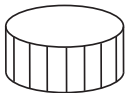
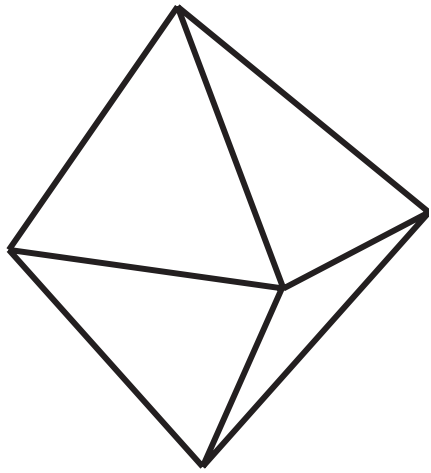


On Quaternions and Octonions



On Quaternions and Octonions:

Their Geometry, Arithmetic, and Symmetry

John H. Conway
Derek A. Smith

A K Peters
Natick, Massachusetts

Editorial, Sales, and Customer Service Office

A K Peters, Ltd.
63 South Avenue
Natick, MA 01760
www.akpeters.com

Library of Congress Cataloging-in-Publication Data

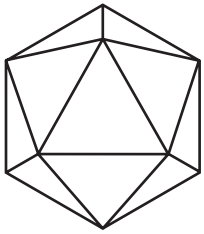
Conway, John Horton.
On quaternions and octonions : their geometry, arithmetic, and symmetry / John H. Conway, Derek A. Smith.
p. cm.
ISBN 1-56881-134-9
1. Quaternions. 2. Cayley numbers. I. Smith, Derek Alan, 1970- II. Title.

QA196 .C66 2002
512'.5–dc21

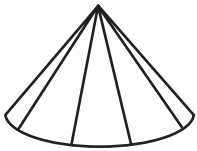
2002035555

Printed in Canada
07 06 05 04 03 10 9 8 7 6 5 4 3 2 1

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



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.

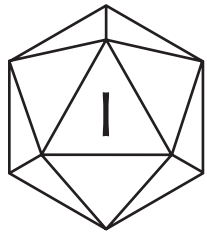
Very complicated arguments have been needed to deduce properties of the algebras over arbitrary fields from minimal hypotheses such as the alternative law. We have preferred to keep our arguments simple by starting from the composition property and restricting to the classical algebras over the real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



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

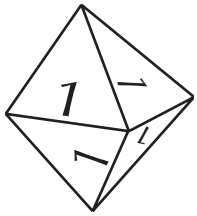
We suppose you understand the real numbers! The complex numbers are formal expressions $x_0 + x_1 i$ (with x_0, x_1 real), combined by

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

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

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.)

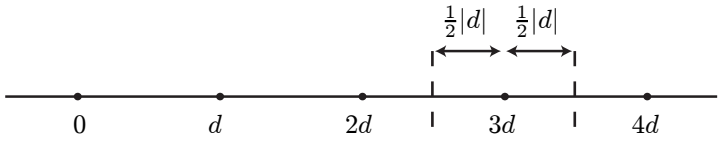


Figure 1.1. Maximal remainder for $\mathbb{Z}$.

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

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

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.

1.3 The Orthogonal Groups

The ***G*eneral *O*rthogonal group** GO_n is the set of all isometries of n-dimensional Euclidean space $\mathbb{R}^n$ that fix the origin. The following lemma implies that GO_n is generated by reflections.

Lemma 3. *Every element α of GO_n that fixes a k-dimensional subspace can be written as a product of at most $n-k$ reflections.*

Proof. Take a vector v *not* fixed by α, say $v \to w$. Then reflection in $v-w$ restores w to v (see Figure 1.2) while fixing any vector u fixed by α (for $v-w$ is orthogonal to u since we must have $[u,v]=[u,w]$).

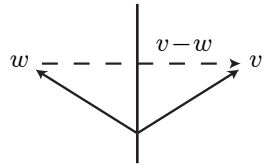


Figure 1.2. Reflection in $v-w$.

We shall suppose that the reader is familiar with the notion of determinant. Since the determinant of a reflection is -1, the determinant of any element of GO_n is ± 1, and the elements of determinant $+1$ form a subgroup of index 2, the ***S*pecial *O*rthogonal group** SO_n. The product of any two reflections (say in r and s) is a simple rotation — it rotates the plane $\langle r,s\rangle$ through some angle and fixes the $n-2$ dimensional space orthogonal to that plane. By grouping reflections in pairs, we see that SO_n is generated by these simple rotations.

Finally, if in GO_n and SO_n we ignore the difference between α and $-\alpha$, we obtain PGO_n and PSO_n, the ***P*rojective *G*eneral** and ***P*rojective *S*pecial *O*rthogonal groups**. The relationship between the four groups GO_n, SO_n, PGO_n, and PSO_n depends on the parity of the dimension and is discussed in Chapters 3 and 4.

It is a consequence of the existence of complex numbers that SO_2 and PSO_2 are commutative; of the existence of quaternions that $PSO_4 \cong PSO_3 \times PSO_3$; and of the existence of octonions that PSO_8 has a "triality" automorphism of order 3.

1.4 The History of Quaternions and Octonions

When we planned this book, we intended to put our own description of the history of our subject into this chapter. Time has prevented us from

doing so, but fortunately we have been saved by John Baez [5]. With his permission, we quote from his paper, "The Octonions":

> Most mathematicians have heard the story of how Hamilton invented the quaternions. In 1835, at the age of 30, he had discovered how to treat complex numbers as pairs of real numbers. Fascinated by the relation between $\mathbb{C}$ and 2-dimensional geometry, he tried for many years to invent a bigger algebra that would play a similar role in 3-dimensional geometry. In modern language, it seems he was looking for a 3-dimensional normed division algebra. His quest built to its climax in October 1843. He later wrote to his son, "Every morning in the early part of the above-cited month, on my coming down to breakfast, your (then) little brother William Edwin, and yourself, used to ask me: 'Well, Papa, can you *multiply* triplets?' Whereto I was always obliged to reply, with a sad shake of the head: 'No, I can only *add* and subtract them'." The problem, of course, was that there exists no 3-dimensional normed division algebra. He really needed a 4-dimensional algebra.
>
> Finally, on the 16th of October, 1843, while walking with his wife along the Royal Canal to a meeting of the Royal Irish Academy in Dublin, he made his momentous discovery. "That is to say, I then and there felt the galvanic circuit of thought *close*; and the sparks which fell from it were the *fundamental equations between* i, j, k; *exactly such* as I have used them ever since." And in a famous act of mathematical vandalism, he carved these equations into the stone of the Brougham Bridge:
>
> $$i^2 = j^2 = k^2 = ijk = -1.$$
>
> One reason this story is so well-known is that Hamilton spent the rest of his life obsessed with the quaternions and their applications to geometry [21], [24]. And for a while, quaternions were fashionable. They were made a mandatory examination topic in Dublin, and in some American universities they were the only advanced mathematics taught. Much of what we now do with scalars and vectors in $\mathbb{R}^3$ was then done using real and imaginary quaternions. A school of "quaternionists" developed, which was led after Hamilton's death by Peter Tait of Edinburgh and Benjamin Peirce of Harvard. Tait wrote 8 books on the quaternions, emphasizing their applications to

physics. When Gibbs invented the modern notation for the dot product and cross product, Tait condemned it as a "hermaphrodite monstrosity." A war of polemics ensued, with luminaries such as Kelvin and Heaviside writing some devastating invective against quaternions. Ultimately the quaternions lost, and acquired a slight taint of disgrace from which they have never fully recovered [12].

Less well-known is the discovery of the octonions by Hamilton's friend from college, John T. Graves. It was Graves' interest in algebra that got Hamilton thinking about complex numbers and triplets in the first place. The very day after his fateful walk, Hamilton sent an 8-page letter describing the quaternions to Graves. Graves replied on October 26th, complimenting Hamilton on the boldness of the idea, but adding, "There is still something in the system which 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." And he asked: "If with your alchemy you can make three pounds of gold, why should you stop there?"

Graves then set to work on some gold of his own! On December 26th, he wrote to Hamilton describing a new 8-dimensional algebra, which he called the "octaves." He showed that they were a normed division algebra, and used this to express the product of two sums of eight perfect squares as another sum of eight perfect squares: the "eight squares theorem" [23].

In January 1844, Graves sent three letters to Hamilton expanding on his discovery. He considered the idea of a general theory of "2^m-ions," and tried to construct a 16-dimensional normed division algebra, but he "met with an unexpected hitch" and came to doubt that this was possible. Hamilton offered to publicize Graves' discovery, but being busy with work on quaternions, he kept putting it off. In July he wrote to Graves pointing out that the octonions were nonassociative: "$A \cdot BC = AB \cdot C = ABC$ if A, B, C be quaternions, but not so, generally, with your octaves." In fact, Hamilton first invented the term "associative" at about this time, so the octonions may have played a role in clarifying the importance of this concept.

Meanwhile the young Arthur Cayley, fresh out of Cambridge, had been thinking about the quaternions ever since Hamilton announced their existence. He seemed to be seeking relationships between the quaternions and hyperelliptic functions. In

> March of 1845, he published a paper in the *Philosophical Magazine* entitled "On Jacobi's Elliptic Functions, in Reply to the Rev. B. Bronwin; and on Quaternions" [9]. The bulk of this paper was an attempt to rebut an article pointing out mistakes in Cayley's work on elliptic functions. Apparently as an afterthought, he tacked on a brief description of the octonions. In fact, this paper was so full of errors that it was omitted from his collected works—except for the part about octonions [10].
>
> Upset at being beaten to publication, Graves attached a postscript to a paper of his own which was to appear in the following issue of the same journal, saying that he had known of the octonions ever since Christmas, 1843. On June 14th, 1847, Hamilton contributed a short note to the Transactions of the Royal Irish Academy, vouching for Graves' priority. But it was too late: the octonions became known as "Cayley numbers." Still worse, Graves later found that his eight squares theorem had already been discovered by C. F. Degen in 1818 [13], [14].
>
> Why have the octonions languished in such obscurity compared to the quaternions? Besides their rather inglorious birth, one reason is that they lacked a tireless defender such as Hamilton. But surely the reason for *this* is that they lacked any clear application to geometry and physics. The unit quaternions form the group SU_2, which is the double cover of the rotation group SO_3. This makes them nicely suited to the study of rotations and angular momentum, particularly in the context of quantum mechanics. These days we regard this phenomenon as a special case of the theory of Clifford algebras. Most of us no longer attribute to the quaternions the cosmic significance that Hamilton claimed for them, but they fit nicely into our understanding of the scheme of things. The octonions, on the other hand, do not.

Our attempts to understand the "cosmic significance" of the octonions have led to this book!

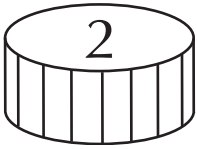
To Baez's brief history we add that although Hamilton really does seem to have been the first to construct the quaternions as an algebra, they have a prior history, starting with Euler's discovery of the 4-square identity (which really defines them) in 1748. Also, O. Rodrigues, in work culminating in a brilliant paper [38] of 1840, parametrized the general rotation by four parameters (often incorrectly called the Euler-Rodrigues parameters) that are in fact the coordinates of the corresponding quaternion. This makes him a precursor of Hamilton, since the multiplication rule he gives for

rotations is the same as Hamilton's 1843 formula for the product of two quaternions. For a fuller description of Rodrigues' work, see *Rotations, Quaternions, and Double Groups* by S. Altmann [3].

The most important later contributions relevant to this book are Hurwitz's characterization of composition algebras [26]; Dickson's work (see [15]), including his doubling rule and his discussion of "integrality"; and Coxeter's geometric [11] and Rankin's arithmetic [36] investigations of the integral octonions O. Here and elsewhere in the book we give very few references and historical remarks. We recommend that interested readers consult

http://www.akpeters.com/QANDO ,

which contains additional references and a link to the online version of Baez's paper.



Complex Numbers and 2-Dimensional Geometry

We suppose that our readers are familiar with the algebra of complex numbers. In this chapter we focus on their relation to the geometry of the Euclidean plane, as a prelude to the corresponding applications of quaternions and octonions to higher-dimensional Euclidean spaces. We also discuss the arithmetic of the two most interesting subrings of the complex numbers—the Gaussian and Eisenstein integers.

2.1 Rotations and Reflections

The geometrical properties of the complex numbers follow from the fact that they form a composition algebra for the Euclidean norm

$$N(x + iy) = x^2 + y^2,$$

which means that

$$N(z_1 z_2) = N(z_1)N(z_2).$$

This entails that multiplication by a fixed (nonzero) number z_0 multiplies all lengths by $\sqrt{N(z_0)}$; that is to say, it is a Euclidean similarity (see Figure 2.1).

In the important case when $N(z_0) = 1$, $z \to z_0 z$ is a Euclidean congruence, or **isometry**. Moreover, any such "unit" z_0 can be continuously reached from 1 by a path that traverses only units (see Figure 2.2), so this congruence can be obtained by a continuous motion from the identity. Such congruences are called **rotations**.

The standard formula

$$x' = x\cos\theta - y\sin\theta$$
$$y' = x\sin\theta + y\cos\theta$$

for a rotation follows immediately from the multiplication

$$(\cos\theta + i\sin\theta)(x + iy) = (x\cos\theta - y\sin\theta) + i(x\sin\theta + y\cos\theta)$$

and the definitions of the trigonometric functions (see Figure 2.3).

However, **reflections** are another kind of Euclidean congruence, exemplified by

$$x' = x$$
$$y' = -y$$

which corresponds to complex conjugation

$$\overline{x + iy} = x - iy.$$

We have

Theorem 1. *If u is a complex unit, then the map $z \to uz$ is a rotation, while $z \to u\overline{z}$ is a reflection.*

The matrices of these two are

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \text{ and } \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

whose determinants, 1 and -1, show that they belong respectively to SO_2 and $GO_2 \backslash SO_2$.

Moreover, every element (a_{ij}) of the 2-dimensional orthogonal group GO_2 is of one of these two types. For the first orthogonality condition $a_{11}^2 + a_{12}^2 = 1$ implies $a_{11} = \cos\theta$, $a_{12} = \sin\theta$ for some θ, and the remaining conditions imply $a_{21} = \mp\sin\theta$, $a_{22} = \pm\cos\theta$.

We have identified the 2-dimensional orthogonal groups:

Theorem 2. *SO_2 consists of all multiplications $z \to uz$ by complex units, while GO_2 consists of these together with the maps $z \to u\overline{z}$.*

This provides a topological identification of SO_2 as the circle of real angles θ, considered mod 2π. GO_2 has two components, each of which is a circle.

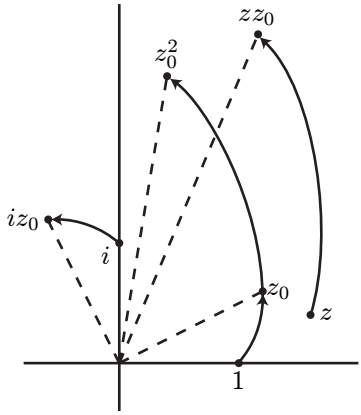


Figure 2.1. The Euclidean similarity $z \to zz_0$.

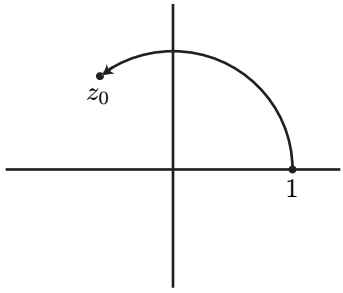


Figure 2.2. Euclidean congruences are connected to the identity.

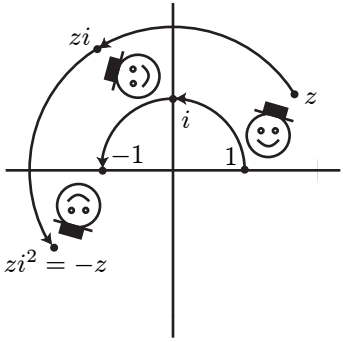


Figure 2.3. The Euclidean rotation $z \to zi$.

2.2 Finite Subgroups of GO_2 and SO_2

Let us consider the smallest positive θ for which the rotation through θ belongs to a given finite subgroup G of SO_2. Then θ has the form $\frac{2\pi}{m}$, for if m is the smallest positive integer for which $m\theta \geq 2\pi$, we must in fact have $m\theta = 2\pi$, since otherwise if $m\theta = 2\pi + \theta'$, we have $0 < \theta' < \theta$.

Also, G is generated by the rotation through $\frac{2\pi}{m}$, since if it contained a rotation through any other angle θ, we could write θ as a multiple of $\frac{2\pi}{m}$ plus a positive "remainder angle" ϕ strictly less than $\frac{2\pi}{m}$, a contradiction. This is the rotational or chiral point group $m\bullet$ in the "orbifold notation" (see Appendix).

So, we have proved that

Theorem 3. *The general finite subgroup of SO_2 is $m\bullet$, consisting of rotations through multiples of $\frac{2\pi}{m}$.*

The subgroups of SO_2 are called **chiral** ("handed") because they preserve the left- and right-handedness of 2-dimensional objects (see Figure 2.4). Correspondingly, the subgroups of GO_2 not contained in SO_2 are **achiral** ("unhanded") since they can reverse handedness (see Figure 2.5).

By adjoining the reflection in any line through the origin, we obtain the reflectional or achiral point group, denoted $*m\bullet$ in the orbifold notation. It is now easy to see that

Theorem 4. *The general finite subgroup of GO_2 is $*m\bullet$*

(since its chiral subgroup of index 2 must be $m\bullet$ for some m).

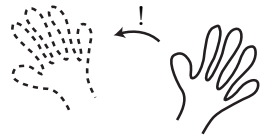


Figure 2.4. 2-dimensional chirality.

Figure 2.5. 2-dimensional achirality.

2.3 The Gaussian Integers

Gauss defined a notion for complex numbers analogous to integrality for real numbers. Namely, the complex number $x + iy$ is a **Gaussian integer** just if its real and imaginary parts are ordinary integers. The Gaussian integers form a ring, since the sum, difference, or product of two Gaussian integers is a third.

Geometrically, the Gaussian integers form a square lattice; see Figure 2.6, in which two points closest to each other differ by one of the four Gaussian units, 1, -1, i, $-i$.

Perhaps the most interesting property of the Gaussian integers is their unique factorization theorem:

Theorem 5. *Each nonzero, nonunit Gaussian integer has a factorization $\pi_1\pi_2\ldots\pi_k$ into Gaussian primes. From any one such factorization, we can get to any other by*

- *reordering the primes*
- *unit-migration: replace π_s, π_{s+1} by $\pi_s u, \overline{u}\pi_{s+1}$*

Here a **Gaussian prime** is a Gaussian integer whose norm is an ordinary prime, so that in all its 2-term factorizations, just one factor is a unit.

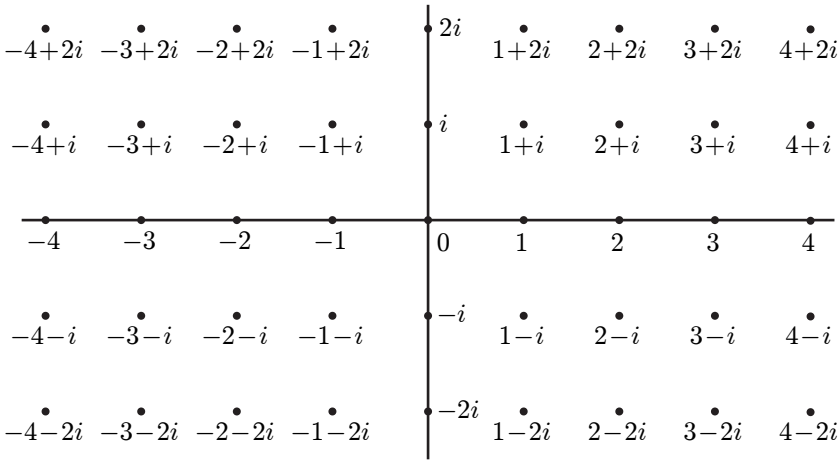


Figure 2.6. The Gaussian integers.

When we proved the unique factorization theorem for ordinary integers in Chapter 1, we only used the fact that you could divide one number by another and get a smaller remainder. In fact, if you allow negative remainders, you can get within $\frac{1}{2}|d|$ of a multiple of the number d you're dividing by (see Figure 1.1, where $|d|$ is the distance from 0 to d).

Figure 2.7 shows how every Gaussian integer is within $|d|/\sqrt{2}$ of a multiple of a Gaussian integer d. Since $1/\sqrt{2}$ is less than 1, the remainder is smaller in size than the divisor and our proof of unique factorization will work as well for the Gaussian integers.

The units of the Gaussian integers are the fourth roots of unity. Gauss's disciple, Eisenstein, gave an alternative system involving the third and sixth roots of unity. The **Eisenstein integers** are the numbers $a + b\omega$, where $\omega = (-1 + i\sqrt{3})/2$ is one of the roots of $x^3 = 1$, the other two being 1 and $\omega^2 = (-1 - i\sqrt{3})/2$. The Eisenstein integers form a triangular lattice (see Figure 2.8). Figure 2.9 is similar to Figure 2.7 and shows that every Eisenstein integer is within a distance $\frac{1}{\sqrt{3}}|d|$ of some multiple of a given Eisenstein integer, so that these integers, too, have unique factorization into primes.

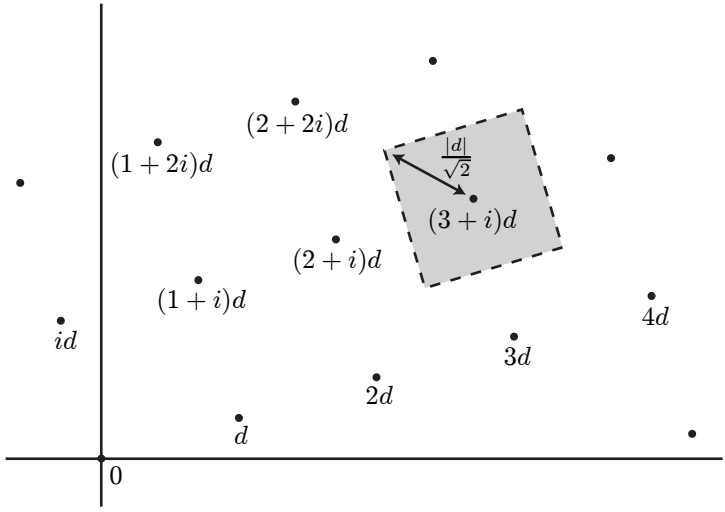


Figure 2.7. Maximal remainder for the Gaussian integers.

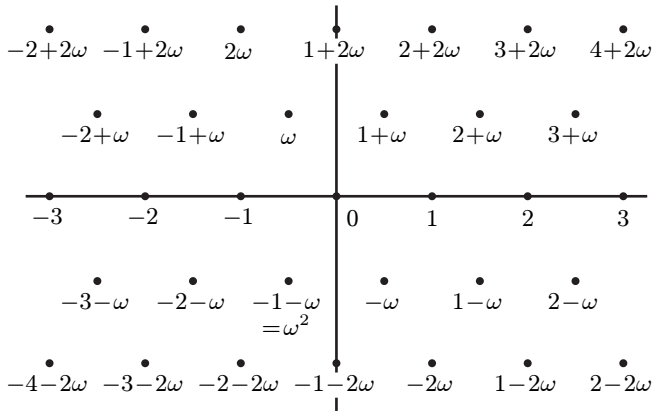


Figure 2.8. The Eisenstein integers.

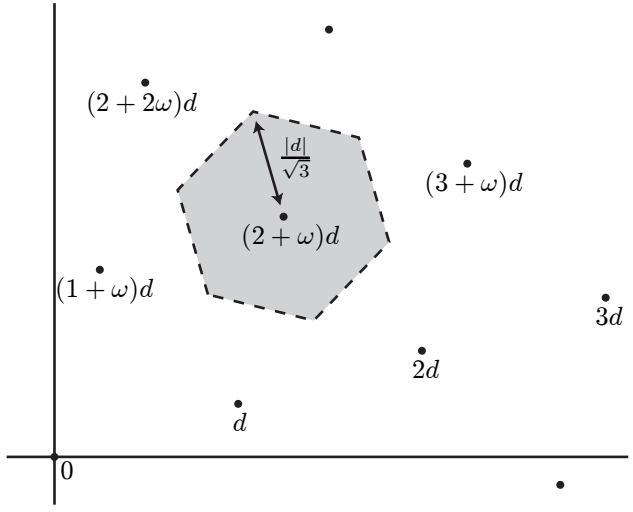


Figure 2.9. Maximal remainder for the Eisenstein integers.

2.4 The Kleinian Integers

It is a famous theorem, proved by Heegner and reestablished independently by A. Baker and H. M. Stark, that there are only nine imaginary quadratic fields with unique factorization, namely those with discriminants

$$3, 4, 7, 8, 11, 19, 43, 67, 163.$$

The next simplest ring to the Eisenstein (discriminant 3) and Gaussian (discriminant 4) ones has been called "**the Kleinian ring**" , which consists of all numbers of the form $a + b\lambda$ $(a, b \in \mathbb{Z})$, where $\lambda = \frac{-1+\sqrt{-7}}{2}$ (see Figure 2.10). The most important features are that this ring has just the two units ± 1, and that 2 factorizes as $\lambda\mu$, where $\mu = \frac{-1-\sqrt{-7}}{2}$.

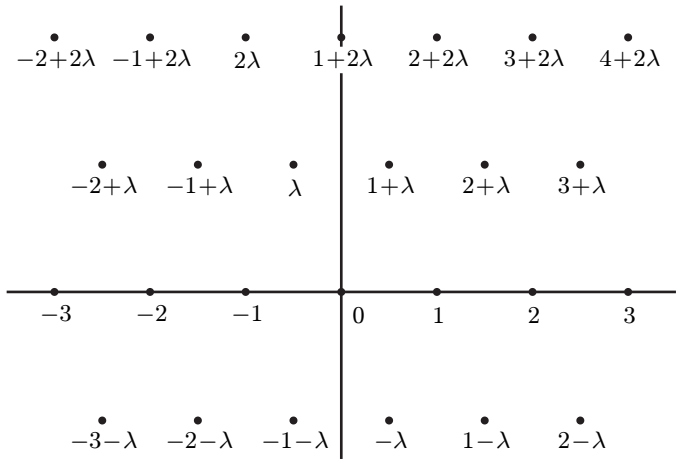


Figure 2.10. The Kleinian ring.

2.5 The 2-Dimensional Space Groups

We have already discussed the 2-dimensional point groups in the body of this chapter. Here we briefly describe the 17 2-dimensional space groups, since their theory is closely related to that of the 3-dimensional point groups of the next chapter.

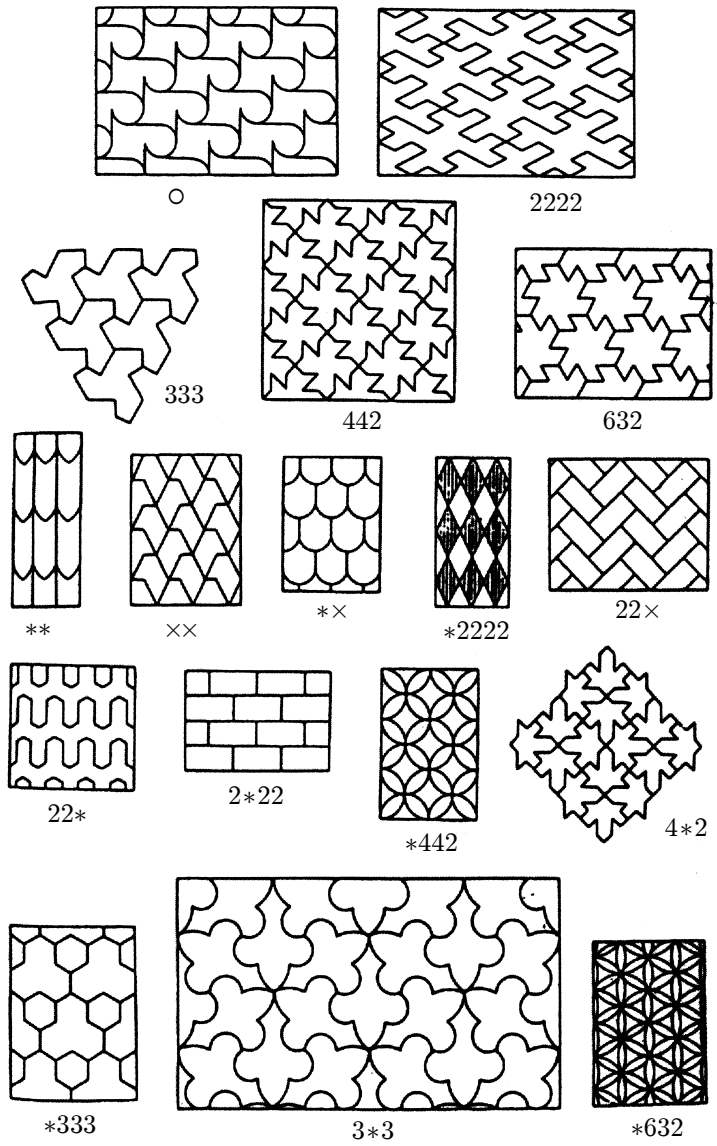


Figure 2.11. We here reproduce G. Pólya's 1924 illustration representing the 17 different plane symmetry groups, replacing his names with the orbifold names.

In **the orbifold notation**, the 17 groups are

$$*632, 632$$
$$*442, 4*2, 442$$
$$*333, 3*3, 333$$
$$*2222, 2*22, 22*, 22\times, 2222$$
$$**, *\times, \times\times, \circ$$

where

- A digit $A \geq 2$ not following a $*$ indicates a type of point with local symmetry $A\bullet$.
- A string of digits $a_1 \geq 2, a_2 \geq 2, \ldots, a_k \geq 2$ after a $*$ indicates a type of kaleidoscope, i.e., a connected system of mirror lines on which there are distinct types of point with local symmetries $*a_1\bullet$, $*a_2\bullet$, $\ldots$, $*a_k\bullet$.
- $\times$ indicates a "miracle," i.e., the presence of an orientation-reversing path that meets no mirror.
- $\circ$ indicates a "wonder," i.e., a repetition of motif not yet accounted for.

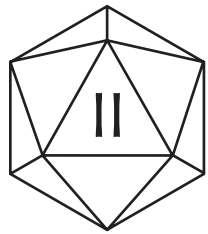
(We do not give more precise definitions here.)

Each of these features has a cost:

Feature	Cost
A	$(A-1)/A$
$*$	1
a_i after $*$	$(a_i-1)/2a_i$
$\times$	1
$\circ$	2

and the "Magic Theorem" asserts that the above 17 groups are precisely those whose total cost is 2 (see Figure 2.11).

The proof of the Magic Theorem relates these names to the features of the **orbifold**, the plane considered modulo the group. In this interpretation, $*a_1a_2\ldots a_k$ denotes a boundary with k corners having angles $\frac{\pi}{a_1}$, $\frac{\pi}{a_2}$, $\ldots$, $\frac{\pi}{a_k}$, while A (not after a $*$) is a cone point of angle $\frac{2\pi}{A}$, $\times$ denotes a crosscap, and $\circ$ denotes a handle.



The Quaternions and Their Applications to 3- and 4-Dimensional Geometry

The quaternions are formal expressions $x_0 + x_1 i + x_2 j + x_3 k$ (with x_0, x_1, x_2, x_3 real), combined by

$$\begin{aligned}&(x_0 + x_1 i + x_2 j + x_3 k) + (y_0 + y_1 i + y_2 j + y_3 k)\\ &= (x_0 + y_0) + (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k\end{aligned}$$

$$\begin{aligned}&(x_0 + x_1 i + x_2 j + x_3 k)(y_0 + y_1 i + y_2 j + y_3 k)\\ &=\\ &(x_0 y_0 - x_1 y_1 - x_2 y_2 - x_3 y_3)\\ &+(x_0 y_1 + x_1 y_0 + x_2 y_3 - x_3 y_2)i\\ &+(x_0 y_2 - x_1 y_3 + x_2 y_0 + x_3 y_1)j\\ &+(x_0 y_3 + x_1 y_2 - x_2 y_1 + x_3 y_0)k;\end{aligned}$$

that is to say, they constitute the algebra over the reals generated by basic units i, j, k that satisfy Hamilton's celebrated equations

$$ij = k \qquad jk = i \qquad ki = j$$

$$ji = -k \qquad kj = -i \qquad ik = -j$$

$$i^2 = j^2 = k^2 = -1.$$

Quaternions and 3-Dimensional Groups

In the previous chapter, we enumerated the finite subgroups of SO_2 and GO_2 and related them to complex numbers. Our aim in this chapter is to enumerate the finite subgroups of SO_3 and GO_3 and relate them to quaternions.

3.1 The Quaternions and 3-Dimensional Rotations

What's the relation between quaternions and 3-dimensional geometry? Ultimately, this comes from the fact that the norm of a product of quaternions is the product of their norms. This implies

$$N(q_1 v q_2) = N(q_1)N(v)N(q_2),$$

showing that the map $v \to q_1 v q_2$ is a similarity of Euclidean 4-space that multiplies lengths by $\sqrt{N(q_1)N(q_2)}$, and so is a congruence if $N(q_1)N(q_2) = 1$. If this operation fixes $v = 1$, it will also fix the 3-dimensional space perpendicular to 1, whose typical elements are the vectors of the form $xi + yj + zk$ (i.e., with no "real part"), which we call (3-dimensional) **vectors**. Since the condition for this is $q_1 q_2 = 1$, we obtain

Theorem 1. *The map* $[q] : v \to q^{-1}vq$ *is a congruence of Euclidean 3-space.*

In fact, this congruence is a **simple rotation**, that is to say, it fixes a vector (in n dimensions, a simple rotation is one that fixes an $(n-2)$-

space). To be more precise, we shall show in the appendix to this chapter that if $q = r(\cos\theta + u\sin\theta)$, where u is a unit 3-vector, then $[q]$ is a rotation through the angle 2θ about u.

Noting that every simple rotation takes this form (by choice of u and θ), we obtain an immediate proof of

Theorem 2. (Euler's Theorem on Rotations) *The product of any two simple rotations is another.*

For, the product of simple rotations

$$x \to q_1^{-1} x q_1 \quad \text{and} \quad x \to q_2^{-1} x q_2$$

is $x \to (q_1 q_2)^{-1} x (q_1 q_2)$, another simple rotation. We shall give a geometric proof of Euler's theorem in the next section.

Since we showed in Chapter 1 that the special orthogonal group is generated by simple rotations, we have

Theorem 3. *Every element of SO_3 has the form $x \to q^{-1}xq$ for some quaternion q, and is a simple rotation.*

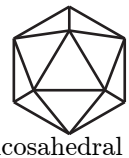
At first sight, this correspondence between quaternions and rotations is "∞-to-1" since all the non-zero scalar multiples of a given quaternion plainly yield the same rotation. We reduce this multiplicity by demanding that q be a unit quaternion; this makes it 2-to-1 since two opposite unit quaternions q and $-q$ yield the same rotation.

Theorem 4. *The map that takes q to the map $[q] : x \to q^{-1}xq$ is a 2-to-1 homomorphism from the group of unit quaternions to SO_3.*

In the standard language, the set of unit quaternions is a "double cover" of SO_3 called the **spin group Spin$_3$**. The spin groups exist in all dimensions, but to give their general definition would lead us too far astray. We shall meet just three more instances, Spin$_4$, Spin$_7$, and Spin$_8$, in later chapters.

One of the subtleties of this subject is the presence of several distinct 2-to-1 maps: our notation makes these explicit by using *square brackets* (when necessary). Thus, we have seen that two unit quaternions $+q$, $-q$ determine the same 3-dimensional isometry $[q] : x \to \overline{q}xq$. Again, two n-dimensional isometries $+g$, $-g$ in GO_n determine the same projective isometry $[g]$ in PGO_n. We'll use $[\![q]\!]$ rather than $[[q]]$ for the result of successively applying two such maps to q.

