Chapter 2
Number Sets and Algebra

2.1 Introduction

In this chapter we review some basic ideas of number sets, and how they are manipulated arithmetically and algebraically. We look briefly, at expressions and equations and the rules used for their construction and evaluation. These, in turn, reveal the need to extend every-day numbers with so called complex numbers.

The second part of the chapter is used to define groups, rings and fields.

2.2 Number Sets

2.2.1 Natural Numbers

Natural numbers are the whole numbers 1, 2, 3, 4, etc., and by definition (DIN 5473), the *set* of natural numbers and zero $\{0, 1, 2, 3, 4, \ldots\}$ are represented by the symbol $\mathbb{N}$ and we express this assignment using:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}.$$

The statement

$$k \in \mathbb{N}$$

implies that k belongs to the set $\mathbb{N}$, where $\in$ means *belongs to*, or in other words, k is a natural number. We employ this notation throughout this book to ensure that there is no confusion about the type of numerical quantity being used.

$\mathbb{N}^*$ is used to represent the set $\{1, 2, 3, 4, \ldots\}$.

2.2.2 Real Numbers

Scientific calculations employ a wide range of mathematical objects such as *scalars*, *vectors* and *matrices*. A scalar has a single numerical value, whereas a vector has

J. Vince, *Quaternions for Computer Graphics*,
DOI 10.1007/978-0-85729-760-0_2, © Springer-Verlag London Limited 2011

two or more numbers that encode the vector's magnitude and direction. A matrix is a rectangular array of numbers that may have all sorts of attributes.

Decimal numbers form the set of *reals* identified by $\mathbb{R}$. Such numbers are signed and can be organised as a line which stretches towards $-$ infinity and $+$ infinity and includes zero. The concept of infinity is a strange one, and was investigated by the German mathematician, Georg Cantor (1845–1918). Cantor also invented set theory and proved that real numbers are more numerous than natural numbers. Fortunately, we don't need to employ such concepts within this book.

2.2.3 Integers

The set of *integers* $\mathbb{Z}$ embrace the natural numbers and their negatives:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

$\mathbb{Z}$ stands for *Zahlen*—the German for 'numbers'.

2.2.4 Rational Numbers

The set of *rational* numbers is $\mathbb{Q}$, and contains numbers of the form:

$$\frac{a}{b}$$

where $a, b \in \mathbb{Z}$ and $b \neq 0$.

2.3 Arithmetic Operations

We manipulate numbers using the arithmetic operations addition, subtraction, multiplication and division, whose result is *closed* or not, or *undefined*, depending on the underlying set. For example, when we add two natural numbers together, the result is *always* another natural number and therefore, the operation is closed:

$$3 + 4 = 7.$$

However, when we subtract two natural numbers, the result may not necessarily be a natural number. For instance, although

$$6 - 2 = 4$$

is a closed operation,

$$2 - 6 = -4$$

is not closed, because -4 is not a member of the set of natural numbers.

The product of two natural numbers is *always* a closed operation, however, division causes some problems. To begin with, dividing an even natural number by 2 is a closed operation:

$$16/2 = 8.$$

Whereas, dividing an odd natural number by an even natural number gives rise to a decimal quantity:

$$7/2 = 3.5$$

and does not close because 3.5 does not belong to the set of natural numbers. In the language of sets, this is written

$$3.5 \notin \mathbb{N}$$

where $\notin$ means *does not belong to*.

Multiplying any number by zero results in zero—which is a closed operation; however, dividing any number by zero is undefined, and has to be excluded.

Real numbers do not have any of the problems associated with natural numbers, and there is closure on addition, multiplication and division:

$$\begin{aligned} a+b=c \quad & a,b,c \in \mathbb{R} \\ ab=c \quad & a,b,c \in \mathbb{R} \\ a/b=c \quad & a,b,c \in \mathbb{R} \text{ and } b \neq 0. \end{aligned}$$

Note that ab is shorthand for $a \times b$.

