

计算机图形学中的四元数

John Vince 著

郭飞 译

2023年

谨以此书献给 *Heidi*.

译序

序

50多年前，当我正在学习成为一名电气工程师时，我遇到了复数，它们被用来用 j 操作符表示异相电压和电流。我相信使用的是字母 j ，而不是 i ，因为后者代表电流。因此，从我学习的一开始，我就在脑海中清晰地描绘了一个假想的单位，它是一个旋转算子，可以在时间上推进或延缓电量。

当事情决定我要从事计算机编程而不是电气工程的职业时，我不需要复数，直到Mandlebrot关于分形的工作出现。但那只是暂时的阶段，我从来都不需要在我的任何电脑图形软件中使用复数。然而在1986年，当我加入飞行模拟行业时，我看到了一份关于四元数的内部报告，它被用于控制模拟飞机的旋转方向。

我仍然记得我对四元数的困惑，仅仅是因为它们包含了很多虚数。然而，经过大量研究，我开始了解它们是什么，但不知道它们是如何工作的。与此同时，我对数学的哲学方面产生了兴趣，并试图通过伯特兰·罗素的著作来理解数学的“真正意义”。因此，像 i 这样的概念是一个智力挑战。

我现在对虚数 i 不过是一个符号的想法感到满意，并且在代数的上下文中允许定义 $i^2 = -1$ 。我相信，试图发现它存在的更深层次的意义是徒劳的。尽管如此，它在数学中是一个令人惊叹的对象，我经常想是否会有类似的对象等待被发明出来。

当我开始写关于计算机图形学的数学书籍时，我学习了复分析，以便有信心地写复数。就在那时，我发现了向量和四元数发明背后的历史事件，主要是通过Michael Crowe的优秀著作《向量分析的历史¹》。这本书让我认识到理解数学发明如何以及为什么发生的重要性。

最近，我读到了Simon Altmann的书《旋转、四元数和双群²》，这本书提供了关于十九世纪四元数消亡³的进一步信息。Altmann非常热衷于确保Olinde Rodrigues的数学工作得到认可，后者发表了一个与汉密尔顿四元数生成的公式非常相似的公式。罗德里格斯发表论文的一个重要方面是，它比汉密尔顿在1843年发明四元数早了三年。然而，罗德里格斯并没有发明四元数代数——这个奖必须颁给汉密尔顿——但他确实理解三角函数中半角的重要性，三角函数用于围绕任意轴旋转点。

¹A History of Vector Analysis

²Rotations, Quaternions, and Double Groups

³demise, 感觉不应该译为消亡

任何使用过欧拉变换的人都会意识到它的缺点，尤其是它的阿喀琉斯之踵：万向节锁。因此，任何可以围绕任意轴旋转点的设备都是程序员工具包中受欢迎的补充。在平面和空间中有许多旋转点和帧的技术，我在我的书《计算机图形的旋转变换⁴》中详细介绍了这些技术。那本书还涵盖了欧拉-罗德里格斯参数化和四元数，但只是在提交了手稿准备出版之后，我才决定写这本专门关于四元数的书，以及它们是如何和为什么被发明的，以及它们在计算机图形学中的应用。

在研究这本书的同时，阅读William Rowan Hamilton和他的朋友P.G. Tait的一些早期书籍和论文非常有启发性。我现在明白了完全理解四元数的意义是多么困难，以及如何利用它们。当时，没有围绕任意轴旋转点的主要需求；然而，需要一个数学系统来处理矢量。最后，四元数不再是当月的宠儿，慢慢地淡出了人们的视线。尽管如此，能够表示向量并对它们进行算术操作是汉密尔顿的一个重大成就，尽管乔赛亚·吉布斯(Josiah Gibbs)有远见地创建了一个简单可行的代数框架。

在这本书中，我试图描述一些围绕四元数发明的历史，以及对四元数代数的描述。我绝不认为自己是四元数方面的权威。我只是想谈谈我是如何理解它们的，希望对你们有用。四元数有不同的表示方式，但我最喜欢的是有序对，这是我在Simon Altmann的书中发现的。