The rest of this chapter describes the finite subgroups of GO_3 (see Figure 3.1) and the way they are represented by quaternions. The next few sections first enumerate the finite subgroups of SO_3. We start our next section with some useful spherical geometry.



Holo-icosahedral group
$*532 = \pm I$

Chiro-icosahedral group
$532 = +I$

Holo-octahedral group
$*432 = \pm O$

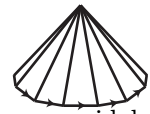
Chiro-octahedral group
$432 = +O$

Pyritohedral group
$3*2 = \pm T$

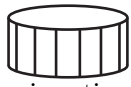
Holo-tetrahedral group
$*332 = TO$

Chiro-tetrahedral group
$332 = +T$

Holo-pyramidal group
$*nn$

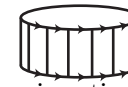


Chiro-pyramidal group
nn



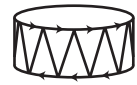
Holo-prismatic group
$*22n = \pm D(n)/DD(2n)$

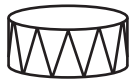
Chiro-prismatic group
$22n = D(n)$



Pro-prismatic group
$n* = \pm C(n)/CC(2n)$

Chiro-antiprismatic group





Holo-antiprismatic group
$2*n = DD(2n)/\pm D(n)$

Pro-antiprismatic group
$n\times = CC(2n)/\pm C(n)$

Figure 3.1. 3-dimensional groups from polyhedra (see also Section 3.9).

3.2 Some Spherical Geometry

We begin with

Theorem 5. *Any finite group of congruences of Euclidean n-space fixes a point.*

For if $P_1, P_2, \ldots, P_N$ are the images of any point P_1, then $\frac{1}{N}(P_1 + P_2 + \cdots + P_N)$ is plainly fixed.

So, from now on, we will suppose that the finite group we are interested in fixes the origin, and we study it in terms of its action on the unit sphere.

Theorem 6. *The product of simple rotations about the vertices of a spherical triangle, through twice the angles of that triangle (with the sign convention as in Figure 3.2), is the identity.*

For if P, Q, R are reflections in the sides of that triangle, then the three rotations are PQ, QR, RP, (where PQ means "P followed by Q") and

$$PQ \cdot QR \cdot RP = PQ^2R^2P = PP = 1.$$

In particular, since we can "complete the triangle" for any two rotations A (through 2α) and B (through 2β) as in Figure 3.3, we obtain a geometric proof of Euler's theorem on rotations.

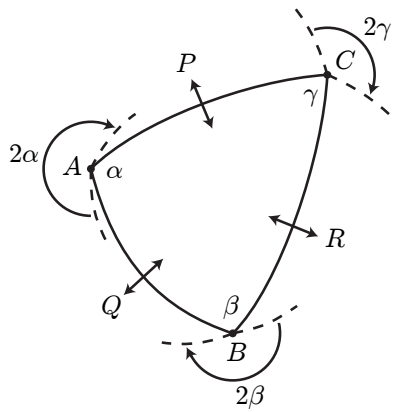


Figure 3.2. PQ is the indicated rotation about A through angle 2α, QR is the indicated rotation about B through angle 2β, and RP is the indicated rotation about C through angle 2γ.

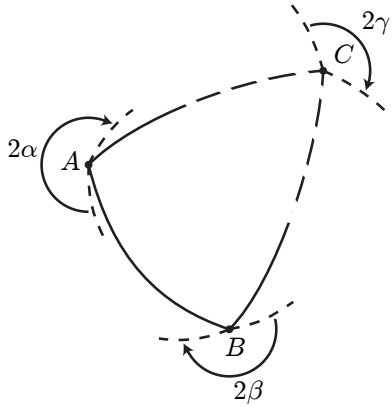


Figure 3.3. The product of rotations through 2α about A and 2β about B is one through 2γ about C, completing the triangle.

So a group generated by simple rotations consists entirely of such rotations. These **rotation groups** are the most important groups in what follows, and we'll see later that each of them can be generated by two rotations.

A **reflection group** is a group generated by reflections.

Theorem 7. *A group generated by two rotations R_1, R_2 is contained to index 2 in a reflection group.*

We obtain the desired reflection group from the rotation group by adjoining M, the reflection in the plane containing the axes of R_1 and R_2. This *is* a reflection group, since we can write $R_1 = MM_1$, $R_2 = MM_2$ for two further reflections $M_1 = MR_1$, $M_2 = MR_2$. Any element of it can be represented by a word in R_1, R_2, M, in which we can use the relations $R_1M = MR_1$, $R_2M = MR_2$ to bring all occurrences of M to the front, and then use $M^2 = 1$ to put it into the form w or Mw, where w is a word in R_1, R_2 only.

Theorem 8. *Any finite reflection group is generated by the reflections in the sides of a convex spherical polygon whose angles are of the form $\frac{\pi}{n}$.*

For consider the way that the fixed planes of all of the reflections in the group cut the unit sphere. Plainly they divide the sphere into a number of convex polygons. Also, when two such polygons abut along a common edge, they are reflected into each other by the reflection across that edge. This shows that all the polygons have the same shape, and that the reflections corresponding to one generate those corresponding to its neighbor, and so by repetition, generate the whole group.

In the orbifold notation, the group generated by reflections in sides of a polygon of angles $\frac{\pi}{a}, \frac{\pi}{b}, \ldots, \frac{\pi}{z}$ is called $*ab\ldots z$. We allow digits of 1 to be freely inserted or deleted in orbifold notations, since this simplifies general statements.

Theorem 9. (The Spherical Excess Theorems)

$$\begin{aligned} A+B+C &= \pi + \triangle \\ A+B+C+D &= 2\pi + \square \\ A+B+C+D+E &= 3\pi + \pentagon \\ &\vdots \end{aligned}$$

where $\triangle(\square, \pentagon, \ldots)$ *denotes the area of a triangle (quadrilateral, pentagon, . . .) with angles* A, B, C *(*D*,* E*, . . .).*

Figure 3.4 reduces the proof for higher polygons to that of the triangle, which is proved by Figures 3.5 and 3.6.

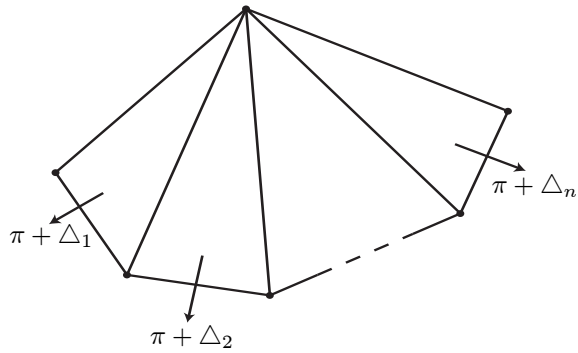


Figure 3.4. Triangulating a higher polygon and its angle sum.

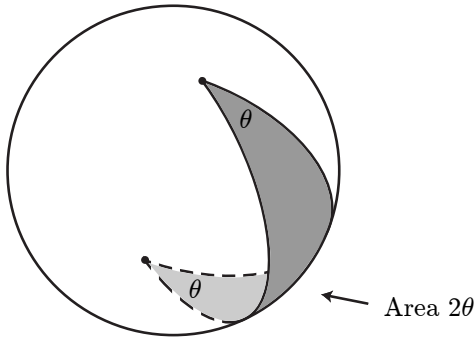


Figure 3.5. The area of a lune is obviously proportional to its angle θ, and must be 2θ since the total area of the sphere is 4π.

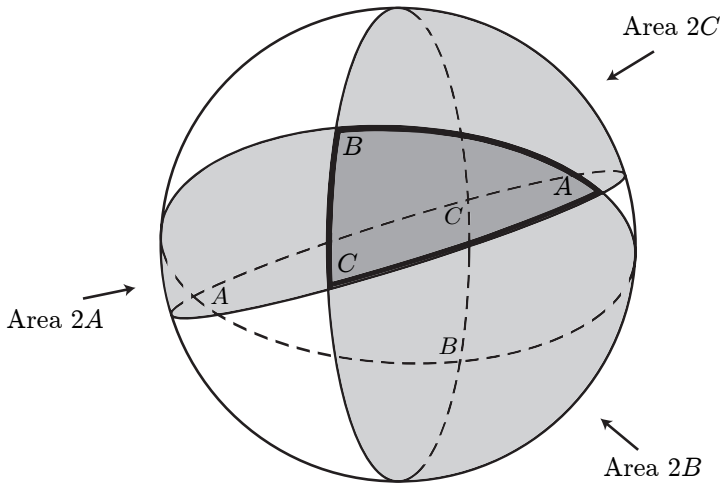


Figure 3.6. The sphere (of total area 4π) is divided into eight triangles, of which the four shaded ones have area 2π (since opposite triangles have the same area). The total area of the three shaded lunes is $2A + 2B + 2C$, which must be $2\pi + 2\triangle$ since the common triangle of area $\triangle$ is covered three times.

3.3 The Enumeration of Rotation Groups

We first find the corresponding enumeration of reflection groups, namely:

Theorem 10. *Every finite reflection group is one of*

$$*532 \quad *432 \quad *332 \quad *22n \quad *nn \ (n \geq 1).$$

For the angle sum for a k-gon is $\frac{k\pi}{2}$, but by the previous theorem it must be greater than $(k-2)\pi$, implying $k \leq 3$.

Now, if $k = 3$, the largest angle must be $\frac{\pi}{2}$ (otherwise the angle sum would be at most $\frac{\pi}{3} + \frac{\pi}{3} + \frac{\pi}{3} = \pi$), the next largest must be $\frac{\pi}{2}$ or $\frac{\pi}{3}$ (otherwise the angle sum would be at most $\frac{\pi}{2} + \frac{\pi}{4} + \frac{\pi}{4} = \pi$), and finally if those were $\frac{\pi}{2}$ and $\frac{\pi}{3}$, the remaining angle must be at least $\frac{\pi}{5}$ (otherwise the angle sum would be at most $\frac{\pi}{2} + \frac{\pi}{3} + \frac{\pi}{6} = \pi$). This gives the cases $*22n, *233, *234, *235$.

If $k = 2$, the polygon is a lune formed by two great semicircles, whose two angles are equal, and if they are $\frac{\pi}{n}$, the group is $*nn$ (which when $n = 1$ includes the case when the "polygon" is a hemisphere).

The cornerstone of this chapter is

Theorem 11. *The finite rotation groups are*

$$532 \quad 432 \quad 332 \quad 22n \quad nn \ (n \geq 1).$$

Firstly, a preceding argument shows that this is true for those groups that can be generated by at most two rotations.

Can there be a group G that needs more than two generating rotations? No, because any two rotations of G generate one of the above, which restricts their distances, and a further rotation center would be prohibitively near to one of the existing ones (see Figure 3.7).

Therefore, we have found infinitely many groups, but we find it more convenient to speak of them as "five groups," two of which depend on a parameter.

3.4 Discussion of the Groups

The first three groups are collectively called the **polyhedral rotation groups**, since they consist of the rotations that fix the appropriate regular polyhedra, while the remaining two are the **axial rotation groups**, since they fix an axis.

Abstractly, they are isomorphic to various well-known permutation groups $G(n)$ on n letters, as seen in Figure 3.8. The individual cases are

$$\begin{aligned}
532 = I &= I_{60} \cong A(5), \quad \text{the } \textbf{icosahedral} \text{ group} \\
432 = O &= O_{24} \cong S(4), \quad \text{the } \textbf{octahedral} \text{ group} \\
332 = T &= T_{12} \cong A(4), \quad \text{the } \textbf{tetrahedral} \text{ group} \\
22n = D &= D_{2n} \cong D(n), \quad \text{the } \textbf{dihedral} \text{ group} \\
nn = C &= C_n \cong C(n), \quad \text{the } \textbf{cyclic} \text{ group}
\end{aligned}$$

These are the traditional, rather confusing names. We shall later prefix them by "chiro-" to distinguish these rotation groups from the "holo-polyhedral" groups, which are the full groups of symmetries of the appropriate polyhedra.

There is some confusion in the literature since group theorists usually write D_{2n} for the dihedral group of order $2n$, while geometers prefer names that display the parameter n. As geometers who are also group theorists, we sometimes write D_{2n} and sometimes $D(n)$, so doing both!

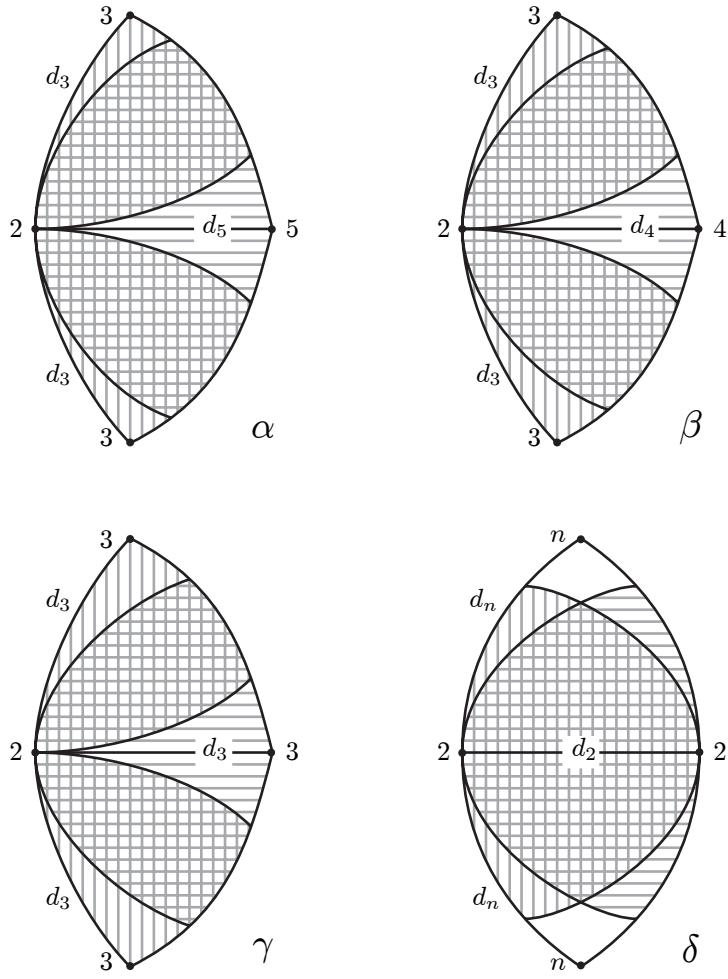
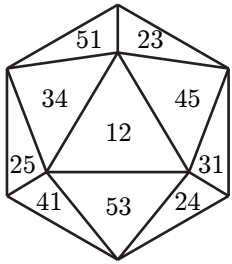
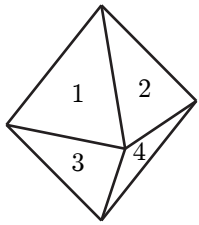


Figure 3.7. We'll write n for a center of n-fold rotation and d_n for the shortest distance from one of these to any other rotation center. The smallest possible values for d_5 and d_3 are seen in 532, so G can't contain 532 since any putative new rotation center must be within d_5 or d_3 of 2 (see α). Otherwise, the smallest d_4 and d_3 are in 432, which is precluded since any new center would be within d_4 or d_3 of 2 (see β). The next smallest value of d_3 is in 332, which is precluded for a similar reason (see γ). In all remaining cases, if the largest order rotation is n-fold ($n \geq 2$), then it and any other rotation can only generate a $22n$ and so $d_n = \frac{\pi}{2}$ and $d_2 = \frac{\pi}{n}$, which again precludes a further rotation (see δ).

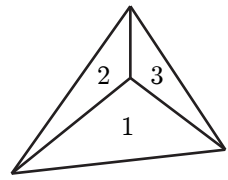


The opposite face to ij is ji

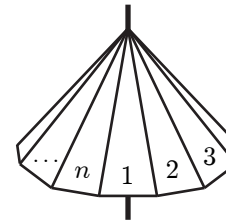
The **Icosahedral group I** consists of the rotations that fix an icosahedron. If the faces are labelled by pairs of numbers from $1, \ldots, 5$ as shown, it induces the alternating group $A(5)$ of degree 5.



Opposite faces have same label



Back face labelled 4



Pyramid

Octahedral group O induces $S(4)$

Tetrahedral group T induces $A(4)$

Cyclic group C$=C_n$ induces $C(n)$

The **Dihedral group D**$=D_n$ consists of the rotations that fix a prism, whose rectangular faces are numbered $1, \ldots, n$. It is isomorphic to $D(n) = \langle\, (12\ldots n), (1\ n)(2\ n{-}1)\ldots \,\rangle$.

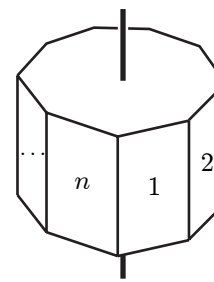


Figure 3.8. The polyhedral and axial groups are isomorphic to various permutation groups $D(n)$ on n symbols.

3.5 The Finite Groups of Quaternions

We pause to enumerate the finite groups of quaternions. Under the 2-to-1 map that takes a unit quaternion q to the rotation $[q] : x \to \overline{q}xq$, a finite group Q of quaternions must be taken to a group $[Q] = \{[q] \mid q \in Q\}$, say, among C, D, T, O, I. The order of Q will be 2 or 1 times that of $[Q]$, according to whether -1 is or is not in Q.

The cases when $-1 \in Q$ we call $2C_n, 2D_{2n}, 2T, 2O, 2I$, with $2G$ meaning $\{q \mid [q] \in G\}$. If $-1 \notin Q$, then G can contain no order 2 rotation g, since if $[q] = g$ then $q^2 = -1$ must be in Q. This leaves only the cases C_n (n odd), which is the image of an order n group Q (eg. $\langle e^{2\pi i/n} \rangle$), to which we give the name $1C_n$. We summarize:

Theorem 12. *The finite groups of quaternions are*

$$2I \quad 2O \quad 2T \quad 2D_{2n} \quad 2C_n \quad 1C_n \ (n \text{ odd}).$$

Generators for these groups are given below:

$$\begin{array}{rcl} 2I = \langle i_I, \omega \rangle & & i_I = \frac{i+\sigma j+\tau k}{2},\ \sigma = \frac{\sqrt{5}-1}{2},\ \tau = \frac{\sqrt{5}+1}{2} \\ 2O = \langle i_O, \omega \rangle & \text{where} & i_O = \frac{j+k}{\sqrt{2}},\ \omega = \frac{-1+i+j+k}{2} \\ 2T = \langle i_T, \omega \rangle & & i_T = i \\ 2D_{2n} = \langle e_n, j \rangle & & e_n = e^{\pi i/n} \\ 2C_n = \langle e_n \rangle & & \\ 1C_n = \langle e_{n/2} \rangle & & \end{array}$$

3.6 Chiral and Achiral, Diploid and Haploid

The word "chiral" (meaning "handed") was introduced to science by Lord Kelvin before 1896 to denote objects that cannot be moved into coincidence with their mirror images. For the opposite concept, the word "achiral" ("unhanded") or "amphichiral" ("either-handed") has been used.

We shall use these terms not only for such objects, but also for their symmetry groups. Thus, a symmetry group is **chiral** if all its operations can be achieved by rigid motions and **achiral** otherwise.[1]

For a finite physical object, all symmetries fix the center of gravity, and, when we take this to be the origin, are represented by orthogonal matrices whose determinants are necessarily ± 1. The group is chiral just if every determinant is $+1$, and achiral if it contains some element of determinant -1.

[1] We adhere to this standard usage, despite the inconsistency that each 3-dimensional "chiral group" coincides with its own mirror image. We expand on this in Chapter 4.

The dual distinction does not seem hitherto have been named. We shall do so by borrowing a pair of terms from the biologists. We call a group **diploid** ("formed of couples") if it contains the "central symmetry" $-\mathbf{1} : x \to -x$, because then its matrices come in pairs $\pm g$. The other groups are called **haploid** ("formed of singletons").

In general, these distinctions yield four classes of groups: chiral diploid, chiral haploid, achiral diploid, and achiral haploid. However, here one type is missing. For since we are working in an odd number of dimensions, the central symmetry $-\mathbf{1}$ has determinant -1, and so a diploid group is necessarily achiral. We therefore get only three classes, namely:

- The **diploid** groups (which are necessarily achiral)
- The **chiral** groups (which are necessarily haploid), and
- The **hybrid** groups (namely those that are achiral but haploid).

In the next few pages, we use these notions to enumerate types of groups.

3.7 The Projective or Elliptic Groups

To work **projectively** is to regard elements as identical if they are scalar multiples of each other. For us, the only relevant scalars are ± 1, so working projectively replaces $+g$ and $-g$ by a single element $[g]$.

Recall that GO_n, the n-dimensional general orthogonal group, consists of all $n \times n$ orthogonal matrices, or equivalently all congruences of n-dimensional Euclidean space that fix the origin, while SO_n, the n-dimensional special orthogonal group, consists of all elements of GO_n of determinant 1. From these we obtain PGO_n and PSO_n, the n-dimensional projective general and special orthogonal groups, by working projectively.

However, for odd n, we have $\det(-\mathbf{1}) = -1$, which entails that $PGO_n = PSO_n$ and also $PSO_n \cong SO_n$. This is because just one of $g, -g$ has determinant 1, so that their projective image is the projective image of this "positive" one, while considering SO_n projectively involves no identification. Applied to the finite subgroups, this gives

Theorem 13. *The finite subgroups of* $PGO_3 = PSO_3$ *are*

$$[I_{60}] \quad [O_{24}] \quad [T_{12}] \quad [D_{2n}] \quad [C_n].$$

The typical operation $[g]$ of each is represented by a pair of opposite matrices: one we call $+g$ of determinant 1, and one, $-g$, of determinant -1. Knowing the projective groups enables us to enumerate all the subgroups of GO_3, as follows.

3.8 The Projective Groups Tell Us All

Chiral groups: Any such consists just of the elements $+g$ for $[g]$ in some projective group $[G]$: We call this $+G$. The cases are:

$$\begin{aligned} +C,&\ \text{the } \textbf{cyclic rotation} \text{ group}\\ +D,&\ \text{the } \textbf{dihedral rotation} \text{ group}\\ +T,&\ \text{the } \textbf{tetrahedral rotation} \text{ group}\\ +O,&\ \text{the } \textbf{octahedral rotation} \text{ group}\\ +I,&\ \text{the } \textbf{icosahedral rotation} \text{ group}\end{aligned}$$

In quaternionic terms, $+G$ consists of the maps $x \to q^{-1}xq$, $q \in 2G$.

Diploid groups: Any such must consist of pairs of elements $+g, -g$ for $[g] \in [G]$. We therefore call it $\pm G$. The cases are:

$$\begin{aligned} \pm C,&\ \text{the } \textbf{diplo-cyclic} \text{ group}\\ \pm D,&\ \text{the } \textbf{diplo-dihedral} \text{ group}\\ \pm T,&\ \text{the } \textbf{diplo-tetrahedral} \text{ group}\\ \pm O,&\ \text{the } \textbf{diplo-octahedral} \text{ group}\\ \pm I,&\ \text{the } \textbf{diplo-icosahedral} \text{ group}\end{aligned}$$

The group $\pm G$ consists of the maps $x \to \pm q^{-1}xq$, $q \in 2G$.

The **hybrid groups** are more subtle: There is a projective group $[G]$ obtained by ignoring signs, and for each element of $[G]$ we must make a choice of sign. Namely, the sign will be $+$ for a certain subgroup $[H]$ consisting of half of the elements of $[G]$ and $-$ for the remaining ones.

So a hybrid group determines and is determined by a pair $[H], [G]$ of projective groups, namely, its projective image $[G]$ and the "half group" $[H]$ of index 2 in $[G]$, at which the sign is $+$. In formal situations we will use the name "$+H - G$", which indicates that the group consists of the elements

$$+h \text{ for } [h] \text{ in } [H] \text{ and } -g \text{ for } [g] \text{ in the rest of } [G].$$

Informally we often abbreviate this to HG. The cases are:

$$\begin{aligned} +C_n - C_{2n} = CC_{2n} = CC(2n),&\ \text{the } \textbf{cyclo-cyclic} \text{ group}\\ +C_n - D_{2n} = CD_{2n} = CD(n),&\ \text{the } \textbf{cyclo-dihedral} \text{ group}\\ +D_{2n} - D_{4n} = DD_{4n} = DD(2n),&\ \text{the } \textbf{dihedro-dihedral} \text{ group}\\ +T_{12} - O_{24} = TO,&\ \text{the } \textbf{tetra-octahedral} \text{ group}\end{aligned}$$

The group $+H-G$ consists of the maps $x \to +q^{-1}xq$, $q \in 2H$, $x \to -q^{-1}xq$, $q \in 2G \backslash 2H$.

From the notation we've been using, it's easy to recover the abstract group structure, so we call it the **algebraic notation**. The rule is that $+G$ and HG are isomorphic to G, and $\pm G$ to $C_2 \times G$.

3.9 Geometric Description of the Groups

Figure 3.1 described all of the groups in terms of familiar polyhedra. In the upper portion we have the full (or "**holo-**") and rotational (or "**chiro-**") groups for the icosahedron ($\pm I = *532$ and $+I = 532$), octahedron ($\pm O = *432$ and $+O = 432$), and tetrahedron ($TO = *332$ and $+T = 332$), as well as the diplo-tetrahedral group ($\pm T = 3 * 2$), more usually called the **pyritohedral** group since crystals of iron pyrites often have this symmetry. In the lower portion we have the "holo-" and "chiro-" groups of prisms ($*22n$ and $22n$), antiprisms ($2*n$ and $2nn$), and pyramids ($*nn$ and nn), as well as the **pro-**prismatic ($n*$) and pro-antiprismatic ($n\times$) groups, obtained from the prismatic and antiprismatic groups by preserving the sense of rotation about the principal axis.

Table 3.1 presents a complete dictionary between these names, the orbifold symbols, and our algebraic notations, while Table 3.2 arranges the groups according to their orders. There is an irritating "switch" between the geometric and algebraic names, which arises because geometers prefer to extend rotations by reflections rather than the algebraically simpler central inversion $-\mathbf{1}$. Our dictionary therefore contains "even/odd" entries, such as $\pm D(n)/DD(2n)$ for $*22n$, meaning that this group is $\pm D(n)$ when n is even but $DD(2n)$ when n is odd.

There are many ways in which one of the groups can have small index in another—all of the index 2 containments appear in Figures 3.9 and 3.10.

The **chiro-icosahedral** group	$532 = +I$
The **holo-icosahedral** group	$*532 = \pm I$
The **chiro-octahedral** group	$432 = +O$
The **holo-octahedral** group	$*432 = \pm O$
The **chiro-tetrahedral** group	$332 = +T$
The **holo-tetrahedral** group	$3*2 = TO$
The **pyritohedral** group	$*332 = \pm T$
	even / odd
The (n-**gonal**) **chiro-prismatic** group	$22n = +D(n)$
The (n-**gonal**) **holo-prismatic** group	$*22n = \pm D(n)$ / $DD(2n)$
The (n-**gonal**) **holo-antiprismatic** group	$2*n = DD(2n)$ / $\pm D(n)$
The (n-**gonal**) **chiro-pyramidal** group	$nn = +C(n)$
The (n-**gonal**) **holo-pyramidal** group	$*nn = CD(n)$
The (n-**gonal**) **pro-prismatic** group	$n* = \pm C(n)$ / $CC(2n)$
The (n-**gonal**) **pro-antiprismatic** group	$n\times = CC(2n)$ / $\pm C(n)$

Table 3.1. A dictionary of the groups.

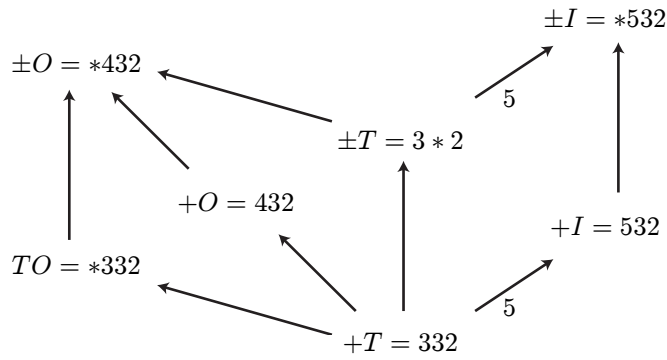


Figure 3.9. Small index containments between the polyhedral groups. (The index is 2 when not mentioned.)

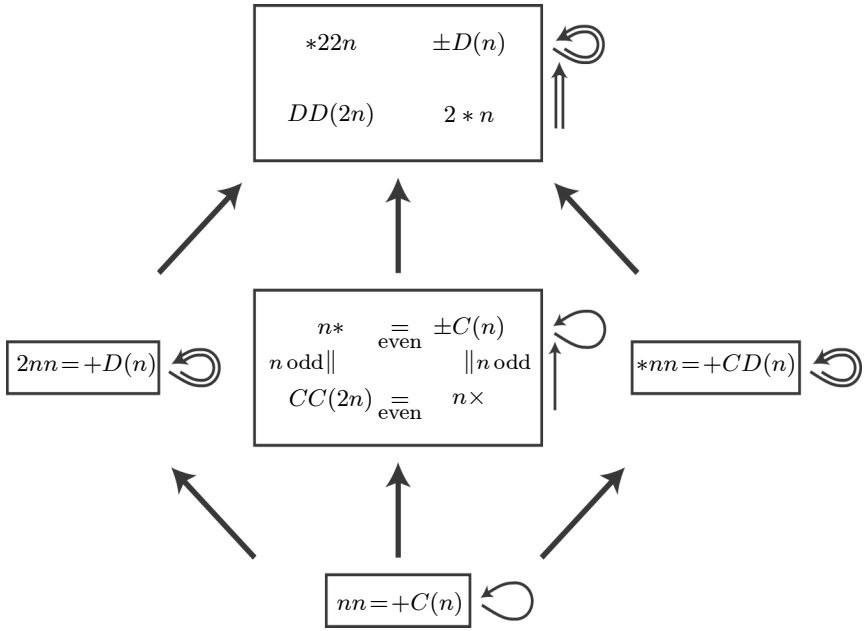


Figure 3.10. Index 2 containments between the axial groups. Such containments between groups with the same parameter n are indicated by the heavy lines between boxes—each group in the upper box contains one group in the lower (the corresponding group, if this is meaningful). All index 2 containments between groups with different parameters n and $m = \frac{n}{2}$ are indicated by the lighter lines beside the boxes. Thus, $*22n$ contains both $*22m$ and $2*m$ (each twice because there are two lines).

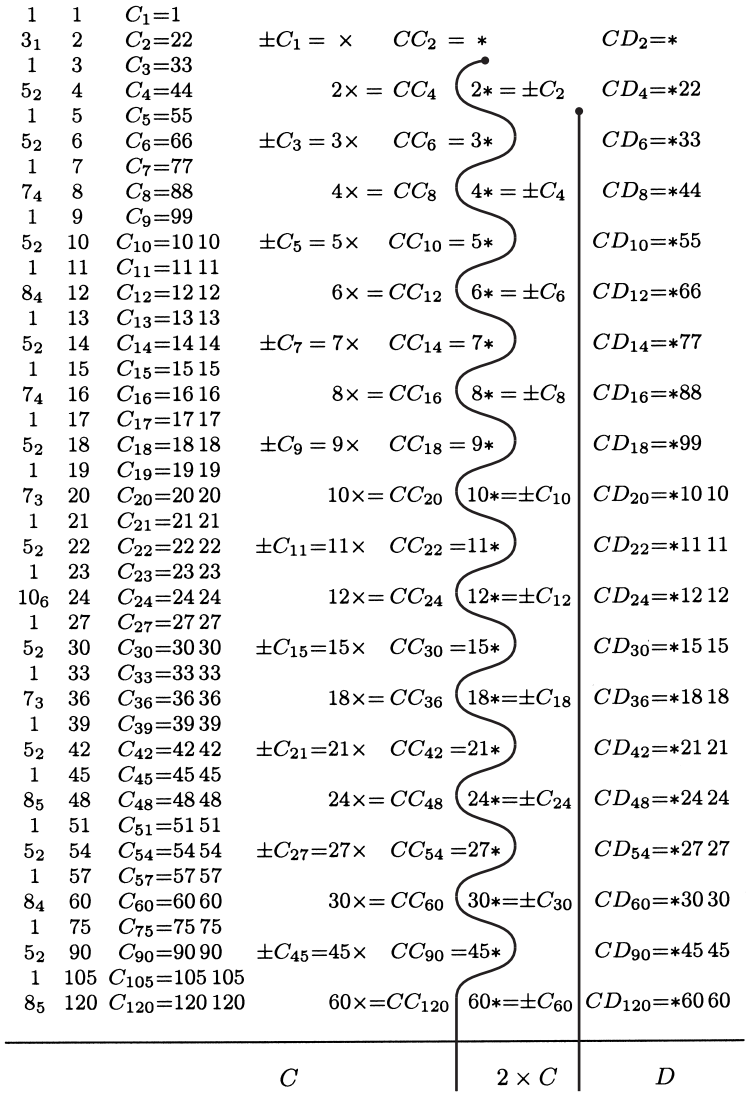


Table 3.2. The groups classified by order. All the groups of a given order appear on one line, preceded by their number, with the number of isomorphism types as a subscript. The "rivers" separate groups of distinct structures (as indicated below the table). The lines for orders $8n$, $8n + 1$, ..., $8n + 7$ that do not appear in the table are like those for orders 16, 17, ..., 23.

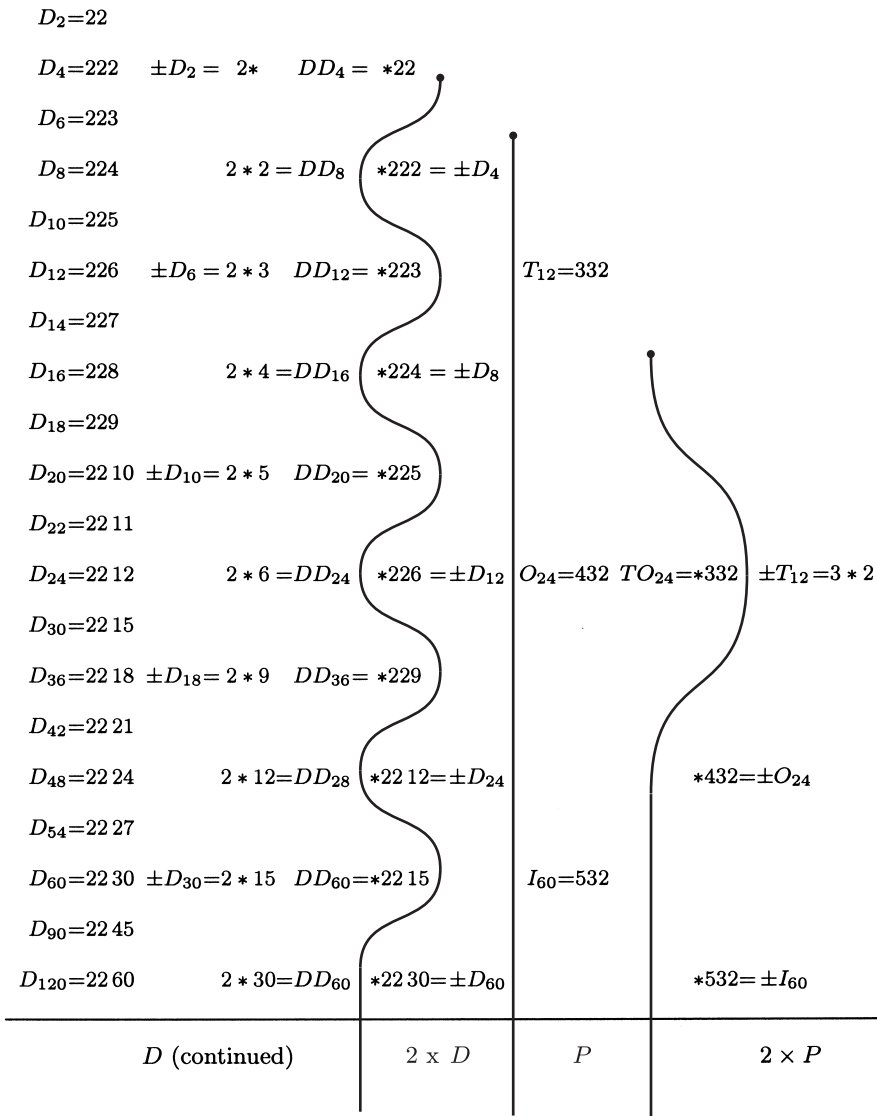


Table 3.2. (continued)

Appendix: $v \to \overline{v}qv$ Is a Simple Rotation

We first prove this in the case when the axis is i, so $q = \cos\theta + i\sin\theta$. Then if $v = xi + yj + zk$, we have

$$\overline{q}vq = \overline{q}(xi)q + \overline{q}(yj + zk)q = xi + \overline{q}^2(yj + zk),$$

since $iq = qi$, while $jq = \overline{q}j$, $kq = \overline{q}k$. By writing this as

$$xi + (\cos(2\theta) - i\sin(2\theta))(y + zi)j$$

we see that the 1-space spanned by i is fixed, while the 2-space spanned by j and k is rotated through 2θ.

