EXERCISES

In case there is any doubt that multiplication of complex numbers could be observed before the numbers themselves were recognized, here is another sighting, by Viète in his *Genesis triangulorum* from around 1590.

Viète independently discovered the rule of Diophantus that takes two triangles and produces a third, but Viète used it for an entirely different purpose. Instead of multiplying hypotenuses, he wanted to *add angles*.

20.2.1 Suppose the right-angled triangle with sides a_1, b_1 has angle θ_1 opposite the side b_1, and the right-angled triangle with sides a_2, b_2 has angle θ_2 opposite the side b_2. Write down $\tan\theta_1$, $\tan\theta_2$, and $\tan(\theta_1+\theta_2)$.

20.2.2 Deduce from Question 20.2.1 that the right-angled triangle with sides $a_1a_2 - b_1b_2$, $b_1a_2 + a_1b_2$ has angle $\theta_1 + \theta_2$. (Opposite which side?)

20.2.3 Interpret the results of Diophantus and Viète in terms of the *polar form* $r(\cos\theta + i\sin\theta)$ of the complex number $a+ib$.

It has even been speculated that multiplication of complex numbers, at least "multiplication of pairs," lies behind the mysterious collection of Pythagorean triples in Plimpton 322 (Section 1.2).

To explore this speculation more fully one needs to have the complete triples (a,b,c) from Exercise 1.2.1. It turns out that every pair (a,b) is of the form $(a_1a_2 - b_1b_2,\ b_1a_2 + a_1b_2)$ for some smaller integer pairs (a_1,b_1) and (a_2,b_2). That is, $a+ib = (a_1+ib_1)(a_2+ib_2)$. Even more amazing, with the exception of the multiple $(45,60,75)$ of $(3,4,5)$, *every* $a+ib$ *is a perfect square*, up to a factor of $\pm i$. Here are some for which this is not hard to verify.

20.2.4 For $(a,c) = (119,169)$ show that $b = 120$ and that $119+120i$ is a perfect square. *Hint*: Observe that $169 = 13^2 = \text{hypotenuse}^2$.

20.2.5 Show that a similar result holds for $(a,c) = (161,289)$.

20.3 Properties of $+$ and $\times$

During the 1830s, Hamilton and his colleagues Peacock, De Morgan, and John Graves pursued the idea of extending the concept of number. The existing concept of number was already the result of a series of extensions—from natural and rational numbers to real and complex numbers—and Peacock observed that some *principle of permanence* was involved. It was tacitly agreed that certain properties of addition and multiplication should continue to hold with each extension of the number concept.

The "permanent" properties were not completely clear at the time, but most of them crystallized in the definition of a *field* given by Dedekind

(1871). This concept had an independent origin, also around 1830, in the work of Galois on the theory of equations. So for convenience we start with the definition of a field and then explain its role in Hamilton's search for an arithmetic of n-tuples.

A field is a set of objects on which operations $+$ and $\times$ are defined, with certain properties or "laws." To state these properties concisely, we also use the $-$ operation. Notice that $-$ is interpreted as the operator that turns a natural number a into its *negative* or *additive inverse* $-a$. The negative of a negative is defined so that $--a = a$ always, and the *difference* $a-b$ is defined to be $a+(-b)$. Then the properties of $+$ and $-$ are as follows.

$$
\begin{aligned}
a+(b+c) &= (a+b)+c && \text{(associative law)}\\
a+b &= b+a && \text{(commutative law)}\\
a+(-a) &= 0 && \text{(additive inverse property)}\\
a+0 &= a && \text{(property of 0)}
\end{aligned}
$$

There is a similar set of properties describing the behavior of $\times$.

$$
\begin{aligned}
a\times(b\times c) &= (a\times b)\times c && \text{(associative law)}\\
a\times b &= b\times a && \text{(commutative law)}\\
a\times 1 &= a && \text{(property of 1)}\\
a\times 0 &= 0 && \text{(property of 0)}
\end{aligned}
$$

and a rule for the interaction of $+$ and $\times$:

$$a\times(b+c) = a\times b + a\times c \qquad \text{(distributive law)}$$

The properties so far define what is called a *commutative ring with unit*, a typical example of which is the set $\mathbb{Z}$ of integers.

