to triangles representing pairs $(a_1, b_1)$ and $(a_2, b_2)$, however, his rule produced what we call their product, $(a_1a_2 - b_1b_2, b_1a_2 + a_1b_2)$. (The rule for producing the other triangle in Diophantus' identity can also be interpreted as a product of complex numbers; see the exercises.) It is all the more surprising that Diophantus devised this rule to solve problems about integers. As we shall see in the next section, its geometric significance goes far deeper than the interpretation of absolute value as a hypotenuse.

**Remark.** The product of triangles is closely related to the parameterization of Pythagorean triples (which Diophantus used in the same problem, by the way, so he was probably aware of a connection). *The triangle with sides* $(u^2 - v^2, 2uv)$ *and hypotenuse* $u^2 + v^2$ *is the "square" of the triangle with sides* $(u, v)$ *with hypotenuse* $\sqrt{u^2 + v^2}$. This is an easy calculation with complex numbers:

$$(u + iv)^2 = u^2 - v^2 + 2iuv.$$

# Exercises

Proving Diophantus' identity is not as hard as discovering it in the first place; just expand both sides and compare them. But if complex numbers are already familiar, the identity may be discovered by factorizing the product $(a_1^2 + b_1^2)(a_2^2 + b_2^2)$ and recombining the factors in a different way. This was done by Euler (1770).

7.1.1. Give a derivation of Diophantus' identity by suitably combining the factors in $(a_1 + ib_1)(a_1 - ib_1)(a_2 + ib_2)(a_2 - ib_2)$.

An interesting generalization of Diophantus' identity was discovered by the Indian mathematician Brahmagupta around 600 A.D.:

$$(a_1^2 - db_1^2)(a_2^2 - db_2^2) = (a_1a_2 + db_1b_2)^2 - d(a_1b_2 + a_2b_1)^2.$$

7.1.2. Give a derivation of Brahmagupta's identity by suitably grouping the factors in $(a_1 + \sqrt{d}b_1)(a_1 - \sqrt{d}b_1)(a_2 + \sqrt{d}b_2)(a_2 - \sqrt{d}b_2)$.

The identities of Diophantus and Brahmagupta are, of course, valid for all real values of $a_1, b_1, a_2, b_2$, and $d$. However, they are of most interest when these values are integers. In that case, they show that *the product of two integers of the form $a^2 - db^2$ is another integer of the same form.* This discovery is the beginning of a very long story we shall take up in Section 7.6.

Now let us return to the second Diophantus identity, with the signs switched.

7.1.3. To which complex numbers should $a_1^2 + b_1^2$ and $a_2^2 + b_2^2$ be attached, for

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 + b_1b_2)^2 + (b_1a_2 - a_1b_2)^2$$

to express the multiplicative property of absolute value?

7.1.4. Find a second form of Brahmagupta's identity, also with signs switched.

## 7.2 Argument and the Square Root of −1

The product of triangles that was implicit in Diophantus became explicit in Viète's *Genesis triangulorum* around 1590. He actually drew diagrams of the right-angled triangles $(a_1, b_1)$ and $(a_2, b_2)$ and their two products, similar to Figure 7.2 but without labeled angles or the $\times$ and $=$ signs.

Viète was interested in the shape of the triangles more than the length of their hypotenuses, and this led him to a wonderful discovery: the product of triangles produces not only the product of hypotenuses, but the *sum* of angles. The angles that are added are those shown in Figure 7.2. In fact, the ratio of the sides in the