这本书分为八章。第一章和最后一章是对本书的介绍和总结，共六章，内容包括以下主题。关于数集和代数的第二章回顾了与本书其余部分相关的符号和语言。有关于数集、公理、有序对、群、环和域的章节。这为读者准备了非交换四元数积，以及为什么四元数被描述为除法环。

第三章回顾了复数，并展示了复数如何表示为有序对和矩阵。第四章继续这一主题，介绍了复平面，并展示了复数的旋转特征。它还为读者准备了一个在19世纪早期提出的问题：是否有一个相当于复数的3D？

第五章通过描述汉密尔顿的发明来回答这个问题：四元数及其相关代数。我在书中加入了一些历史信息，以便读者了解Hamilton著作的重要性。虽然有序对是表示法的主要形式，但我也包括了矩阵表示法。

为了让读者了解四元数的旋转特性，第6章回顾了3D旋转变换，特别是欧拉角和万向节锁。我还开发了一个矩阵，用于使用向量和矩阵变换围绕任意轴旋转一个点。

⁴Rotation Transforms for Computer Graphics

第7章是本书的重点，描述了四元数如何围绕任意轴旋转向量。本章以一些历史信息开始，并解释了不同的四元数乘积如何旋转点。虽然四元数很容易使用它们的复杂形式或有序对符号来实现，但它们也有一个矩阵形式，这是从第一性原理发展而来的。本章继续讨论特征值、特征向量、围绕偏移轴旋转、旋转参照系、插值四元数以及四元数和旋转矩阵之间的转换。

每一章都有很多实际的例子来说明如何计算方程，每章末尾会给出进一步的例子。

写这本书是一段非常愉快的经历，我相信你也会喜欢读它，并从书中发现一些新的东西。

我要感谢米德尔塞克斯大学荣誉读者Tony Crilly博士，他阅读了一份手稿草稿，并纠正和澄清了我的注释和解释。托尼在我的书《计算机图形的旋转变换》中执行了相同的任务。我绝对信任他的数学知识，我感谢他的建议和专业知识。然而，我仍然为我可能犯的任何代数错误承担全部责任。

我还要感谢Patrick Riley教授，他阅读了手稿的一些早期草稿，并提出了一些关于四元数的有趣技术问题。这样的问题让我意识到我对四元数的一些描述需要进一步澄清，希望这些描述已经得到纠正。

我现在已经在我的三本书中使用了 $\text{\LaTeX}2\epsilon$ ，并且对它的符号有了信心。尽管如此，我仍然需要致电施普林格的技术支持团队，感谢他们的帮助。

我不确定这是否是我的最后一本书。如果是的话，我要感谢贝弗利·福特，计算机科学的编辑主任，和海伦·德斯蒙德，施普林格英国计算机科学的副主编，他们在过去几年的专业支持。如果这不是我的最后一本书，那么我期待着在另一个项目上与他们再次合作。

Ringwood, UK

John Vince

目录

第1章	介绍	9
1.1	旋转变换	9
1.2	目标读者	9
1.3	本书的宗旨和目标	9
1.4	数学技术	10
1.5	本书中的假设	10
第2章	数集与代数	11
2.1	介绍	11
2.2	数集	11
2.2.1	自然数	11
2.2.2	实数	11
2.2.3	整数	12
2.2.4	有理数	12
2.3	算术运算	12
2.4	公理	13
2.5	表达式	14
2.6	等式	15
2.7	Ordered Pairs	15
2.8	Groups, Rings and Fields	17
2.9	Summary	21
2.10	Ordered pair	21
2.11	Set	22
2.12	Group	22

2.13 Ring 22

2.14 Field 22

2.15 Division ring 22

第 1 章 | 介绍

1.1 旋转变换

在计算机图形学中，我们使用变换来修改对象或虚拟摄像机的位置和方向。这种变换通常包括:缩放、平移和旋转。前两个变换很简单，但是旋转确实会引起问题。这是因为我们通常从围绕 x - fig -和 z -轴的单独旋转中构造一个旋转变换。尽管这样的转变行之有效，但还远远不够完美。真正需要的是一种直观、简单和准确的技术。