The defining properties of a *field* are those above, together with existence of the *multiplicative inverse* a^{-1}, which is defined for each $a \neq 0$ and satisfies

$$a\times a^{-1} = 1. \quad \text{(multiplicative inverse property)}$$

Typical examples of fields are the number systems $\mathbb{Q}$ of rationals, $\mathbb{R}$ of reals, and $\mathbb{C}$ of complex numbers.

In trying to see beyond these systems, Hamilton was guided by one more property they all have in common: the existence of a *multiplicative absolute value*, a real-valued function $|\ |$ with the properties

$$a \neq 0 \Rightarrow |a| \neq 0, \qquad |ab| = |a||b|.$$

As we have seen in Section 20.2, the multiplicative absolute value for complex numbers was essentially discovered by Diophantus, long before the discovery of complex numbers themselves. Hamilton was unaware of this, because he had not studied number theory, and he was *blissfully* unaware of what number theory had to say about a multiplicative absolute value for triples. The subsequent history of hypercomplex numbers might have been very different had he known what he was up against.

20.4 Arithmetic of Triples and Quadruples

Diophantus' *Arithmetica* contains many results about sums of two squares. This is natural, because of long history of Pythagorean triples, and because of Diophantus' own contribution to the subject in showing that sums of two squares could be "multiplied." There are also some results on sums of four squares, which led Bachet de Méziriac (1621) to the conjecture that every positive integer is the sum of four squares, and the eventual proof of this conjecture by Lagrange (1770). However, Diophantus has nothing much to say about sums of *three* squares, and it was probably obvious to him that sums of three squares could *not* be multiplied.

For example, $3 = 1^2 + 1^2 + 1^2$ and $5 = 0^2 + 1^2 + 2^2$ are both sums of three squares, but their product, 15, is not. It follows that there can be no identity of the form

$$(a_1^2 + b_1^2 + c_1^2)(a_2^2 + b_2^2 + c_2^2) = A^2 + B^2 + C^2,$$

where A, B, and C are combinations of the a_m, b_m, and c_m with integer coefficients. This means in turn that there cannot be a product of triples

$$(a_1, b_1, c_1)(a_2, b_2, c_2) = (A, B, C)$$

with multiplicative absolute value, at least if A, B, and C are such combinations of the a_m, b_m, and c_m.

In one of the most extraordinary oversights in the history of mathematics, Hamilton failed to notice this or any other evidence, and persisted to search for a product of triples for at least 13 years (from 1830 to 1843). For most of this time, he was hoping to achieve all the field properties listed above, together with a multiplicative absolute value.

Following the example of the complex numbers, he wrote the triple (a, b, c) as $a + ib + jc$, thus reducing the problem of multiplication to determining the products i^2, j^2, and ij. He wanted $i^2 = j^2 = -1$, so it only remained to find real coefficients α, β, γ such that $ij = \alpha + i\beta + j\gamma$. But nothing worked. In particular, it seemed impossible to reconcile the distributive law with the commutative law for multiplication. In 1843, he briefly considered making $ij = 0$ (which would violate the multiplicative absolute value), but then

> made what appeared to me a *less harsh* supposition, namely the supposition ... that
>
> $$ij = -ji: \quad \text{or that} \quad ij = +k, ji = -k,$$
>
> the value of the product k being still left undetermined .... This led me to conceive that perhaps instead of seeking to *confine* ourselves to *triplets*, such as $a + ib + jc$ or (a,b,c), we ought to regard these as only *imperfect forms of* QUATERNIONS, such as $a + ib + jc + kd$ or (a,b,c,d), the symbol k being *some new sort of unit operator*.
>
> [Hamilton (1853), pp. 143–144.]