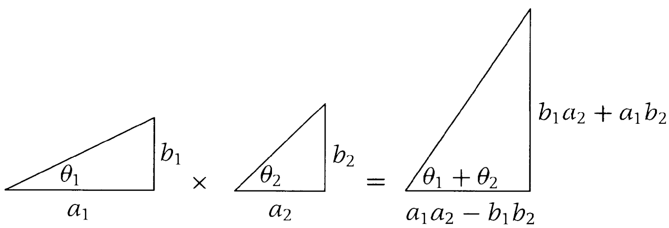


**FIGURE 7.2** The first product of triangles.

product triangle is precisely what we get from the addition formula for tan (Section 5.4):

$$\begin{aligned}\tan(\theta+\phi) &= \frac{\tan\theta+\tan\phi}{1-\tan\theta\tan\phi}\\ &= \frac{\frac{b_1}{a_1}+\frac{b_2}{a_2}}{1-\frac{b_1}{a_1}\frac{b_2}{a_2}}\\ &= \frac{b_1a_2+a_1b_2}{a_1a_2-b_1b_2}.\end{aligned}$$

Like Diophantus, Viète was thinking about triangles, not complex numbers. Nevertheless, just as Diophantus observed the multiplicative property of what we call the absolute value, Viète observed the *additive* property of what we call the *argument* of the complex number $a+ib$, the angle $\theta$ with $\cos\theta = a/\sqrt{a^2+b^2}$ and $\sin\theta = b/\sqrt{a^2+b^2}$. (The only limitation to interpreting complex numbers $a+ib$ as triangles is that $a$ and $b$ cannot be negative or zero. This does mean, however, that there is no interpretation of the crucial object $i$.)

When a complex number $a+ib$ is viewed as a point $(a,b)$ of the plane, its absolute value and argument are its *polar coordinates* $r = \sqrt{a^2+b^2}$ and $\theta$ (Figure 7.3). The multiplicative property of absolute value and the additive property of argument give the product of complex numbers in polar coordinates:

$$\begin{aligned}(a_1+ib_1)(a_1+ib_2) &= r_1(\cos\theta_1+i\sin\theta_1)r_2(\cos\theta_2+i\sin\theta_2)\\ &= r_1r_2\left(\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2)\right).\end{aligned}$$

Because $(a,b)$ is completely determined by $r$ and $\theta$, this is equivalent to the $\times$ rule in the previous section as a definition of product. It shows multiplication in a much more geometric light, and it gives

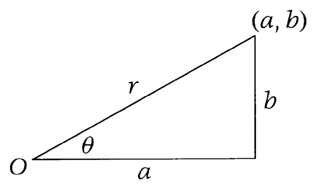


**FIGURE 7.3** Absolute value and argument as polar coodinates.

a geometric interpretation of multiplication by $i = \sqrt{-1}$. Because $i = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$, *multiplication by $i$ adds $\pi/2$ to the argument of each complex number*. That is, *it rotates the plane of complex numbers counterclockwise through $\pi/2$*.

With hindsight, it is natural for multiplication by $i$ to be a quarter turn. After all, multiplication by $i$ twice is multiplication by $-1$, which is a half turn of the real number line. Algebraically speaking, multiplication is an operation of *period* 4, because the powers of $i$ recur every four steps:

$$1, \quad i, \quad -1, \quad -i, \quad 1, \quad i, \quad -1, \quad -i, \quad 1, \quad \ldots.$$

Hence $i = \sqrt{-1}$ can only exist in a system containing operations of period 4. Such a system need not be the full set of complex numbers. For example, it could be the *Gaussian integers*, the set of numbers $a + ib$ where $a$ and $b$ are integers. We shall study these in section 7.4. The system can even be the finite field $\mathbb{Z}/p\mathbb{Z}$ for a suitable value of $p$. As we saw in Exercises 6.5.8 and 6.5.9, $-1$ is a square in $\mathbb{Z}/p\mathbb{Z}$ just in case $p = 4n+1$, and it follows from the existence of primitive roots (mentioned in the exercises for Section 6.7) that this happens precisely when $\mathbb{Z}/p\mathbb{Z}$ has elements of period 4.