The way we derive the system of quaternions in Chapter 6 actually shows that any unit imaginary quaternion may be called i, any perpendicular one j, and their product k. We now verify (without referring to Chapter 6) that the quaternions do indeed have enough symmetries to take any imaginary unit vector $u = li + mj + nk$ to i. For a rotation of the above type (fixing i) can be used to make the coefficient of k vanish, after which a similar rotation (now fixing k) will make that of j vanish, too.

Quaternions and 4-Dimensional Groups

4.1 Introduction

The arguments in Chapter 3 used the fact that a 3-dimensional orthogonal map has the form

$$x \to \overline{q}xq \quad \text{or} \quad -\overline{q}xq = \overline{q}\,\overline{x}q$$

accordingly as it is chiral or achiral. The first task of this chapter is to establish that the general orthogonal map in 4 dimensions has the form

$$x \to \overline{l}xr \quad \text{or} \quad \overline{l}\overline{x}r,$$

where l and r are two unit quaternions.

In Chapter 6, we shall explain why in any composition algebra, the map

$$x \to -q\overline{x}q$$

(where q is any unit quaternion) is the reflection that fixes the hyperplane perpendicular to q (which, henceforth, we shall call "the reflection in q"). However, we don't need to quote this, since we can directly verify it in the quaternionic case. Namely, under this map we have

$$uq \to -q\overline{q}\,\overline{u}q = -\overline{u}q$$

from which it follows that q is negated and iq, jq, kq fixed.

As we showed in Chapter 1, every symmetry of a Euclidean object is a product of reflections. So the product of n reflections takes

$$x \to \pm q_n q_{n-1} \dots q_1 (x \text{ or } \overline{x}) q_1 q_2 \dots q_n$$

and therefore has one of the two forms

$$[l, r] : x \to \overline{l} x r \quad (\text{if } n \text{ is even})$$

and

$$*[l, r] : x \to \overline{l} \overline{x} r \quad (\text{if } n \text{ is odd})$$

where l and r are unit quaternions (the $*$ in the second of these being an alternative name for quaternionic conjugation).

4.2 Two 2-to-1 Maps

This generalizes the 3-dimensional results, since it is easy to see that these maps fix 1 just if $l = r = q$ (say), showing that the maps of Chapter 3 are

$$[q] = [q, q] \quad \text{and} \quad *[q] = *[q, q].$$

In that chapter, we found the map

$$[q] : x \to \overline{q} x q$$

from unit quaternions to elements of SO_3 to be 2-to-1 since the only equality was $[-q] = [q]$. Our new map from ordered pairs of unit quaternions[1] to elements of SO_4 has a similar property, since here the only equality is

$$[-l, -r] = [l, r].$$

(A map $[l, r]$ that is the identity must fix 1, so from the 3-dimensional result, the only non-trivial one is $[-1, -1]$.)

If we work projectively, there is slightly more fusion, since the four expressions $[\pm l, \pm r]$ all name the same projective map, in view of the equalities

$$[-l, -r] = [l, r] \qquad [-l, r] = [l, -r] = -[l, r].$$

In conformity with our convention that $[x]$ denotes a function satisfying $[-x] = [x]$ (only), we shall use $[\![l, r]\!]$ (meaning $[[l, r]]$) for this projective map.

[1] These form a copy of Spin_4, the 4-dimensional spin group.

4.3 Naming the Groups

Postponing some details for the moment, our name for the typical 4-dimensional chiral group will have the form

$$\frac{1}{f}[\![L \times R]\!] \qquad \pm\frac{1}{f}[L \times R] \quad \text{or} \quad +\frac{1}{f}[L \times R]$$

in the

$$\text{projective} \qquad \text{diploid} \qquad \text{or} \qquad \text{haploid}$$

cases, where L and R are two 3-dimensional chiral groups. Such names are apposite because, for instance, $\pm\frac{1}{f}[L \times R]$ correctly suggests that this group consists of a proportion $\frac{1}{f}$ of the appropriate elements $\pm[l, r]$, with both choices of sign. In particular, the orders of these three groups are respectively

$$\frac{|L| \times |R|}{f} \qquad 2\frac{|L| \times |R|}{f} \qquad \text{or} \qquad \frac{|L| \times |R|}{f}.$$

$\frac{1}{f}[\![L \times R]\!]$ consists of the elements $[\![l, r]\!]$ for which $l \in 2L$, $r \in 2R$, and $l^\alpha = r^\beta$, where α and β are two homomorphisms from these onto the same finite group F of order f. The corresponding diploid group $\pm\frac{1}{f}[L \times R]$ consists of the pairs of elements $\pm[l, r]$, satisfying the same conditions, while a haploid group (if one exists) makes a choice of one sign from each pair.

If any of the above has index 2 in an achiral group, then L and R must be the same type of group, say Q, and our name for the larger group has the general form

$$\frac{1}{f}[\![Q \times Q]\!] \cdot 2 \qquad \pm\frac{1}{f}[Q \times Q] \cdot 2 \qquad \text{or} \qquad +\frac{1}{f}[Q \times Q] \cdot 2,$$

and has order

$$2\frac{|Q|^2}{f} \qquad 4\frac{|Q|^2}{f} \qquad \text{or} \qquad 2\frac{|Q|^2}{f},$$

respectively.

Usually, the homomorphisms α and β are sufficiently determined by L and R and the number f. When they are not, we distinguish cases by some "ornamentation" attached to L or R. Namely, we write a numerical parameter as a parenthesized superscript, while a bar identifies the less obvious

of two cases, and we allow ourselves to omit $\frac{1}{f}$ or (s) or (t) when f or s or t is 1. Similarly, in the achiral cases, different choices for the element $*[a,b]$ that extends the corresponding chiral group are indicated when necessary by ornamenting the final '2'. The individual ornamentations are sufficiently explained by the generating quaternions in Tables 4.1, 4.2, and 4.3, which enumerate the groups.

Group	Generators
$\pm[I\times O]$	$[i_I,1],[\omega,1],[1,i_O],[1,\omega]$;
$\pm[I\times T]$	$[i_I,1],[\omega,1],[1,i],[1,\omega]$;
$\pm[I\times D_{2n}]$	$[i_I,1],[\omega,1],[1,e_n],[1,j]$;
$\pm[I\times C_n]$	$[i_I,1],[\omega,1],[1,e_n]$;
$\pm[O\times T]$	$[i_O,1],[\omega,1],[1,i],[1,\omega]$;
$\pm[O\times D_{2n}]$	$[i_O,1],[\omega,1],[1,e_n],[1,j]$;
$\pm\frac{1}{2}[O\times D_{2n}]$	$[i,1],[\omega,1],[1,e_n]$;$[i_O,j]$
$\pm\frac{1}{2}[O\times \overline{D}_{4n}]$	$[i,1],[\omega,1],[1,e_n],[1,j]$;$[i_O,e_{2n}]$
$\pm\frac{1}{6}[O\times D_{6n}]$	$[i,1],[j,1],[1,e_n]$;$[i_O,j],[\omega,e_{3n}]$
$\pm[O\times C_n]$	$[i_O,1],[\omega,1],[1,e_n]$;
$\pm\frac{1}{2}[O\times C_{2n}]$	$[i,1],[\omega,1],[1,e_n]$;$[i_O,e_{2n}]$
$\pm[T\times D_{2n}]$	$[i,1],[\omega,1],[1,e_n],[1,j]$;
$\pm[T\times C_n]$	$[i,1],[\omega,1],[1,e_n]$;
$\pm\frac{1}{3}[T\times C_{3n}]$	$[i,1],[1,e_n]$;$[\omega,e_{3n}]$
$\pm\frac{1}{2}[D_{2m}\times \overline{D}_{4n}]$	$[e_m,1],[1,e_n],[1,j]$;$[j,e_{2n}]$
$\pm[D_{2m}\times C_n]$	$[e_m,1],[j,1],[1,e_n]$;
$\pm\frac{1}{2}[D_{2m}\times C_{2n}]$	$[e_m,1],[1,e_n]$;$[j,e_{2n}]$
$+\frac{1}{2}[D_{2m}\times C_{2n}]$	$-\quad,\quad-\quad;\quad+$
$\pm\frac{1}{2}[\overline{D}_{4m}\times C_{2n}]$	$[e_m,1],[j,1],[1,e_n]$;$[e_{2m},e_{2n}]$

Table 4.1. Chiral groups, I. These are most of the "metachiral" groups—see section 4.6—some others appear in the last few lines of Table 4.2.

The enumeration is guided by the (easy) theory of subgroups G of a direct product $A\times B$ of two groups, which was found in 1889 by Goursat [20] in this very connection. Namely, the elements $l\in A$, $r\in B$ for which there exists an element $(l,r)\in G$ form subgroups L and R of A and B, respectively, which we call the "left and right subgroups," and the elements l, r for which $(l,1)$ or $(1,r)$ is in G form normal subgroups L_0 and R_0 of these, the "left and right kernels."

Now, if $l_0 \in L_0$, $r_0 \in R_0$, then

$$(l, r) \in G \Leftrightarrow (ll_0, rr_0) \in G,$$

so the condition that $(l, r) \in G$ really depends only on l and r modulo L_0 and R_0. In fact, this condition sets up an isomorphism between the left and right quotient groups L/L_0 and R/R_0, which must therefore be copies of the same abstract group F. If F has order f, G will have index f in $L \times R$.

Since the typical element, $[\![l, r]\!]$ of the 4-dimensional projective group PSO_4 is independent of the signs of l, r, it is determined by the pair $[l]$, $[r]$ of corresponding elements of PSO_3, showing that $PSO_4 \cong PSO_3 \times PSO_3$. By Goursat's theory, its typical finite subgroup therefore has the form

$$\{[\![l, r]\!] \mid [l] \in L, [r] \in R, [l]^\alpha = [r]^\beta\}$$

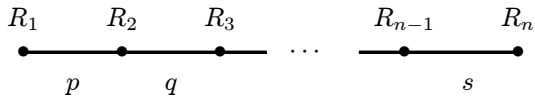
where L, R are two finite subgroups of PSO_3 and α, β homomorphisms from these onto the same abstract group F. It does no harm to regard α, β as defined on the corresponding quaternion groups $2L$, $2R$, with -1 in their kernels. This shows that our form "$\frac{1}{f}[\![L \times R]\!]$" does indeed cover all projective chiral groups, and the proofs for the other cases are similar (in the haploid cases one must consider the subgroup of $2L \times 2R$ for which $[l, r]$ is in the group).

We have just seen how quaternions can be used to give a short and elegant complete enumeration of 4-dimensional groups. However, if we are presented with a group defined geometrically in some other way, it can be hard to determine its quaternionic name, and vice versa. The next section addresses an important case.

4.4 Coxeter's Notations for the Polyhedral Groups

Coxeter's notations (adapted from Schläfli) for regular polytopes and associated groups are widely used. In this section, we extend his system slightly so as to obtain a complete set of notations for the "polyhedral" groups, which are also given in Tables 4.2 and 4.3.

Coxeter uses $[p, q, \ldots, r, s]$ for the symmetry group of the n-dimensional polytope $\{p, q, \ldots, r, s\}$—this is generated by reflections R_1, ..., R_n, corresponding to the nodes of the n-node diagram



Group	Generators	Coxeter Name
$\pm[I\times I]$	$[i_I,1],[\omega,1],[1,i_I],[1,\omega]$;	$[3,3,5]^+$
$\pm\frac{1}{60}[I\times I]$	;$[\omega,\omega],[i_I,i_I]$	$2.[3,5]^+$
$+\frac{1}{60}[I\times I]$	; + , +	$[3,5]^+$
$\pm\frac{1}{60}[I\times\overline{I}]$	;$[\omega,\omega],[i_I,i'_I]$	$2.[3,3,3]^+$
$+\frac{1}{60}[I\times\overline{I}]$	; + , +	$[3,3,3]^+$
$\pm[O\times O]$	$[i_O,1],[\omega,1],[1,i_O],[1,\omega]$;	$[3,4,3]^+:2$
$\pm\frac{1}{2}[O\times O]$	$[i,1],[\omega,1],[1,i],[1,\omega]$;$[i_O,i_O]$	$[3,4,3]^+$
$\pm\frac{1}{6}[O\times O]$	$[i,1],[j,1],[1,i],[1,j]$;$[\omega,\omega],[i_O,i_O]$	$[3,3,4]^+$
$\pm\frac{1}{24}[O\times O]$	;$[\omega,\omega],[i_O,i_O]$	$2.[3,4]^+$
$+\frac{1}{24}[O\times O]$	; + , +	$[3,4]^+$
$+\frac{1}{24}[O\times\overline{O}]$	; + , −	$[2,3,3]^+$
$\pm[T\times T]$	$[i,1],[\omega,1],[1,i],[1,\omega]$;	$[^+3,4,3^+]$
$\pm\frac{1}{3}[T\times T]$	$[i,1],[j,1],[1,i],[1,j]$;$[\omega,\omega]$	$[^+3,3,4^+]$
$\cong\pm\frac{1}{3}[T\times\overline{T}]$	$[i,1],[j,1],[1,i],[1,j]$;$[\omega,\overline{\omega}]$	”
$\pm\frac{1}{12}[T\times T]$	;$[\omega,\omega],[i,i]$	$2.[3,3]^+$
$\cong\pm\frac{1}{12}[T\times\overline{T}]$	;$[\omega,\overline{\omega}],[i,-i]$	”
$+\frac{1}{12}[T\times T]$	; + , +	$[3,3]^+$
$\cong+\frac{1}{12}[T\times\overline{T}]$	; + , +	”
$\pm[D_{2m}\times D_{2n}]$	$[e_m,1],[j,1],[1,e_n],[1,j]$;	
$\pm\frac{1}{2}[\overline{D}_{4m}\times\overline{D}_{4n}]$	$[e_m,1],[j,1],[1,e_n],[1,j]$;$[e_{2m},e_{2n}]$	
$\pm\frac{1}{4}[D_{4m}\times\overline{D}_{4n}]$	$[e_m,1],[1,e_n]$;$[e_{2m},j],[j,e_{2n}]$	Conditions
$+\frac{1}{4}[D_{4m}\times\overline{D}_{4n}]$	− , − ; + , +	m,n odd
$\pm\frac{1}{2f}[D_{2mf}\times D^{(s)}_{2nf}]$	$[e_m,1],[1,e_n]$;$[e_{mf},e^s_{nf}],[j,j]$	$(s,f)=1$
$+\frac{1}{2f}[D_{2mf}\times D^{(s)}_{2nf}]$	− , − ; + , +	m,n odd, $(s,2f)=1$
$\pm\frac{1}{f}[C_{mf}\times C^{(s)}_{nf}]$	$[e_m,1],[1,e_n]$;$[e_{mf},e^s_{nf}]$	$(s,f)=1$
$+\frac{1}{f}[C_{mf}\times C^{(s)}_{nf}]$	− , − ; +	m,n odd, $(s,2f)=1$

Table 4.2. Chiral groups, II. These groups are mostly “orthochiral,” with a few “parachiral” groups in the last few lines. The generators should be taken with both signs except in the haploid cases, for which we just indicate the proper choice of sign. The “Coxeter names” are explained in Section 4.4.

Group	Extending element	Coxeter Name
$\pm[I\times I]\cdot 2$	$*$	$[3,3,5]$
$\pm\frac{1}{60}[I\times I]\cdot 2$	$*$	$2.[3,5]$
$+\frac{1}{60}[I\times I]\cdot 2_3$ or 2_1	$*$ or $-*$	$[3,5]$ or $[3,5]^\circ$
$\pm\frac{1}{60}[I\times \overline{I}]\cdot 2$	$*$	$2.[3,3,3]$
$+\frac{1}{60}[I\times \overline{I}]\cdot 2_3$ or 2_1	$*$ or $-*$	$[3,3,3]^\circ$ or $[3,3,3]$
$\pm[O\times O]\cdot 2$	$*$	$[3,4,3]:2$
$\pm\frac{1}{2}[O\times O]\cdot 2$ or $\overline{2}$	$*$ or $*[1,i_O]$	$[3,4,3]$ or $[3,4,3]^{+\cdot}2$
$\pm\frac{1}{6}[O\times O]\cdot 2$	$*$	$[3,3,4]$
$\pm\frac{1}{24}[O\times O]\cdot 2$	$*$	$2.[3,4]$
$+\frac{1}{24}[O\times O]\cdot 2_3$ or 2_1	$*$ or $-*$	$[3,4]$ or $[3,4]^\circ$
$+\frac{1}{24}[O\times \overline{O}]\cdot 2_3$ or 2_1	$*$ or $-*$	$[2,3,3]^\circ$ or $[2,3,3]$
$\pm[T\times T]\cdot 2$	$*$	$[3,4,3^+]$
$\pm\frac{1}{3}[T\times T]\cdot 2$	$*$	$[^+3,3,4]$
$\pm\frac{1}{3}[T\times \overline{T}]\cdot 2$	$*$	$[3,3,4^+]$
$\pm\frac{1}{12}[T\times T]\cdot 2$	$*$	$2.[^+3,4]$
$\pm\frac{1}{12}[T\times \overline{T}]\cdot 2$	$*$	$2.[3,3]$
$+\frac{1}{12}[T\times T]\cdot 2_3$ or 2_1	$*$ or $-*$	$[^+3,4]$ or $[^+3,4]^\circ$
$+\frac{1}{12}[T\times \overline{T}]\cdot 2_3$ or 2_1	$*$ or $-*$	$[3,3]^\circ$ or $[3,3]$
$\pm[D_{2n}\times D_{2n}]\cdot 2$	$*$	
$\pm\frac{1}{2}[\overline{D}_{4n}\times \overline{D}_{4n}]\cdot 2$ or $\overline{2}$	$*$ or $*[1,e_{2n}]$	
$\pm\frac{1}{4}[D_{4n}\times \overline{D}_{4n}]\cdot 2$	$*$	Conditions
$+\frac{1}{4}[D_{4n}\times \overline{D}_{4n}]\cdot 2_3$ or 2_1	$*$ or $-*$	n odd
$\pm\frac{1}{2f}[D_{2nf}\times D^{(s)}_{2nf}]\cdot 2^{(\alpha,\beta)}$ or $\overline{2}$	$*[e^\alpha_{2nf}, e^{\alpha s+\beta f}_{2nf}]$ or $*[1,j]$	*See*
$+\frac{1}{2f}[D_{2nf}\times D^{(s)}_{2nf}]\cdot 2^{(\alpha,\beta)}$ or $\overline{2}$	$*[e^\alpha_{2nf}, e^{\alpha s+\beta f}_{2nf}]$ or $*[1,j]$	*Text*
$\pm\frac{1}{f}[C_{nf}\times C^{(s)}_{nf}]\cdot 2^{(\gamma)}$	$*[1, e^{\gamma(f,s+1)}_{2nf}]$	*in*
$+\frac{1}{f}[C_{nf}\times C^{(s)}_{nf}]\cdot 2^{(\gamma)}$	$*[1, e^{\gamma(f,s+1)}_{2nf}]$	*Appendix*

Table 4.3. Achiral groups.

In terms of these, it has a presentation

$$1 = R_1^2 = (R_1R_2)^p = R_2^2 = (R_2R_3)^q = \cdots = R_{n-1}^2 = (R_{n-1}R_n)^s = R_n^2 \\ = (R_iR_j)^2 \ \ (j > i+1).$$

This has an obvious subgroup $[p, q, \ldots, r, s]^+$ of index 2, consisting of the even length words in R_1, ..., R_n, i.e., those which "mention R_1, ..., R_n evenly."

When just one of the numbers $p, q, \ldots, r, s$ is even, say that between R_k and R_{k+1}, there are two further subgroups, namely

$$[^+p, q, \ldots, r, s] \ \text{ and } \ [p, q, \ldots, r, s^+]$$

consisting of words that mention respectively

$$R_1, \ldots, R_k \ \text{ and } \ R_{k+1}, \ldots, R_n$$

evenly, whose intersection is the index 4 subgroup $[^+p, q, \ldots, r, s^+]$ of words that mention *both* of these sets evenly. We've slightly modified Coxeter's notation—he writes $[p^+, \ldots]$ for our $[^+p, \ldots]$ and uses only some special cases.

To obtain elegant names for all of the "polyhedral" groups in dimension 4, we supplement Coxeter's notation by writing G° for the "opposite" group to G, obtained by replacing the element g of G by $+g$ or $-g$ accordingly as $\det = +1$ or -1. Finally, an initial "2." indicates doubling the group by adjoining negatives, while a final ":2" or "$'$2" indicates doubling in some other way, either split or non-split.

4.5 Previous Enumerations

The enumeration of these groups has a long history, starting with Goursat's enumeration of the elliptic groups in 1889. In 1931, Threlfall and Seifert [40] enumerated all the groups, and discovered some of their implications for topology. A standard reference in English has been Du Val's [41] elegant little book *Homographies, Quaternions, and Rotations.*

However, we shall point out that Goursat and Du Val omit certain groups, and that there is another important sense in which *all* these enumerations are incomplete. Every group does appear in Seifert and Threlfall's list, but appears an uncertain number of times, since the equivalences between the groups that depend on parameters are *not* completely listed. The only previous place in the literature when the problem was addressed is in the determination of the crystallographic groups by Hurley [25], who distinguished them with an ad hoc list of invariants. Brown, Bülow, Neubüser, Wondratschek and Zassenhaus [7] continue the use of Hurley's invariants in their enumeration of 4-dimensional space groups.

That the problem is not entirely trivial is neatly illustrated by the fact that all permissible values of h and k in the group Du Val calls

$$(D_{\frac{1}{2}nr}/C_n; D_{\frac{1}{2}nr}/C_n)^*_{s,h,k-}$$

lead to geometrically isomorphic groups! In our system, with different parameters, this group becomes $\pm\frac{1}{2f}[D_{2nf} \times D^{(s)}_{2nf}] \cdot \overline{2}$.

4.6 A Note on Chirality

The subject of chirality is more subtle than it seems. We have already mentioned that when we call the symmetry group of an object "chiral," what we really mean is that the *object* is chiral. In three dimensions, the finite subgroups of the orthogonal group, even the "chiral" ones, are all the same as their mirror images.

However, among the 219 crystallographic space-groups in 3 dimensions are 11 that differ from their mirror images. (For this reason some authors give the total number as 230.) Such groups we call **metachiral**. Metachirality is common among subgroups of the 4-dimensional orthogonal group, since any of the groups $\pm\frac{1}{f}[L \times R]$ or $+\frac{1}{f}[L \times R]$ for which $L \neq R$ is obviously metachiral.

However, there is another interesting phenomenon that first shows itself in this dimension. In lower dimensions, any chiral group that is not metachiral is the chiral part of some achiral group. We call such groups "orthodoxly chiral," or **orthochiral**. Another way to say this is that the corresponding chiral object can be superimposed on a copy of its mirror image so as to yield an achiral one.

In four dimensions, this is not always true, and the groups for which it is not we call **parachiral**. For example, the parachiral group $\pm\frac{1}{7}[C_7 \times C^{(2)}_7]$ is contained to index 14 in the achiral group $\pm[C_7 \times C_7] \cdot 2$, but is not the chiral part of any achiral group since its mirror image is $\pm\frac{1}{7}[C_7 \times C^{(4)}_7]$.

Yet another distinction is made by some chemists—that between "shoe chirality" and "potato chirality." We expect neither shoes nor potatoes to be achiral, but yet we discriminate left shoes from right shoes, but not "left potatoes" from "right potatoes!" Why is this?

The answer is that a potato can be continuously deformed into its mirror image while preserving its property of being a chiral potato at all times. Topologists call such a deformation an "isotopy" within the class of chiral potatoes, and so we shall call the shoe kind of chirality **isochirality** (meaning, "chirality" even modulo isotopy).

In two dimensions, the class of chiral (i.e., scalene) triangles is isochiral, since the sides either increase counter-clockwise (for "left" triangles) or

clockwise (for "right" ones). In three dimensions, chiral tetrahedra aren't isochiral, since all chiral tetrahedra are isotopic inside the class of them.

Appendix: Completeness of the Tables

We establish this by showing that they handle all possible pairs of homomorphisms from L, R onto the same abstract finite F. But since

$$[l, r]^{[l_1, r_1]} = [l^{l_1}, r^{r_1}],$$

we can replace L, R by independent conjugates of themselves, so we need only work up to this notion of "geometric equivalence".

The Completeness of Tables 4.1 and 4.2

Now it is easy to classify normal subgroups of the 3-dimensional chiral groups: There is just one for each of the orders

$$\begin{array}{ccc} 1, 4, 12 & \text{for} & T \\ 1, 4, 12, 24 & \text{for} & O \\ 1, 60 & \text{for} & I \\ m & (\text{where } m|n) \text{ for} & C_n \text{ or } D_n, \end{array}$$

except that when n is even, D_{2n} has two normal subgroups C_n and D_n of order n. So the *kernel* of α or β is determined by the *index* f, except for the two cases for D_{2n} when n is even and $f = 2$:

$$\begin{array}{l} \frac{1}{2}[\ldots D_{2n} \ldots] \text{ indicates that } ker = C_n \\ \frac{1}{2}[\ldots \overline{D}_{2n} \ldots] \text{ indicates that } ker = D_n. \end{array}$$

However, there are different cases that have homomorphisms with the same kernel because F has an automorphism not induced by any element of GO_3 (and so necessarily outer). It is easily checked that these are:

Our notation	Sufficient description of automorphism
$\frac{1}{60}[\ldots \overline{I} \ldots]$	extends A_5 to S_5
$+\frac{1}{24}[\ldots \overline{O} \ldots]$	negates elements of $2S_4 \backslash 2A_4$ [2]
$\frac{1}{4}[\ldots \overline{D} \ldots]$	moves the "cyclic part" [3]
$\frac{1}{f}[\ldots D^{(s)}_{nf} \ldots]$	acts as s^{th} power
$\frac{1}{f}[\ldots C^{(s)}_{nf} \ldots]$	map on cyclic part

There are three groups in Table 4.2 for which we give alternative notations involving $\overline{T}$. This peculiar repetition simplifies Table 4.3.

[2] This entry can be ignored in the projective and diploid cases.

[3] Goursat, and following him, Du Val, omitted $\frac{1}{4}[D_{4m} \times \overline{D}_{4n}]$, which arises because $F \cong D_4$ has automorphisms freely permuting its non-identity elements, unlike a larger D_{2k}, whose "cyclic part" C_k is uniquely determined.

The Completeness of Table 4.3

Here we obtain G from the "half-group" H corresponding to some isomorphism $L/L_0 \cong R/R_0$ by adjoining an extending element $*[a,b]$, which must normalize H. We shall show that (at some cost) the extending element may be reduced to the form $*[1,c]$, and also that (at no cost) c can be multiplied by any element of R_0, or altered by any inner automorphism of R, while finally c must be in the part of R that is fixed (mod R_0) by the isomorphism (since $(*[1,c])^2 = [c,c]$ must be in H).

For, conjugation by $[1,a]$ replaces $*[a,b]$ by

$$(*[a,b])^{[1,a]} = [1,\overline{a}] * [a,b][1,a] = *[\overline{a}a, ba] = *[1,c], \text{ say,}$$

at the cost of replacing $[l,r]$ by $[l,\overline{a}ra]$, which changes the isomorphism to a geometrically equivalent one. If $r_0 \in R_0$, $*[1,cr_0]$ defines the same group as does $*[l_1,cr_1]$ for any $[l_1,r_1] \in H$, and this reduces to $*[1,cr_1l_1]$ on conjugation by $[1,l_1]$, which replaces the r in $[l,r]$ by $\overline{l_1}rl_1$, its image under an arbitrary inner automorphism of R.

These considerations almost always suffice to restrict the extending element to

$$*[1,\pm 1] = * \text{ or } -*,$$

notated respectively by $\cdot 2_3$ or $\cdot 2_1$ (the subscript being the dimension of the negated space). The exceptions are the "$D \times D$" and "$C \times C$" cases, for which Table 4.3 lists every c, and just two more cases, denoted

$$\pm\frac{1}{2}[O \times O] \cdot \overline{2} \quad \text{and} \quad \pm\frac{1}{4}[\overline{D}_{4n} \times \overline{D}_{4n}] \cdot \overline{2}$$

in which we can take $c = i_O$ and e_{2n}, respectively.

As we remarked, the reduction to the form $*[1,c]$ comes at the cost of replacing the isomorphism by a geometrically equivalent one, and in the "$T \times T$" case, this sometimes replaces the identity isomorphism by the one we indicate by $\overline{T}$, namely

$$\omega \to \overline{\omega} \quad \text{and} \quad \quad i \to \overline{i} = -i.$$

The Last Eight Lines of Table 4.3

For $\pm[D \times D] \cdot 2$, we start from the fact that the extending element $*[a,b]$ may be reduced (mod H) and must normalize H, and therefore also E,

since E is a characteristic subgroup of H (except in the easy cases when $f \leq 2$, which we exclude). This puts a and b in $e^{\mathbb{R}}(1 \text{ or } j)$, and so (since $[j,j] \in H$) we can take $*[a,b] = *[e^\lambda, e^\mu]$ (leading to $\pm[D \times D] \cdot 2^{(\alpha,\beta)}$) or $*[a,b] = *[e^\lambda, e^\mu j]$ (leading to $\pm[D \times D] \cdot \overline{2}$—see footnote 4.) In the first case, we must have

$$[j,j]^{*[e^\lambda, e^\mu]} = [j,j]^{[e^\lambda, e^\mu]} = [je^{2\lambda}, je^{2\mu}] \in H,$$

which forces $\lambda = \frac{\alpha}{2}$ and $\mu = \frac{\alpha s + \beta f}{s}$, where $\alpha, \beta \in \mathbb{Z}$. The fact that the square of this is in H imposes the condition $\alpha g + \beta f \equiv 0 \pmod 2$.

G is unaltered when we increase α or β by 2 since $[e, e^s]$, $[1, e^f] \in H$. For a similar reason, s is initially only defined (mod f), but the equation

$$*[e^{\frac{\alpha}{2}}, e^{\frac{\alpha s + \beta f}{2}}] = *[e^{\frac{\alpha}{2}}, e^{\frac{\alpha(s+f)+(\beta-\alpha)f}{2}}]$$

shows that

$$\langle s, \alpha, \beta \rangle \approx \langle s + f, \alpha, \beta - \alpha \rangle,$$

so from now on it is better to regard s as defined mod $2f$. Since $[e^s, s] = [e, e^s]^{*[a,b]}$ and $[e, e^{s^2}]$ are both in H, we must have $s^2 = fg + 1$ for some integer $g \in \mathbb{Z}$.

To discuss equalities, we must consider all possibilities for an element that transforms this group $\langle s, \alpha, \beta \rangle$ to a similar one $\langle s', \alpha', \beta' \rangle$. The transforming element can also be reduced mod H and after taking account of $*$ and $[1,j]$ (which takes $\langle s, \alpha, \beta \rangle$ to itself or $\langle -s, \alpha, -\beta \rangle$), can be supposed to normalize H and therefore have the form $[e^{\frac{a}{2}}, e^{\frac{as+bf}{2}}]$, with $a, b \in \mathbb{Z}$. We find that transforming by this adds some multiple (which can be odd) of (f, g) to (α, β), so the only further relation is $\langle s, \alpha, \beta \rangle \approx \langle s, \alpha + f, \beta + g \rangle$.

To summarize, we have for this group

Variables	Conditions	Equalities
$\alpha \pmod 2$	$s^2 = fg + 1$	$\langle s, \alpha, \beta \rangle$
$\beta \pmod 2$	$\alpha g + \beta f \equiv 0 \pmod 2$	$\approx \langle -s, \alpha, -\beta \rangle$
$s \pmod{2f}$		$\approx \langle s + f, \alpha, \beta - \alpha \rangle$
		$\approx \langle s, \alpha + f, \beta + g \rangle$,

[4] In the second case we can choose new generators to simplify the group; namely, conjugation by $[1, e^\lambda]$ fixes E and replaces $*[e^\lambda, e^\mu j]$ by $*[1, e^{\mu - \lambda} j] = *[1, J]$, and then J can replace j, since $(*[1,J])^2 = [J,J]$ must be in H.

while for $\pm[D \times D^{(s)}] \cdot \overline{2}$ we have

Variables	Conditions	Equalities
$s \pmod f$	$s^2 = fg - 1$	$\langle s \rangle \approx \langle -s \rangle$.

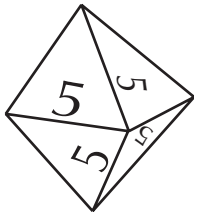
Equalities in the other cases are summarized as:

Group	Variables	Conditions	Equalities
$+[D \times D^{(s)}] \cdot 2^{(\alpha,\beta)}$	$\alpha \pmod 2$ $\beta \pmod 4$ $s \pmod{4f}$	$s^2 = fg + 1$ $\alpha g \equiv 0 \pmod 4$ n odd, g even	$\langle s, \alpha, \beta \rangle$ $\approx \langle -s, \alpha, -\beta \rangle$ $\approx \langle s + 2f, \alpha, \beta - 2\alpha \rangle$ $\approx \langle s, \alpha, \beta + 2h \rangle$
$+[D \times D] \cdot \overline{2}$	$s \pmod{2f}$	$s^2 = fg - 1, g = 2h$ even	$\langle s \rangle \approx \langle -s \rangle$
$\pm[C \times C] \cdot 2^{(\gamma)}$	$s \pmod f$ $\gamma \pmod 2$ $*[1, e^{\frac{\gamma(f,s+1)}{2}}]$	$s^2 = fg - 1$ $(g, s-1)\gamma \equiv 0 \pmod 2$ $(f, s+1)\gamma \equiv 0 \pmod 2$ g even	$\langle s, \gamma \rangle$ $\approx \langle s, -\gamma \rangle$
$+[C \times C] \cdot 2^{(\gamma)}$	$s \pmod{2f}$ $\gamma \pmod{2d}$ $*[1, e^{\frac{\gamma(f,s+1)}{2}}]$ $d = \frac{(2f,s+1)}{(f,s+1)}$	$s^2 = fg - 1$ $(g, s-1)\gamma \equiv 0 \pmod 4$ $(f, s+1)\gamma \equiv 0 \pmod 2$ n odd, $g = 2h$ even	$\langle s, \gamma \rangle$ $\approx \langle s, -\gamma \rangle$

Table 4.4 summarizes the different achiral groups among the last four lines of Table 4.3. In the last eight lines, it is always permissible to replace D_2 by C_2 and $\overline{D_4}$ by D_4.

f, g even	:	$\cdot 2^{(0,0)}, \cdot 2^{(0,1)}, \cdot 2^{(1,0)}, \cdot 2^{(1,1)}$ and $\cdot \overline{2}$	
else		$\cdot 2$ and $\cdot \overline{2}$	
f, h even	:	$\cdot 2^{(0,0)}, \cdot 2^{(0,2)}, \cdot 2^{(1,0)}, \cdot 2^{(1,2)}$ and $\cdot \overline{2}$	
else		$\cdot 2$ and $\cdot \overline{2}$	
g even	:	$\cdot 2^{(0)}, \cdot 2^{(1)}$ and $\cdot \overline{2}$	
else		$\cdot 2$ and $\cdot \overline{2}$	
h even	:	$\cdot 2^{(0)}, \cdot 2^{(d)}$ and $\cdot \overline{2}$	$d = \frac{(2f,s+1)}{(f,s+1)}$
else		$\cdot 2$ and $\cdot \overline{2}$	

Table 4.4. Different achiral groups.