Thus Hamilton abandoned commutative multiplication, but everything else fell into place. This is how he described it later, in a letter to his son:

> But on the 16th day of the month [namely, October 1843] which happened to be a Monday and a council day of the Royal Irish Academy—I was walking along to preside, and your mother was walking with me, along the Royal Canal ... and although she talked with me now and then, yet an undercurrent of thought was going on in my mind, which gave at last a result ... An electric current seemed to close, and a spark flashed forth, the herald (as I foresaw immediately) of many long years to come of definitely directed thought and work ...
>
> I pulled out on the spot a pocket-book, which still exists, and made an entry there and then. Nor could I resist the impulse—unphilosophical as it may have been—to cut with a knife on a stone of Brougham Bridge the fundamental formula with the symbols i, j, k:
>
> $$i^2 = j^2 = k^2 = ijk = -1,$$
>
> which contains the solution of the Problem, but of course, as an inscription it has long since mouldered away.
>
> [Hamilton (1865)]

The pocket-book contains not only the values of ij, ji, jk, kj, ki, ik, which follow from the fundamental formula, but also the four components of the general product of quaternions:

$$\begin{aligned}(a+ib+jc+kd)(\alpha+i\beta+j\gamma+k\delta) = \quad & (a\alpha-b\beta-c\gamma-d\delta)\\ & +i(a\beta+b\alpha+c\delta-d\gamma)\\ & +j(a\gamma-b\delta+c\alpha+d\beta)\\ & +k(a\delta+b\gamma-c\beta+d\alpha).\end{aligned}$$

Like all his previous attempts, Hamilton's starting point for his fundamental formula was the multiplicative property of the absolute value, or as he put it: "the modulus of a product is equal to the product of the moduli of the factors." This generalizes the multiplicative property of the absolute value for complex numbers, and shows that the product of two nonzero quaternions is nonzero.

The square of the absolute value of the quaternion $\alpha+\beta i+\gamma j+\delta k$ is $\alpha^2+\beta^2+\gamma^2+\delta^2$, so the product formula for quaternions gives the following identity, which shows that the product of sums of four squares is a sum of four squares:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) = \quad & (a\alpha-b\beta-c\gamma-d\delta)^2\\ & +(a\beta+b\alpha+c\delta-d\gamma)^2\\ & +(a\gamma-b\delta+c\alpha+d\beta)^2\\ & +(a\delta+b\gamma-c\beta+d\alpha)^2.\end{aligned}$$

If Hamilton had studied number theory he would have known this, because the identity was discovered by Euler (1748c), and used by Euler and Lagrange to prove that every natural number is the sum of four squares.

Hamilton thought at first his four-square identity was original, but in the months following the discovery of quaternions he and his friend John Graves caught up with the news on three and four squares. It dawned on Graves that they should never have expected a three-square identity, because $3 = 1^2+1^2+1^2$ and $21 = 1^2+2^2+4^2$ are sums of three squares, but their product 63 is not. He then consulted the literature and

> On Friday last I looked into Lagrange's [he meant Legendre] Théorie des Nombres and found for the first time that I had lately been on the track of former mathematicians. For example, the mode by which I satisfied myself that a general

theorem

$$(x_1^2+x_2^2+x_3^2)(y_1^2+y_2^2+y_3^2)=z_1^2+z_2^2+z_3^2$$

was impossible was the very mode mentioned by Legendre, who gives the very example that occurred to me, viz., $3\times 21=63$, it being impossible to compound 63 of three squares.

I then learned that the theorem

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=z_1^2+z_2^2+z_3^2+z_4^2$$

was Euler's. [Graves (1844) letter to Hamilton]

It is tempting to think that Hamilton could have discovered quaternions much more easily had he known there was an identity for sums of four squares, and none for sums of three squares. But the course of mathematical discovery is seldom so smooth. Perhaps the hopeless struggle with triples was good for him, because he did not want it to be in vain—he may not have been willing to abandon commutative multiplication otherwise.

EXERCISES

It can be checked that 15 is not a sum of three (integer) squares by trying all possible sums of the squares $0, 1, 4, 9$ that are less than 15. However, a much more general result is possible. As Exercises 3.2.1 and 3.2.2 show, no natural number of the form $8n+7$ is a sum of three squares.

With an infinite supply of such numbers on tap, it becomes easy to understand how both Legendre and Graves stumbled on the example $3\times 21=63$.

20.4.1 Find the smallest number of the form $8n+7$ (hence not a sum of three squares) that is the product of sums of three *nonzero* squares.