多年来，旋转变换包括方向余弦，欧拉角，欧拉-罗德里格斯参数化，四元数和多向量。最后两种技术是最新的，并且与历史相关。然而，这本书的主题是四元数，以及它们如何在计算机图形学中使用。

1.2 目标读者

这本书的目标读者学习或工作在计算机图形学和需要一个四元数的概述。他们可能就是我在互联网论坛上遇到过的询问四元数、它们如何工作以及如何编码的人。希望这本书能回答大部分问题。

1.3 本书的宗旨和目标

这本书的主要目的是向读者介绍四元数的主题，以及它们如何用于围绕任意轴旋转点。第二个目标是让读者意识到所有数学发现背后的人的层面。就我个人而言，我认为我们绝不能忽视这样一个事实:数学家也是人。尽管他们可能被赋予了非凡的数学技能，但他们恋爱、结婚、成家、死亡，留下了一座令人惊叹的知识大厦，我们都从中受益。

鼓励那些对数学的人类维度感兴趣的读者阅读四元数的发明，并发现爱、兴趣、坚韧、灵感和奉献是如何导致一项重大数学发现的。迈克尔·克罗的《矢量分析的历史》[10]是一本必不可少的书。这提供了导致四元数发明的事件的彻底分析，以及向量分析的出现。第二本书是Simon Altmann的《旋转、四元数和双群[1]》，除了提供了四元数代数的现代分析外，还介绍了Olinde Rodrigues，他比通常被公认为四元数之父的William Rowan Hamilton早三年发明了一些与四元数相关的数学。

Simon Altmann对四元数代数的分析对我自己对四元数的看法产生了深远的影响，我试图在接下来的章节中传达这一点。特别地，我采用了使用有序对来表示四元数的思想。

本书的首要目标是使读者能够设计和编码四元数算法。读完这本书后，这应该是一个简单的练习，尽管我们处理的是一个四维数学对象。

1.4 数学技术

一旦读者理解了四元数，就会认为它们很简单。然而，如果这是你第一次遇到他们，他们可能会显得很奇怪。但像所有事物一样，熟悉带来理解和信心。

为了描述四元数，我需要用到一点三角学，一些向量理论和矩阵代数。由于四元数被描述为“超复数”，因此有一章是关于复数的。

1.5 本书中的假设

很多时候，从事计算机图形工作的人——比如我自己——没有机会学习技术文献中经常使用的数学水平。因此，我故意在写这本书的时候，温和地介绍了从复杂代数到四元数代数的形式数学符号。

第 2 章 | 数集与代数

2.1 介绍

在本章中，我们将回顾数集的一些基本思想，以及如何用算术和代数方法处理它们。我们简要地看一下表达式和方程，以及用于构造和求值的规则。这些反过来又揭示了用所谓的复数扩展日常数字的需要。

本章的第二部分用于定义组、环和域。

2.2 数集

2.2.1 自然数

自然数是整数1,2,3,4等，根据定义(DIN 5473)，自然数的集合和零 $\{0, 1, 2, 3, 4, \dots\}$ 由符号 \mathbb{N} 表示，我们使用：

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

该语句

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

意味着 k 属于集合 \mathbb{N} ，其中 \in 表示属于，或者换句话说， k 是一个自然数。我们在本书中使用这种符号，以确保对所使用的数值量的类型没有混淆。

\mathbb{N}^* 用于表示集合 $\{1, 2, 3, 4, \dots\}$ 。

2.2.2 实数

科学计算使用大量的数学对象，如标量、向量和矩阵。标量只有一个数值，而矢量有两个或两个以上的数字来编码矢量的大小和方向。矩阵是一个矩形数组

的数字，可能有各种各样的属性。

十进制数构成由 \mathbb{R} 标识的实数集。这样的数字是有符号的，可以组织成一条线，延伸到 $-\infty$ 和 $+\infty$ ，其中包括0。无限的概念很奇怪，德国数学家康托(Georg Cantor, 1845-1918)研究过这个概念。康托尔还发明了集合论，证明了实数比自然数多。幸运的是，我们不需要在本书中使用这些概念。

2.2.3 整数

整数集 \mathbb{Z} 包含自然数及其负数：

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

\mathbb{Z} 代表zahlen——德语“数字”的意思。

2.2.4 有理数

有理数的集合是 \mathbb{Q} ，包含如下形式的数：

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

其中 $a, b \in \mathbb{Z}$ 且 $b \neq 0$.

