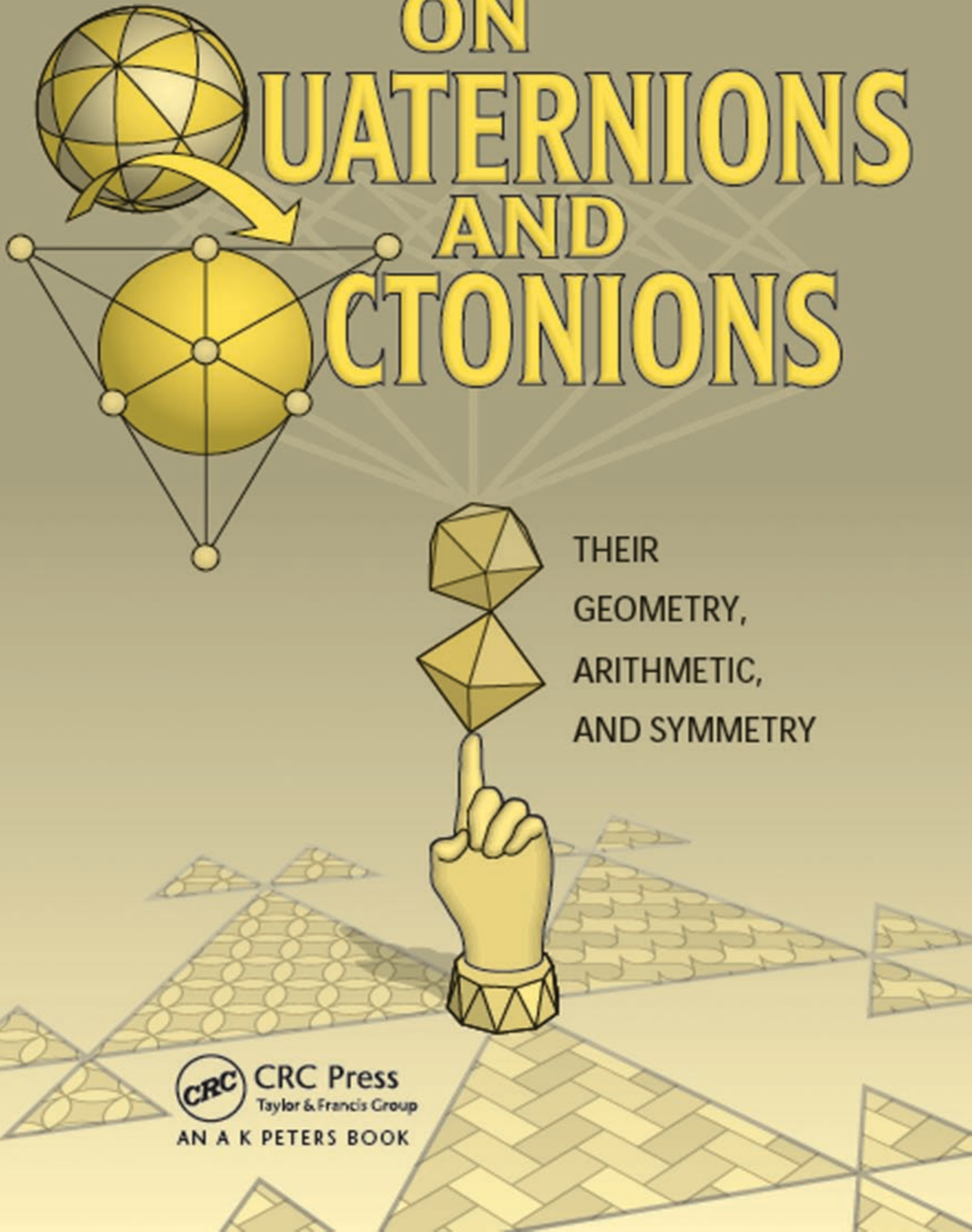
JOHN H. CONWAY
DEREK A. SMITH

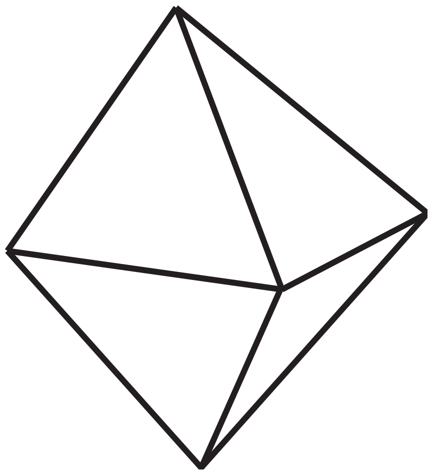
ON QUATERNIONS AND OCTONIONS



THEIR GEOMETRY, ARITHMETIC, AND SYMMETRY

CRC Press
Taylor & Francis Group
AN A K PETERS BOOK

On Quaternions and Octonions



On Quaternions and Octonions:

Their Geometry, Arithmetic, and Symmetry

John H. Conway
Derek A. Smith

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN A K PETERS BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20131202

International Standard Book Number-13: 978-1-56881-134-5 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Conway, John Horton.
On quaternions and octonions / John H. Conway, Derek A. Smith.
p. cm.
ISBN 978-1-56881-134-5
1. Quaternions. 2. Cayley numbers. I. Smith, Derek Alan, 1970-. II. Title.