2.4 Axioms

When we construct algebraic expressions we employ specific laws called *axioms*. For addition and multiplication, we know that the grouping of numbers makes no difference to the end result: e.g. $2 + (4 + 6) = (2 + 4) + 6$ and $2 \times (3 \times 4) = (2 \times 3) \times 4$. This is the *associative axiom* and is expressed as:

$$\begin{aligned} a+(b+c) &= (a+b)+c \\ a(bc) &= (ab)c. \end{aligned}$$

We also know that order makes no difference to the end result when adding or multiplying: e.g. $2 + 6 = 6 + 2$ and $2 \times 6 = 6 \times 2$. This is the *commutative axiom* and is expressed as:

$$\begin{aligned} a+b &= b+a \\ ab &= ba. \end{aligned}$$

Algebraic expressions contain all sorts of products involving a single real number and a string of reals that obey the *distributive axiom*:

$$a(b+c) = ab + ac$$
$$(a+b)(c+d) = ac + ad + bc + bd.$$

The reason why we have reviewed these axioms is that they should not be regarded as carved in mathematical stone, and apply to everything that is invented. For when we come to quaternions we will discover that they do not obey the commutative axiom, which is not that strange. If you have used matrices you will know that matrix multiplication is also non-commutative, but is associative.

2.5 Expressions

Using the above axioms we are able to construct all sorts of expressions such as:

$$a(2+c) - d/e + a - 10$$
$$g/(ac - bd) + h/(de - fg).$$

We also employ notation for raising a quantity to some power such as n^2. This notation introduces another set of observations:

$$a^n a^m = a^{n+m}$$
$$\frac{a^n}{a^m} = a^{n-m}$$
$$(a^n)^m = a^{nm}$$
$$\frac{a^n}{a^n} = a^0 = 1$$
$$\frac{1}{a^n} = a^{-1}$$
$$a^{1/n} = \sqrt[n]{a}.$$

Next, we have to include all sorts of functions such as square-roots, sines and cosines, which may seem rather innocent. But we must be wary of them. For example, $\sqrt{16} = 4$ by convention. However, $x^2 = 16$ has two solutions: $\pm\sqrt{16} = \pm 4$. Whereas, there is no natural or real number solution for $\sqrt{-16}$. Consequently, the expression $\sqrt{a}$ has no real roots if $a < 0$.

Similarly, when working with trigonometric functions such as sine and cosine, we must remember that these take on a range of values between -1 and $+1$, including 0, which means that if they are employed as a denominator, the result could be undefined. For example, this expression is undefined if $\sin\alpha = 0$

$$\frac{a}{\sin\alpha}.$$

2.6 Equations

Next, we come to equations where we assign the value of an expression to a variable. In most situations the assignment is straightforward and leads to a real result such as

$$x^2 - 16 = 0$$

where $x = \pm 4$. But what is interesting is that just by reversing the sign to

$$x^2 + 16 = 0$$

we create an equation for which there is no real solution. However, there is a *complex* solution, which is the subject of Chap. 3.

2.7 Ordered Pairs

An *ordered pair* or *couple* (a, b) is an object having two entries, coordinates or projections, where the first or left entry, is distinguishable from the second or right entry. For example, $(a,\ b)$ is distinguishable from (b, a) unless $a = b$. Perhaps the best example of an ordered pair is (x, y) that represents a point on the plane, where the order of the entries is always the x-coordinate followed by the y-coordinate.

Ordered pairs and ordered triples are widely used in computer graphics to represent points on the plane (x, y), points in space (x, y, z), and colour values such as (r, g, b) and (h, s, v). In these examples, the fields are all real values. There is nothing to stop us from developing an algebra using ordered pairs that behaves like another algebra, and we will do this for complex numbers in Chap. 3 and quaternions in Chap. 5. For the moment, let's explore some ways ordered pairs can be manipulated.

