)$ such that

$$f(x) = (x - a)q(x) + f(a)$$

where $\deg(q(x)) = n - 1$.

Proof. Write $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ where the a_i are numbers, so that

$$f(a) = a_0 + a_1a + a_2a^2 + \cdots + a_na^n$$

If these expressions are subtracted, the constant terms cancel and we obtain

$$f(x) - f(a) = a_1(x - a) + a_2(x^2 - a^2) + \cdots + a_n(x^n - a^n).$$

Hence it suffices to show that, for each $k \geq 1$, $x^k - a^k = (x - a)p(x)$ for some polynomial $p(x)$ of degree $k - 1$. This is clear if $k = 1$. If it holds for some value k, the fact that

$$x^{k+1} - a^{k+1} = (x - a)x^k + a(x^k - a^k)$$

shows that it holds for $k + 1$. Hence the proof is complete by induction. □

There is a systematic procedure for finding the polynomial $q(x)$ in the remainder theorem. It is illustrated below for $f(x) = x^3 - 3x^2 + x - 1$ and $a = 2$. The polynomial $q(x)$ is generated on the top line one term at a time as follows: First x^2 is chosen because $x^2(x - 2)$ has the same x^3-term as $f(x)$, and this is subtracted from $f(x)$ to leave a "remainder" of $-x^2 + x - 1$. Next, the second term on top is $-x$ because $-x(x - 2)$ has the same x^2-term, and this is subtracted to leave $-x - 1$. Finally, the third term on top is

-1, and the process ends with a “remainder” of -3.

$$
\begin{array}{rrrrr}
 & & x^2 & -\ x & -\ 1 \\ \cline{2-5}
x-2 \,\big) & x^3 & -\ 3x^2 & +\ x & -\ 1 \\
 & x^3 & -\ 2x^2 & & \\ \cline{2-5}
 & & -x^2 & +\ x & -\ 1 \\
 & & -x^2 & +\ 2x & \\ \cline{3-5}
 & & & -x & -\ 1 \\
 & & & -x & +\ 2 \\ \cline{4-5}
 & & & & -\ 3
\end{array}
$$

Hence $x^3-3x^2+x-1=(x-2)(x^2-x-1)+(-3)$. The final remainder is $-3=f(2)$ as is easily verified. This procedure is called the **division algorithm**.[1]

A real number a is called a **root** of the polynomial $f(x)$ if

$$f(a)=0$$

Hence for example, 1 is a root of $f(x)=2-x+3x^2-4x^3$, but -1 is not a root because $f(-1)=10\neq 0$. If $f(x)$ is a multiple of $x-a$, we say that $x-a$ is a **factor** of $f(x)$. Hence the remainder theorem shows immediately that if a is root of $f(x)$, then $x-a$ is factor of $f(x)$. But the converse is also true: If $x-a$ is a factor of $f(x)$, say $f(x)=(x-a)q(x)$, then $f(a)=(a-a)q(a)=0$. This proves the

Theorem D.3: Factor Theorem

If $f(x)$ is a polynomial and a is a number, then $x-a$ is a factor of $f(x)$ if and only if a is a root of $f(x)$.

Example D.2

If $f(x)=x^3-2x^2-6x+4$, then $f(-2)=0$, so $x-(-2)=x+2$ is a factor of $f(x)$. In fact, the division algorithm gives $f(x)=(x+2)(x^2-4x+2)$.

Consider the polynomial $f(x)=x^3-3x+2$. Then 1 is clearly a root of $f(x)$, and the division algorithm gives $f(x)=(x-1)(x^2+x-2)$. But 1 is also a root of x^2+x-2; in fact, $x^2+x-2=(x-1)(x+2)$. Hence

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

and we say that the root 1 has **multiplicity** 2.

Note that non-zero constant polynomials $f(x)=b\neq 0$ have *no* roots. However, there do exist non-constant polynomials with no roots. For example, if $g(x)=x^2+1$, then $g(a)=a^2+1\geq 1$ for every real number a, so a is not a root. However the *complex* number i is a root of $g(x)$; we return to this below.

[1] This procedure can be used to divide $f(x)$ by any nonzero polynomial $d(x)$ in place of $x-a$; the remainder then is a polynomial that is either zero or of degree less than the degree of $d(x)$.

Now suppose that $f(x)$ is any nonzero polynomial. We claim that it can be factored in the following form:

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_m)g(x)$$

where $a_1,\ a_2,\ \dots,\ a_m$ are the roots of $f(x)$ and $g(x)$ has no root (where the a_i may have repetitions, and may not appear at all if $f(x)$ has no real root).

By the above calculation $f(x) = x^3 - 3x + 2 = (x-1)^2(x+2)$ has roots 1 and -2, with 1 of multiplicity two (and $g(x) = 1$). Counting the root -2 once, we say that $f(x)$ has three roots counting multiplicities. The next theorem shows that no polynomial can have more roots than its degree even if multiplicities are counted.

Theorem D.4

If $f(x)$ is a nonzero polynomial of degree n, then $f(x)$ has at most n roots counting multiplicities.

Proof. If $n = 0$, then $f(x)$ is a constant and has no roots. So the theorem is true if $n = 0$. (It also holds for $n = 1$ because, if $f(x) = a + bx$ where $b \neq 0$, then the only root is $-\frac{a}{b}$.) In general, suppose inductively that the theorem holds for some value of $n \geq 0$, and let $f(x)$ have degree $n+1$. We must show that $f(x)$ has at most $n+1$ roots counting multiplicities. This is certainly true if $f(x)$ has no root. On the other hand, if a is a root of $f(x)$, the factor theorem shows that $f(x) = (x-a)q(x)$ for some polynomial $q(x)$, and $q(x)$ has degree n by Theorem D.1. By induction, $q(x)$ has at most n roots. But if b is any root of $f(x)$, then

$$(b-a)q(b) = f(b) = 0$$

so either $b = a$ or b is a root of $q(x)$. It follows that $f(x)$ has at most n roots. This completes the induction and so proves Theorem D.4. □

As we have seen, a polynomial may have *no* root, for example $f(x) = x^2 + 1$. Of course $f(x)$ has complex roots i and $-i$, where i is the complex number such that $i^2 = -1$. But Theorem D.4 even holds for complex roots: the number of complex roots (counting multiplicities) cannot exceed the degree of the polynomial. Moreover, the fundamental theorem of algebra asserts that the only nonzero polynomials with no complex root are the non-zero constant polynomials. This is discussed more in Appendix A, Theorems A.4 and A.5.