QA196.C66 2002
512'.5-dc21 2002035555

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

This book is dedicated to Lilian Smith and Gareth Conway,
without whom we would have finished this book much sooner.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Contents

Preface

This is a book on the geometry and arithmetic of the quaternion and octonion algebras. These algebras are intimately connected with special features of the geometry of the appropriate Euclidean spaces, which makes them a useful tool for understanding symmetry groups in low dimensions. For example, there is a special relationship between 3- and 4-dimensional groups that is clearly revealed by the quaternions because a 3-dimensional rotation can be specified by a single quaternion, and a 4-dimensional one by a pair of quaternions. The details are subtle, because certain maps are 2-to-1 instead of 1-to-1.

Many people are familiar with quaternions, so in the first part of our book we take their properties for granted and use them to enumerate the finite groups in 3 and 4 dimensions (following a similar treatment of 2-dimensional groups using complex numbers). We close the first part with a discussion of what geometry says about the arithmetic of Hurwitz's integral quaternions, and in particular establish the unique factorization theorem.

A major theme of the second part of our book is the remarkable "triality symmetry" that arises in connection with the octonions. However, the properties of the octonions are not so familiar, so we start by proving the celebrated theorem of Hurwitz that $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$ are the only algebras of their kind, since this also yields the best way to construct them. Using the methods of the proof, we show that these algebras form Moufang loops, and we study Moufang loops in a way that exhibits the triality, applying this to the particular case of the 8-dimensional orthogonal group.

The study of the arithmetic of the integral octonions defined by Dickson, Bruck, and Coxeter has not progressed very far. In the final chapters of our book, we improve this situation in several ways. We use a method due to Rehm to create a new factorization theory for the integral octonions.

We also describe the action of their automorphism group on important subrings, finding maximal subgroups to be stabilizers of certain of these. In one case, we are led to read the integral octonions mod 2.

We close with a very brief chapter on the celebrated octonion projective plane.

Very complicated arguments have been needed to deduce properties of the algebras over arbitrary fields from minimal hypotheses such as the alternative law. We have preferred to keep our arguments simple by starting from the composition property and restricting to the classical algebras over the real field.

The programmers of video games make heavy use of quaternions, as do the controllers of spacecraft, since in both these disciplines it is necessary to compose rotations with minimal computation. We have eschewed writing of these and other practical applications, which are amply treated in the recent book of Kuipers [29].

We thank John Baez, Warren Smith, Daniel Allcock, Warren Johnson, and Mohammed Abouzaid for their useful comments on various things in the book. Derek thanks the Academic Research Committee at Lafayette College for its financial support through a summer research fellowship. Alice and Klaus Peters have been the most helpful publishers one could imagine. We thank them, Jonathan Peters, Heather Holcombe, Darren Wotherspoon, Ariel Jaffe, and Susannah Peters for their work on this book. Finally, we thank our wives Barbara and Diana for their patience.

John Conway and Derek Smith

November 2002

I

The Complex Numbers and Their Applications to 1- and 2-Dimensional Geometry

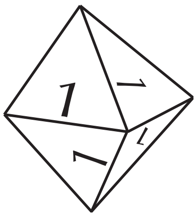
We suppose you understand the real numbers! The complex numbers are formal expressions $x_0 + x_1 i$ (with x_0, x_1 real), combined by

$$(x_0 + x_1 i) + (y_0 + y_1 i) = (x_0 + y_0) + (x_1 + y_1)i$$

$$(x_0 + x_1 i)(y_0 + y_1 i) = (x_0 y_0 - x_1 y_1) + (x_0 y_1 + x_1 y_0)i;$$

that is to say, they constitute the algebra over the reals generated by a basic unit i that satisfies

$$i^2 = -1.$$



Introduction

1.1 The Algebra $\mathbb{R}$ of Real Numbers

After the work of the ancient Greek and later geometers, it is customary to parametrize the Euclidean line by the algebra $\mathbb{R}$ of real numbers. In this parametrization, the distance between a and b is the absolute value of their difference, $|a-b|$, which can also be written as $\sqrt{(a-b)^2}$. It is an important property of $\mathbb{R}^1$ that $|xy| = |x||y|$.

The isometries (i.e., the maps that preserve distance) of $\mathbb{R}^1$ are the

$$\textbf{translations} \quad x \to k + x \quad \text{and} \quad \textbf{reflections} \quad x \to k - x.$$

So the 1-dimensional general orthogonal group GO_1 consists of the two isometries $x \to \pm x$ that fix the origin.

The real numbers $\mathbb{R}$ contain the rational numbers $\mathbb{Q}$, and in particular, the (rational) integers $\mathbb{Z}$ that are the subject of number theory. In particular, they satisfy the unique factorization theorem (the essentials of which were also discovered by Euclid) whose traditional statement is that each positive integer is a product of (positive) prime numbers in a way that is unique up to order.