Say we choose to describe a generic ordered pair as

$$a = (a_1, a_2) \quad a_1, a_2 \in \mathbb{R}.$$

We will define the addition of two such objects as

$$\begin{aligned} a &= (a_1, a_2) \\ b &= (b_1, b_2) \\ a + b &= (a_1 + b_1, a_2 + b_2). \end{aligned}$$

For example:

$$\begin{aligned} a &= (2, 3) \\ b &= (4, 5) \\ a + b &= (6, 8). \end{aligned}$$

We will define the product as

$$ab = (a_1 b_1,\ a_2 b_2)$$

which, using the above values, results in

$$ab = (8, 15).$$

Remember, we are in charge, and we define the rules.

Another rule will control how an ordered pair responds to scalar multiplication. For example:

$$\lambda(a_1, a_2) = (\lambda a_1, \lambda a_2) \quad \lambda \in \mathbb{R}$$
$$3(2, 3) = (6, 9).$$

With the above rules, we are in a position to write

$$\begin{aligned}(a_1,\ a_2) &= (a_1, 0) + (0, a_2)\\ &= a_1(1, 0) + a_2(0, 1)\end{aligned}$$

and if we square these unit ordered pairs $(1, 0)$ and $(0, 1)$ using the product rule, we obtain

$$(1, 0)^2 = (1, 0)$$
$$(0, 1)^2 = (0, 1)$$

which suggests that they behave like real numbers, and is not unexpected.

This does not appear to be very useful, but wait and see what happens in the context of complex numbers and quaternions.

2.8 Groups, Rings and Fields

Mathematicians employ a bewildering range of names to identify their inventions, which seemingly, appear on a daily basis. Even the name 'quaternion' is not original, and appears throughout history often in the context of "a quaternion of soldiers":

> "The Romans detached a quaternion or four men for a night guard ..." [19].

Without becoming too formal, let's explore some more mathematical structures that are relevant to the ideas contained in this book.

2.8.1 Groups

We have already covered the idea of a set, and what it means to belong to a set. We have also discovered that when we apply certain arithmetic operations to members of a set we can secure closure, non-closure, or the result is undefined.

When combining sets with arithmetic operations, it is convenient to create another entity: a *group*, which is a set, together with the axioms describing how elements of the set are combined. The set might contain numbers, matrices, vectors, quaternions, polynomials, etc., and are represented below as a, b and c.

The axioms employ the '$\circ$' symbol to represent any binary operation such as $+, -, \times$. And a group is formed from a set and a binary operation. For example, we may wish to form a group of integers under addition: $(\mathbb{Z}, +)$, or we may wish to examine whether quaternions form a group under the operation of multiplication: $(\mathbb{H}, \times)$.

To be a group, **all** the following axioms **must** hold for the set S. In particular, there must be a special *identity element* $e \in S$, and for each $a \in S$ there must exist an *inverse element* $a^{-1} \in S$, so that the following axioms are satisfied:

Closure:	$a \circ b \in S$	$a, b \in S$.
Associativity:	$(a \circ b) \circ c = a \circ (b \circ c)$	$a, b, c \in S$.
Identity element:	$a \circ e = e \circ a = a$	$a, e \in S$.
Inverse element:	$a \circ a^{-1} = a^{-1} \circ a = e$	$a, a^{-1}, e \in S$.

We describe a group as $(S, \circ)$, where S is the set and '$\circ$' the operation. For instance, $(\mathbb{Z}, +)$ is the group of integers under the operation of addition, and $(\mathbb{R}, \times)$ is the group of reals under the operation of multiplication.

Let's bring these axioms to life with three examples.

$(\mathbb{Z}, +)$: The integers $\mathbb{Z}$ form a group under the operation of addition:

$$\begin{aligned} \textit{Closure}: &\quad -23 + 24 = 1 \\ \textit{Associativity}: &\quad (2 + 3) + 4 = 2 + (3 + 4) = 9 \\ \textit{Identity}: &\quad 2 + 0 = 0 + 2 = 2 \\ \textit{Inverse}: &\quad 2 + (-2) = (-2) + 2 = 0. \end{aligned}$$

$(\mathbb{Z}, \times)$: The integers $\mathbb{Z}$ do **not** form a group under multiplication:

$$\begin{aligned} \textit{Closure}: &\quad -2 \times 4 = -8 \\ \textit{Associativity}: &\quad (2 \times 3) \times 4 = 2 \times (3 \times 4) = 24 \\ \textit{Identity}: &\quad 2 \times 1 = 1 \times 2 = 2 \\ \textit{Inverse}: &\quad 2^{-1} = 0.5 \quad (0.5 \notin \mathbb{Z}). \end{aligned}$$

Also, the integer 0 has no inverse.