The Hurwitz Integral Quaternions

5.1 The Hurwitz Integral Quaternions

How shall we define what it means for the quaternion $q = a + bi + cj + dk$ to be **integral**? One obvious possibility (following the example of the Gaussian integers) is to demand that a, b, c, and d be ordinary rational integers. Technically, we say that $a + bi + cj + dk$ is a **Lipschitz integer** exactly when a, b, c, $d \in \mathbb{Z}$. This is equivalent to $q = z_1 + z_2 j$, where z_1 and z_2 are Gaussian integers. However, Hurwitz later found a different definition that turns out to have nicer properties. We say that $a+bi+cj+dk$ is a **Hurwitz integer** just if either all of a, b, c, d are in $\mathbb{Z}$ or all are in $\mathbb{Z} + \frac{1}{2}$.

When we studied the arithmetics of the Gaussian integers in Chapter 2, an important role was played by "division with small remainder," namely that one can divide any (Gaussian) integer, Z, by any non-zero one, z, so as to have an integer quotient, Q, and a remainder, R, strictly smaller than the divisor. Recall how this was proved: If $Z/z = a + bi$ and we let $Q = A + Bi$, where A, B are nearest integers to a, b, then

$$R/z = Z/z - Q = (a - A) + (b - B)i$$

so

$$N(R/z) = (a - A)^2 + (b - B)^2 \leq (1/2)^2 + (1/2)^2 = 1/2 < 1.$$

However, if Z and $z \neq 0$ are Lipschitz-integral quaternions with $q = Zz^{-1} = a + bi + cj + dk$, and we let A, B, C, D be the nearest inte-

gers to a, b, c, d and define $Q = A + Bi + Cj + Dk$ and $R = Z - qz$, then we find

$$N(Rz^{-1}) = (a-A)^2 + \cdots + (d-D)^2 \leq (1/2)^2 + \cdots + (1/2)^2 = 1,$$

showing only that $N(R) \leq N(z)$. Unfortunately, the fact that this inequality is not strict makes all the difference in the world, because the arguments depend on repeated norm-reductions.

Note that the only case when $N(R) = N(z)$ is when

$$|a-A| = |b-B| = |c-C| = |d-D| = 1/2,$$

that is to say, when a, b, c, d are all in $\mathbb{Z} + \frac{1}{2}$. This is what makes Hurwitz' definition preferable, for if we suppose Z, $z \neq 0$ are Hurwitz-integral and define q, Q, and R as above, then either we have

$$Z = Qz + R \text{ with } N(R) < N(z)$$

or

$$N(R) = N(z),$$

in which case the above argument shows q is actually a Hurwitz integer and $Z = qz + 0$ (in which $N(0) < N(z)$).

We have proved: The Hurwitz integers, but not the Lipschitz ones, have the "division with small remainder" property. This makes it easier to work in H rather than in L. Theorems about L are usually proved by reduction to theorems about H.

5.2 Primes and Units

We now turn to the theory of prime factorization of Hurwitz integers. A prime Hurwitz integer P is one whose norm is a rational prime p. Analogously to the fact that $p = p \times 1$ and $p = 1 \times p$ are the only ways p is the product of two rational primes, its only factorizations into two Hurwitz integers must have the form

$$P = P' \times U \text{ and } P = V \times P'',$$

where $N(P') = N(P'') = p$ and $N(U) = N(V) = 1$. So, we must also study the **Hurwitz units**, namely the Hurwitz integers of norm 1.

Theorem 1. *There are precisely 24 Hurwitz units, namely the eight Lipschitz units* ± 1, $\pm i$, $\pm j$, $\pm k$, *and the 16 others* $\pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$.

Proof. For a Lipschitz unit, we must have one of $|a|$, $|b|$, $|c|$, $|d| \geq 1$, and the equation $a^2 + b^2 + c^2 + d^2 = 1$ implies that that coordinate is ± 1 and the rest are 0. In the remaining cases, we must have $|a|$, $|b|$, $|c|$, $|d| \geq \frac{1}{2}$, and since $a^2 + b^2 + c^2 + d^2 = 1$, all are $\pm\frac{1}{2}$.

The Hurwitz units completely solve the problem of factorizing a Hurwitz prime. Namely, if P is a Hurwitz prime, then its only factorizations as a product of two Hurwitz integers are

$$P = PU^{-1} \times U \quad \text{and} \quad P = V \times V^{-1}P$$

as U and V run over the 24 Hurwitz units. These are the only possibilities, since we already showed that one factor must be a unit, and either factor determines the other, and indeed they are factorizations since if U, V are units, so are U^{-1}, V^{-1}, so that PU^{-1} and $V^{-1}P$ are Hurwitz integers.

The way a Hurwitz integer factors into primes depends heavily on whether that integer is imprimitive (i.e., divisible by some natural number $n > 1$). In the primitive case, we have

Theorem 2. *To any factorization of the norm q of a primitive Hurwitz integer Q into a product $p_0 p_1 \cdots p_k$ of rational primes, there is a factorization*

$$Q = P_0 P_1 \cdots P_k$$

*of Q into a product of Hurwitz primes with $N(P_0) = p_0$, ..., $N(P_k) = p_k$. We shall say that "the factorization $P_0 P_1 \ldots P_k$ of Q is **modelled on** the factorization $p_0 p_1 \ldots p_k$ of $N(Q)$." Moreover, if $Q = P_0 P_1 \cdots P_k$ is any one factorization modelled on $p_0 p_1 \ldots p_k$, then the others have the form*

$$Q = P_0 U_1 \cdot U_1^{-1} P_1 U_2 \cdot \ldots \cdot U_k^{-1} P_k$$

*i.e., "the factorization on a given model is unique up to **unit-migration**."*

Thus, a primitive Hurwitz quaternion of norm 60 has, up to unit-migration, just 12 factorizations into prime quaternions, namely those modelled on the 12 factorizations

2.2.3.5	2.2.5.3	2.3.2.5	2.5.2.3	2.3.5.2	2.5.3.2
3.2.2.5	5.2.2.3	3.2.5.2	5.2.3.2	3.5.2.2	5.3.2.2

of 60 into rational primes. The full number of factorizations will be $24^3 \times 12 = 165888$, since the 24 units can migrate across any one of three places.

Proof. The ideal $p_0\mathsf{H} + Q\mathsf{H}$ must be principal, so that we have

$$p_0\mathsf{H} + Q\mathsf{H} = P_0\mathsf{H}$$

for some P_0. Here, $[P_0]$ must divide $[p_0] = p_0^2$, so it is one of 1, p_0, p_0^2.

However, if $[P_0] = 1$, then $p_0\mathsf{H} + Q\mathsf{H}$ would be all of H, which cannot be, since its typical element $p_0a + Qb$ has norm

$$[p_0a] + 2[p_0a, Qb] + [Qb] = p_0^2[a] + 2p_0[a, Qb] + p_0 \cdots p_k[b],$$

divisible by p_0. Nor can P_0 have norm p_0^2, for then since P_0 divides p_0 we should have $p_0 = P_0U$, where U is a unit (since $[U] = 1$), which shows that p_0 divides Q (since $p_0U^{-1} = P_0$ does). The only possibility that remains is $[P_0] = p_0$, showing that P_0 is a Hurwitz prime dividing Q.

So we have $Q = P_0Q_1$, where $[Q_1] = p_1 \cdots p_k$, and P_0 is unique up to right multiplication by a unit. Repeating the argument, we can produce similar factorizations

$$Q_1 = P_1Q_2, \quad Q_2 = P_2Q_3, \quad \ldots$$

in which P_1, P_2, ... are Hurwitz primes of norms p_1, p_2, ... This gives $Q = P_0P_1 \cdots P_kQ'$, where Q' must be a unit (and thus can be absorbed into P_k). The argument has shown that the factorization is unique up to unit-migration.

5.3 Quaternionic Factorization of Ordinary Primes

Before we complete the discussion, we must study the quaternionic factorizations of rational integers and, in particular, of a rational prime p. Recall that

$$(i) \text{ a } \textbf{quadratic residue } r \text{ satisfies } r \equiv a^2 \pmod{p}, \\ \text{for some } a \not\equiv 0 \pmod{p},$$

while the **quadratic non-residues** are the other numbers $\not\equiv 0 \pmod{p}$. We show that

$$(ii) \text{ each quadratic non-residue } n \text{ satisfies } n \equiv a^2 + b^2 \pmod{p}, \\ \text{for some } a, b \not\equiv 0 \pmod{p},$$

and

$$(iii)\ 0 \equiv a^2 + b^2 + c^2 \pmod{p}, \\ \text{for some } a, b, c \not\equiv 0 \pmod{p}.$$

Since the non-residues are the multiples of any fixed one by the residues, it suffices to prove (*ii*) for n, the least possible non-residue. But then $n = r + 1$ for a quadratic residue r, and so for $r \equiv a^2 \pmod{p}$ we deduce $n = a^2 + 1^2 \pmod{p}$. Finally, $0 = -1 + 1^2$, which is congruent to the sum of ≤ 3 squares (including 1^2), since -1 is congruent to the sum of ≤ 2 squares. This enables us to prove the following

Theorem 3. *Each rational prime p admits at least one quaternionic factorization*

$$p = P_0\overline{P_0}.$$

Proof. Since $x^2 \equiv (p-x)^2 \pmod{p}$, we can suppose in (*iii*) that $0 \leq a, b, c \leq p/2$, thereby obtaining a solution of $a^2 + b^2 + c^2 = mp$ with $0 < m < p$, and a quaternion $Q = a + bi + cj$ of norm mp. Then if $p\mathbb{H} + Q\mathbb{H} = P_0\mathbb{H}$, we see as before that $[P_0] = p$.

In fact p has as many such factorizations as there are quaternions P of norm p. By analytic methods it can be shown that the total number is $24(p+1)$ (if $p > 2$) or 24 (if $p = 2$).

What happens to unique factorization when Q need not be primitive? We shall suppose that Q of norm $2^{n_0}p_1^{n_1}p_2^{n_2}\ldots p_k^{n_k}$ is exactly divisible by the rational integer $2^{s_0}p_1^{s_1}p_2^{s_2}\ldots p_k^{s_k}$. Then the answer is given by

Theorem 4. *The number of factorizations (counted up to unit-migration) that are modelled on a given factorization of $N(Q)$ into primes is the product*

$$\prod_{i\geq 1} C_{n_i,s_i}(p_i)$$

of "truncated Catalan polynomials," evaluated at the odd primes involved.

The first few Catalan polynomials are

$$\begin{aligned} C_0(x) = C_1(x) &= 1 \\ C_2(x) &= x + 1 \\ C_3(x) &= 2x + 1 \\ C_4(x) &= 2x^2 + 3x + 1, \end{aligned}$$

and their coefficients in general can be read from the "Catalan triangle" (Figure 5.1 — see also [22]). The truncated Catalan polynomial $C_{n,s}(x)$ consists of the terms of $C_n(x)$ that have degree at most s.

Proof. It will suffice to consider factorizations of the form

$$Q = P_1 P_2 \dots P_n$$

where all the P_i have the same prime norm p.

To this end, suppose Q (of norm p^n) is divisible by p^s but not p^{s+1}, and write $Q = p^s P$. Then since P is primitive, it has a factorization

$$P = P'_1 P'_2 \dots P'_{n-2s}$$

that is unique up to unit-migration.

We quote the result that (up to unit right multiplications) there are just $p+1$ quaternions of norm p and ask (still up to unit right multiplications) whether P_1 is or is not equal to P'_1. The one case when it is leads to the factorization problem for a quaternion of norm p^{n-1} that is still exactly divisible by p^s, which inductively has $C_{n-1,s}(p)$ solutions. The p cases when it is not lead to problems for quaternions of norm p^{n-1} that are exactly divisible by p^{s-1}, and so each has $C_{n-1,s-1}(p)$ solutions. The argument establishes the recursion

$$C_{n,s}(p) = C_{n-1,s}(p) + pC_{n-1,s-1}(p)$$

that defines the Catalan polynomials. For example, the reduced problems for factorization of a norm p^7 quaternion exactly divisible by p^2 are one for a norm p^6 quaternion exactly divisible by p^2 (leading to $C_{6,2} = 9p^2 + 5p + 1$ solutions) and p for a norm p^6 quaternion exactly divisible by p (each leading to $C_{6,1} = 5p + 1$ solutions), in agreement with

$$9p^2 + 5p + 1 + p(5p + 1) = 14p^2 + 6p + 1 = C_{7,2}(p).$$

×								
	1							
×		1						
	1		1					
×		2		1				
	2		3		1			
×		5		4		1		
	5		9		5		1	
×		14		14		6		1
	14		28		20		7		1
×		42		48		27		8		1

Figure 5.1. The Catalan triangle is formed in the same manner as Pascal's triangle, except that no number may appear to the left of the vertical bar.

For a quaternion of norm $p^m q^n \dots$ exactly divisible by $p^s q^t \dots$, we still get exactly these numbers of choices for the factors of norm p, no matter where they are placed, so the total number of factors up to unit-migration is the product of these numbers for the distinct prime factors.

5.4 The Metacommutation Problem

Even rational integers do not have unique factorizations; for instance,

$$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2 \cdot 5 \cdot 3 \cdot 2 = (-3) \cdot 2 \cdot 5 \cdot (-2) = \cdots$$

However, the term "unique factorization" is justified since all such factorizations are readily obtained from any one of them.

Now Theorem 2 is usually called the unique factorization theorem for primitive (Hurwitzian) quaternions, and it really deserves this name for factorizations on a given model because any two such are related by the well-understood operation of unit-migration (to which we should add recombination— see below—in the imprimitive case).

However, this does not completely justify the term "unique factorization" for Hurwitzians. To do so would require solving a problem we call the **metacommutation problem**: How does a prime factorization PQ modelled on pq determine a corresponding factorization $Q'P'$ modelled on qp? This difficult problem does not seem to have been addressed in the literature.

There are, in fact, three basic ways in which prime factorization can be changed. We have already met "unit-migration" which replaces PQ by $PU \cdot \overline{U}Q$. There is also **recombination** which replaces a pair $P\overline{P}$ of conjugate primes of norm p by any other such pair $P'\overline{P'}$. Finally, any product PQ of distinct Hurwitz primes of norms p and q can be refactorized as a product $Q'P'$ of Hurwitz primes of norms q and p. We call this last operation **metacommutation** of P and Q; the resulting factorization $Q'P'$ is unique up to unit-migration. It is not hard to see that any two prime factorizations of a quaternion are related by repeated applications of these three "operations."

5.5 Factoring the Lipschitz Integers

In order to understand Lipschitzian factorizations, we must understand how they are related to the Hurwitzians, both additively and multiplicatively.

Geometrically, the Lipschitzians $\mathsf{L} = I_4$ form one copy of the 4-dimensional cubic lattice I_4. There are two more copies of I_4 inside the Hurwitzians, namely $\omega\mathsf{L} = I_4'$ and $\overline{\omega}\mathsf{L} = I_4''$. The intersection of these three I_4s (which is the intersection of any two of them) is

$$\mathsf{L} \cap \omega\mathsf{L} \cap \overline{\omega}\mathsf{L} = D_4,$$

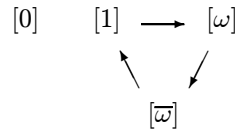
(a copy of the four-dimensional "orthoplex lattice," or root lattice of type D_4). The lattice of all Hurwitzians is their union

$$\mathsf{H} = \mathsf{L} \cup \omega\mathsf{L} \cup \overline{\omega}\mathsf{L} = D_4^*,$$

so-called because it is, in fact, the lattice dual to D_4.

Additively, D_4 has four cosets $[0], [1], [\omega], [\overline{\omega}]$ in D_4^*, and the lattices we have mentioned are various unions of these (Figure 5.2).

Multiplicatively, the important fact is that multiplication by ω (on either side) has the effect



and so fixes D_4 and D_4^* but cyclically permutes I_4, I_4', I_4''.

The Hurwitzians of even norm are precisely those in $[0]$; in fact, they will stay in $[0]$ upon multiplication by ω or $\overline{\omega}$ (on either side). A Hurwitzian of odd norm is in just one of $[1]$, $[\omega]$, and $[\overline{\omega}]$; equivalently, just one of Q, ωQ, and $\overline{\omega}Q$ is in $[1]$.

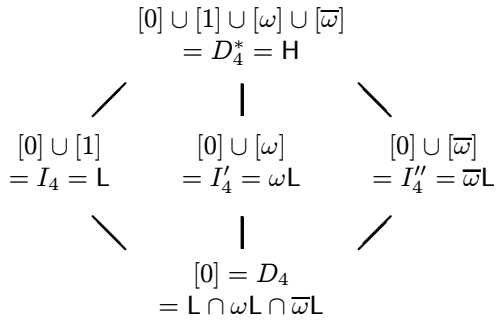


Figure 5.2. Containment among sublattices of H.

5.5.1 Counting Lipschitzian Factorizations

This enables us to prove

Lemma 1. *Any factorization of a Lipschitzian into Hurwitzians is equivalent by unit-migration to one into Lipschitzians.*

Since the units we use will be powers of ω, which is not Lipschitz-integral, this means that the factorization into Lipschitzians is definitely not "unique."

Proof. We study the effect of "ω-migration"

$$\alpha = \beta\gamma \to \alpha = \beta\omega \cdot \overline{\omega}\gamma$$

on a 2-term factorization of a Lipschitzian α. Since α is in [0] or [1], Figure 5.3 includes all possibilities for the cosets of β and γ, and there is a factorization in each triple for which both factors are Lipschitzian.

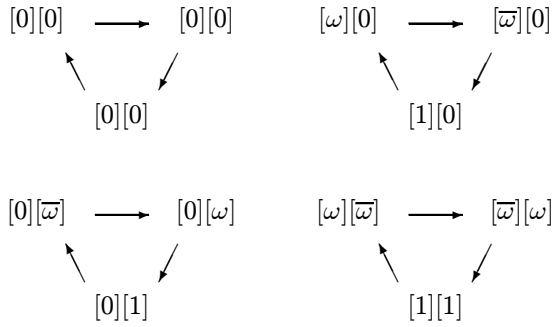


Figure 5.3. "$\beta\gamma \to \beta\omega \cdot \overline{\omega}\gamma$."

A more detailed investigation shows

Theorem 5. *The number of Lipschitzian factorizations equivalent by unit-migration to*

$$P_1 P_2 \dots P_k$$

is $8^{k-1}3^{l-1}$*, where* l *is the number of factors of even norm.*

For between p_i and $p_{i+1} \dots p_k$, we can always transfer all eight Lipschitzian units, and also the three powers of ω just when both have even norm.

The Octonions and Their Applications to 7- and 8-Dimensional Geometry

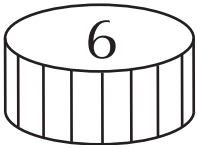
The octonions are formal expressions

$$x_\infty + x_0 i_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6$$

(x_t real), which constitute the algebra over the reals generated by units $i_0, \ldots, i_6$ that satisfy

$$i_n^2 = -1 \quad \text{and}$$
$$i_{n+1} i_{n+2} = i_{n+4} = -i_{n+2} i_{n+1}$$
$$i_{n+2} i_{n+4} = i_{n+1} = -i_{n+4} i_{n+2}$$
$$i_{n+4} i_{n+1} = i_{n+2} = -i_{n+1} i_{n+4}$$

(where the subscripts run modulo 2).



The Composition Algebras

In Chapter 2, we interpreted the two-square identity

$$(x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2)$$

as saying that in the algebra of complex numbers the norm of a product equals the product of the norms, which here we write[1]

$$[z_1 z_2] = [z_1][z_2].$$

In Chapters 3 and 4, we made heavy use of the corresponding result for Hamilton's algebra of quaternions.

In this chapter, we shall prove Hurwitz's celebrated theorem that the only algebras with such a composition law are the well-known ones in 1, 2, 4, and 8 dimensions (*exactly*, for the algebras with a multiplicative identity, and *up to isotopy*, if not). We shall suppose at first that our algebra does possess a two-sided identity element 1, so that $1x = x = x1$, and as usual,

$$[x, y] = \frac{[x + y] - [x] - [y]}{2}$$

(we are working over the reals, where 2 is invertible). We repeatedly use the principle that if $[x, t] = [y, t]$ for all t, then $x = y$.

[1] The use of square brackets for norms and inner products in this chapter should, of course, not be confused with that for certain maps in earlier chapters.

6.1 The Multiplication Laws

We first deduce some consequences of

(M1) **The Composition Law:** $[xy] = [x][y]$.

(M2) **The Scaling Laws:** $[xy, xz] = [x][y, z]$ (and $[xz, yz] = [x, y][z]$) .

Proof. Replacing y by $y + z$ in (M1) gives

$$[xy] + [xz] + 2[xy, xz] \stackrel{M1}{=} [x]([y] + 2[y, z] + [z]),$$

from which we cancel some terms and divide by 2.

(M3) **The Exchange Law :** $[xy, uz] = 2[x, u][y, z] - [xz, uy]$.

Proof. Replacing x by $x + u$ in (M2) gives

$$[xy, xz] + [xy, uz] + [uy, xz] + [uy, uz] \stackrel{M2}{=} ([x] + 2[x, u] + [u])[y, z]$$

from which we cancel some terms and rearrange.

6.2 The Conjugation Laws

Now, we prove three laws involving the conjugation $\overline{x} = 2[x, 1] - x$.

(C1) **Braid Laws:** $[xy, z] = [y, \overline{x}z]$ (and $[xy, z] = [x, z\overline{y}]$) .

Proof. Put $u = 1$ in (M3) to get

$$2[x, 1][y, z] - [xz, y] = [y, (2[x, 1] - x)z].$$

(Figure 6.1 explains the name.)

(C2) **Biconjugation:** $\overline{\overline{x}} = x$.

Proof. Put $y = 1$ and $z = t$ and use (C1) twice to get

$$[x, t] = [x1, t] = [1, \overline{x}t] = [\overline{\overline{x}}1, t] = [\overline{\overline{x}}, t] \text{ for all } t.$$

Product Conjugation: $\overline{xy} = \overline{y}\,\overline{x}$. (C3)

Proof. Repeated use of (C2) gives

$$[\overline{y}\,\overline{x}, t] = [\overline{x}, yt] = [\overline{x}\,\overline{t}, y] = [\overline{t}, xy] = [\overline{t}, xy.1] = [\overline{t}\,\overline{xy}, 1] = [\overline{xy}, t].$$

6.3 The Doubling Laws

We now let H be an n-dimensional subalgebra containing 1, let i be a unit vector orthogonal to H, and $a, b, c, \ldots$ denote typical elements of H. Then $\overline{i} = -i$, and $[i, a] = 0$, which will often cause the term $2[x, u][y, z]$ to vanish in applications of the exchange law. Our next three laws evaluate the inner product, conjugation, and product on the "Dickson double algebra" $H + iH$ in terms of those on H.

Inner-Product Doubling: $[a + ib, c + id] = [a, c] + [b, d]$. (D1)

Proof. This is proved by the three equations

$$[a, id] = [a\overline{d}, i] = 0, \quad [ib, c] = [i, c\overline{b}] = 0, \quad [ib, id] = [i][b, d] = [b, d].$$

Conjugation Doubling: $\overline{a + ib} = \overline{a} - ib$ (so $ib = -\overline{ib} = -\overline{b}\,\overline{i} = \overline{b}i$) . (D2)

Proof. $\overline{ib} = 2[ib, 1] - ib = -ib$.

Composition Doubling: $(a + ib)(c + id) = (ac - d\overline{b}) + i(cb + \overline{a}d)$. (D3)

Proof. This is proved by the three equations

$$[a.id, t] \overset{C1}{=} [id, \overline{a}t] \overset{M3}{=} 0 - [it, \overline{a}d] \overset{C1}{=} [t, i.\overline{a}d]$$

$$[ib.c, t] \overset{C1}{=} [ib, t\overline{c}] \overset{D2}{=} [\overline{b}i, t\overline{c}] \overset{M3}{=} 0 - [\overline{b}\,\overline{c}, ti] \overset{C1}{=} [\overline{b}\overline{c}.i, t] \overset{D2}{=} [i.cb, t]$$

$$[ib.id, t] \overset{C1}{=} -[ib, t.id] \overset{M3}{=} 0 + [i.id, tb] \overset{C1}{=} -[id, i.tb] \overset{M2}{=} -[i][d, tb] \overset{C1}{=} [-d\overline{b}, t].$$

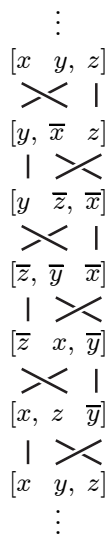


Figure 6.1. Six inner products related by the braid law.

6.4 Completing Hurwitz's Theorem

What this has shown is that whenever our composition algebra Z contains a proper subalgebra, it also contains its Dickson double. Therefore, if Z is finite-dimensional it must be obtained by repeated doubling from its smallest subalgebra $\mathbb{R}$, and in particular must itself be the double of an algebra Y, which might in turn be the double of an algebra X, and so on. We shall now show that the composition property can survive at most three doubling operations.

When is $Z = Y + i_Z Y$ a composition algebra? Just when for all $a, b, c, d \in Y$ we have

$$[a + i_Z b][c + i_Z d] = [(ac - d\overline{b}) + i_Z(cb + \overline{a}d)].$$

However, since this expands to

$$[a][c] + [a][d] + [b][c] + [b][d] = [ac] - 2[ac, d\overline{b}] + [d\overline{b}] + [cb] + 2[cb, \overline{a}d] + [\overline{a}d],$$

the answer is precisely when

$$[ac, d\overline{b}] = [cb, \overline{a}d],$$

or equivalently, when

$$[ac.b, d] = [a.cb, d],$$

which holds just when $ac.b = a.cb$ for all $a, b, c \in Y$.

So the answer is

Lemma 1. *Z is a composition algebra just when Y is an associative composition algebra.*

When is $Y = X + i_Y X$ an associative composition algebra? Obviously, X must also have these properties, but since $i_Y b.c = i_Y.cb$ for all $b, c \in X$, we shall need to have $bc = cb$; that is to say, X must also be commutative.

But now, for $a, b, c, d, e, f \in X$, we find

$$\begin{aligned}(a + i_Y b)(c + i_Y d).(e + i_Y f) &= [(ac - d\overline{b}) + i_Y(cb + \overline{a}d)](e + i_Y f)\\ &= (ac - d\overline{b})e - f(\overline{b}\overline{c} + \overline{d}a) + i_Y[e(cb + \overline{a}d) + (\overline{c}\,\overline{a} - b\overline{d})f]\\ &= [ac.e - d\overline{b}.e - f.\overline{b}\overline{c} - f.\overline{d}a] + i_Y[e.cb + e.\overline{a}d + \overline{c}\overline{a}.f - b\overline{d}.f],\end{aligned}$$

and similarly

$$\begin{aligned}(a + i_Y b).(c + i_Y d)(e + i_Y f) &= (a + i_Y b)[(ce - f\overline{d}) + i_Y(ed + \overline{c}f)]\\ &= a(ce - f\overline{d}) - (ed + \overline{c}f)\overline{b} + i_Y[(ce - f\overline{d})b + \overline{a}(ed + \overline{c}f)]\\ &= [a.ce - a.f\overline{d} - ed.\overline{b} - \overline{c}f.\overline{b}] + i_Y[ce.b - f\overline{d}.b + \overline{a}.ed + \overline{a}.\overline{c}f],\end{aligned}$$

which coincide when we use the commutative and associative properties of X.

We conclude that

Lemma 2. *Y is an associative composition algebra just when X is a commutative, associative composition algebra.*

When is $X = W + i_X W$ a commutative, associative composition algebra? Suppose $a, b, c, d, e \in W$. Since $ie = \overline{e}i$, we'll need $e = \overline{e}$ for all $e \in W$: in other words, conjugation must be trivial in W.

But now

$$(a + i_X b)(c + i_X d) = (ac - d\overline{b}) + i_X(cb + \overline{a}d)$$

and

$$(c + i_X d)(a + i_X b) = (ca - b\overline{d}) + i_X(ad + \overline{c}b),$$

which coincide using the commutative and trivial conjugation properties of W. Therefore,

Lemma 3. *X is a commutative, associative composition algebra just when W is a commutative, associative composition algebra with trivial conjugation.*

We therefore have

Theorem 1. (Hurwitz) $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, *and* $\mathbb{O}$ *are the only composition algebras.*

For $\mathbb{R}$ is a commutative, associative composition algebra with trivial conjugation. So $\mathbb{C}$ is a commutative, associative composition algebra with *non-trivial conjugation.* So $\mathbb{H}$ is an associative composition algebra which is *non-commutative.* So $\mathbb{O}$ is a composition algebra which is *non-associative*, and its Dickson double is no longer a composition algebra.

We have proved Hurwitz's celebrated theorem that a composition algebra with identity on a real Euclidean space is one of these four algebras. We now show that this is true up to isotopy for algebras without identities.

In an arbitrary composition algebra, choose u and v of norm 1. Then $x \to xv$ and $y \to uy$ are orthogonal maps, and so have inverses α and β, say. Now, define a new multiplication by $x \star y = x^{\alpha} y^{\beta}$. Then

$$[x \star y] = [x^{\alpha} y^{\beta}] = [x^{\alpha}][y^{\beta}] = [x][y],$$

showing that $\star$ still gives a composition algebra; and

$$uv \star uy = (uv)^{\alpha}(uy)^{\beta} = uy$$

$$xv \star uv = (xv)^{\alpha}(uv)^{\beta} = xv,$$

showing that uv is a two-sided identity for the new multiplication.[2]

6.5 Other Properties of the Algebras

We define $x^{-1} = x/[x]$ for $x \neq 0$.

$$\textbf{Inverse Laws:} \quad \overline{x}.xy = [x]y = yx.\overline{x},$$
$$\text{or equivalently } x^{-1}.xy = y = yx.x^{-1}\ .$$

Proof. $[\overline{x}.xy, t] = [xy, xt] = [x][y, t] = [[x]y, t]$.

[2]In the language of the next chapter, this shows that any norm 1 element can be converted into an identity element by applying an isotopy, so that the monotopies are transitive on such elements (which is the condition for a Moufang Loop).

Alternative Laws: $x.xy = x^2y$ and $yx.x = yx^2$.

Proof. Substitute $\overline{x} = 2[x,1] - x$ in $\overline{x}.xy = \overline{x}x.y$.

Remarks: In fact, the Bruck-Kleinfeld theorem [8] characterizes the algebras just from the alternative property. Sometimes $x.yx = xy.x$ is called the third alternative law. We shall prove it immediately after we prove the following laws.

Moufang Laws: $xy.zx = x(yz).x = x.(yz)x$.

Proof.

$$\begin{aligned}[xy.zx,t] = [xy,t.\overline{x}\,\overline{z}] &= 2[x,t][y,\overline{x}\,\overline{z}] - [x.\overline{x}\,\overline{z},ty] \\ &= 2[x,t][yz,\overline{x}] - [\overline{x}\,\overline{z},\overline{x}.ty] \\ &= 2[yz,\overline{x}][x,t] - [x][\overline{z}\,\overline{y},t] \\ &= 2[x,\overline{yz}][x,t] - [x][\overline{yz},t].\end{aligned}$$

So $xy.zx = 2[x,\overline{yz}]x - [x]\overline{yz}$ is a function of x and yz only. We can therefore replace y and z by any two other elements with the same product, and so deduce

$$xy.zx = x(yz).1x = x(yz).x \quad \text{and} \quad xy.zx = x1.(yz)x = x.(yz)x.$$

Again, since $y1 = 1y = y$, we can deduce the third alternative law

$$xy.x = xy.1x = x1.yx = x.yx.$$

W. D. Smith informs us that R. D. Schafer proved that *all* the algebras obtained from $\mathbb{R}$ by repeated Dickson doubling are power associative, satisfy $(ab)a = a(ba)$ and $(ab)a^2 = a(ba^2)$, and have the property that every element satisfies a quadratic equation. He also remarks that the "real parts" of octonions are associative: $[ab.c,1] = [a.bc,1]$.

6.6 The Maps $\mathtt{L}_x$, $\mathtt{R}_x$, and $\mathtt{B}_x$

The failure of the associative law suggests the study of multiplication operators. Accordingly, we define the Left-multiplication, Right-multiplication, and Bi-multiplication maps:

$$\mathtt{L}_x : y \to xy, \quad \mathtt{R}_x : y \to yx, \quad \mathtt{B}_x : y \to xyx$$

The third alternative law shows that $\mathtt{B}_x$ is well-defined and is the product of $\mathtt{L}_x$ and $\mathtt{R}_x$ in either order:

$$y^{\mathtt{L}_x\mathtt{R}_x} = xy.x = y^{\mathtt{B}_x} = x.yx = y^{\mathtt{R}_x\mathtt{L}_x}.$$

We shall also show that $\mathtt{B}_x$ has a geometrical interpretation in terms of reflections. For comparing our formula

$$xy.zx = 2[x, \overline{yz}]x - [x]\overline{yz}$$

with the usual expression

$$\mathrm{ref}(x) : t \to t - \frac{2[x,t]}{[x]}x$$

that represents the reflection in a vector x, we see that

$$xy.zx = -[x](\overline{yz})^{\mathrm{ref}(x)} = [x](yz)^{\mathrm{ref}(1)\cdot\mathrm{ref}(x)},$$

showing that $\mathtt{B}_x$ is just a scalar multiple of $\mathrm{ref}(1)\cdot\mathrm{ref}(x)$.

Let's look at the associative law more closely. Writing it in the forms

$$(yz)^{\mathtt{L}_x} = y^{\mathtt{L}_x}z,\ (yz)^{\mathtt{R}_x} = yz^{\mathtt{R}_x},$$

what it tells us is that one can left or right multiply a product of two factors by left or right multiplying one of the factors. Again, the Moufang bimultiplication law $xy.zx = x(yz)x$ when written in the form $(yz)^{\mathtt{B}_x} = y^{\mathtt{L}_x}z^{\mathtt{R}_x}$ shows that one can bimultiply a product by individually left and right multiplying the two factors.

There are two other Moufang laws, usually written

$$x(y.xz) = xyx.z \ \text{ and } \ (yx.z)x = y.xzx,$$

which makes them hard to use. We prefer to write them in the equivalent forms ("Moufang left and right multiplication laws")

$$x(yz) = xyx.x^{-1}z \ \text{ and } \ (yz)x = yx^{-1}.xzx$$

which makes it clear how they substitute for the associative law, because they show how to left or right multiply a product by performing multiplications on the individual factors:

$$(yz)^{\mathtt{L}_x} = y^{\mathtt{B}_x}z^{\mathtt{L}_{x^{-1}}} \ \text{ and } \ (yz)^{\mathtt{R}_x} = y^{\mathtt{R}_{x^{-1}}}z^{\mathtt{B}_x}.$$

We have not yet proved that our algebras obey the two new Moufang laws. In the next chapter we shall do so by showing that all three Moufang laws are equivalent (using the inverse laws).