For the purposes of this book, it is better to delete the positivity requirement, when the statement becomes that each positive or negative integer is a product of positive or negative primes in a way that is unique up to order and sign change.

We briefly sketch the traditional proof, which makes essential use of the fact that any number n of $\mathbb{Z}$ can be divided by any nonzero number d to leave a remainder r strictly smaller than the divisor. (In fact, we can make $|r| \leq \frac{1}{2}|d|$; see Figure 1.1.)

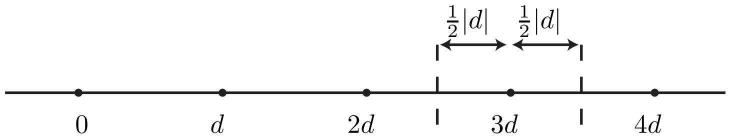


Figure 1.1. Maximal remainder for $\mathbb{Z}$.

An **ideal** of $\mathbb{Z}$ is a subset $\mathcal{I}$ with the following properties:

- $0 \in \mathcal{I}$
- The sum of any two elements in $\mathcal{I}$ is in $\mathcal{I}$
- All of the multiples of any member of $\mathcal{I}$ by arbitrary integers are again in $\mathcal{I}$

It is a **principal ideal** only if it consists of all multiples of some integer g, called the generator.

Then we have

Lemma 1. *Any ideal of $\mathbb{Z}$ is principal.*

Proof. $\{0\}$ is principal. If $\mathcal{I} \neq \{0\}$, let d be a non-zero element of $\mathcal{I}$ with smallest absolute value. We show that $\mathcal{I}$ must consist of just the multiples of d. For if $\mathcal{I}$ contains any other integer, say n, we can write

$$n = qd + r, \quad \text{where } 0 \leq r < |d|.$$

But since n and d are in the ideal, so is r (of smaller absolute value than d), a contradiction.

We use this to prove

Lemma 2. *If p is a prime number, then p divides a product if and only if it divides one of the factors.*

Proof. It will suffice to suppose that p divides ab. Then the ideal of numbers of the form $mp + na$ must be a principal ideal whose generator g must be a divisor of p, and so can be chosen to be p or 1. But if $g = p$, then p divides a, while $g = 1$ implies $1 = mp + na$ for some m, n, and so $b = mpb + nab$, which is a multiple of p.

These lemmas combine to prove the theorem, for if

$$p_1 p_2 \dots \quad \text{and} \quad q_1 q_2 \dots$$

are two prime factorizations of the same number, we can deduce that q_1 must divide one of the p_i, and so be that p_i—say p_1—up to sign. After cancelling p_1, we find that q_2 must equal p_2 (say) up to sign, etc.

1.2 Higher Dimensions

The results with which we have just opened Chapter 1 concern 1-dimensional space $\mathbb{R}^1$ and its sublattice $\mathbb{Z}$. It is the purpose of this book to generalize these results to certain higher dimensions.

Chapter 2 handles the 2-dimensional case, where we discuss plane geometry in terms of the algebra $\mathbb{C}$ of complex numbers, and say something about its two most famous arithmetics $\mathbb{Z}[i]$ of Gaussian integers and $\mathbb{Z}[\omega]$ of Eisenstein integers.

It is a remarkable fact that the analogous discussion of 3-dimensional geometry requires a 4-dimensional algebra, that of *quaternions*. This made them hard to discover, as is seen in the famous story Baez quotes later in this chapter.

In Chapter 3 we define the quaternions $\mathbb{H}$ and use them to enumerate the finite groups of 3-dimensional isometries. In Chapter 4, we provide a similar service for 4-dimensional space, which is of course the natural setting for the quaternions.

The correspondence between chapters and dimensions is broken in the next few chapters. Chapter 5 discuss what it means for a quaternion to be "integral." We find that Hurwitz's system of integers has a form of unique factorization, and so must be preferred to the more naive system of Lipschitz.

What other algebras have properties like those of the quaternions? It turns out that the most important property $[xy] = [x][y]$ is the one that defines "composition algebras." In Chapter 6 we prove Hurwitz's famous result that the only composition algebras are the famous ones in dimensions 1, 2, 4, and 8. It turns out that multiplication in the 8-dimensional composition algebra $\mathbb{O}$ of *octonions* is not associative, but it satisfies the Moufang laws, an intriguing substitute for associativity. In Chapter 7, we explain how the Moufang laws may be regarded as a symmetry condition.

Chapter 8, analogous to Chapter 4, discusses octonions and 8-dimensional geometry. We discuss Cartan's wonderful "triality" of PSO_8, and use it to prove our "7-multiplication theorem."

Chapter 9, analogous to Chapter 5, explores the correct definition of integrality for octonions and then erects the correct factorization theory for it. The next two chapters study the automorphisms of the octavian integers in great detail. Chapter 10 explores the units, and Chapter 11 shows how more information can be obtained by working modulo 2.

Finally, Chapter 12 uses the octonions to construct a most intriguing projective plane.