$(\mathbb{Q}, \times)$: The group of non-zero rational numbers form a group under multiplication:

$$\begin{aligned} \textit{Closure}: &\quad \frac{2}{5} \times \frac{2}{3} = \frac{4}{15} \\ \textit{Associativity}: &\quad \left(\frac{2}{5} \times \frac{2}{3}\right) \times \frac{1}{2} = \frac{2}{5} \times \left(\frac{2}{3} \times \frac{1}{2}\right) = \frac{2}{15} \\ \textit{Identity}: &\quad \frac{2}{3} \times \frac{1}{1} = \frac{1}{1} \times \frac{2}{3} = \frac{2}{3} \\ \textit{Inverse}: &\quad \frac{2}{3} \times \frac{3}{2} = \frac{1}{1} \quad \left(\text{where } \frac{3}{2} = \left(\frac{2}{3}\right)^{-1}\right). \end{aligned}$$

2.8.2 Abelian Group

Lastly, an *abelian group*, named after the Norwegian mathematician, Neils Henrik Abel (1802–1829), is a group where the order of elements does not influence the result, i.e. the group is commutative. Thus there are five axioms: closure, associativity, identity element, inverse element, and commutativity:

Commutativity:	$a \circ b = b \circ a$	$a, b \in S.$

For example, the set of integers forms an abelian group under ordinary addition $(\mathbb{Z}, +)$. However, because 3D rotations do not generally commute, the set of all rotations in 3D space forms a non-commutative group.

2.8.3 Rings

A *ring* is an extended group, where we have a set of objects which can be added and multiplied together, subject to some precise axioms. There are rings of real numbers, complex numbers, integers, matrices, equations, polynomials, etc. A ring is formally defined as a system where $(S, +)$ and $(S, \times)$ are abelian groups and the distributive axioms:

Additive associativity:	$a + (b + c) = (a + b) + c$	$a, b, c \in S.$
Multiplicative associativity:	$a \times (b \times c) = (a \times b) \times c$	$a, b, c \in S.$
Distributivity:	$a \times (b + c) = (a \times b) + (a \times c)$	and
	$(a + b) \times c = (a \times c) + (b \times c)$	$a, b, c \in S.$

For example, we already know that the integers $\mathbb{Z}$ form a group under the operation of addition, but they also form a ring, as the set satisfies the above axioms:

$$2 \times (3 \times 4) = (2 \times 3) \times 4$$
$$2 \times (3 + 4) = (2 \times 3) + (2 \times 4)$$
$$(2 + 3) \times 4 = (2 \times 4) + (3 \times 4).$$

2.8.4 Fields

Although rings support addition and multiplication, they do not necessarily support division. However, as division is such an important arithmetic operation, the *field* was created to support it, with one proviso: division by zero is not permitted. Thus we have fields of real numbers $\mathbb{R}$, rational numbers $\mathbb{Q}$, and as we shall see, the complex numbers $\mathbb{C}$. However, we will discover that quaternions do not form a field, but they do form what is called a *division ring*.

It follows that every field is a ring, but not every ring is a field.