6.7 Coordinates for the Quaternions and Octonions

We now turn to the problem of recovering the classical definitions of the algebras from our description of them in terms of Dickson doubles. We note that two units that are orthogonal to 1 and each other—say i and j—have the property that $iji = j$, since $\mathtt{B}_i = \mathrm{ref}(1) \cdot \mathrm{ref}(i)$ obviously fixes j. So,

$$ij = k \Rightarrow ki = j \quad (\text{and } ij = k \Rightarrow jk = i, \text{ similarly}).$$

Also,

$$k^2 = ijij = jj = -1$$

and

$$ji = \overline{j}\,\overline{i} = \overline{k} = -k.$$

If we take i to be the unit that extends $\mathbb{R}$ to $\mathbb{C}$, and j that of the next extension, we have Hamilton's celebrated relations:

$$\begin{gathered} i^2 = j^2 = k^2 = 1 \\ ij = k \quad jk = i \quad ki = j \\ ji = -k \quad kj = -i \quad ik = -j \end{gathered}$$

For the octonions, we shall find a set of seven units $i_0, \ldots, i_6$ for which the permutations

$$\alpha : i_n \to i_{n+1} \quad \beta : i_n \to i_{2n} \quad (\text{subscripts mod } 7)$$

are symmetries of the multiplication. We do this by calling the units of our starting quaternion subalgebra

$$i = i_1 \quad j = i_2 \quad k = i_4,$$

and then using i_0 to extend this and defining $i_0 i_n = i_{3n}$, so that

$$i_0 i_1 = i_3 \quad i_0 i_2 = i_6 \quad i_0 i_4 = i_5.$$

Now recall that if b, c are in the quaternion subalgebra $\langle 1, i_1, i_2, i_4 \rangle$, we have $i_0 b.c = i_0 .cb$. This tells us that

$$\begin{aligned} i_6 i_1 = i_0 i_2 . i_1 = i_0 . i_1 i_2 = i_0 i_4 = i_5 \\ i_5 i_2 = i_0 i_4 . i_2 = i_0 . i_2 i_4 = i_0 i_1 = i_3 \\ i_3 i_4 = i_0 i_1 . i_4 = i_0 . i_4 i_1 = i_0 i_2 = i_6, \end{aligned}$$

showing that i_x, i_y, i_z behave just like Hamilton's i, j, k for each of the seven "quaternion triplets" of subscripts

$$xyz = 124, 235, 346, 450, 561, 602, 013.$$

Since the general such system is

$$i_{n+1}, i_{n+2}, i_{n+4} \quad (\text{subscripts mod } 7),$$

this verifies our original assertion.

6.8 Symmetries of the Octonions: Diassociativity

The above argument also gives us information about the automorphism group of the octonions. Namely, any unit orthogonal to 1 could be taken as i_1; any unit orthogonal to 1 and i_1 could be taken as i_2; and any unit orthogonal to $1, i_1, i_2$, and $i_1 i_2$ could be taken as i_0.

To be more precise, if we let j_1 be any unit orthogonal to 1, then j_2 any unit orthogonal to 1 and j_1, and finally j_0 any unit orthogonal to $1, j_1, j_2$ and $j_1 j_2$, then there is just one automorphism taking $i_1 \to j_1$, $i_2 \to j_2$, $i_0 \to j_0$. The choices for j_1 are points of the unit sphere in the 7-space orthogonal to 1; those for j_2 are points of the unit sphere in the 6-space orthogonal to $1, j_1$; and those for j_0 are points of the unit sphere in the 4-space orthogonal to $1, j_1, j_2, j_1 j_2$. These spaces are manifolds of dimensions 6, 5, and 3, and so the symmetries we have found form a continuous group of dimension $6 + 5 + 3 = 14$. In the standard notation of the Lie theory, this is the Lie group G_2. We shall discuss G_2 further in Chapter 8.

Here we use G_2 to prove Artin's "diassociativity" property of the octonions:

Theorem 2. *The algebra generated by any two octonions is associative.*

For up to symmetries of the octonions, the first one can be taken as $x + i_1 y$, and the second $X + i_1 Y + i_2 Z$, which puts them both in the quaternion subalgebra $\langle 1, i_1, i_2, i_4 \rangle$.

6.9 The Algebras over Other Fields

Our principal concern in this book is with composition algebras for the standard positive definite quadratic form $x_1^2 + x_2^2 + \cdots + x_n^2$ over the real field. However, the proofs in this chapter actually apply almost without change to the case of composition algebras for arbitrary non-degenerate quadratic forms over all fields not of characteristic 2.

Recall that a quadratic form $[x]$ is **non-degenerate** if the corresponding bilinear form satisfies

$$[x, t] = 0 \text{ for all } t \Rightarrow x = 0.$$

This is enough to justify our method of deducing $x = y$ from $[x, t] = [y, t]$. The only change is that one cannot guarantee to find an element orthogonal

to H that has norm 1. Therefore the extending element i must be permitted to have an arbitrary non-zero norm α, making the doubling rules be

$$(a+ib)(c+id) = (ac - \alpha d\overline{b}) + i(cb + \overline{a}d)$$

and $[a+ib] = [a] + \alpha[b]$.

The argument "really" works also for characteristic 2, where the doubling can be continued infinitely – see Albert [1](and Kaplansky [27]). The problem there is not with the algebras, but with the quadratic form—it is just that one cannot guarantee to find a basis of mutually orthogonal vectors. However, a "Dickson double" of H can still be defined using an i not orthogonal to H—this merely complicates the formulae without affecting the structure of the argument.

There is one important way in which these more general algebras may differ from the standard ones—there can exist non-zero elements without inverses. Namely, even for a non-degenerate quadratic form there can be (and in fact there necessarily is, over a finite field) a non-zero x for which $[x] = 0$.

6.10 The 1-, 2-, 4-, and 8-Square Identities

The existence of the four algebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$ is equivalent to that of the N-square identities

$$x_1^2\, y_1^2 = (x_1y_1)^2$$

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2$$

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)&(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2\\ &+ (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2\\ &+ (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2\\ &+ (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2\end{aligned} \quad .$$

$$\begin{aligned}(x_1^2 + \cdots + x_8^2)&(y_1^2 + \cdots + y_8^2)\\ &= (x_\infty y_\infty - x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6)^2\\ &+ (x_\infty y_0 + x_0y_\infty + x_1y_3 + x_2y_6 + x_4y_5 - x_3y_1 - x_6y_2 - x_5y_4)^2\\ &+ (x_\infty y_1 + x_1y_\infty + x_2y_4 + x_3y_0 + x_5y_6 - x_4y_2 - x_0y_3 - x_6y_5)^2\\ &+ (x_\infty y_2 + x_2y_\infty + x_3y_5 + x_4y_1 + x_6y_0 - x_5y_3 - x_1y_4 - x_0y_6)^2\\ &+ (x_\infty y_3 + x_3y_\infty + x_4y_6 + x_5y_2 + x_0y_1 - x_6y_4 - x_2y_5 - x_1y_0)^2\\ &+ (x_\infty y_4 + x_4y_\infty + x_5y_0 + x_6y_3 + x_1y_2 - x_0y_5 - x_3y_6 - x_2y_1)^2\\ &+ (x_\infty y_5 + x_5y_\infty + x_6y_1 + x_0y_4 + x_2y_3 - x_1y_6 - x_4y_0 - x_3y_2)^2\\ &+ (x_\infty y_6 + x_6y_\infty + x_0y_2 + x_1y_5 + x_3y_4 - x_2y_0 - x_5y_1 - x_4y_3)^2\end{aligned}$$

Hurwitz's theorem shows that such an identity, say

$$(x_1^2 + \cdots + x_N^2)(y_1^2 + \cdots + y_N^2) = z_1^2 + \cdots + z_N^2,$$

in which the z_k are bilinear functions of the x_i and y_j, can exist only for $N = 1, 2, 4, 8$ (and in these cases is then necessarily "isotopic" to one of those above).

6.11 Higher Square Identities: Pfister Theory

In view of these, it came as a great surprise when in 1967 A. Pfister [34] proved that

Theorem 3. *In any field and for every n, the product of two sums of 2^n squares is always another such sum.*

He did this by showing that there is an N-square identity

$$(x_1^2 + \cdots + x_N^2)(y_1^2 + \cdots + y_N^2) = z_1^2 + \cdots + z_N^2,$$

which the z_k are rational functions of the x_i and y_j whenever N is a power of 2 (and, unless the characteristic is 2, only when N is a power of 2). In fact, the z_k can always be made linear in either the x_i or the y_j.

It does not seem to be generally known that such identities can be produced by various modifications of the Dickson doubling procedure.[3] For example, we obtain a 16-square identity (for ordered pairs $a+ib$, $c+id$ of octonions) from the "definition"

$$\begin{aligned}(a + ib)(c + id) &= ab.b^{-1}c - d\overline{b} + i(cb + \overline{a}d)\\ &= X + iY, \text{ say,}\end{aligned}$$

in which "$ab.b^{-1}c$" is to be interpreted as ac if $b = 0$.

This is because the norm of the right-hand side is

$$[X] + [Y] = [ab.b^{-1}c] + [d\overline{b}] + [cb] + [\overline{a}d] - 2[ab.b^{-1}c, d\overline{b}] + 2[cb, \overline{a}d]$$

which equals

$$[a][c] + [d][b] + [c][b] + [a][d] = ([a] + [b])([c] + [d])$$

since the inner product terms cancel:

[3] Pfister did not originally obtain his identities this way.

$$[ab.b^{-1}c, d\overline{b}] = [(ab.b^{-1}c)b, d] = [a.cb, d] = [cb, \overline{a}d],$$

where the middle step uses a Moufang law (Chapter 7)

$$(xy)z = xz^{-1}.zyz.$$

This is only one of various ways to replace any term ac, $\overline{d}b$, cb, $\overline{a}d$ in the formula

$$(a + ib)(c + id) = (ac - d\overline{b}) + i(cb + \overline{a}d)$$

that produce 16-square identities. Some of them can be repeated indefinitely to produce 2^n-square identities for all n. One such formula is

$$(a + bi)(c + di) = (ac - \overline{\overline{b}d}) + (b\overline{c} + b(\overline{\overline{a}.\overline{b^{-1}d}}))i.$$

Pfister went on to create an entire theory of sums of squares and other multiplicative quadratic forms. We confine ourselves to an easy result.

Theorem 4. *If in a certain field $\mathbb{F}$, the number -1 can be expressed as the sum of N squares, then the least possible value of N (which Pfister calls the "Stufe" of $\mathbb{F}$) is a power of 2.*

For suppose -1 is the sum of $2^n + k$ squares, where $0 < k < 2^n$, say

$$-1 = x_1^2 + \cdots + x_{2^n}^2 + y_1^2 + \cdots + y_k^2,$$

but not the sum of fewer (so that $x_1^2 + \cdots + x_{2^n}^2 \neq 0$). We write this in the form

$$-(x_1^2 + \cdots + x_{2^n}^2) = y_1^2 + \cdots + y_k^2 + 1^2 = y_1^2 + \cdots + y_{2^n}^2, \text{ say,}$$

and multiply by $s = x_1^2 + \cdots + x_{2^n}^2$ to get an equation of the form

$$-s^2 = (x_1^2 + \cdots + x_{2^n}^2)(y_1^2 + \cdots + y_{2^n}^2) = z_1^2 + \cdots + z_{2^n}^2$$

using a 2^n-square identity, from which it follows that

$$-1 = (z_1/s)^2 + \cdots + (z_{2^n}/s)^2,$$

a contradiction.

Appendix: What Fixes a Quaternion Subalgebra?

The automorphisms (or "symmetries") that preserve a quaternion subalgebra H are nicely described in the language of Chapter 4. As usual, we let i be a fixed unit orthogonal to H, and we write the general octonion as $x + iy$ with x, y in H, as in the Dickson doubling process. Then we assert:

Theorem 5. *The automorphisms of the octonions that take H to itself form a copy of SO_4. The general one,*[4] *$[u, v] = [-u, -v]$, is parametrized by two units in H and takes $x + iy \to \overline{u}xu + i.\overline{u}yv$.*

Proof. Plainly any symmetry of H extends to the Dickson double of H. Since all such automorphisms are the SO_3 maps $x \to \overline{u}xu$, this gives us the symmetries

$$[u, u] : x + iy \to \overline{u}xu + i.\overline{u}yu.$$

Modulo these, it suffices to consider the symmetries that fix H pointwise. If such a symmetry takes i to I, then it takes $x + iy$ to $x + Iy$. But then we can write $I = iv$ for some unit v in H, and we see that

$$[1, v] : x + iy \to x + i.yv$$

has this effect, since $i.yv = iv.y$ by (D3).

The two types of symmetry $[u, u]$ and $[1, v]$ that we have just found generate all of the symmetries $[u, v]$ (since $[u, v] = [u, u][1, \overline{u}v]$).

The three special cases $[u, 1]$, $[1, v]$, $[u, u]$ have very different properties. Most important are the **quasiconjugations** $Q_u = [u, 1]$. We can see why this is by changing our notation: Writing $X = x$, $Y = iy$, we find that

$$[u, 1] : X + Y \to \overline{u}Xu + uY$$

(since $uY = u.iy = i.\overline{u}y$ by (D3)), which shows that $[u, 1]$ is independent of the choice of i. It does however depend on the choice of subalgebra H containing u. In full, we call it **quasiconjugation by u for the subalgebra H**. The quasiconjugations for a given H form a normal subgroup of the automorphisms that preserve H.

The **H-stabilizers** $S_v = [1, v]$ are the next most important. As their name implies, they are the elements that fix H pointwise and they form another normal subgroup. However, the parameter v that describes a given H-stabilizer unfortunately depends on i as well as H.

The **diagonal symmetries** $D_u = [u, u]$ are the least important, since whether a symmetry is or is not called diagonal can change if we apply

[4] Here we revert to the use of $[u, v]$ for the general element of SO_4.

another symmetry. This is because the conjugate of $[u, u]$ by $[a, b]$ is $[u^a, u^b]$, which might no longer be diagonal. Algebraically, this corresponds to the fact that the diagonal symmetries form a subgroup that is not normal.

We shall use these ideas in Chapter 10.

Moufang Loops

7.1 Inverse Loops

An **inverse loop** is a set with a distinguished element 1, binary operation xy, and inverse $^{\dashv}$ satisfying

$$\begin{gathered} x1 = x = 1x \\ x^{\dashv}(xy) = y = (yx)x^{\dashv} \\ (x^{\dashv})^{\dashv} = x \end{gathered}$$

for all x, y. (We write the inverse as $x^{\dashv}$ rather than the usual x^{-1} for reasons that may soon be apparent.)

A major theme of this chapter is that the basic relation $xy = z$ can be written in six ways (Figure 7.1). We call this a **hexad** of relations.

Now, since the equivalence

$$yz^{\dashv} = x^{\dashv} \Leftrightarrow z^{\dashv}x = y^{\dashv}$$

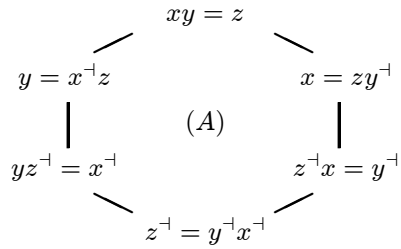


Figure 7.1. Duplex form of the basic hexad.

can be written

$$(yz^{\dashv})x = 1 \Leftrightarrow y(z^{\dashv}x) = 1,$$

we see that the relations $(XY)Z = 1$ and $X(YZ) = 1$ are equivalent and so can be written without parentheses as $XYZ = 1$.

We'll call $xy = z$ and $xyz^{\dashv} = 1$ the **duplex** and **triplex** forms of the same relation. Converting the six relations of Figure 7.1 to triplex form (after replacing z by $z^{\dashv}$) makes their symmetry easier to understand (Figure 7.2).

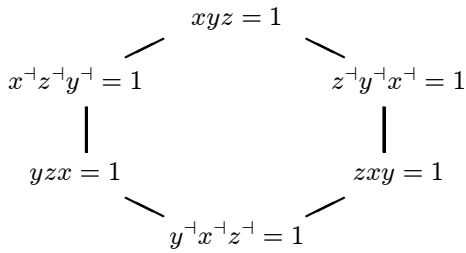


Figure 7.2. Triplex form of the basic hexad.

7.2 Isotopies

An **isotopy** of an inverse loop is a triple of invertible maps that preserve this basic relation. Two notations are appropriate according as the relation is in duplex or triplex form. We write $(\alpha, \beta \mid \gamma)$ to mean $x^{\alpha}y^{\beta} = (xy)^{\gamma}$; we write (α, β, γ) to mean $xyz = 1 \Rightarrow x^{\alpha}y^{\beta}z^{\gamma} = 1$.

If $(\alpha, \beta \mid \gamma)$ is an isotopy in duplex form, then

$$xyz = 1 \Rightarrow xy = z^{\dashv} \Rightarrow x^{\alpha}y^{\beta} = z^{\dashv\gamma} \Rightarrow x^{\alpha}y^{\beta}z^{\dashv\gamma\dashv} = 1,$$

showing that $(\alpha, \beta, \dashv\gamma\dashv)$ is its name in triplex form.

Applying $(\alpha, \beta \mid \gamma)$ to the hexad (A) of relations gives the similar hexad (B), which undoes to (C) (see Figure 7.3). This shows that when $(\alpha, \beta \mid \gamma)$ is an isotopy, so are all six members of the hexad (D) (see Figure 7.4). Once again, the symmetry is made more apparent by converting (D) into triplex form (after replacing γ by $\dashv\gamma\dashv$) as given in (E).

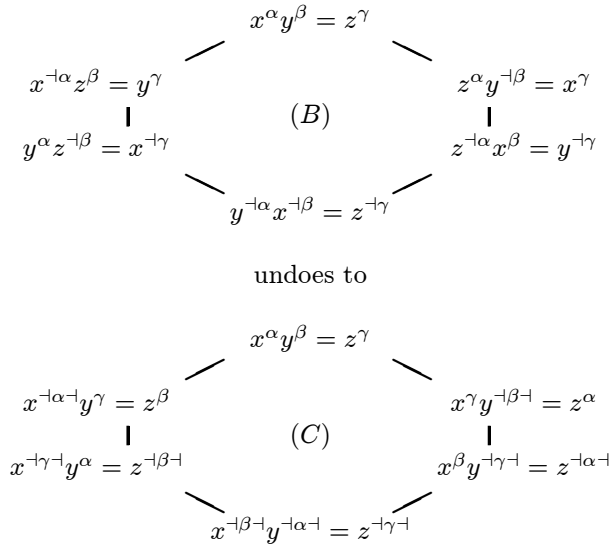


Figure 7.3. Undoing a hexad of isotopies.

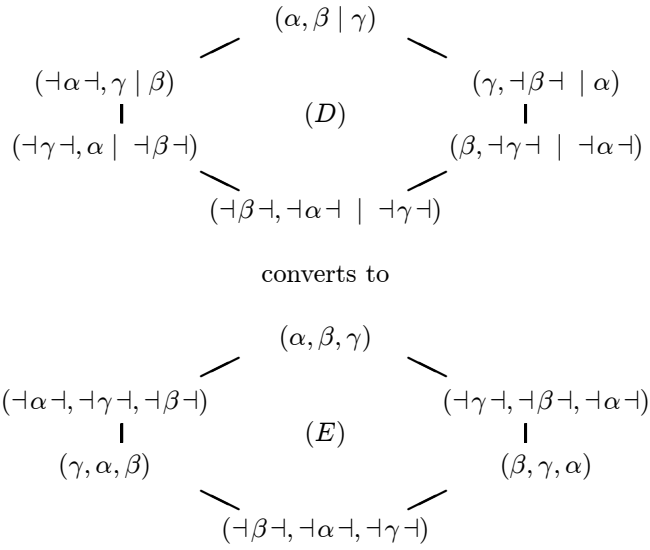


Figure 7.4. Isotopies in duplex and triplex form.

7.3 Monotopies and Their Companions

We define a **monotopy** to be any of the three maps in an isotopy. Hexads (D) and (E) show that we get the same concept whichever one we choose.

So if γ is a monotopy there exist two maps α, β so that

$$xy = z \Rightarrow x^\alpha y^\beta = z^\gamma.$$

In particular,

$$z^\alpha 1^\beta = z^\gamma, \text{ so } z^\alpha = z^\gamma 1^{\beta\dashv} = z^\gamma b$$

$$1^\alpha z^\beta = z^\gamma, \text{ so } z^\beta = 1^{\alpha\dashv} z^\gamma = a z^\gamma.$$

This shows that γ is a monotopy if and only if there are loop elements b and a for which $(xy)^\gamma = x^\gamma b.a y^\gamma$. We call b and a a pair of **companions** for γ. This shows that isotopies are remarkably similar to automorphisms (an automorphism is just a monotopy that has $1, 1$ as a pair of companions).

In general, the determinations of a and b above show that the three maps of an isotopy are very closely related: In terms of the left and right multiplication operations

$$\mathtt{L}_a : x \to ax \qquad \mathtt{R}_b : x \to xb,$$

we see that $\alpha = \gamma \mathtt{R}_b$ and $\beta = \gamma \mathtt{L}_a$.

But even more is true! Let us take the quotient

$$(\alpha, \beta \mid \gamma)^{-1} \cdot (\dashv\alpha\dashv, \gamma \mid \beta) = (\alpha^{-1} \dashv\alpha\dashv, \beta^{-1}\gamma \mid \gamma^{-1}\beta)$$

of two of the equivalent isotopies from (D). Then since $\gamma^{-1}\beta = \mathtt{L}_a$ and so $\beta^{-1}\gamma = (\mathtt{L}_a)^{-1} = \mathtt{L}_{a^\dashv}$, this isotopy has the special form

$$(\alpha^{-1} \dashv\alpha\dashv, \mathtt{L}_{a^\dashv} \mid \mathtt{L}_a).$$

Applying this to xa yields

$$a(xa) = x^{\alpha^{-1}\dashv\alpha\dashv}.a^\dashv a = x^{\alpha^{-1}\dashv\alpha\dashv}.$$

This identifies the map $\alpha^{-1}\dashv\alpha\dashv$ taking x to $a(xa)$, and shows that

$$a(xa).a^\dashv y = a(xy),$$

and in particular that

$$a(xa).a^{\dashv} = ax, \text{ so } a(xa) = (ax)a.$$

This allows us to use our standard notation $\mathtt{B}_a$ for the map taking x to $a(xa) = (ax)a$, so that our isotopy is $(\mathtt{B}_a, \mathtt{L}_{a^{\dashv}} \mid \mathtt{L}_a)$. Like every isotopy, this is one of six, the full hexad being (F) (Figure 7.5), as we see using

$$\dashv \mathtt{L}_a \dashv = \mathtt{R}_{a^{\dashv}}, \quad \dashv \mathtt{R}_a \dashv = \mathtt{L}_{a^{\dashv}}, \quad \text{and} \quad \dashv \mathtt{B}_a \dashv = \mathtt{B}_{a^{\dashv}}.$$

Since this hexad is symmetric in a and $a^{\dashv}$, we have proved

Theorem 1. *If a is the image of* 1 *under some monotopy, then we have all the isotopies of (F), and so* $\mathtt{L}_a$, $\mathtt{L}_{a^{\dashv}}$, $\mathtt{R}_a$, $\mathtt{R}_{a^{\dashv}}$, $\mathtt{B}_a$, *and* $\mathtt{B}_{a^{\dashv}}$ *are monotopies. In particular, if there is* any *monotopy that takes* 1 *to a, then* $\mathtt{L}_a$ *and* $\mathtt{R}_a$ *are such monotopies.*

This in turn implies a theorem that explains the significance of the Moufang law:

Theorem 2. *The monotopies are transitive just if the Moufang identity*

$$zx.yz = z(xy)z$$

holds.

Proof. For then $(\mathtt{L}_z, \mathtt{R}_z \mid \mathtt{B}_z)$ must be an isotopy for every z.

Such a loop is called a **Moufang loop** (or, informally, a "Moup").

Martin Liebeck [31] has proved that the only finite simple Moufang loops other than groups are those obtained by reading the octonions mod p.

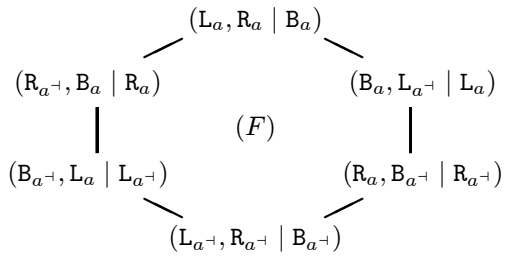


Figure 7.5. A hexad of isotopies involving $\mathtt{L}_a$, $\mathtt{R}_a$, $\mathtt{B}_a$.

7.4 Different Forms of the Moufang Laws

Applied to xy, the six isotopies of (F) are equivalent to the three laws

$$\begin{aligned} z(xy)z &= zx.yz && \textbf{(Bi-)Moufang Law} \\ z(xy) &= zxz.z^{\dashv}y && \textbf{Left Moufang Law} \\ (xy)z &= xz^{\dashv}.zyz && \textbf{Right Moufang Law} \end{aligned}$$

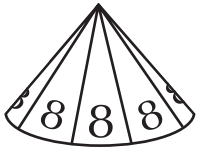
where z is either a or $a^{\dashv}$. The traditional forms of the last two laws are slightly different:

$$\begin{aligned} z(x(zt)) &= zxz.t \\ ((tz)y)z &= t.zyz \end{aligned}$$

These are obtained by setting $y = zt$ and $x = tz$ in the left and right Moufang laws.

Moufang loops are named after Ruth Moufang, who discovered them in connection with the coordinatization of certain projective planes – see [33]. But in a sense, this was not really their first entry into mathematics, since the non-zero real octonions constitute the archetypical Moufang loop. Indeed, we conjecture that the loop generated by n generic real octonions is in fact the free Moufang loop on n generators.

Of course, the Moufang identities can be regarded as weakened forms of the associative law. Indeed, one of the most famous theorems about this is Artin's diassociativity theorem: Any 2-generator Moufang loop is associative. However, we've seen that a better reason for studying abstract Moufang loops is that these identities are equivalent to a symmetry property, namely that the monotopies are transitive. We shall use some of their theory—in particular, the properties of companions —in the next chapter.



Octonions and 8-Dimensional Geometry

We know that the multiplications by unit complex numbers or quaternions generate the respective orthogonal groups SO_2 and SO_4, and we'll prove in this chapter the corresponding result that the multiplications by unit octonions generate SO_8.

However, there are differences between the three cases, controlled by the validity or otherwise of the commutative and associative laws. The associative law in the forms

$$\mathtt{L}_{xy} = \mathtt{L}_y\mathtt{L}_x, \quad \mathtt{R}_{xy} = \mathtt{R}_x\mathtt{R}_y$$

for units x and y would tell us that the product of two multiplications of the same kind should be a third, so that when it holds, the left and right multiplications form subgroups of the special orthogonal groups.

In the complex case, the commutative law, in the form $\mathtt{L}_x = \mathtt{R}_x$, tells us that these groups are the same, and both are in fact the whole group SO_2. In the quaternionic case, both the left and right groups form proper subgroups, and we saw in Chapter 4 that every element of SO_4 is the product of one multiplication of each kind. Since the associative law fails for octonions, it is no longer true that the product of two multiplications of the same kind is another. We shall see in this chapter that in fact the octonion multiplications of either kind generate the whole group SO_8.

8.1 Isotopies and SO_8

We first prove that the octonions are strongly non-associative, in the sense that

Theorem 1. *If $x(ry) = (xr)y$ for all octonions x, y, then r is real.*

For we have $(i_1 i_0)i_2 = -i_1(i_0 i_2)$, so if $(i_1 r)i_2 = i_1(ri_2)$ the coefficient of i_0 in r must be 0, as must that of $i_n (1 \leq n \leq 6)$, using $(i_{n+1} i_n)i_{n+2} = -i_{n+1}(i_n i_{n+2})$.

This implies that companions (Chapter 7) are essentially unique:

Theorem 2. *If a, b is any pair of companions for the monotopy γ, then any other pair has the form $ar, r^{-1}b$ where r is real.*

Proof. The condition that A, B should be a second pair of companions is the identity

$$x^\gamma a.by^\gamma = x^\gamma A.By^\gamma \text{ for all } x, y.$$

Writing $x^\gamma = X, y^\gamma = Y$, the identity becomes

$$Xa.bY = XA.BY \text{ for all } X, Y.$$

In this, setting $A = ar$ and putting $X = a^{-1}, Y = 1$ gives $b = rB$, so $B = r^{-1}b$, so the identity is now that

$$Xa.bY = X(ar).(r^{-1}b)Y \text{ for all } X, Y.$$

In this, putting $Y = (r^{-1}b)^{-1} = b^{-1}r$ shows $(Xa)r = X(ar)$, while putting $X = (ar)^{-1} = r^{-1}a^{-1}$ shows $r^{-1}(bY) = (r^{-1}b)Y$, transforming the identity still further to

$$Xa.bY = (Xa)r.r^{-1}(bY) \text{ for all } X, Y.$$

Finally, putting $Xa = x, bY = ry$ transforms it to

$$x(ry) = (xr)y \text{ for all } x, y,$$

which completes the proof by showing that r is real.

We are ready now for the application to SO_8:

Theorem 3. *If γ is any element of SO_8, there exist α, β in SO_8 for which $(\alpha, \beta \mid \gamma)$ is an isotopy (so γ is a monotopy). Moreover, α, β are uniquely determined up to sign, the only other pair being $-\alpha, -\beta$.*

We shall prove this using the

Lemma 1. *The operations* $\mathrm{ref}(1)\mathrm{ref}(a)$ *and* $\mathrm{ref}(a)\mathrm{ref}(1)$ *are bimultiplications by unit octonions.*

Proof. These are unaffected if we rescale a to have norm 1. But then the first one we found to be $\mathtt{B}_a$ in Chapter 6, and the second is its inverse, $\mathtt{B}_{a^{-1}} = \mathtt{B}_{\overline{a}}$.

Proof of the theorem. We can write γ as the product of an even number of reflections, say

$$\gamma = \mathrm{ref}(a_1)\mathrm{ref}(b_1)\mathrm{ref}(a_2)\mathrm{ref}(b_2)\cdots\mathrm{ref}(a_{2n})\mathrm{ref}(b_{2n}).$$

Now

$$\mathrm{ref}(a_i)\mathrm{ref}(b_i) = \mathrm{ref}(a_i)\mathrm{ref}(1)\mathrm{ref}(1)\mathrm{ref}(b_i)$$

is the product by two bimultiplications in unit octonions, so γ is the product of $2n$ such unit bimultiplications, say $\mathtt{B}_{c_1}\mathtt{B}_{c_2}\cdots\mathtt{B}_{c_{2n}}$. Then

$$(\alpha, \beta \mid \gamma) = (\mathtt{L}_{c_1}\cdots\mathtt{L}_{c_{2n}}, \mathtt{R}_{c_1}\cdots\mathtt{R}_{c_{2n}} \mid \mathtt{B}_{c_1}\cdots\mathtt{B}_{c_{2n}})$$

is the desired isotopy. (Since $c_1, \ldots, c_{2n}$ are unit octonions, α and β are indeed in SO_8.) But we also know that α and β are unique up to scalar multiplication, and the only non-trivial scalar that keeps them in SO_8 is -1, so the only other such isotopy is

$$(-\alpha, -\beta \mid \gamma) = (\alpha, \beta \mid \gamma).$$

8.2 Orthogonal Isotopies and the Spin Group

In the foregoing arguments, it was convenient to use isotopies in the duplex form $(\alpha, \beta \mid \gamma)$. As we approach triality, it will be convenient to switch to the triplex form (α, β, γ), in which the isotopies we have just found take the form

$$(\mathtt{L}_a\mathtt{L}_b\cdots,\ \mathtt{R}_a\mathtt{R}_b\cdots,\ \mathtt{B}_{\overline{a}}\mathtt{B}_{\overline{b}}\cdots).$$

We call (α, β, γ) an **orthogonal isotopy** if its three monotopies α, β, γ are elements of SO_8. What we have shown is that the group of orthogonal isotopies is a 2-to-1 cover of SO_8, which we call the **spin group** Spin_8 Readers who are familiar with the usual definition of the spin groups will recognize this one as an instance. As we remarked in Chapter 3, we prefer to avoid giving a general definition in this book.

8.3 Triality

Our definition of the spin group makes it clear that

Theorem 4. *The spin group has an outer automorphism of order 3, namely that taking* $(\alpha, \beta, \gamma) \to (\beta, \gamma, \alpha)$.

Proof. This is clearly an automorphism. That it is an outer isomorphism (i.e., not a conjugation of the form $g \to h^{-1}gh$) is clear because the images $\mathtt{B}_{i_0}$ and $\mathtt{L}_{i_0}$ of the triality-related elements

$$(\mathtt{L}_{i_0}, \mathtt{R}_{i_0}, \mathtt{B}_{i_0} = \mathtt{B}_{\overline{i_0}}) \text{ and } (\mathtt{R}_{i_0}, \mathtt{B}_{i_0}, \mathtt{L}_{i_0})$$

in SO_8 are not conjugate ($\mathtt{B}_{i_0}$ fixes a 6-space, while $\mathtt{L}_{i_0}$ is fixed-point-free).

The special orthogonal group SO_8 does not have this triality, because γ determines α and β only up to sign. However,

Theorem 5. *The projective special orthogonal group PSO_8 does have a triality automorphism.*

For if $\varphi \in SO_8$, let us define $[\varphi] = \{+\varphi, -\varphi\}$, so that $[\varphi] \in PSO_8$. Then the set of triples $([\alpha], [\beta], [\gamma])$ arising from orthogonal isotopies (α, β, γ) is plainly isomorphic to PSO_8 (since now $[\gamma]$ uniquely determines $[\alpha]$ and $[\beta]$), and has the triality

$$([\alpha], [\beta], [\gamma]) \to ([\beta], [\gamma], [\alpha]).$$

Acting on PSO_8, triality takes

$$[\mathtt{L}_u] \to [\mathtt{R}_u] \to [\mathtt{B}_{\overline{u}}] \to [\mathtt{L}_u]$$

for every unit octonion u.

8.4 Seven Rights Can Make a Left

An immediate consequence of triality is

Theorem 6. *SO_8 is generated by the left multiplications by octonion units, or equally by the right ones.*

Proof. SO_8 is generated by the bimultiplications, and so applying triality, equally by the left ones or the right ones.

In particular, any left multiplication can be expressed as a product of right ones, or vice-versa. Just how many right multiplications are needed to represent a given $\mathtt{L}_x$? The answer is given by

Theorem 7. (The 7-Multiplication Theorem) *Any element of SO_8 is the product of at most seven right (or seven left) multiplications.*

This is best possible:

Theorem 8. *The general left multiplication is the product of seven right ones, but no fewer.*

Proof. If $\alpha \in SO_8$, then $\mathrm{ref}(1) \cdot \alpha \in GO_8 \setminus SO_8$, and so is the product of at most seven reflections, showing that

$$\alpha = \mathrm{ref}(1)\mathrm{ref}(u_1)\mathrm{ref}(u_2)\ldots\mathrm{ref}(u_7),$$

which we can write as the product of seven bimultiplications:

$$\alpha = \mathtt{B}_{u_1}\mathtt{B}_{\overline{u_2}}\mathtt{B}_{u_3}\mathtt{B}_{\overline{u_4}}\mathtt{B}_{u_5}\mathtt{B}_{\overline{u_6}}\mathtt{B}_{u_7}$$

using

$$\mathrm{ref}(u)\mathrm{ref}(v) = \mathrm{ref}(u)\mathrm{ref}(1)\mathrm{ref}(1)\mathrm{ref}(v) = \mathtt{B}_{\overline{u}}\mathtt{B}_v.$$

By triality, α is equally the product of seven left multiplications or seven right ones. In particular, any left multiplication is the product of seven right ones; for instance, we find

$$\mathtt{L}_{i_0} = \mathtt{R}_{i_{2\overline{645}}}\mathtt{R}_{i_{2\overline{64}\overline{5}}}\mathtt{R}_{i_6}\mathtt{R}_{i_5}\mathtt{R}_{i_{\infty\overline{01}3}}\mathtt{R}_{i_{\infty 0\overline{1}3}}\mathtt{R}_{i_3}$$

and

$$\mathtt{L}_{i_{\infty 365}} = \mathtt{R}_{i_0}\mathtt{R}_{i_{\overline{01}\overline{24}}}\mathtt{R}_{i_{01\overline{2}4}}\mathtt{R}_{i_{\overline{012}4}}\mathtt{R}_{i_{\infty\overline{64}1}}\mathtt{R}_{i_{\infty 51\overline{2}}}\mathtt{R}_{i_{\infty\overline{32}4}},$$

which we shall use in Chapter 9.