2.3 算术运算

我们使用加法、减法、乘法和除法运算来操作数字，其结果是闭的还是不闭的，或者是未定义的，这取决于底层集合。例如，当我们将两个自然数相加时，结果总是另一个自然数，因此，运算是封闭的：

$$3 + 4 = 7.$$

然而，当我们减去两个自然数时，结果不一定是一个自然数。例如，尽管

$$6 - 2 = 4$$

是一个封闭的操作，

$$2 - 6 = -4$$

不是封闭的，因为 -4 不是自然数集合中的一员。两个自然数的乘积通常是一个封闭的运算，但是除法会引起一些问题。首先，将一个偶数除以 2 是一个封闭运算：

$$16/2 = 8.$$

然而，将一个奇数自然数除以一个偶数自然数得到一个十进制数：

$$7/2 = 3.5$$

并且不封闭，因为 3.5 不属于自然数集合。这是用集合语言写的

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

其中 \notin 表示不属于。

将任何数字乘以零都得到零——这是一个封闭运算；然而，任何数字除以零都是没有定义的，必须排除。

实数没有任何与自然数相关的问题，并且在加法、乘法和除法上有闭包：

$$a + b = c \quad a, b, c \in \mathbb{R}$$

$$ab = c \quad a, b, c \in \mathbb{R}$$

$$a/b = c \quad a, b, c \in \mathbb{R} \text{ and } b \neq 0.$$

注意， ab 是 $a \times b$ 的简写。

2.4 公理

当我们构造代数表达式时，我们使用称为公理的特定定律。对于加法和乘法，我们知道数字的分组对最终结果没有影响：例如 $2 + (4 + 6) = (2 + 4) + 6$ 和 $2 \times (3 \times 4) = (2 \times 3) \times 4$ 。这是结合律公理，表示为：

$$a + (b + c) = (a + b) + c$$

$$a(bc) = (ab)c.$$

我们也知道，当加或乘时，顺序对最终结果没有影响：例如 $2 + 6 = 6 + 2$ 和 $2 \times 6 = 6 \times 2$ 。这是交换公理，表示为：

$$a + b = b + a$$

$$ab = ba.$$

代数表达式包含各种各样的乘积，涉及一个实数和一串实数，它们服从分配律：

$$a(b + c) = ab + ac$$

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

我们回顾这些公理的原因是，它们不应该被视为刻在数学石头上的，而适用于所有被发明的东西。因为当我们讲到四元数时，我们会发现它们不遵守交换公理，这并不奇怪。如果你用过矩阵，你就会知道矩阵乘法也是不可交换的，但是是结合的。

2.5 表达式

使用上述公理，我们能够构造各种表达式，例如：

$$a(2 + c) - d/e + a - 10$$

$$g/(ac - bd) + h/(de - fg).$$

我们还使用符号来提高一个量的幂，如 n^2 。这个符号引入了另一组观察结果：

$$a^n a^m = a^{n+m}$$

$$\frac{a^n}{a^m} = a^{n-m}$$

$$(a^n)^m = a^{nm}$$

$$\frac{a^n}{a^n} = a^0 = 1$$

$$\frac{1}{a^n} = a^{-1}$$

$$a^{1/n} = \sqrt[n]{a}.$$

接下来，我们必须包括各种各样的函数，比如平方根、正弦和余弦，这些函数看起来相当简单。但我们必须警惕他们。例如，按惯例， $\sqrt{16} = 4$ 。但是， $x^2 = 16$ 有两个解： $\pm\sqrt{16} = \pm 4$ 。然而， $\sqrt{-16}$ 不存在自然数或实数解。因此，如果 $a < 0$ ，表达式 \sqrt{a} 就没有实根。