More of a surprise is that $i$, the fourth root of 1, together with the real numbers, gives a nontrivial $n$th root of 1 for *all* natural numbers $n$. In fact, it follows from the additive property of argument that

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

so $\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ is a nontrivial $n$th root of 1. (Nontrivial, because it is not equal to 1 itself.) The *fundamental theorem of algebra*, whose proof is beyond the scope of this book, says that much more is true: *any equation $p(x) = 0$, where $p$ is a polynomial with real coefficients, has a solution in the set $\mathbb{C}$ of complex numbers.*

## Exercises

The complex numbers are such a fundamental part of mathematics that it is no wonder that aspects of them (such as the multiplicative property of absolute value) were glimpsed long before they were recognized as numbers. The latter possibility could not arise until there was reason to add *and* multiply them. This did not happen until the 16th century, when a number of Italian mathematicians discovered how to solve cubic equations. It turned out, for example, that the solutions of

$$x^3 = px + q$$

are given by the *Cardano formula*:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}.$$

7.2.1. Substitute $u + v$ for $x$ in $x^3 = px + q$, and deduce that $u + v$ will satisfy this equation if $3uv = p$ and $u^3 + v^3 = q$.

7.2.2. Substitute $v = p/3u$ in $u^3 + v^3 = q$ and solve the resulting quadratic in $u^3$. Deduce that

$$u^3, v^3 = \frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}$$

and explain the Cardano solution of $x^3 = px + q$.

This is all very well, but does it account for the obvious solution $x = 4$ of $x^3 = 15x + 4$?

7.2.3. Show that, according to the Cardano formula, the solutions of $x^3 = 15x + 4$ are

$$x = \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}}.$$

Rafael Bombelli (1572) had a hunch that this apparent conflict might be resolved as follows. He guessed there was an $n$ with

$$\sqrt[3]{2 + 11\sqrt{-1}} = 2 + n\sqrt{-1},$$
$$\sqrt[3]{2 - 11\sqrt{-1}} = 2 - n\sqrt{-1},$$

so the solution $x = 4$ could result from cancelation of imaginary terms $n\sqrt{-1}$ and $-n\sqrt{-1}$. This hunch turned out to be correct.

7.2.4. Show that $(2 + \sqrt{-1})^3 = 2 + 11\sqrt{-1}$ and $(2 - \sqrt{-1})^3 = 2 - 11\sqrt{-1}$.

These calculations, which involve both addition and multiplication of complex numbers, were enough to convince many mathematicians that complex numbers were subject to the same laws as the reals. Still, whenever possible one made an independent check using real numbers alone.

Viète found an interesting way to do this for cubic equations in cases where the Cardano formula leads to square roots of negative numbers. He used the formula

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

and coaxed the equation $x^3 - px = q$ into the form $4y^3 - 3y = c$, where $c$ could be set equal to $\cos 3\theta$ for some angle $\theta$. Then $y = \cos\theta$ is a solution of $4y^3 - 3y = c$, and $x$ is easily found from $y$.

7.2.5. Find a substitution $x = ky$ so that $2x^3 = 3x - 1$ becomes $4y^3 - 3y = -1/\sqrt{2} = \cos\frac{3\pi}{4}$, and hence find a solution of $2x^3 = 3x - 1$ by Viète's method.

(You will probably only find the obvious solution, but see whether it is so obvious from Cardano's formula.)

## 7.3 Isometries of the Plane

Rotation of the plane about $O$ through $\pi/2$ is one of the isometries of the plane we studied in Section 3.6. The discovery that this rotation is simply multiplication by the complex number $i$ prompts us to look at isometries again. It seems as though they can be very concisely described in terms of complex numbers.