On the other hand, if u is a unit other than ± 1, then $\mathtt{L}_u$ cannot be written as a product of six unit right multiplications, since then $\mathtt{R}_u$ would be the corresponding product of six bimultiplications, and so of six reflections, and so fix a vector, which it does not.

Since positive scalar factors can be absorbed into all three types of multiplication, we need not restrict to units: $\mathtt{L}_x$ can be a product of six right multiplications only if x is real.

8.5 Other Multiplication Theorems

What happens for products of multiplications that may be of mixed types? If $\mathtt{X}, \mathtt{Y}, \mathtt{Z}$ are chosen from $\mathtt{L}, \mathtt{R}, \mathtt{B}$, we define $\mathtt{XYZX}$, for instance, to be the set of all elements of SO_8 that are expressible in the form $\mathtt{X}_a\mathtt{Y}_b\mathtt{Z}_c\mathtt{X}_d$ for arbitrary octonion units a, b, c, d.

Theorem 9. *Sets of the types below have the respective dimensions:*

X	XX	XXX	XXXX	XXXXX	XXXXXX	XXXXXXX
7	13	18	22	25	27	28

XY	XXY	XXXY	XXXXY
14	20	25	28

Proof. Since octonion conjugation interchanges $\mathtt{L}$ and $\mathtt{R}$ while fixing $\mathtt{B}$, while triality rotates $\mathtt{L}$, $\mathtt{R}$, $\mathtt{B}$, we can suppose $\mathtt{X} = \mathtt{B}$ and $\mathtt{Y} = \mathtt{R}$. The answer in the first line now follows from the fact that the set of products of n $\mathtt{B}$s is the set of products of n reflections, if n is even, or that set multiplied by ref(1), if n is odd.

We next show that the dimensions of $\mathtt{XY}$, $\mathtt{XXY}$, $\mathtt{XXXY}$ are seven more than those of $\mathtt{X}$, $\mathtt{XX}$, $\mathtt{XXX}$. This follows immediately from the fact that the equation

$$\mathtt{B}_a\mathtt{B}_b\mathtt{B}_c\mathtt{R}_d = \mathtt{B}_{a'}\mathtt{B}_{b'}\mathtt{B}_{c'}\mathtt{R}_{d'}$$

implies $d = d'$ (and so $\mathtt{B}_a\mathtt{B}_b\mathtt{B}_c = \mathtt{B}_{a'}\mathtt{B}_{b'}\mathtt{B}_{c'}$). This is because it makes $\mathtt{R}_{d'}\mathtt{R}_{\overline{d}}$ belong to $\mathtt{BBBBBB}$ and so fix a 2-space. But if $e \neq 0$ is in this 2-space, we have $(ed')\overline{d} = e$, and so $ed' = ed$, whence indeed $d' = d$.

The similar equation

$$\mathtt{B}_a\mathtt{B}_b\mathtt{B}_c\mathtt{B}_d\mathtt{R}_e = \mathtt{B}_{a'}\mathtt{B}_{b'}\mathtt{B}_{c'}\mathtt{B}_{d'}\mathtt{R}_{e'}$$

only implies the trivial

$$\mathtt{R}_{e'}\mathtt{R}_{\overline{e}} \in \mathtt{BBBBBBBB}$$

and so does *not* imply $e' = e$. However, we can still compute the dimension of $\mathtt{BBBBR}$ (which is 28 rather than 29) by counting the dimension of the set of such equivalences. We suppress the details.

Many other mixed products reduce to the ones mentioned using

Lemma 2. *We have the equations*

$$\mathtt{LR} = \mathtt{RB} = \mathtt{BL}$$
$$\mathtt{RL} = \mathtt{LB} = \mathtt{BR}$$

For example, these imply $\mathtt{BLL} = \mathtt{LRL} = \mathtt{LLB}$ showing (in two ways) that LRL has dimension 20.

Proof. The identities

$$\begin{aligned} \mathtt{L}_a\mathtt{R}_b &= \mathtt{R}_{b\overline{a}}\mathtt{B}_a = \mathtt{B}_b\mathtt{L}_{a\overline{b}} \\ \mathtt{R}_a\mathtt{L}_b &= \mathtt{B}_b\mathtt{R}_{\overline{b}a} = \mathtt{L}_{\overline{a}b}\mathtt{B}_a \end{aligned}$$

follow from the Moufang laws.

In fact, the only set of length at most 4 not covered by our theorem is XXYY (LLRR, RRLL, RRBB, BBRR, BBLL, LLBB are indeed all the same set, by Lemma 2), while those of length 5 or more are probably the whole group; namely, we conjecture

The 5-Multiplication Proposition. *If* $\mathtt{V}, \mathtt{W}, \mathtt{X}, \mathtt{Y}, \mathtt{Z}$ *are any 5 letters chosen from* L, R, B *that are not all equal, then the set* VWXYZ *contains every element of* SO_8.

Our lemma shows that every case can be reduced to XXXXY, which we already know to have the full dimension 28, so very little is missing.

8.6 Three 7-Dimensional Groups in an 8-Dimensional One

The best way to understand the relationship between Spin_8 and SO_8 is via the 2-to-1 map that passes from a triple to its last coordinate:

$$\begin{matrix} (\alpha,\beta,\gamma) \\ (-\alpha,-\beta,\gamma) \end{matrix} \searrow\!\nearrow \ \gamma.$$

Technically, this is an 8-dimensional representation of Spin_8.

The 7-dimensional spin group Spin_7 is the preimage of SO_7 in this map, so the triples (α,β,γ) for which γ fixes 1 form a copy of Spin_7. Obviously, by demanding instead that α or β fix 1, we obtain two other copies of Spin_7 in Spin_8.

All these groups have 8-dimensional representations obtained by restricting the one above, and these three representations are very different. One of them is reducible (because 1 is fixed), and not faithful (because $(-1,-1,1)$ is in the kernel). The other two are both irreducible and faithful. This is because on one hand, the nontrivial element $(-1,-1,1)$ of the kernel is in neither one of those groups, while on the other hand, they are transitive on the unit ball. For consider the particular isotopy

$$(\alpha,\beta,\gamma) = (\mathtt{R}_{\overline{u}}, \mathtt{B}_u, \mathtt{L}_{\overline{u}})(\mathtt{B}_{\overline{u}}, \mathtt{L}_u, \mathtt{R}_u),$$

in which $\gamma : x \to \overline{u}xu$ fixes 1, while α and β take $1 \to \overline{u}^3$ and u^3, which can be any unit octonions.

Theorem 10. *The intersection of any two of these copies of* Spin_7 *in* Spin_8 *is the intersection of all three. This is the automorphism group of the octonions.*

Proof. Applying α, β, γ to the equation $1 \cdot 1 \cdot 1 = 1$, we find that $1^\alpha 1^\beta 1^\gamma = 1$, showing that if any two of α, β, γ fix 1, then all three do. But now if a and b are the companions of γ, so that $\alpha = \gamma \mathrm{R}_a$, $\beta = \gamma \mathrm{L}_b$, this entails that $a = b = 1$, showing that γ is an isomorphism.

This is the Lie group usually called G_2. It is the smallest of the five "exceptional" Lie groups.

Figure 8.1 illustrates the relationship between the groups we have mentioned. To go down any line on this graph, one demands that one of α, β, γ fixes 1—this reduces the dimension by 7 since it could have taken 1 to any point of the unit 7-sphere.

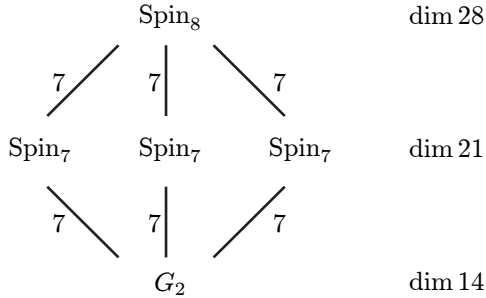


Figure 8.1. The automorphism group G_2 of the octonions is the intersection of any two Spin_7s in Spin_8.

The elements of Spin_8 come in quartets

$$(\alpha, \beta, \gamma) \quad (\alpha, -\beta, -\gamma) \quad (-\alpha, \beta, -\gamma) \quad (-\alpha, -\beta, \gamma),$$

that are related by multiplication by elements of its center:

$$(1, 1, 1) \quad (1, -1, -1) \quad (-1, 1, -1) \quad (-1, -1, 1).$$

The map $(\alpha, \beta, \gamma) \to \gamma$ onto SO_8 obscures some of the symmetry by fusing these in two pairs:

$$\begin{matrix} (\alpha, \beta, \gamma) \\ (-\alpha, -\beta, \gamma) \end{matrix} \searrow\nearrow \ \gamma \qquad \begin{matrix} (\alpha, -\beta, -\gamma) \\ (-\alpha, \beta, -\gamma) \end{matrix} \searrow\nearrow \ -\gamma.$$

We can regain it by passing to PSO_8, which identifies γ and $-\gamma$ to $[\gamma]$:

$$\begin{array}{rcl} (\alpha,\beta,\gamma) & \searrow & \\ (-\alpha,-\beta,\gamma) & \nearrow & [\gamma] \end{array} \quad \begin{array}{lcl} & \swarrow & (\alpha,-\beta,-\gamma) \\ & \nwarrow & (-\alpha,\beta,-\gamma) \end{array}$$

So Spin_8 and PSO_8 have a triality symmetry that SO_8 lacks. We discuss this further in the next section.

8.7 On Companions

Putting together various results from this chapter and the last, we have

Theorem 11. *Given any element $\gamma \in SO_8$ there exists a pair a, b of unit octonions called its* ***companions*** *such that*

$$(xy)^\gamma = x^\gamma a.by^\gamma.$$

The companions are uniquely determined up to negation, the only other pair being $(-a, -b)$.

It is not hard to find the "multiplication rule" for companions:

Theorem 12. *If the companions of γ and δ are a, b and c, d, then those of $\gamma\delta$ are $cd.a^\delta c$, $db^\delta.cd$.*

Proof.

$$\begin{aligned} (xy)^{\gamma\delta} &= (x^\gamma a.by^\gamma)^\delta \\ &= (x^\gamma a)^\delta c.d(by^\gamma)^\delta \\ &= (x^{\gamma\delta}c : da^\delta)c.d(b^\delta c : dy^{\gamma\delta}) \\ &= (x^{\gamma\delta} : c(da^\delta)c)(d(b^\delta c)d : y^{\gamma\delta}) \\ &= (x^{\gamma\delta} : cd.a^\delta c)(db^\delta.cd : y^{\gamma\delta}). \end{aligned}$$

The first three equalities are from the definition of companions, while the remaining two use the Moufang laws.

We can use these to find the companions for any combination of left, right, and bimultiplications, starting from

Theorem 13. *The companions of $\mathtt{L}_a$, $\mathtt{R}_a$, and $\mathtt{B}_a$ are respectively*

$$a, a^{-2} \qquad a^{-2}, a \qquad a^{-1}, a^{-1}.$$

Proof.

$$\begin{aligned} a(xy) &= axa.a^{-1}y = ax.a : a^{-2}.ay \\ (xy)a &= x^{-1}a.aya = xa.a^{-2} : a.ya \\ a(xy)a &= \quad ax.ya \quad = axa.a^{-1} : a^{-1}.axa \end{aligned}$$

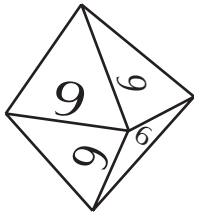
In group theory, the map $\mathtt{T}_a : x \to a^{-1}xa$, called **transformation** or **conjugation** by a, is important as yielding an automorphism. In the octonions, this is not generally true, but (after Zorn [44]) we know all cases when it is:

Theorem 14. *$\mathtt{T}_a$ is an automorphism just when a^3 is real.*

Proof. The following argument shows that $\mathtt{T}_a$ has companions a^{-3}, a^3, the last equality using diassociativity (twice):

$$\begin{aligned} a^{-1}(xy)a &= a^{-1}xa^{-1}.ay : a \\ &= a^{-1}xa^{-1}.a^{-1} : a(ay)a \\ &= a^{-1}xa.a^{-3} : a^3.a^{-1}ya \end{aligned}$$

In particular $\mathtt{T}_\omega$, where $\omega = -\frac{1}{2} + \frac{1}{2}i_1 + \frac{1}{2}i_2 + \frac{1}{2}i_4$, is an automorphism of the octonions, and even of the integral ones that we shall define in the next chapter.



The Octavian Integers O

In this chapter, we first find the correct way to define "the integral octonions" and investigate the geometry of the very interesting lattice E_8 that they form. We deduce that the ring $\mathsf{O} = \mathsf{O}^8$ of "octavian integers" has the Euclidean property—that we can divide with a remainder smaller than the divisor. Unfortunately, this does not lead to the expected theory of ideals and unique factorization, since, as we shall show, the ideals of O are rather trivial. Finally, a new theory that appears for the first time in this book finally illuminates both the arithmetic and geometry of the divisors of an arbitrary octavian integer. It was prompted by H. P. Rehm's discovery of an interesting new form of the Euclidean algorithm.

The elements of O have been called "The Integral Cayley Numbers" since Coxeter's paper [11] of that title. Later, Coxeter remarked "If I had read F. van der Blij's 'History of the octaves' [42] before writing [that paper], I would have entitled it 'Integral Octaves.' " However, the term "octonion" seems now to have become standard. By way of compromise, we propose to use "octavian" (analogous to "Hurwitzian") for "octonion integer," and in further homage to Graves, "Gravesian" for the analogue of "Lipschitzian."

9.1 Defining Integrality

We recall from Chapter 5 the two notions of quaternion integer due to Lipschitz and Hurwitz, and we ask what it should mean to be an octo-

nion **integer**? Nowadays, algebraists take "integer" to mean member of what's called a **maximal order**, following Dickson, who used the term "arithmetic."

The concept (of **order**) arose first for algebraic number fields (i.e., finite algebraic extensions of the rationals), where it means "a subring each whose elements satisfy an equation of the form

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0 \text{ with } c_{n-1}, \ldots, c_0 \in \mathbb{Z}."$$

Dickson defined an **arithmetic** to be a maximal order.

In $\mathbb{Q}(\sqrt{-3})$, for example, $a + b\sqrt{-3}$ satisfies $x^2 - 2ax + (a^2 + 3b^2) = 0$, and certainly the set $\mathbb{Q}[\sqrt{-3}]$ (consisting of those $a+b\sqrt{-3}$ with $a, b \in \mathbb{Z}$) is an order. However, the larger ring of Eisenstein integers (with $2a, a+b \in \mathbb{Z}$) is also an order, so that $\mathbb{Q}[\sqrt{-3}]$ is not a *maximal* order, or arithmetic.

We shall use the same terminology for the "ring" $\mathbb{Q}(i_0, i_1, i_2, i_3, i_4, i_5, i_6)$ of rational octonions even though this is not associative. Since the minimal polynomial of $\alpha = a_\infty + a_0 i_0 + \cdots + a_6 i_6$ is

$$x^2 - 2a_\infty x + (a_\infty^2 + a_0^2 + \cdots + a_6^2) = 0,$$

the condition is that the "trace" $2a_\infty$ and "norm" $a_\infty^2 + a_0^2 + \cdots + a_6^2$ must be ordinary integers for any element of an order or arithmetic in $\mathbb{Q}(i_0, i_1, i_2, i_3, i_4, i_5, i_6)$.

9.2 Toward the Octavian Integers

The most obvious order inside $\mathbb{Q}(i_0, i_1, i_2, i_3, i_4, i_5, i_6)$ consists of those octonions for which all the coordinates $a_\infty, \ldots, a_6$ are ordinary integers—we call these the **Gravesian octaves** or **integers**. In this section, we prove that

Theorem 1. *The orders containing the Gravesian integers are precisely the 16 integer systems of Figure 9.1.*

In what follows, we shall have many occasions to refer to an octonion α whose coordinates are in $\frac{1}{2}\mathbb{Z}$. In this case, the coordinates that are not also in $\mathbb{Z}$ form what we shall call the **halving-set** of subscripts for α.

Lemma 1. *In an element α of such an order, the doubles $2a_r$ of all the coordinates of α are integers, and the size m of every halving-set is a multiple of 4.*

Proof. For the first assertion, multiply α by i_r. For the second, observe that

$$a_\infty^2 + \cdots + a_6^2 \equiv \frac{m}{4} \pmod 1.$$

In view of this lemma, we introduce the notation

$$i_{abcd} \text{ for } \frac{i_a + i_b + i_c + i_d}{2},$$

and use bars on subscripts to indicate negation, for example

$$i_{a\bar{b}c\bar{d}} \text{ for } \frac{i_a - i_b + i_c - i_d}{2}.$$

We can specify one of the 16 systems by saying just which the halving-sets are. The multiplicative structure of the octonions already involves a distinguished family of quadruplets, namely those that correspond to quaternion subalgebras, together with their complements. These, together with the empty and full sets, we call the sixteen ∞-**sets**:

$\emptyset$	∞124	∞235	∞346	∞450	∞561	∞602	∞013
$\Omega = \infty$0123456	0356	0146	0125	1236	0234	1345	2456.

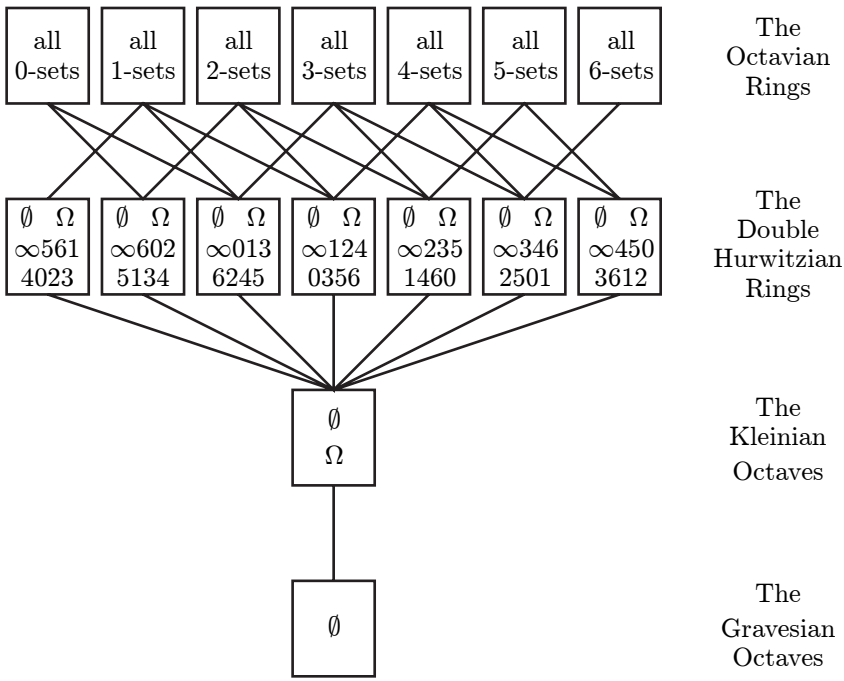


Figure 9.1. The sixteen orders containing the Gravesian octaves, G^8.

An octonion whose halving-set is an ∞-set we call an "∞-**integer**" or "**Kirmse integer**," after J. Kirmse, who naturally but mistakenly supposed that they formed a maximal order.[1]

However, Coxeter found that

The ∞-integers are not multiplicatively closed.

For example, the product of the ∞-integers $i_{\infty 026}$ and $i_{\infty 013}$ is i_{0235}, which is not an ∞-integer, and the product of this with the ∞-integer $i_{\infty 235}$ is

$$-\frac{3}{4}+\frac{1}{4}(i_0-i_1+i_2+i_3-i_4+i_5+i_6),$$

whose minimal polynomial $x^2+\frac{3}{2}x+1$ is manifestly non-integral.

Dickson found the appropriate correction, which was rediscovered and completed by Bruck. We define the n-**sets** and n-**integers** ($n=0,\dots,6$) by interchanging ∞ with n in the definition of ∞-sets and ∞-integers.

∞124	0356
∞235	1460
∞346	2501
∞450	3612
∞561	4023
∞602	5134
∞013	6245
∅	Ω

$\infty-$ sets

0124	**∞356**
0235	**146∞**
0346	**25∞1**
∞450	3612
0561	**4∞23**
∞602	5134
∞013	6245
∅	Ω

$0-$ sets

∞124	0356
1235	**∞460**
1346	**250∞**
1450	**36∞2**
∞561	4023
1602	**5∞34**
∞013	6245
∅	Ω

$1-$ sets

∞124	0356
∞235	1460
2346	**∞501**
2450	**361∞**
2561	**40∞3**
∞602	5134
2013	**6∞45**
∅	Ω

$2-$ sets

3124	**0∞56**
∞235	1460
∞346	2501
3450	**∞612**
3561	**402∞**
3602	**51∞4**
∞013	6245
∅	Ω

$3-$ sets

∞124	0356
4235	**1∞60**
∞346	2501
∞450	3612
4561	**∞023**
4602	**513∞**
4013	**62∞5**
∅	Ω

$4-$ sets

5124	**03∞6**
∞235	1460
5346	**2∞01**
∞450	3612
∞561	4023
5602	**∞134**
5013	**624∞**
∅	Ω

$5-$ sets

6124	**035∞**
6235	**14∞0**
∞346	2501
6450	**3∞12**
∞561	4023
∞602	5134
6013	**∞245**
∅	Ω

$6-$ sets

Figure 9.2. All n-sets, with outer n-sets in bold.

[1]Other people have made this very natural assumption, so it is convenient that it has a standard name, "Kirmse's Mistake." The product of two randomly chosen Kirmse integers happens to be a Kirmse integer rather more than one-third of the time.

Then we have

Lemma 2. *The n-integers are multiplicatively closed for each* $n = 0, \ldots, 6$.

Proof. The seven systems are obviously isomorphic, so we study the 0-integers, for which the halving-sets are

$\emptyset$	0124	0235	0346	∞450	0561	∞602	∞013
$\Omega = \infty$0123456	∞356	∞146	∞125	1236	∞234	1345	2456.

This shows that the 0-integers are spanned by $i_{\infty 356}$, i_{0235}, i_{0463}, and i_{0156} over the Gravesian integers, so the result is established by the multiplication table:

	$i_{\infty 356}$	i_{0235}	i_{0463}	i_{0156}
$i_{\infty 356}$	$i_{\overline{\infty}356}$	$i_{\overline{\infty}234}$	$i_{\overline{\infty}461}$	$i_{\overline{\infty}152}$
i_{0235}	$i_{\overline{\infty}0\overline{4}5}$	-1	$i_{\overline{\infty}1\overline{2}5}$	$i_{\overline{\infty}\overline{4}1\overline{6}}$
i_{0463}	$i_{\overline{\infty}0\overline{1}3}$	$i_{\overline{\infty}\overline{1}2\overline{5}}$	-1	$i_{\overline{\infty}2\overline{4}3}$
i_{0156}	$i_{\overline{\infty}0\overline{2}6}$	$i_{\overline{\infty}4\overline{1}6}$	$i_{\overline{\infty}\overline{2}4\overline{3}}$	-1

The resulting systems are seven of the sixteen orders of Theorem 1, the seven maximal ones (see Figure 9.1). The intersections of pairs of these, which are also the intersections of certain triples, yield the seven "double Hurwitzian" systems. (The halving-sets $\emptyset$, Ω, ∞124, 0356 for the typical one of these show that it is obtained by Dickson doubling from a Hurwitzian ring of quaternions.) The intersection of all seven maximal systems, which is equally the intersection of any two of the double Hurwitzian systems, we call the **Kleinian octaves**, since they can be obtained from Graves's integer octaves by adjoining $\frac{1}{2}(1 + i_0 + \cdots + i_6)$, which, being of the form $\frac{1}{2}(1 + \sqrt{-7})$, is a "Kleinian" integer (see Chapter 2).

We now complete the proof of Theorem 1. We see that every possible halving-set is an n-set for some $n \neq \infty$, since every set of 0 or 4 or 8 coordinates appears in Figure 9.2. We call it an **inner** or **outer** n-set according as it is or is not also an ∞-set.

First we deal with the outer n-sets.

Lemma 3. *Together with the Gravesian integers, any octonion* α *whose halving-set is an outer n-set generates all the n-integers.*

Proof. We can suppose that the halving-set is one of the eight outer 0-sets. By subtracting a Gravesian integer, we can reduce α to the form

$$\alpha = \frac{1}{2}(\pm i_a \pm i_b \pm i_c \pm i_d),$$

where, for the same reason, the choice of signs is unimportant. Then Figure 9.3 shows how multiplication by three Gravesian units connects all eight outer 0-sets. Since each inner 0-set is the sum of two outer ones, the resulting octonions additively generate all the 0-integers.

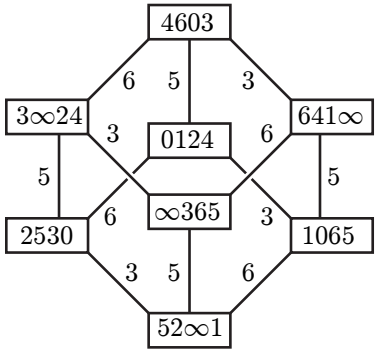


Figure 9.3. The eight outer 0-sets, related by multiplication by i_3, i_5, and i_6, ignoring signs.

Now we deal with the inner n-sets, which are also ∞-sets.

Lemma 4. *In the presence of the Gravesian integers: (i) Two octavian integers whose halving-sets are complementary 4-element ∞-sets generate each other. (ii) Two octonions whose halving-sets are distinct non-complementary ∞-sets generate the n-integers for some n (see Figure 9.4).*

Proof. (i) Left multiplication by i_0 converts $\frac{1}{2}(i_\infty + i_1 + i_2 + i_4)$ to $\frac{1}{2}(i_0 + i_3 + i_6 + i_5)$, etc.

(ii) We can suppose by (i) that both sets mention ∞, so one is obtained from the other by increasing subscripts by 1, 2, or 4 (mod 7), so without loss of generality by 1 in view of the subscript-doubling symmetry $\beta = (i_1 i_2 i_4)(i_3 i_6 i_5)$. So, again without loss of generality, the two halving-sets are $\infty 602$ and $\infty 013$, and we have already seen that the product of $i_{\infty 602}$ and $i_{\infty 013}$ has halving-set 0235, an outer 0-set.

The proof that an order containing the Gravesian integers is one of our sixteen is now easy. If it isn't the Gravesian or Kleinian octaves, it must involve a 4-element halving-set, and therefore also the complementary one, as well as $\emptyset$ and Ω. If these are all the halving-sets, it is a double Hurwitzian ring. Otherwise, it must involve either an outer n-set or two distinct non-complementary inner ones, and so contain all the n-integers for some n.

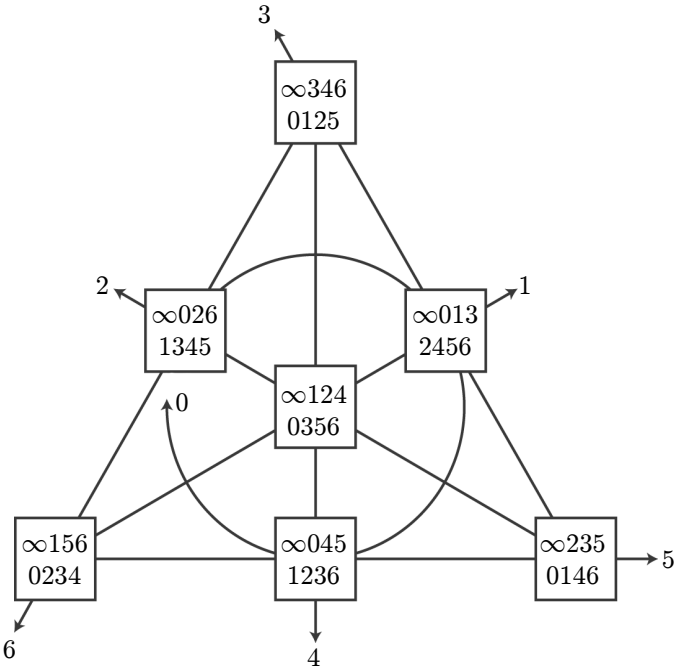


Figure 9.4. If two "points" in this "plane" lie on the "line" marked n, octonions with the corresponding halving-sets generate the n-integers.

Any still larger order would, by the same argument, contain the n-integers for two distinct values of n. But applying the subscript-doubling symmetry β allows us to suppose that these differ by 2, so without loss of generality, the order contains the 0-integer $i_{\infty 235}$ and the 2-integer i_{0235}, which, as we have seen, give a non-integral product.

9.3 The E_8 Lattice of Korkine, Zolotarev, and Gosset

We now fix our arithmetic to be a particular one of the seven maximal orders, defining the **octavian integers** (or briefly, "the octavians") to be the 0-integers. Geometrically, the octavian integers O^8 form a well-known and very interesting lattice usually called the E_8 **root lattice** (or, since its geometry was investigated by Thorold Gosset [19], the **Gosset lattice**).[2]

[2]It is also the unique "even unimodular" lattice in eight dimensions, and as such was proved to exist by H. J. S. Smith [39] in 1867. Korkine and Zolotarev [28] explicitly constructed it in their 1877 study of sphere packings. (They were anticipated to some extent by Rodrigues.) Blichfeldt [6] proved in 1935 that it does indeed yield the densest lattice packing of spheres in eight dimensions.

Its arithmetical properties have also been much studied: We quote from the analytic theory of quadratic forms the fact that the number of vectors in E_8 of norm $2n > 0$ is 240 times the sum of the cubes of the divisors of n. In the following sections, we give a simple new geometrical definition of this lattice and use it to prove that octavians have the "division with small remainder" property.

9.3.1 The Simplex Lattice A_n

An n-dimensional **regular simplex** is the convex hull of $n+1$ points whose distances from each other are all equal. The n-dimensional **simplex lattice** A_n is generated by vectors along the edges of such a simplex. If we take the vertices to be

$$v_i = (0, 0, \ldots, \overset{i}{1}, \ldots, 0, 0)$$

in $(n+1)$-space, then the generators are

$$v_i - v_j = (0, 0, \ldots, \overset{i}{1}, \ldots, \overset{j}{-1}, \ldots, 0, 0),$$

which identifies A_n as the set of all vectors $(x_0, \ldots, x_n)$ of $n+1$ integer coordinates with zero sum.

9.3.2 The Orthoplex Lattice D_n

The name **regular orthoplex** is our term for what has also been called a **cross polytope**, the analogue of the 2-dimensional square and the 3-dimensional octahedron (see Figure 9.5). Its vertices $(\pm 1^1, 0^{n-1})$ are the ends of unit vectors along the axes of an orthonormal frame, and it has one (simplicial) cell for each of the resulting orthants of n-dimensional space (so that "orthoplex" abbreviates "orthant-complex").

The n-dimensional **orthoplex lattice** D_n is the lattice generated by the vectors along the edges of a regular n-dimensional orthoplex. If we take vertices of the orthoplex to be

$$v_i = (0, 0, \ldots, \overset{i}{1}, \ldots, 0, 0) \text{ and } \overline{v_i} = (0, 0, \ldots, \overset{i}{-1}, \ldots, 0, 0) \quad (i = 1, \ldots, n),$$

then the generators of D_n are all of the vectors $(\pm 1^2, 0^{n-2})$ and D_n is identified with the lattice of all the vectors $(x_1, \ldots, x_n)$ of integer coordinates that have even sum.

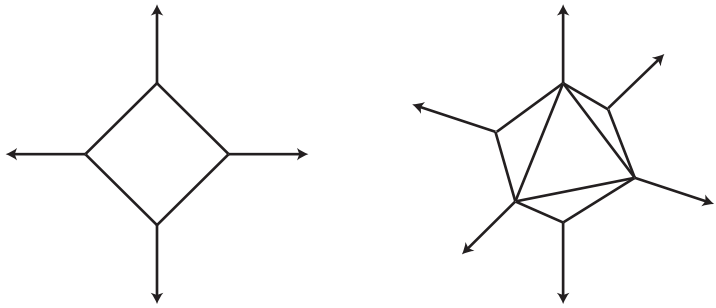


Figure 9.5. The 2-dimensional orthoplex is a square. Its four edges correspond to the four quadrants of the plane. The 3-dimensional orthoplex is a regular octahedron. Its eight triangular faces correspond to the eight octants of space.

9.3.3 Defining E_8

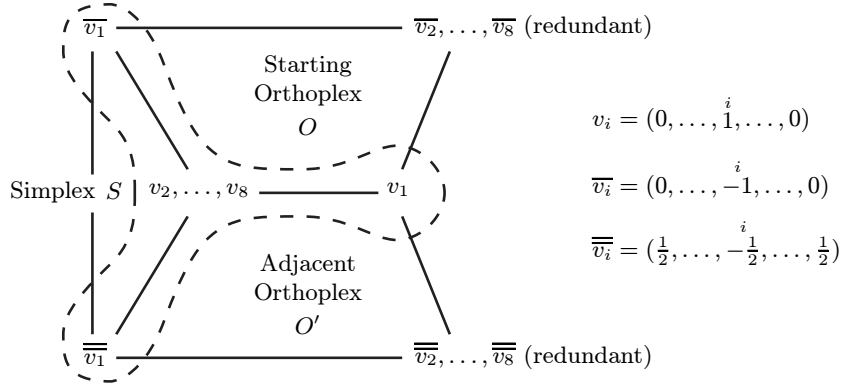
We define E_8 to be the lattice $\langle S, O\rangle$ generated by the edge-vectors of a simplex (of dimension 8) S together with an adjacent orthoplex O. Figure 9.6 shows several things:

- E_8 contains copies of both A_8 and D_8. In fact, we shall see that it contains A_8 to index 3 and D_8 to index 2.

- If O' is the orthoplex on an adjacent face of S, then $\langle S, O\rangle = \langle S, O'\rangle$, so the construction has the full symmetry of S: E_8 is generated by the edges of S together with those of the orthoplex on any one of its nine faces.

- If instead O' is the orthoplex on an adjacent face of O, then $\langle S, O\rangle$ equals the lattice $\langle O, O'\rangle$ generated by the edges of O and O', which are related to each other by reflection in the plane that separates them. So the construction has only half of the symmetry of O: E_8 is generated by the edges of O and a *simplex* (S) on any of 128 of its faces or of O and the *orthoplex* (O') obtained by reflecting it in any of the other 128 faces.

The figure also shows incidentally that the 8-dimensional space containing an E_8 is covered by simplexes and orthoplexes equivalent by symmetries



Vertices of O are $v_1, \ldots, v_8, \overline{v_1}, \ldots, \overline{v_8}$ and center is (0^8)
Vertices of O' are $v_1, \ldots, v_8, \overline{\overline{v_1}}, \ldots, \overline{\overline{v_8}}$ and center is $(\frac{1}{4}{}^8)$
Vertices of S are $\overline{v_1}, \overline{\overline{v_1}}, v_2, \ldots, v_8$ and center is $(-\frac{1}{6}, \frac{1}{6}{}^7)$

Figure 9.6. The three lattices $\langle S, O\rangle$, $\langle S, O'\rangle$, $\langle O, O'\rangle$ all coincide with the lattice generated by differences of the ten indicated vectors $\overline{v_1}, \overline{\overline{v_1}}, v_1, v_2, \ldots, v_8$ in view of the identities $v_1 + \overline{v_1} = \ldots = v_8 + \overline{v_8}$ and $v_1 + \overline{\overline{v_1}} = \ldots = v_8 + \overline{\overline{v_8}}$.

to those mentioned. For, half of the walls of an such orthoplex lead to equivalent orthoplexes and the other half to simplexes, while from a simplex any wall leads to an orthoplex. Hence

Lemma 5. *For any α of 8-dimensional space, there is a point β of the E_8 lattice for which $[\alpha - \beta] \leq 1$.*

For α is in either a simplex or an orthoplex, so can be no further from the lattice than is the center of that polytope.