类似地，在处理正弦和余弦等三角函数时，我们必须记住，这些函数的值范围在 -1 和 $+1$ 之间，包括 0 ，这意味着如果将它们用作分母，结果可能是未定义的。例如，如果 $\sin \alpha = 0$ ，则此表达式未定义

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

2.6 等式

接下来，我们来到方程，我们将表达式的值赋给变量。在大多数情况下，任务是直接的，并导致一个真实的结果，如

$$x^2 - 16 = 0$$

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:

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

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

$$\begin{aligned}
 (1, 0)^2 &= (1, 0) \\
 (0, 1)^2 &= (0, 1)
 \end{aligned}$$

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.

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:

Associativity:

Identity element:

Inverse element: $a \circ b \in S$

$$(a \circ b) \circ c = a \circ (b \circ c)$$

$$a \circ e = e \circ a = a$$

$$a \circ a^{-1} = a^{-1} \circ a = e \quad a, b \in S$$

$$a, b, c \in S$$

$$a, e \in S.$$

$$a, a^{-1}, e \in S$$

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:

$$\text{Closure: } -23 + 24 = 1$$

$$\text{Associativity: } (2 + 3) + 4 = 2 + (3 + 4) = 9$$

$$\text{Identity: } 2 + 0 = 0 + 2 = 2$$

$$\text{Inverse: } 2 + (-2) = (-2) + 2 = 0.$$

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

$$\text{Closure: } -2 \times 4 = -8$$

$$\text{Associativity: } (2 \times 3) \times 4 = 2 \times (3 \times 4) = 24$$

$$\text{Identity: } 2 \times 1 = 1 \times 2 = 2$$

$$\text{Inverse: } 2^{-1} = 0.5 \quad (0.5 \notin \mathbb{Z}).$$

Also, the integer 0 has no inverse.

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

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

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.

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:

$$\begin{aligned}
\text{Additive associativity: } & a + (b + c) = (a + b) + c & a, b, c \in S. \\
\text{Multiplicative associativity: } & a \times (b \times c) = (a \times b) \times c & a, b, c \in S. \\
\text{Distributivity: } & a \times (b + c) = (a \times b) + (a \times c) \quad \text{and} \\
& (a + b) \times c = (a \times c) + (b \times c) & a, b, c \in S.
\end{aligned}$$

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:

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

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

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

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.

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:

$$a \times (b + c) = (a \times b) + (a \times c) \text{ and}$$

$$(b + c) \times a = (b \times a) + (c \times a) \quad a, b, c \in S.$$

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.

Summary of Definitions

2.10 Ordered pair

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

2.11 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.

2.12 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: $a \circ a^{-1} = a^{-1} \circ a = e$.
 $a, a^{-1}, e \in S$.

2.13 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 $(a + b) \times c = (a \times c) + (b \times c)$ $a, b, c \in S$.

2.14 Field

Definition: A field is a ring that supports division.

2.15 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:

Additive commutativity:

Additive identity 0 :

Additive inverse:

Multiplicative associativity: $(a \times b) \times c = a \times (b \times c)$

Multiplicative identity 1: $1 \times a = a \times 1$

Multiplicative inverse:

Distributivity:

$$(a + b) + c = a + (b + c) \quad a, b, c \in S.$$

$$a + b = b + a \quad a, b \in S.$$

$$0 + a = a + 0 \quad a, 0 \in S.$$

$$a + (-a) = (-a) + a = 0 \quad a, -a \in S.$$

$$(a \times b) \times c = a \times (b \times c) \quad a, b, c \in S.$$

$$1 \times a = a \times 1 \quad a, 1 \in S.$$

$$a \times a^{-1} = a^{-1} \times a = 1 \quad a, a^{-1} \in S, a \neq 0.$$

$$a \times (b + c) = (a \times b) + (a \times c) \quad \text{and}$$

$$(b + c) \times a = (b \times a) + (c \times a) \quad a, b, c \in S.$$