We interpret the Euclidean plane as the set $\mathbb{C}$ of complex numbers, so isometries are certain functions on $\mathbb{C}$. Translations are the easiest to grasp. Translating each point $x + iy$ by $a$ in the $x$-direction and $b$ in the $y$-direction is the same as *adding* $a + ib$ to $x + iy$, so the translation function $\mathrm{tran}_{a,b}$ is the function of a complex variable $z = x + iy$ defined by

$$\mathrm{tran}_{a,b}(z) = z + a + ib.$$

By the additive property of the argument, rotation about $O$ through $\theta$ is multiplication by $\cos\theta + i\sin\theta$, hence

$$\mathrm{rot}_{O,\theta}(z) = (\cos\theta + i\sin\theta)z.$$

Because $\cos^2\theta + \sin^2\theta = 1$, this is multiplication of $z$ by a complex number of absolute value 1. Conversely, any complex number $c$ of absolute value 1 is of the form $\cos\theta + i\sin\theta$; in fact, $\theta$ is the argument of $c$. Thus rotation about $O$ is multiplication by a fixed complex number of absolute value 1.

Rotation about any point $P = (u, v)$, through angle $\theta$, is the composite of three functions:

- $\mathrm{tran}_{-u,-v}$ = translation of $P$ to $O$,
- $\mathrm{rot}_{O,\theta}$ = rotation about $O$ through $\theta$,
- $\mathrm{tran}_{u,v}$ = translation of $O$ back to $P$.

Thus any rotation may be composed from the functions $\mathrm{tran}_{a,b}$ and $\mathrm{rot}_{O,\theta}$.

In the exercises to Section 3.8* it was shown that translations and rotations together are all the products of an even number of reflections, and that they also are the orientation-preserving isometries of the plane. Complex functions give another very neat way to describe them, without assuming these previous results.

**Characterization of translations and rotations.** *The translations and rotations of the Euclidean plane are the complex functions of the form*

$$f(z) = cz + d,$$

*where $c$ is a complex number with $|c| = 1$ and $d$ is an arbitrary complex number.*

*Proof* We know that translations and rotations about $O$ are of the required form. Also, if $f_1(z) = c_1z + d_1$ and $f_2(z) = c_2z + d_2$ are of the required form, then so is

$$f_1f_2(z) = c_1(c_2z + d_2) + d_1 = (c_1c_2)z + (c_1d_2 + d_1),$$

because $|c_1c_2| = |c_1||c_2| = 1 \times 1 = 1$ by the multiplicative property of absolute value. Thus any composite of translations and rotations about $O$, which we know includes rotations about arbitrary points, is of the form $f(z) = cz + d$ with $|c| = 1$.

Conversely, suppose we are given a function $f(z) = cz + d$ with $|c| = 1$. If $c = 1$, then we simply have the translation $f(z) = z + d$. If not, consider the rotation about the point $e$ obtained by composing

$$f_1(z) = z + e,$$
$$f_2(z) = cz,$$
$$f_3(z) = z - e,$$

where $e$ remains to be determined. We have

$$f_1 f_2 f_3(z) = c(z - e) + e = cz - ce + e,$$

which equals the given function if

$$d = -ce + e = e(1 - c);$$

that is, if

$$e = \frac{d}{1 - c}.$$

By hypothesis, $1 - c \neq 0$, so we can find the point $e$, and $f(z) = cz + d$ is a rotation about it. □

# Exercises

Another important isometry is reflection in the $x$-axis, the function that sends $x + iy$ to its *conjugate* $x - iy$. The conjugate of $z$ is denoted by $\bar{z}$ and has the following easily checked properties.

7.3.1. Check that $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ and $z\bar{z} = |z|^2$.

Composing conjugation with translations and rotations gives a further class of isometries

$$\bar{f}(z) = c\bar{z} + d \quad \text{where } |c| = 1.$$

These, together with the functions $f(z) = cz + d$ already found, make up *all* isometries of the Euclidean plane. A quick way to prove this is to combine the characterization of translations and rotations with the three reflections theorem and related results in Section 3.6. By Exercises 3.6.3 and 3.6.4, the composite of two reflections is a translation or rotation, hence of the form $f(z) = cz + d$ with $|c| = 1$.

7.3.2. Suppose a Euclidean isometry $g$ is a composite of one or three reflections. Show that $\overline{g(z)}$ is a rotation or translation.