To show that the octavian integers include a scaled copy of the E_8 lattice, it suffices to find among them the vertices of a simplex and an adjacent orthoplex. This is done in Figure 9.7. Since the norms of these vectors are half those of our previous E_8, we obtain the restated

Lemma 6. *For any real octonion α, there is an octavian integer β for which $[\alpha - \beta] \leq \frac{1}{2}$.*

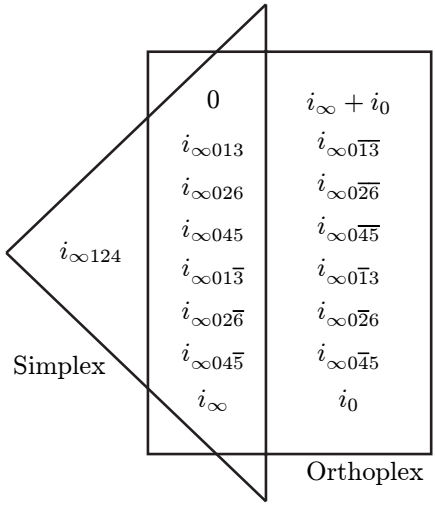


Figure 9.7. The octavian integers generate E_8.

9.4 Division with Remainder, and Ideals

Applying this to $\delta^{-1}\alpha$ (or alternatively $\alpha\delta^{-1}$), we immediately deduce the

Theorem 2. *If α and δ are octavian integers with $\delta \neq 0$, then we can write $\alpha = \delta\beta + \rho$ (or alternatively $\alpha = \beta\delta + \rho$) for octavian integers β and ρ with $[\rho] \leq \frac{1}{2}[\delta]$.*

Since in particular we have $[\rho] < [\delta]$, this entails as usual that

Theorem 3. *Any left or right ideal in O^8 is principal.*

The usual reason to be interested in ideals is because they appear in the standard proofs of factorization theorems. In a non-commutative ring, the left and right ideals are distinct concepts. However, O^8 is an unusual ring:

Lemma 7. *Every ideal in O^8 is 2-sided.*

Proof. In particular, a right ideal $\mathcal{I}$ is closed under unit right multiplications. In Chapter 8 we showed that the left multiplications by the particular units i_0 and $i_{\infty 365}$ were products of seven right multiplications

by octavian units. In Chapter 10, we shall see that it follows easily that every left multiplication by an octavian unit is a product of seven right ones. Therefore $\mathcal{I}$ is closed under left multiplication by octavian units, and so by arbitrary octavian integers, since any such is a sum of octavian units.

We can say more:

Theorem 4. *Any 2-sided ideal* Λ *in* O^8 *is the principal ideal* $n\mathsf{O}^8$ *generated by a rational integer* n.

This turns out to destroy the possibility of using ideals to prove unique factorization. This result was partially proved by Mahler [32], sketched by van der Blij and Springer [43], and completed by Lamont [30]. Our geometrical results will make it easy.

Proof. This is because Λ is invariant under bimultiplications by unit octavians, which generate all even symmetries of its underlying scaled E_8 lattice. We now apply

Theorem 5. *If a sublattice* Λ *of* E_8 *is fixed under all even automorphisms of* E_8*, then* $\Lambda = nE_8$.

To see this, use the "orthoplex" coordinates for E_8. Let $v_1 = (a\ b\ c\ d\ e\ f\ g\ h)$ be an element of minimal nonzero norm in Λ. We first show that some two coordinates may be supposed to be 0. For if not, we can apply even permutations to suppose g, h are the coordinates of smallest absolute value, after which there is an even symmetry taking v_1 to $v_2 = (a\ b\ c\ d\ e\ f\ -g\ -h)$, so that the norm of $v_3 = v_1 - v_2 = (0\ 0\ 0\ 0\ 0\ 0\ 2g\ 2h)$ is at most that of v_1.

Next we show that there is at most one nonzero coordinate. Otherwise, if the last two coordinates are 0, there exists an even symmetry (a 3-cycle) taking $v_1' = (a\ b\ c\ d\ e\ f\ 0\ 0)$ to $v_2' = (a\ b\ c\ d\ e\ 0\ f\ 0)$, where f is the nonzero coordinate of least absolute value, and again the norm of $v_3' = v_1' - v_2' = (0\ 0\ 0\ 0\ 0\ f\ -f\ 0)$ is at most that of v_1'. This shows that one minimal nonzero vector of Λ is f times a minimal vector of E_8, and applying even symmetries we see that f times any minimal vector of E_8 is in Λ, and so $\Lambda = fE_8$.

It remains to consider the case when a minimal vector of Λ has only one nonzero coordinate. But then (being in E_8) it must have the form $(2f\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$, which is taken to $(f\ f\ f\ f\ 0\ 0\ 0\ 0)$ by a suitable even symmetry, and we resort to the arguments of the previous case.

So ideal theory will not help us study octavian factorization. A more fruitful approach appears in the next section.

9.5 Factorization in O^8

In this section, we show that a primitive octavian integer ρ of norm mn has precisely 240 left-hand divisors of norm m and 240 right-hand divisors of norm n, each set geometrically similar to the 240 units of O^8.[3] This result is analogous to the result of Chapter 5 for the Hurwitz integers, except that in O^8, the factorizations are not unique "up to unit-migration" in view of the lack of associativity in $\mathbb{O}$. More generally, we shall show that the set of left-hand divisors of a given octavian integer is geometrically similar to the set of all octavian integers of a certain norm.

It is remarkable that the argument does not use the full octavian form of the division with small remainder property. It does, however, use the corresponding property of E_8 and so fails for our coarser octavian integer systems. The failure is more acute than that for the Lipschitz quaternions.

We first present an intriguing "reversing" Euclidean algorithm due to Rehm [37]. The *forward stage* (Figure 9.8) starts with a pair ρ_1, m_1, where ρ_1 is an octavian whose norm is divisible by the rational integer m_1 (but for a technical reason we conjugate the remainder). We take $[\rho_1] = m_0 m_1$ and determine successive numbers m_i and octavians γ_i, ρ_i by:

$$\begin{array}{rll}
\rho_1 = \gamma_1 m_1 + \overline{\rho_2} & [\rho_1] = m_0 m_1 & \\
\rho_2 = \gamma_2 m_2 + \overline{\rho_3} & [\rho_2] = m_1 m_2 & m_1 > m_2 \\
\vdots & \vdots & \vdots \\
\rho_{N-1} = \gamma_{N-1} m_{N-1} + \overline{\rho_N} & [\rho_{N-1}] = m_{N-2} m_{N-1} & m_{N-2} > m_{N-1} \\
\rho_N = \gamma_N m_N & [\rho_N] = m_{N-1} m_N & m_{N-1} > m_N > 0
\end{array}$$

Figure 9.8. The forward stage of Rehm's algorithm.

We briefly explain. Why is $[\rho_2]$ divisible by m_1 (so that $m_2 = [\rho_2]/m_1$ is an integer)? Because m_1 divides every term on the right-hand side of

$$[\overline{\rho_2}] = [\rho_1 - \gamma_1 m_1] = [\rho_1] + m_1^2[\gamma_1] - m_1(2[\rho_1, \gamma_1]).$$

Why is $m_2 < m_1$? Because $m_1 m_2 = [\rho_2] \leq \frac{m_1^2}{2}$.

If $m_2 > 0$, we can repeat the arguments above with ρ_2 and m_2, leading to ρ_3 and $m_3 < m_2$, and so on. Since the m_i are decreasing after m_0, at some point we must reach an $m_{N+1} = 0$, and we then obtain a finite collection of elements in O^8 whose relationships are summarized in Figure 9.8.

[3] The first results along these lines are due to Rankin and Lamont. The geometrical assertion appears to be new.

We now enter the *reverse stage*, displayed in Figure 9.9, which sets up 1-to-1 correspondences

$$\mu_N \leftrightarrow \mu_{N-1} \leftrightarrow \cdots \leftrightarrow \mu_1 \leftrightarrow \mu_0,$$

that are in fact similarities, between certain divisors of the ρ_i. For let μ_N be any element of norm m_N. Since $\mathbb{O}$ is diassociative, we may write

$$\rho_N = \gamma_N m_N = \gamma_N(\mu_N\overline{\mu_N}) = (\gamma_N\mu_N)\overline{\mu_N}.$$

Set $\mu_{N-1} = \gamma_N\mu_N$, so that μ_{N-1} is a left-hand divisor of ρ_N of norm m_{N-1}. Then $\overline{\mu_{N-1}}$ is a right-hand divisor of both $\overline{\rho_N}$ and m_{N-1}, and thus also of ρ_{N-1}, since

$$\begin{aligned}\rho_{N-1} = \gamma_{N-1}m_{N-1} + \overline{\rho_N} &= (\gamma_{N-1}\mu_{N-1})\overline{\mu_{N-1}} + \mu_N\overline{\mu_{N-1}} \\ &= (\gamma_{N-1}\mu_{N-1} + \mu_N)\overline{\mu_{N-1}}.\end{aligned}$$

Setting $\mu_{N-2} = \gamma_{N-1}\mu_{N-1} + \mu_N$, we obtain a left-hand divisor of ρ_{N-1} of norm m_{N-2}. We can continue this procedure until we arrive at a left-hand divisor μ_0 of $\rho = \rho_1$ of norm $m = m_0$ and a corresponding right-hand divisor $\overline{\mu_1}$ of norm $n = m_1$. Figure 9.9 summarizes this process, which can be thought of as tracing the left-hand column of Figure 9.8 from bottom to top, factoring along the way.

$$\begin{array}{rll} & & [\mu_N] = m_N \\ \rho_N = \mu_{N-1}\overline{\mu_N} & \mu_{N-1} = \gamma_N\mu_N & [\mu_{N-1}] = m_{N-1} \\ \rho_{N-1} = \mu_{N-2}\overline{\mu_{N-1}} & \mu_{N-2} = \gamma_{N-1}\mu_{N-1} + \mu_N & [\mu_{N-2}] = m_{N-2} \\ \rho_{N-2} = \mu_{N-3}\overline{\mu_{N-2}} & \mu_{N-3} = \gamma_{N-2}\mu_{N-2} + \mu_{N-1} & [\mu_{N-3}] = m_{N-3} \\ \vdots & \vdots & \vdots \\ \rho_2 = \mu_1\overline{\mu_2} & \mu_1 = \gamma_2\mu_2 + \mu_3 & [\mu_1] = m_1 \\ \rho_1 = \mu_0\overline{\mu_1} & \mu_0 = \gamma_1\mu_1 + \mu_2 & [\mu_0] = m_0 \end{array}$$

Figure 9.9. The reverse stage of Rehm's algorithm.

We remark that the multiplication of the algebra is not used in an essential way in Figure 9.8. Moreover, products involving triples of elements in Figure 9.9 occur only within associative subalgebras.

9.5.1 The Structure of the Divisor Sets

We are now able to describe the sets of all possible left-hand and right-hand divisors of $\rho = \rho_1$ of norms $m = m_0$ and $n = m_1$. We shall see that the size of these is the number of octavian integers μ_N whose norm is the integer m_N in the last line of Figure 9.8. For the geometrical configurations of these sets, we use the following:

Lemma 8. *Let the octavian integer γ be factored in two ways as $\gamma = \alpha\beta = \alpha'\beta'$, where $[\alpha] = [\alpha'] \neq 0$ and $[\beta] = [\beta'] \neq 0$. Then the angle θ_a between α and α' is equal to the angle θ_b between β and β'.*

Proof. Taking the inner product of γ with $\alpha\beta'$, we obtain

$$[\alpha][\beta, \beta'] = [\alpha\beta, \alpha\beta'] = [\gamma, \alpha\beta'] = [\alpha'\beta', \alpha\beta'] = [\alpha', \alpha][\beta'],$$

which yields

$$\cos\theta_a = \frac{[\alpha, \alpha']}{[\alpha]} = \frac{[\beta, \beta']}{[\beta']} = \cos\theta_b.$$

Let $\{\mu_N\}, \{\mu_{N-1}\}, \ldots, \{\mu_0\}$ denote the sets of all the μ_k that can appear in the reverse stage (Figure 9.9). We have shown that in fact $\{\mu_N\}$ is the set of all octavian integers of norm m_N. It is obviously similar to its conjugate set $\{\overline{\mu_N}\}$, but we could also deduce this by setting $\gamma = m_N$ in Lemma 8. We indicate this relationship by

$$\{\mu_N\} \overset{m_N}{\sim} \{\overline{\mu_N}\}.$$

In a similar way, we find the similarities

$$\{\overline{\mu_N}\} \overset{\rho_N}{\sim} \{\mu_{N-1}\} \overset{m_{N-1}}{\sim} \{\overline{\mu_{N-1}}\} \overset{\rho_{N-1}}{\sim} \cdots \overset{m_1}{\sim} \{\overline{\mu_1}\} \overset{\rho_1}{\sim} \{\mu_0\}$$

by alternately setting $\gamma = \rho_i$ and m_i for appropriate i. But $\{\mu_0\}$ and $\{\overline{\mu_1}\}$ are precisely the set of left-hand and right-hand divisors of ρ_1 of norm n.

This leads to the

Theorem 6. *Let $\rho = \rho_1$ be an octavian integer of norm mn, where m, n are positive rational integers. Let d be the greatest common rational integer divisor of ρ, m, n. Then the set of left-hand divisors (μ_0) of ρ of norm m and the set of right-hand divisors $(\overline{\mu_1})$ of ρ of norm n are geometrically similar to the set of all octavian integers (μ_N) of norm $d(= m_N)$.*

Proof. We have done everything except identify the norm, so we have only to determine m_N. Let $\gcd(\eta_1, \ldots, \eta_k)$ denote the greatest common rational integer divisor of $\eta_1, \ldots, \eta_k$ in O^8. Then:

Lemma 9. *Let $d_i = \gcd(\rho_i, m_{i-1}, m_i)$ for $1 \leq i \leq N$. Then $d_i = d_{i+1}$ for $1 \leq i \leq N-1$.*

Proof. First, see that d_i divides $\overline{\rho_{i+1}} = \rho_i - \gamma_i m_i$ since d_i divides ρ_i and m_i, so d_i divides ρ_{i+1}. It divides m_i by definition. Finally, d_i divides m_{i+1} since d_i divides each term in the last line of

$$\begin{aligned} m_{i+1} = \tfrac{[\overline{\rho_{i+1}}]}{m_i} &= (\tfrac{1}{m_i})([\rho_i] + m_i^2[\gamma_i] - m_i(2[\gamma_i, \rho_i])) \\ &= m_{i-1} + m_i[\gamma_i] - 2[\gamma_i, \rho_i]. \end{aligned}$$

Therefore, d_i divides d_{i+1}. By a similar argument, d_{i+1} divides d_i as well, so $d_i = d_{i+1}$.

Our theorem now follows, since

$$d_N = \gcd(\rho_N, m_{N-1}, m_N) = m_N,$$

and therefore

$$m_N = d_1 = \gcd(\rho_1, m_0, m_1) = \gcd(\rho, m, n) = d.$$

One could use this theorem to count factorizations into more than two factors, of arbitrary norms and "imprimitivity status." The following sections discuss only factorizations into primes.

9.6 The Number of Prime Factorizations

In Chapter 5, we counted the prime factorizations of a quaternion modelled on the factorizations of its norm. For instance, up to unit-migration there are just 12 factorizations of a primitive Hurwitzian of norm 60 into primes, modelled on the 12 factorizations

2.2.3.5	2.2.5.3	2.3.2.5	2.5.2.3	2.3.5.2	2.5.3.2
3.2.2.5	5.2.2.3	3.2.5.2	5.2.3.2	3.5.2.2	5.3.2.2

of 60 into rational primes.

For octonions, the failure of the associative law causes the situation to change in two ways. On the one hand, there are now $5 \times 12 = 60$ factorizations of 60 into ordinary primes:

$$\begin{aligned} 60 &= ((2.2)3)5 = (2(2.3))5 = (2.2)(3.5) = 2((2.3)5) = 2(2(3.5)) \\ &= ((2.2)5)3 = (2(2.5))3 = \quad \cdots \quad . \end{aligned}$$

But also, the factorizations of Q modelled on a given one of its norm are no longer related by unit-migration, since $\alpha u.u^{-1}\beta$ need not equal $\alpha\beta$.

However, we call a change that affects just two adjacent factors **metamigration**, since it "imitates" unit-migration. Note that the number of factorizations $\beta u.u^{-1}\gamma$ obtained by unit-migration from $\beta\gamma$ is the number of units, and the set of left-hand factors βu is geometrically similar to the set of units u. Our 2-term factorization theorem easily implies:

Theorem 7. *The number of factorizations of a primitive octavian, say* $Q = ((P_1P_2)(P_3(P_4...P_k)))$*, modelled on a given factorization of its norm is* 240^{k-1}*. Moreover, if all but* P_i *and* P_j *are fixed, then the sets of values for* P_i *and* P_j *are geometrically similar to the set of 240 units.*

What if Q need not be primitive?

Theorem 8. *An octavian of norm* $p_1^{n_1} \dots p_k^{n_k}$ *that is exactly divisible by* $p_1^{s_1} \dots p_k^{s_k}$ *has exactly*

$$240^{n-1} \prod C_{n_i,s_i}(p_i^3)$$

prime factorizations on any given model, where the "truncated Catalan polynomials" $C_{n,s}(x)$ *are as defined in Chapter 5, and* $n = n_1 + \dots + n_k$*.*

Proof. As in the quaternion case, it suffices to consider the cases that involve only one rational prime p. For factorizations of the form

$$P_1(P_2(\dots(P_{n-1}P_n)\dots)),$$

the argument is exactly as in Chapter 5 except that we cannot work up to unit-migration and so must count the factors of 240 as they arise, and p must be replaced by p^3 since there are $240(p^3+1)$ octavians of norm p. (The prime 2 is no longer special.)

A similar argument applies for factorizations such as

$$P_1((P_2P_3)P_4)$$

that can be built up by repeatedly adjoining single prime factors. To deal with factorizations not of this form, such as

$$(P_1P_2)(P_3P_4),$$

one can use a "metassociation lemma," according to which there will be equal numbers of factorizations of the forms $(AB)C$ and $A'(B'C')$ provided that the octavians in each of the pairs (A, A'), (B, B'), (C, C') have the same norm and are divisible by the same rational integers. We suppress the details.

Letting the model vary, we see that the total number of prime factorizations will be 240^{n-1} times the product of:

- the numbers $C_{n_1,s_1}(p_1^3)$, ..., $C_{n_k,s_k}(p_k^3)$ that count factorizations on a given model "up to metamigration,"

- the multinomial coefficient $\binom{n}{n_1, \ldots, n_k}$ that counts possible orderings for the primes in the model, and finally,
- the Catalan number C_{n-1} that counts the possible arrangements of parentheses.

(For the corresponding result for quaternions, replace 240 by 24, p_i^3 by p_i, and omit C_{n-1} in virtue of their associativity.)

We can hardly call octavian prime factorization "unique" before we have solved the metamigration, metacommutation, and metassociation problems below. However, Rankin and Lamont remark that prime factorization of an odd norm primitive octavian can be made unique by demanding that the factors be congruent (mod 2) to specified units.

9.7 "Meta-Problems" for Octavian Factorization

Recall that we reduced unique factorization for the Hurwitzians to the **metacommutation problem**: What is the relation between factorizations PQ and $Q'P'$ modelled on pq and qp? For octavian factorization, we also have the **metassociation problem**: What is the relation between $(PQ)R$ and $P'(Q'R')$ modelled on $(pq)r$ and $p(qr)$? Moreover, there is even a **metamigration problem** that asks for the relation between factorizations PQ and $P'Q'$ modelled on the same factorization pq, since they are no longer related by unit migration.

There is also the problem of understanding factorizations in the Gravesian case. The assertion that corresponds to Theorem 6 is due to C. Feaux [16]:

Theorem 9. *If p, q are distinct primes, then a Gravesian integer of norm pq has exactly 16 factorizations*

$$P_1Q_1 = (-P_1)(-Q_1) = \ldots = P_8Q_8 = (-P_8)(-Q_8)$$

modelled on pq. Moreover, the left-hand factors are geometrically similar to the Gravesian units (i.e., $P_1, \ldots, P_8$ are mutually orthogonal) as are the right-hand ones.

The metamigration problem for Gravesian integers asks how these 16 factors can be recovered from one of them. We can partially solve it when the integer belongs to a Lipschitzian subring:

Theorem 10. *If $L = PQ$ and $L = Q'P'$ are factorizations of a Lipschitzian $L = a + bi_1 + ci_2 + di_4$ modelled on pq and qp, then the Gravesian factorizations of L modelled on pq are*

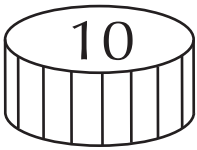
$$PU.\overline{U}Q \quad \textit{and} \quad P'V.\overline{V}Q',$$

where U runs over $\pm 1, \pm i_1, \pm i_2, \pm i_4$ and V over $\pm i_0, \pm i_3, \pm i_5, \pm i_6$.

Proof. This follows immediately from the Composition Doubling formula

$$(a + i_0 b)(c + i_0 d) = (ac - d\overline{b}) + i_0(cb + \overline{a}d).$$

So in this case, the Gravesian metamigration problem reduces to the Lipschitzian metacommutation problem.



Automorphisms and Subrings of O

In this chapter, we shall study the octavian units in some detail, and then use them to find the automorphism group of $\mathsf{O} = \mathsf{O}^8$ and to study some of its subrings.

10.1 The 240 Octavian Units

The following little table gives the quaternion triplets abc (for which i_a, i_b, i_c behave like i, j, k) in its first column, which can be supplemented by ∞ or 0 to give seven "quads" that are halving-sets for the octavians, as are their complements.

triplet		
124	0	∞365
235	0	∞461
346	0	∞512
450	∞	6123
561	0	∞234
602	∞	1345
013	∞	2456
quad		co-quad

The **octavian units** are those octavian integers whose inverses are also octavian integers. How many of them are there?

Theorem 1. *There are just 240 octavian units.*

Proof. The units can only be of the two forms

$$\pm 1,\ \pm i_0,\ \ldots,\ \pm i_6 \quad \text{and} \quad \frac{1}{2}(\pm i_a \pm i_b \pm i_c \pm i_d),$$

where *abcd* is one of the 14 4-element 0-sets. Since there are 16 choices of sign on the right, the total number is $16 + 14 \cdot 16 = 240$.

It is almost as easy to classify these by their multiplicative orders. We have

1 of each order 1 or 2, namely $+1$ and -1;

56 of each order 3 or 6, namely $\pm\frac{1}{2}(-1 \pm i_a \pm i_b \pm i_c)$,
where *abc* is one of 356 146 125 450 234 602 013;

and 126 of order 4, namely $\pm i_n$ and $\frac{1}{2}(\pm i_d \pm i_e \pm i_f \pm i_g)$,
where *defg* is one of 0124 0235 0346 1236 0561 1345 2456.

We shall call the elements of multiplicative orders 3 and 4 "ω"s and "i"s, respectively, and use the notations

$$\omega_{abc} = \frac{1}{2}(-1 + i_a + i_b + i_c) \quad \text{and} \quad i_{defg} = \frac{1}{2}(i_d + i_e + i_f + i_g)$$

for them, putting a bar over a subscript to indicate negation of a component, for example

$$\omega_{ab\bar{c}} = \frac{1}{2}(-1 + i_a + i_b - i_c) \quad \text{and} \quad i_{d\bar{e}\bar{f}g} = \frac{1}{2}(i_d - i_e - i_f + i_g).$$

When we ask what collections of these generate, it's natural to pair inverses with each other. Taking this point of view, what we are studying is a beast that has 63 pairs of **eyes** ("i"s) and 28 pairs of **arms** ("oms" = "ω"s)!

10.2 Two Kinds of Orthogonality

In the next few sections, we shall study the automorphism group $\mathrm{Aut}(\mathsf{O})$ of the ring O of octavian integers. In a way, this is a discrete analogue of what we did in Chapter 6, where we found the automorphism group of the real octaves to be the 14-dimensional Lie group $G_2(\mathbb{R})$, which we abbreviate to G_2. We shall find that of the octavian ring to be the analogous group $G_2(\mathbb{F}_2)$ over the field $\mathbb{F}_2$ of two elements, usually abbreviated by group theorists to $G_2(2)$.

Our discrete theory usually follows the continuous one, but with minor differences. For instance, in the continuous case we found that any unit orthogonal to 1 was like any other, and any orthogonal pair of such units was like any other such pair. The first of these remains true in the discrete case, but the second does not. Thus the 126 units orthogonal to 1—the "i"s—are all equivalent under the group, but the pairs i, j of orthogonal "i"s are of two kinds. We call i, j **evenly orthogonal** if $\frac{1+i+j+ij}{2}$ is also an octavian integer, and **oddly orthogonal** if not. In the same circumstances, we call i, j, ij an **even** or **odd** quaternion triplet.

We shall use i'_{abcd} for an octavian integer of type $\frac{1}{2}(\pm i_a \pm i_b \pm i_c \pm i_d)$ with an odd number of minus signs, i''_{abcd} for one with an even number, and i^*_{abcd} for either kind.

Lemma 1. *i_0 is orthogonal to just 60 other "i"s, of which it is evenly orthogonal to 12, namely $\pm i_1, \pm i_2, \ldots, \pm i_6$, and oddly orthogonal to 48, namely $i^*_{1236}, i^*_{2465}, i^*_{4153}$.*

Proof. Since each i other than $\pm i_n$ has the form i^*_{abcd}, and since 1236, 2465, 4153 are the only 0-sets that contain neither ∞ nor 0, there are indeed just 60 possibilities. As regards the type of orthogonality, the subscript-doubling symmetry $(i_1 i_2 i_4)(i_3 i_6 i_5)$ makes it sufficient to prove that $j = i_1$ or i_3 is evenly orthogonal to $i = i_0$ (which they are, since

$$\frac{1 + i + j + ij}{2} = \frac{1 + i_0 \pm i_1 \pm i_3}{2})$$

is in O^8) and $j = i^*_{1236}$ oddly so (which they are, since

$$\frac{1 + i + (j + ij)}{2} = \frac{1 + i_0 + (\pm i_{1 \text{ or } 3} \pm i_{2 \text{ or } 6})}{2}$$

is not in O^8).

10.3 The Automorphism Group of O

By joining each "i" to the six other "i"s that are evenly orthogonal to it, we obtain a graph we call the hyperhexagon.[1] Figure 10.1 shows the part of this graph near i_0, and Figure 10.2 shows the remainder.

[1] Usually called a generalized hexagon—see the end of this section.

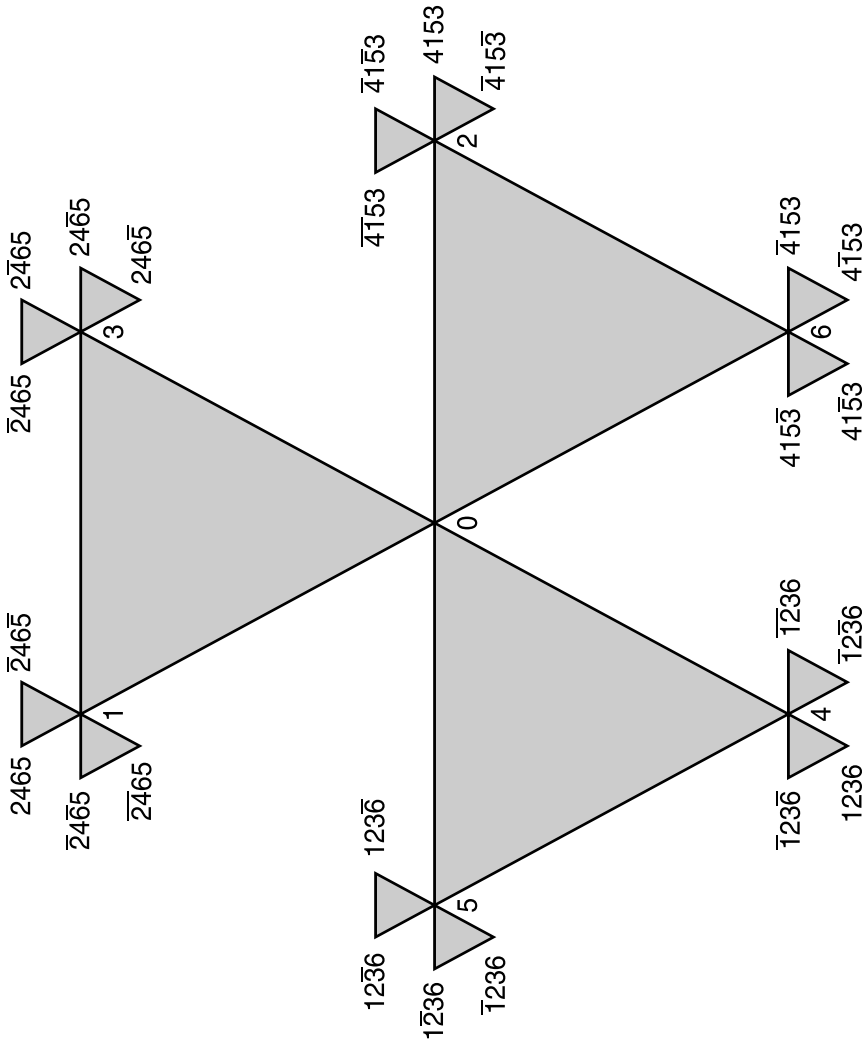


Figure 10.1. The 15 triangles of the hyperhexagon graph near i_0 (the "near side"). Each outer vertex here appears in 2 further triangles that are drawn as lines in Figure 10.2.

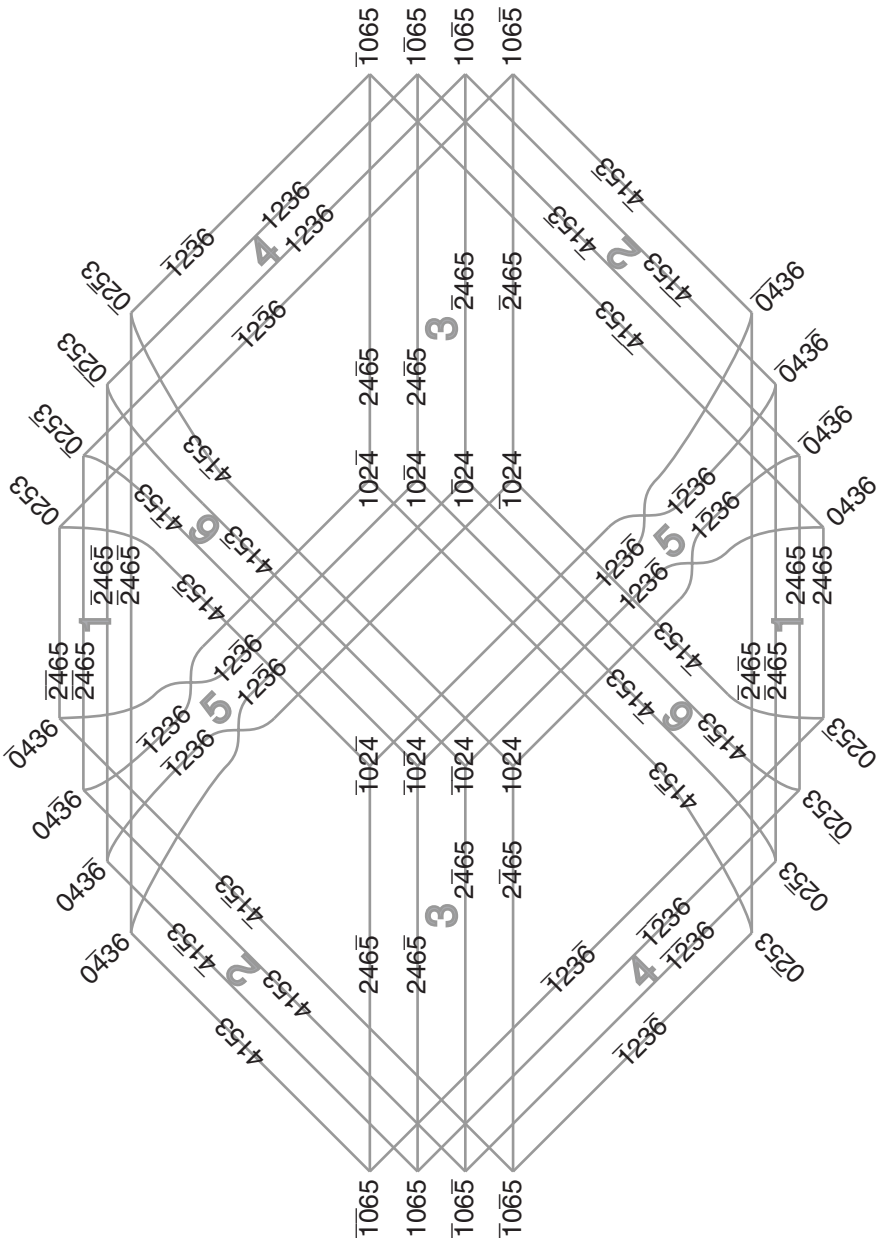


Figure 10.2. The 48 triangles of the "far side" of the hyperhexagon graph.

We use this graph to deduce

Theorem 2. *Aut(O) is transitive on "i"s.*

Proof. For any ω of order 3, the map $x \to \overline{\omega} x \omega$ is an automorphism of octonion multiplication by Theorem 14 of Chapter 8, and it takes O to O if ω is in O. So for example, conjugation by $\omega = \frac{1}{2}(-1 + i_0 + i_1 + i_3)$ is an automorphism of O that takes i_0 to i_1 to i_3.

In an exactly similar way, we can obtain an automorphism permuting the vertices of any triangle in the hyperhexagon, and since the graph is connected, these establish the transitivity.

What can we say about the images $i_0^\dagger$, $i_1^\dagger$, $i_2^\dagger$ of i_0, i_1, i_2 under the general automorphism of O? Since i_0 is evenly orthogonal to i_1 and i_2, which are oddly orthogonal to each other, $i_0^\dagger$, $i_1^\dagger$, $i_2^\dagger$ must have the same properties. On the other hand,

Theorem 3. *If $i_0^\dagger$, $i_1^\dagger$, $i_2^\dagger$ are three mutually orthogonal "i"s, in which just the orthogonalities involving $i_0^\dagger$ are even, then there is a unique automorphism of* O *taking $i_0 \to i_0^\dagger$, $i_1 \to i_1^\dagger$, $i_2 \to i_2^\dagger$.*

Proof. The uniqueness is immediate, since when we have the images of i_0, i_1, i_2 we know those of $i_4 = i_1 i_2$, $i_3 = i_0 i_1$, $i_6 = i_0 i_2$, $i_5 = i_0 i_4$. For instance, we shall determine the automorphism for which $i_0^\dagger = i_0$, $i_1^\dagger = i_2$, $i_2^\dagger = i_1$. We find

$$\begin{aligned} i_4^\dagger &= i_1^\dagger i_2^\dagger = i_2 i_1 = -i_4 \\ i_3^\dagger &= i_0^\dagger i_1^\dagger = i_0 i_2 = i_6 \\ i_6^\dagger &= i_0^\dagger i_2^\dagger = i_0 i_1 = i_3 \\ i_5^\dagger &= i_0^\dagger i_4^\dagger = i_0(-i_4) = -i_5, \end{aligned}$$

giving the map $(i_0)(i_1 i_2)(i_3 i_6)(i_4 - i_4)(i_5 - i_5)$, which is easily checked to be an automorphism. In a similar way we find the particular symmetries

$$\begin{aligned} &(i_0)(i_1\ i_2\ i_4)(i_3\ i_6\ i_5) \\ &(i_0)(i_2)(i_6)(i_1\ i_3 - i_1 - i_3)(i_5\ i_4 - i_5 - i_4) \\ &(i_0)(i_1)(i_3)(i_2\ i_4 - i_2 - i_4)(i_6\ i_5 - i_6 - i_5) \\ &(i_0)(i_1)(i_3)(i_2\ i_5 - i_2 - i_5)(i_4\ i_6 - i_4 - i_6). \end{aligned}$$

We show in general that the automorphisms of the theorem exist as follows. First, the transitivity allows us to reduce to the case $i_0^\dagger = i_0$. Then $i_1^\dagger$ and $i_2^\dagger$ must be among the $\pm i_n$, since these are the only "i"s that are evenly orthogonal to i_0. The symmetries above now enable us to reduce $i_1^\dagger$

to i_1 (while fixing i_0) and $i_2^\dagger$ to i_2 (fixing i_0 and i_1), and so establish the theorem.