2.8.5 Division Ring

A *division ring* or *division algebra*, is a ring in which every element has an inverse element, with the proviso that the element is non-zero. The algebra also supports non-commutative multiplication. Here is a formal description of the division ring $(S, +, \times)$:

Additive associativity:	$(a+b)+c = a+(b+c)$	$a, b, c \in S$.
Additive commutativity:	$a+b = b+a$	$a, b \in S$.
Additive identity 0:	$0+a = a+0$	$a, 0 \in S$.
Additive inverse:	$a+(-a) = (-a)+a = 0$	$a, -a \in S$.
Multiplicative associativity:	$(a \times b) \times c = a \times (b \times c)$	$a, b, c \in S$.
Multiplicative identity 1:	$1 \times a = a \times 1$	$a, 1 \in S$.
Multiplicative inverse:	$a \times a^{-1} = a^{-1} \times a = 1$	$a, a^{-1} \in S, a \neq 0$.
Distributivity:	$a \times (b+c) = (a \times b) + (a \times c)$	and
	$(b+c) \times a = (b \times a) + (c \times a)$	$a, b, c \in S$.

In 1878 the German mathematician, Ferdinand Georg Frobenius (1849–1917), proved that there are only three associative division algebras: real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, and quaternions $\mathbb{H}$.

2.9 Summary

The objective of this chapter was to remind you of the axiomatic systems underlying algebra, and how the results of arithmetic operations can be open, closed, or undefined. Perhaps some of the ideas of ordered pairs, sets, groups, fields and rings are new, and they have been included as this notation is often used in association with quaternions.

All of these ideas emerge again when we consider the algebra of complex numbers and later on, quaternions.

2.9.1 Summary of Definitions

Ordered pair

An object with two distinguishable components: $(a,\ b)$ such that $(a, b) \neq (b, a)$ unless $a = b$.

Set

Definition: A set is a collection of objects.

Notation: $k \in \mathbb{Z}$ means k belongs to the set $\mathbb{Z}$.

$\mathbb{C}$: Set of complex numbers

$\mathbb{H}$: Set of quaternions

$\mathbb{N}$: Set of natural numbers

$\mathbb{Q}$: Set of rational numbers

$\mathbb{R}$: Set of real numbers

$\mathbb{Z}$: Set of integers.

Group

Definition: A group $(S, \circ)$ is a set S and a binary operation '$\circ$' and the axioms defining closure, associativity, an identity element, and an inverse element.

Closure:	$a \circ b \in S$	$a, b \in S.$
Associativity:	$(a \circ b) \circ c = a \circ (b \circ c)$	$a, b, c \in S.$
Identity element:	$a \circ e = e \circ a = a$	$a, e \in S.$
Inverse element:	$a \circ a^{-1} = a^{-1} \circ a = e.$	$a, a^{-1}, e \in S.$

Ring

Definition: A ring is a group whose elements can be added/subtracted *and* multiplied, using some precise axioms:

Additive associativity:	$a + (b + c) = (a + b) + c$	$a, b, c \in S.$
Multiplicative associativity:	$a \times (b \times c) = (a \times b) \times c$	$a, b, c \in S.$
Distributivity:	$a \times (b + c) = (a \times b) + (a \times c)$	and
	$(a + b) \times c = (a \times c) + (b \times c)$	$a, b, c \in S.$

Field

Definition: A field is a ring that supports division.

Division ring

Every element of a division ring has an inverse element, with the proviso that the element is non-zero. The algebra also supports non-commutative multiplication.

Additive associativity:	$(a + b) + c = a + (b + c)$	$a, b, c \in S.$
Additive commutativity:	$a + b = b + a$	$a, b \in S.$
Additive identity 0:	$0 + a = a + 0$	$a, 0 \in S.$
Additive inverse:	$a + (-a) = (-a) + a = 0$	$a, -a \in S.$
Multiplicative associativity:	$(a \times b) \times c = a \times (b \times c)$	$a, b, c \in S.$
Multiplicative identity 1:	$1 \times a = a \times 1$	$a, 1 \in S.$
Multiplicative inverse:	$a \times a^{-1} = a^{-1} \times a = 1$	$a, a^{-1} \in S,\ a \neq 0.$
Distributivity:	$a \times (b + c) = (a \times b) + (a \times c)$	and
	$(b + c) \times a = (b \times a) + (c \times a)$	$a, b, c \in S.$

http://www.springer.com/978-0-85729-759-4

Quaternions for Computer Graphics

Vince, J.

2011, XIV, 140 p., Hardcover
ISBN: 978-0-85729-759-4