We can also improve the result of Exercise 3.2.2 to one about sums of *rational* squares (which would have been more interesting to Diophantus).

20.4.2 Show that if there are rationals x, y, and z such that $x^2+y^2+z^2=7$, then $7s^2$ is a sum of three integer squares, for some integer s. Show that the latter is impossible.

20.4.3 Generalize the argument of Question 20.4.2 to show that $8n+7$ is not the sum of three rational squares, for any integer n.

It is interesting that Diophantus actually remarked (in his Book VI, Problem 14) that 15 is not a sum of two rational squares. Question 20.4.3 shows that 15 is not even the sum of three rational squares—a result Diophantus may also have known, since the most obvious proofs of the two results are similar. (To prove that 15 is not a sum of two rational squares it suffices to use remainders on division by 4. Try it!)

20.5 Quaternions, Geometry, and Physics

Hamilton may have seen, at the instant of discovery, that quaternions would be worth his attention for the rest of his life, but even his best friends were sceptical at first. On 26 October 1843, John Graves wrote to him:

> You must have been in a very bold mood to start the happy idea that ij might be different from ji . . . Have you any inkling of the existence in nature of processes, or operations, or phenomena, or conceptions analogous to the circuit
>
> $$ij = -ji = k$$
> $$jk = -kj = i$$
> $$ki = -ik = j?$$

And after receiving a letter from Hamilton hinting at applications to physics, and announcing that quaternions could certainly be used to derive theorems of spherical trigonometry, Graves replied:

> There is still something in the system that gravels me. I have not yet any clear views as to the extent to which we are at liberty arbitrarily to create imaginaries, and to endow them with supernatural properties . . . But supposing that your symbols have their physical antitypes, which might have led to your quaternions, what right have you to such luck, getting at your system by such an *inventive* mode as yours?

[For more of these letters, see the biography of Hamilton written by Graves' brother Robert: Graves (1975), vol. 3, p. 443.]

Of course, Graves' question about luck was tongue-in-cheek, but it is still a good question. Many mathematicians and physicists have marvelled at the capacity of pure mathematics to become applied, for number theory and algebra to become geometry and physics. In the case of quaternions, more surprises were in store.

Not only was it true that quaternions had implications for spherical trigonometry, their geometric aspect had already been discovered twice before! The first discovery was the unpublished work of Gauss (1819) on rotations of the sphere, which Hamilton could not have known about; the second was a publication by Rodrigues (1840) that (typically) escaped his attention.

The result of Gauss is easiest to explain, because we have already mentioned it in Section 18.6: every rotation of the sphere can be expressed by a complex function of the form

$$f(z)=\frac{az+b}{-\bar{b}z+\bar{a}}.$$

Any such function can be represented by the matrix of its coefficients,

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix},$$

and it is easily checked that the matrix of $f_1 f_2$ is the product of the matrices for f_1 and f_2. Thus rotations of the sphere can be studied via products of matrices of the above type, involving pairs of complex numbers a, b. Such a matrix can also be written in terms of four *real* parameters α, β, γ, δ if we set

$$a=\alpha+i\beta, \quad b=\gamma+i\delta.$$

And we can then write the resulting matrix as a linear combination of four special matrices with coefficients α, β, γ, δ:

$$\begin{aligned}\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} &= \begin{pmatrix} \alpha+i\beta & \gamma+i\delta \\ -\gamma+i\delta & \alpha-i\beta \end{pmatrix} \\ &= \alpha\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}+\beta\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}+\gamma\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}+\delta\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= \alpha\mathbf{1}+\beta\mathbf{i}+\gamma\mathbf{j}+\delta\mathbf{k}.\end{aligned}$$

The four special matrices $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ play the role of 1, i, j, k in the quaternions, because

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=\mathbf{ijk}=-\mathbf{1}.$$

In fact, the same matrices were discovered by Cayley (1858), who proposed them as a new realization of the quaternions. Today, they are often known as *Pauli* matrices, particularly in physics. They were rediscovered in quantum theory, where the rotations of the sphere are also important.

EXERCISES

The Cayley matrices

$$\mathbf{1}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i}=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j}=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k}=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

make it easy to prove the basic properties of quaternions.