There is an immediate corollary:

Corollary. *Aut(O) has order exactly 12096.*

Proof. $i_0^\dagger$ can be any one of the 126 "i"s. Then if $i_0^\dagger = i_0$, $i_1^\dagger$ can be any of $\pm i_1, \ldots, \pm i_6$, the 12 "i"s evenly orthogonal to i_0, and if also $i_1^\dagger = i_1$, $i_2^\dagger$ can be any of $\pm i_2, \pm i_4, \pm i_6, \pm i_5$, the 8 "$i$"s orthogonal evenly to i_0 but oddly to i_1. So the order is

$$126 \times 12 \times 8 = 12096.$$

Theorem 4. *Aut(O) is also transitive on (1) even quaternion triplets, (2) odd quaternion triplets, and (3) "ω"s.*

Proof. (1) If $i \to i_0$ and $j \to i_1$, then $k \to i_3$. (2) If $i \to i_1$ and $j \to i_2$, then $k \to i_4$.

(3) It will suffice to find for any $\omega = \frac{1}{2}(-1 \pm i_a \pm i_b \pm i_c)$ an even quaternion triplet i, j, k for which $\omega = \frac{1}{2}(-1 + i + j + k)$; and $i = \pm i_a$, $j = i^\omega$, $k = j^\omega$ will do.[2]

Usually, the graph we illustrated in Figures 10.1 and 10.2 is called a **generalized hexagon**, but we prefer the name "hyperhexagon." An ordinary polygon is a connected set of vertices and edges in which each object of either kind is incident with just two of the other. It is called an n-gon if the circuit formed by alternating vertices and incident edges contains n of each. We obtain the notion of a generalized n-gon by replacing the number 2 in the above by a larger number, in our case 3. The vertices of our hyperhexagon are "i"s counted up to sign. Its "hyperedges" are even quaternion triples i, j, k of such "i"s (again up to sign).

10.4 The Octavian Unit Rings

An **octavian unit ring** is a subring of O^8 generated by units. We shall show in the appendix that

[2] We cannot always take i, j, k to be $\pm i_a, \pm i_b, \pm i_c$, since this might not be a quaternion triplet. For $\omega = \omega_{365}$ the argument of the text leads to $i = i_3$, $j = i_{\overline{2}46\overline{5}}$, $k = i_{2\overline{4}6\overline{5}}$.

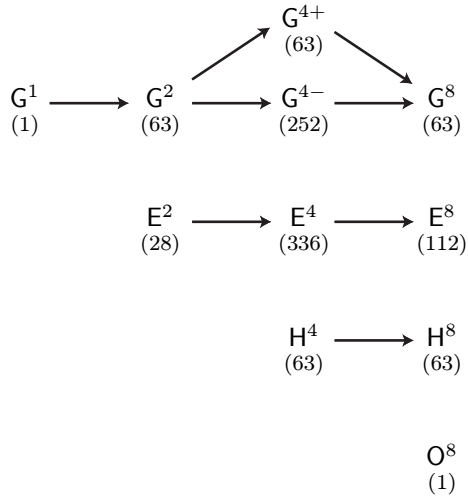


Figure 10.3. The unit rings. Here, G^1 is the ordinary integer $\mathbb{Z}$; E^2 is an Eisenstein ring $\mathbb{Z}[\omega]$ generated by an element ω of order 3 in O^8; H^4 is a Hurwitzian ring $\mathbb{Z}[i, j, k, \frac{1}{2}(-1 + i + j + k)]$; and finally, O^8 is the full octavian ring. An arrow $\mathsf{R}^n \to \mathsf{R}^{2n}$ indicates that R^{2n} is a Dickson double $\langle \mathsf{R}^n, i\rangle$ for some i orthogonal to R. The number of each type of ring is given in parentheses.

Theorem 5. *Up to isomorphism, there are precisely four types (*G^1, E^2, H^4, O^8*) of integer rings generated by odd-order elements, from which all of the octavian unit rings can be obtained by Dickson doubling* (see Figure 10.3).

It turns out that, with one important exception, if two unit rings are abstractly isomorphic, they are related by a symmetry of O^8. The exception is that there are two orbits of abstract type $\mathsf{G}^4 = \langle i, j, k\rangle$: G^{4+} in which i, j, k are evenly orthogonal, and G^{4-} in which i, j, k are oddly so.

We briefly discuss the transitivities in the nontrivial cases, paying particular attention to those that correspond to maximal subgroups. The transitivity on rings of type G^2 and G^8 follows since these are in 1-1 correspondence with each other[3] and with the vertices of the hyperhexagon. That on those of types G^{4+}, H^4, H^8 follows since these are also in 1-1 correspondence with each other[4] and with the "hyperedges" of the hyperhexagon.

[3]The G^8 corresponding to the G^2 generated by $\langle i\rangle$ is generated by the "i"s evenly orthogonal to that i.

[4]The H^4 corresponding to $\mathsf{G}^{4+} = \langle i, j, k\rangle$ is $\langle i, j, k, \frac{1}{2}(-1 + i + j + k)\rangle$, and the H^8 is generated by this and all "i"s orthogonal to it.

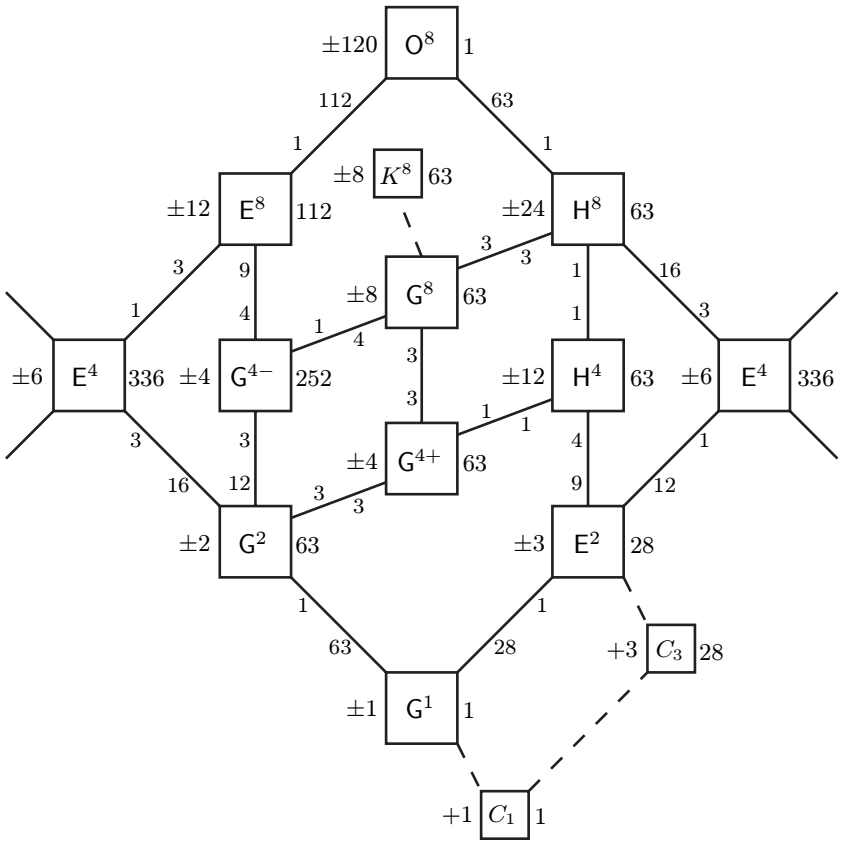


Figure 10.4. Inclusions between certain subthings of O^8. $\pm n$ precedes a ring that has n pairs of opposite units. $+n$ precedes a group consisting of n units. n follows one of n such things. Numbers against lines indicate numbers of containments – thus each E^4 lies in 16 H^8s, while each H^8 contains 3 E^4s. For simplicity, E^4 appears on both sides.

The transitivity on rings G^{4-} follows from transitivity on odd quaternion triples. However, all automorphisms that fix $\langle i_1, i_2, i_4\rangle$ fix i_0 also,[5] which with them generates a G^8, so this is not a maximal subgroup. A ring G^8 contains four rings G^{4-} in this way. For example, this one contains

$$\langle i_1, i_2, i_4\rangle,\ \langle i_1, i_5, i_6\rangle,\ \langle i_2, i_3, i_5\rangle,\ \langle i_4, i_6, i_3\rangle.$$

[5] $\pm i_0$ are the only "i"s evenly orthogonal to i_1, i_2, i_4.

The transitivity on rings $\mathsf{E}^2 = \mathbb{Z}[\omega]$ follows from transitivity on "ω"s. Since a ring of type E^4 or E^8 contains a unique one of type E^2 (generated by its odd-order elements), its stabilizer is not a maximal subgroup—we leave the transitivity to the interested reader.[6]

Figure 10.4 indicates all inclusions between these unit rings (and a few other things). More detailed discussions of them will be found in the next section. With just two exceptions, every loop generated by units is the loop of units of one of these unit rings. The exceptions are the trivial group C_1 and the group C_3 of order 3, generated by an ω. Their inclusion makes Figure 10.4 complete also for unit-loop inclusions. In Chapter 11 we shall obtain four non-unit subrings K^1, K^2, K^4, K^8 by considering octavians modulo 2, and we have included K^8 in our figure.

10.5 Stabilizing the Unit Subrings

The following sections provide more detailed information. The stabilizers of the general quaternionic subsystem Q^4 spanned by the quaternion triplet i, j, k) can be described uniformly by regarding Q^8 as the Dickson double $\mathsf{Q}^4+h\mathsf{Q}^4$ (in which h is the "doubler") and using the ideas of section 6.6 and the notation of Chapter 4. We don't need to discuss G^{4+} since it obviously has the same stabilizer as the unique H^4 that contains it. In the remaining cases, Q^8 is generated by Q^4 and units orthogonal to Q^4, so $\mathrm{Stab}(\mathsf{Q}^4)$ is contained in $\mathrm{Stab}(\mathsf{Q}^8)$.

10.5.1 Subring G^{4-}

An example is generated by $i = i_1$, $j = i_2$, $k = i_4$, for which a suitable doubler is $h = i_0$. The following table (in which only the subscripts are shown) shows the actions of a generating set of automorphisms on these.

	i	j	k	h	hi	hj	hk
$[u,v]$	1	2	4	0	3	6	5
$[\omega,\omega]$	2	4	$\overline{1}$	0	6	5	$\overline{3}$
$[\zeta,\zeta]$	2	1	$\overline{4}$	0	6	3	$\overline{5}$
$[i,i]$	1	$\overline{2}$	$\overline{4}$	0	3	$\overline{6}$	$\overline{5}$
$[1,-1]$	1	2	4	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{5}$

$$\omega = \tfrac{-1+i+j+k}{2}$$

$$\zeta = \tfrac{i+j}{\sqrt{2}}$$

[6] The 36 $\langle i\rangle$s orthogonal to $\langle\omega\rangle$ fall into twelve triples. Adjoining any one such triple yields an E^4, while an E^8 is obtained by adjoining a suitable three of them.

These must generate, since the first three yield all automorphisms of $\langle i_1, i_2, i_4\rangle$, any further generator can be supposed to fix i_1, i_2, i_4, and must therefore take i_0 to $\pm i_0$, since these are the only "i"s evenly orthogonal to each of i_1, i_2, i_4.

In the notation of Chapter 4, the structure of $\mathrm{Stab}(\mathsf{G}^{4-})$ is

$$\pm\frac{1}{24}[O \times O],$$

since $-1 = [1, -1]$ is present, while $[\omega, \omega]$, $[\zeta, \zeta]$, $[i, i]$ define the identity isomorphism between L and R, which are both copies of the binary octahedral group $2O = \langle \omega, \zeta, i\rangle$.

Any automorphism that fixes a G^8, e.g., $\langle i_n\rangle$, must fix the G^2 (here $\langle i_0\rangle$) generated by its middle element, and the converse is true since the "i"s evenly orthogonal to $\pm i_0$ are the other $\pm i_n$. Any $\mathsf{G}^{4-} = \langle i, j, k\rangle$ extends to a unique $\mathsf{G}^8 = \langle h, i, j, k\rangle$ by adjoining the middle element h of i, j, k. The case $\mathsf{G}^{4-} = \langle i_1, i_2, i_4\rangle$ yields $\mathsf{G}^8 = \langle i_n\rangle$, which, conversely, contains just four G^{4-}'s:

$$\langle i_1, i_2, i_4\rangle \quad \langle i_1, i_5, i_6\rangle \quad \langle i_2, i_3, i_5\rangle \quad \langle i_4, i_6, i_3\rangle.$$

So $\mathrm{Stab}(\mathsf{G}^{4-})$ has index 4 in $\mathrm{Stab}(\mathsf{G}^8) = \mathrm{Stab}(\mathsf{G}^2 = \langle i_0\rangle)$.

10.5.2 Subring H^4

In this case, exemplified by $i = i_0$, $j = i_1$, $k = i_3$, we take $h = i_6$ and find the following automorphisms:

	i	j	k	h	hi	hj	hk
$[u, v]$	0	1	3	6	2	5	4
$[\omega, 1]$	1	3	0	$\leftarrow 6254^* \rightarrow$			
$[\zeta, \zeta]$	$\overline{0}$	3	1	6	$\overline{2}$	4	5
$[k, k]$	$\overline{0}$	$\overline{1}$	3	6	$\overline{2}$	$\overline{5}$	4
$[j, j]$	$\overline{0}$	1	$\overline{3}$	6	$\overline{2}$	5	$\overline{4}$
$[1, -1]$	0	1	3	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{4}$
$[1, i]$	0	1	3	2	$\overline{6}$	$\overline{4}$	5
$[1, j]$	0	1	3	5	4	$\overline{6}$	$\overline{2}$
$[i, k]$	0	1	3	4	$\overline{5}$	2	$\overline{6}$

$$\omega = \tfrac{-1+i+j+k}{2}$$

$$\zeta = \tfrac{j+k}{\sqrt{2}}$$

They generate a group of structure

$$\pm\frac{1}{2}[O \times \overline{D_8}]$$

since $-1 = [1,-1]$ is present, while i, j, k, ζ generate a $2D_8$ that extends by ω to $2O$, and the "right kernel" is non-cyclic. It is the entire group since it achieves all automorphisms of H^4 and is easily checked to contain all H^4-stabilizers.

Adjoining orthogonal units, we obtain an H^8 which has the same stabilizer since H^4 can be recovered from it as the subring gererated by elements of order 3.

10.5.3 Subring E^4

Up to sign, the units of an E^4 are

$$1,\ \omega,\ \overline{\omega},\ i,\ i' = \omega i,\ i'' = \overline{\omega} i,$$

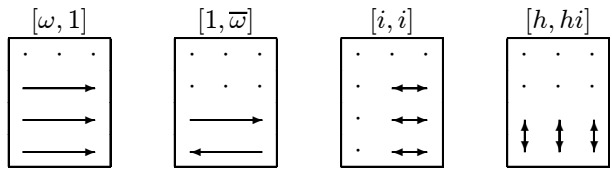
while the orthogonal units are

$$j,\ j' = \omega j,\ j'' = \overline{\omega} j,\ k,\ k' = \omega k,\ k'' = \overline{\omega} k,$$

i, j, k being an odd quaternion triplet and $\omega = \frac{1}{2}(-1 + h\sqrt{-3})$. We display all of these in a rectangular array

$$\begin{array}{|ccc|}\hline 1 & \omega & \overline{\omega} \\ i & i' & i'' \\ j & j' & j'' \\ k & k' & k'' \\ \hline \end{array}$$

We find four automorphisms that act (up to sign) as follows:



and which generate a group[7] of structure

$$+\frac{1}{4}[D_{12} \times \overline{D_{12}}]$$

in the notation of Chapter 4 (because $[1,-1]$ is absent, and the us and vs both generate D_{12}'s that map to D_4 modulo $\langle\omega\rangle$ whose "cyclic coset" $\langle h\rangle$ is interchanged with a noncyclic one $\langle hi\rangle$). That this is the whole stabilizer

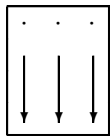
[7] It is interesting to note that this group does not appear in [41], since its elliptic image was omitted from Goursat's original enumeration.

follows since the first map is easily checked to generate the stabilizer of E^4 while the other three generate all achievable automorphisms of E^4.

Adjoining units orthogonal to E^4, we obtain an E^8 whose stabilizer is three times as large, as we see from the example

∞	$\overline{\infty}365$	$\overline{\infty 365}$
1	$\overline{016}5$	$0\overline{1}6\overline{5}$
2	$\overline{025}3$	$0\overline{2}5\overline{3}$
4	$\overline{043}5$	$0\overline{4}3\overline{6}$

, where this automorphism is



.

Appendix: Proof of Theorem 5

We prove the

Theorem 5. *Up to isomorphism, there are precisely four types (G^1, E^2, H^4, O^8) of integer rings generated by odd-order elements, from which all of the octavian unit rings can be obtained by Dickson-Doubling (see Figure 10.3).*

Lemma 2. *Any unit ring can be obtained by Dickson doubling from one that is generated by ωs.*

Proof. Let X be the subring generated by ωs. Then obviously any unit not in X must be an i. But also this i must be orthogonal to every unit u in X (and so to X), since otherwise $\pm ui$ would be an ω not in X. It therefore extends X to its Dickson double, say Y. Replacing X by Y, we can repeat the argument, if necessary, to prove the lemma.

This reduces the theorem to

Theorem 6. *There are just four types of rings generated by ωs, namely G^1, E^2, H^4, O^8.*

Proof. If the ring has at most one generator, it is trivially G^1 or E^2. Since $\mathrm{Aut}(\mathsf{O}^8)$ is doubly-transitive on $\langle\omega\rangle$s, the ring generated by any two "ω"s (that aren't equal or reciprocal) is again of a unique type, H^4. The proof is completed by the easy verification that adjoining any ω outside it to the particular $\mathsf{H}^4 = \langle i_0, i_1, i_3, \omega_{013}\rangle$ yields all of O^8.

Reading O Mod 2

11.1 Why Read Mod 2?

The group Aut(O) of automorphisms of $\mathsf{O} = \mathsf{O}^8$ is nearly simple—in fact, it has a simple subgroup of index 2. The finite simple groups have been classified—which one is this? The answer is best found by reading modulo 2.

One can obtain an interesting ring by reading the octavian integers modulo any prime p (just as when reading the ordinary integers modulo p one obtains an interesting ring that is, in fact, a field). To be precise, one says that two octavian integers are congruent mod p provided that their difference is p times an octavian integer. (So, an "octavian integer mod p" is really a member of the quotient ring $\mathsf{O}/p\mathsf{O}$.)

The finite group $G_2(p)$ (more explicitly written $G_2(\mathbb{F}_p)$) is defined to be the automorphism group of the octonions mod p. Since this topic is peripheral to our book, we shall merely quote the fact that the order of $G_2(p)$ is $p^6(p^2-1)(p^6-1)$. Plainly, any automorphism of O can be read modulo p to yield an element of $G_2(p)$. This gives a map

$$\mathrm{Aut}(\mathsf{O}) \to G_2(p)$$

that is, in fact, an embedding, since only the identity automorphism of O maps to the identity automorphism (mod p). Indeed, for $p = 2$ it is an isomorphism, since by the above formula, $G_2(2)$ has the same order

$$2^6(2^2-1)(2^6-1) = 12096$$

as Aut(O).

So our group is $G_2(2)$. Although $G_2(p)$ is usually simple, the particular case $G_2(2)$ is not–it has a simple subgroup of index 2 that happens to appear elsewhere in the classification—it is the group $U_3(3)$ of "unitary" 3×3 matrices with entries in the field of order 9. We shall use $\mathcal{G}$ for this simple subgroup, so that $G_2(2)$ is $\mathcal{G} \cdot 2$.

Group theorists know that the best way to study a finite simple group is to determine its maximal subgroups. The group $\mathcal{G}$ has (up to conjugacy) four maximal subgroups:

$\mathcal{G}_{\mathsf{G}}$, stabilizing one of the 63 Gaussian subrings G^2
$\mathcal{G}_{\mathsf{H}}$, stabilizing one of the 63 Hurwitzian subrings H^4
$\mathcal{G}_{\mathsf{E}}$, stabilizing one of the 28 Eisenstein subrings E^2
$\mathcal{G}_{\mathsf{K}}$, stabilizing one of the 36 Kleinian subrings K^1

The group $\mathcal{G} \cdot 2$ has, in addition to the four groups $\mathcal{G}_{\mathsf{G}} \cdot 2$, $\mathcal{G}_{\mathsf{H}} \cdot 2$, $\mathcal{G}_{\mathsf{E}} \cdot 2$, $\mathcal{G}_{\mathsf{K}} \cdot 2$ just one further maximal subgroup, namely $\mathcal{G}$ itself. Only three of these have appeared as stabilizers of subrings of the octavian integers, but all four stabilize low-dimensional subrings of the octavians modulo 2.

To get the first three, we can read $\langle i_0 \rangle$, $\langle i_0, i_1, i_3, \omega_{013} \rangle$, $\langle \omega \rangle$ modulo 2. The fourth fixes the ring generated (modulo 2) by a Kleinian integer λ of the form $\frac{1}{2}(-1 + \sqrt{-7})$. It turns out that it also fixes two bases: the "j-frame" $1, j_0, \ldots, j_6$ and the "k-frame" $1, k_0, \ldots, k_6$. Table 11.1 shows the action of all four groups on the subalgebras of all four types.

	Action of			
	$\mathcal{G}_{\mathsf{G}}$	$\mathcal{G}_{\mathsf{H}}$	$\mathcal{G}_{\mathsf{E}}$	$\mathcal{G}_{\mathsf{K}}$
on the 63 G^2s	$1 + 6 + 24 + 32$ G^2 G^{4+} G^{4-} E^4	$3 + 12 + 48$ G^{4+} G^8 H^8	$27 + 36$ H^4 E^4	$14 + 21 + 28$ K^2 K^4 E^4
on the 63 H^4s	$3 + 12 + 48$ G^{4+} G^8 H^8	$1 + 6 + 24 + 32$ G^{4+} G^8 H^8 O^8	$9 + 54$ H^4 H^8	$21 + 42$ K^4 H^8
on the 28 E^2s	$12 + 16$ H^4 E^4	$4 + 24$ H^4 H^8	$1 + 27$ E^2 H^4	28 E^4
on the 36 K^1s (mod 2)	$8 + 12 + 16$ K^2 K^4 E^4	$12 + 24$ K^4 H^8	36 E^4	$1 + 14 + 21$ K^1 K^2 K^4

Table 11.1. Under the group that fixes one type of algebra, the algebras of any given type form orbits as shown. The two given algebras generate a third whose type is indicated below the appropriate number.

11.2 The E_8 Lattice, Mod 2

When we study the lattice of octavian integers mod 2, it will be important to count those of various norms. As described in Chapter 9, the octavian integers form a scaled copy of the E_8 root lattice, and it is known that the number of vectors of any norm $n > 0$ is 240 times the sum of the cubes of the divisors of n.

So there are exactly	240	2160	6720	...
octavian integers of norm	1	2	3	... .

However, all we actually need are the numbers of **short vectors**, by which we mean those of norm at most 2. To make our book self-contained, we count these explicitly from their coordinate shapes:

norm 1 shapes:	$(\pm 1^1, 0^7)$	and	$(\pm \frac{1}{2}^4, 0^4)$				
number:	$2^1.8$	+	$2^4.14$	=	240		

norm 2 shapes:	$(\pm 1^2, 0^7)$	and	$(\pm \frac{1}{2}^4, \pm 1^1, 0^3)$	and	$(\pm \frac{1}{2}^8)$			
number:	$2^2.28$	+	$2^5.14.4$	+	2^8	=	2160.	

Now we consider the congruences modulo 2 between these short vectors.

Lemma 1. *Apart from $v \equiv -v$, the only other congruences (mod 2) between short vectors are between orthogonal ones of norm 2.*

Proof. Suppose $v \equiv w$, with $v \not\equiv \pm w$. Then replacing w by $-w$ if necessary, we can suppose the inner product $[v, w]$ is non-negative, so for the norms we have

$$[v - w] \leq [v] + [w] \leq 4$$

since v, w are short (see Figure 11.1). But $v - w \in 2O^8$ implies $[v - w] \geq 4$, so therefore $[v - w] = 4$, which implies that $[v] = [w] = 2$ with $[v, w] = 0$.

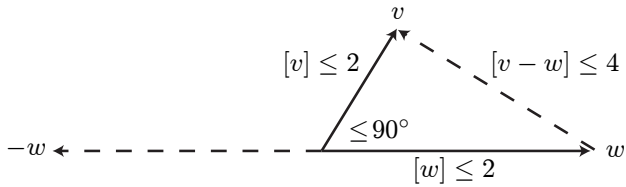


Figure 11.1. If $[v, w] \geq 0$, then $[v - w] \leq 4$.

Since there can be at most eight mutually orthogonal vectors in an 8-dimensional space, it is a corollary that there can be at most sixteen norm 2-vectors in any equivalence class. So, the number of equivalence classes that contain short vectors is at least

$$1 + \frac{240}{2} + \frac{2160}{16} = 1 + 120 + 135 = 256 = 2^8.$$

But since $\mathsf{O}^8/2\mathsf{O}^8$ is an 8-dimensional space over the field of order 2, this is the total number of classes, and we deduce

Theorem 1. *Every mod 2 congruence class contains a short vector. These classes are: one class represented by the* 0 *vector; 120 classes each represented by two vectors* $\pm v$ *of norm 1; and 135 classes each represented by a frame of sixteen vectors* $\pm v_1, \ldots, \pm v_8$ *of norm 2. In the third case,* $v_1, \ldots, v_8$ *are mutually orthogonal, and every norm 2 vector lies in such a frame.*

From now on, we shall call these classes "vectors (mod 2)." Grouped according to their multiplicative structure they are

Norm	Type	Total
0	1 element 0	1
1	1 element ± 1, 63 elements $\pm i$, 56 elements $\pm \omega$	120
2	63 elements $1 + i$, 72 elements λ	135
		$256 = 2^8$

The 16 minimal representatives of a vector of type $1 + i$ are four of the form $\pm 1 \pm i$ and 12 of the form $\pm i' \pm i''$. As an example, for $1 + i_0$ they are

$$\pm 1 \pm i_0, \quad \pm i_1 \pm i_3, \quad \pm i_2 \pm i_6, \quad \pm i_4 \pm i_5.$$

Type λ is one we have not previously seen. Its 16 minimal representatives are all of the form $\frac{1}{2}(\pm 1 \pm \sqrt{-7})$ for various octavian square roots of -7. $G_2(2)$ is transitive on the 72 "λ"s. However, there are only 36 algebras $\langle\lambda\rangle$ (mod 2), since the one generated by a given λ contains a second one, namely $\mu \equiv 1 + \lambda$. The standard case is

$$\lambda = i_{\overline{\infty}0123456} = \frac{-1 + i_0 + \cdots + i_6}{2}$$

and

$$\mu = i_{\infty 0123456} = \frac{1 + i_0 + \cdots + i_6}{2}.$$

The 16 minimal representatives of μ are

$$\pm i_{\infty 0123456}, \quad \pm i_{\infty 01\overline{23456}}, \quad \ldots \text{ (eight such)}.$$

Every vector obtained by adding an ω to an orthogonal i is of type λ, and conversely, every number of type λ can be so expressed (in many ways).

The pair λ, μ determines and is determined by a pair of coordinate frames $1, j_0, \ldots, j_6$ and $1, k_0, \ldots, k_6$. The js and ks are found from the congruences

$$j_n\mu \equiv \mu \equiv \mu k_m \quad \text{and} \quad \lambda j_n \equiv \lambda \equiv k_m\lambda,$$

and conversely, μ is determined from them by the fact that the 28 nonzero values (mod 2) from the 49 products $(1 + j_m)(1 + k_n)$ are congruent to μ.

The two associated frames are interchanged by an element δ that interchanges j_m with k_{-m} and increases the order of the group from 168 to 336. The ks may be regarded as points, and the js lines, of a projective plane as in Figure 11.2. So the new group is the extension by duality of the automorphism group $L_3(2)$ of this plane, which can also be thought of as $PGL_2(7)$. It is the fourth maximal subgroup of $\mathcal{G} \cdot 2$, and we therefore devote the next section to it.

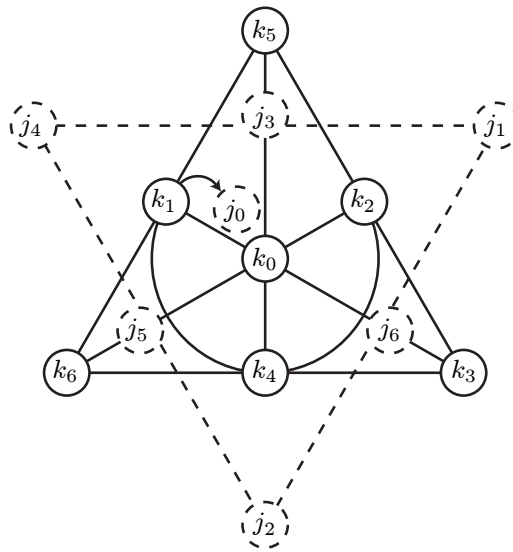


Figure 11.2. Calling the ks points, the js become lines, of an order-2 projective plane, and *vice versa*.

11.3 What Fixes $\langle\lambda\rangle$?

By a (coordinate) **frame**, we mean 16 vectors of the form $\pm 1, \pm v_0, \pm v_1, \ldots, \pm v_6$, where $1, v_0, v_1, \ldots, v_6$ are mutually orthogonal units in O^8. Just as there are even and odd quaternion triplets, there are even and odd frames. An **even frame** is one that contains an even quaternion triplet; in an **odd frame**, all the quaternion triplets are odd.

Lemma 2. *Any two oddly orthogonal "i"s belong to just three frames, of which one is even and the other two odd.*

Proof. We can take the two "i"s to be i_3 and i_5. The only "i"s orthogonal to these are (in the notation of Chapter 10)

$$\pm i_6,\ \pm i_0,\ \pm i_1,\ \pm i_2,\ \pm i_4,\ i^*_{0124},$$

and the only frames that can be selected from the vectors we have mentioned are $\pm 1, \pm i_3, \pm i_5, \pm i_6$ together with

$$\underset{\text{an } i\textbf{-frame}}{\pm i_0, \pm i_1, \pm i_2, \pm i_4} \quad \text{or} \quad \underset{\text{a } j\textbf{-frame}}{i'_{0124}} \quad \text{or} \quad \underset{\text{a } k\textbf{-frame}}{i''_{0124}}.$$

Since $i_0,\ i_1,\ i_3$ is an even triple, we see that the i-frame is even. The calculations that follow show that the j-frame is odd, as must be the k-frame, since j-frames and k-frames are interchanged by the symmetry that negates $i_0,\ i_3,\ i_5,\ i_6$.

11.3.1 The Calculations

The symmetries of the j-frame are easiest seen by expressing all of the octonion units in it. We define

$$j_3 = -i_6,\ j_6 = -j_5,\ i_5 = -i_3,\ j_0 = i_{\overline{0}124},\ j_1 = i_{0\overline{1}24},\ j_2 = i_{01\overline{2}4},\ j_4 = i_{012\overline{4}}.$$

This transformation is easily inverted: we have

$$i_3 = -j_5,\ i_6 = -j_3,\ i_5 = -j_6,\ i_0 = j_{\overline{0}124},\ i_1 = j_{0\overline{1}24},\ i_2 = j_{01\overline{2}4},\ i_4 = j_{012\overline{4}}.$$

(It can be helpful to note that $j_0 + j_1 = i_2 + i_4$, and $j_0 - j_1 = i_1 - i_0$, etc.)

Then we easily find

$$j_0j_1 = j_{23\overline{46}},\ \ j_1j_2 = j_{34\overline{50}},\ \ \ldots,\ \ j_6j_0 = j_{12\overline{35}},$$

relations which are, remarkably, invariant under the maps

$$\alpha : (01\ldots6) \quad \text{and} \quad \beta : (124)(365).$$

Now, we can readily complete the j multiplication table, using the invariance under β and the facts that $j_n^2 = -1$ and $j_nj_m = \overline{j_mj_n}$:

1	j_0	j_1	j_2	j_3	j_4	j_5	j_6
j_0	-1	$j_{2\overline{4}63}$	$j_{4\overline{1}56}$	$j_{\overline{41}5\overline{6}}$	$j_{1\overline{2}35}$	$j_{\overline{24}6\overline{3}}$	$j_{\overline{12}3\overline{5}}$
j_1	$j_{\overline{23}4\overline{6}}$	-1	$j_{3\overline{5}04}$	$j_{5\overline{2}60}$	$j_{\overline{52}6\overline{0}}$	$j_{2\overline{3}46}$	$j_{\overline{35}0\overline{4}}$
j_2	$j_{\overline{46}1\overline{5}}$	$j_{\overline{34}5\overline{0}}$	-1	$j_{4\overline{6}15}$	$j_{6\overline{3}01}$	$j_{\overline{63}0\overline{1}}$	$j_{3\overline{4}50}$
j_3	$j_{4\overline{5}61}$	$j_{\overline{50}2\overline{6}}$	$j_{\overline{45}6\overline{1}}$	-1	$j_{5\overline{0}26}$	$j_{0\overline{4}12}$	$j_{\overline{04}1\overline{2}}$
j_4	$j_{\overline{15}2\overline{3}}$	$j_{5\overline{6}02}$	$j_{\overline{61}3\overline{0}}$	$j_{\overline{56}0\overline{2}}$	-1	$j_{6\overline{1}30}$	$j_{1\overline{5}23}$
j_5	$j_{2\overline{6}34}$	$j_{\overline{26}3\overline{4}}$	$j_{6\overline{0}13}$	$j_{\overline{02}4\overline{1}}$	$j_{\overline{60}1\overline{3}}$	-1	$j_{0\overline{2}41}$
j_6	$j_{1\overline{3}52}$	$j_{3\overline{0}45}$	$j_{\overline{30}4\overline{5}}$	$j_{0\overline{1}24}$	$j_{\overline{13}5\overline{2}}$	$j_{\overline{01}2\overline{4}}$	-1

It turns out that any symmetry that preserves the j-frame also preserves an associated k-frame. Namely, we define

$$\begin{aligned}
k_0 &= j_{0\overline{124}} = -i_0\\
k_1 &= j_{1\overline{235}} = i_{\overline{1}263}\\
k_2 &= j_{2\overline{346}} = i_{\overline{2}456}\\
k_3 &= j_{3\overline{450}} = i_{\overline{12}63}\\
k_4 &= j_{4\overline{561}} = i_{\overline{4}135}\\
k_5 &= j_{5\overline{602}} = i_{\overline{41}35}\\
k_6 &= j_{6\overline{013}} = i_{\overline{245}6},
\end{aligned}$$

noticing that this is invariant under both α and β. Then we compute

$$k_0k_1 = -i_0i_{1\overline{2}63} = i_{3\overline{6}21} = j_{04\overline{5}3} \quad \text{and} \quad j_6k_0 = i_{\overline{5}}i_{\overline{0}} = i_4 = j_{012\overline{4}},$$

which together with the α and β symmetries, give the Tables 11.2 and 11.3.

It turns out that the odd frames can be divided into two classes, the **j-frames** and **k-frames**. An automorphism either fixes each class as a whole (when we call it "even") or interchanges them (when we call it "odd").

The symmetries that fix a given j-frame form a copy of the simple group of order 168 known as $L_3(2)$ or $L_2(7)$, and they also fix a particular k-frame, called the "associated k-frame." For the standard pair of associated frames this is generated by α, β, γ acting as follows:

$$\left.\begin{array}{ll}\alpha & : (01\ldots6)\\ \beta & : (124)(365)\end{array}\right\} \quad \text{on both } j\text{- and } k\text{-subscripts}$$

$$\gamma : \begin{array}{ll}(56)(14)\,\epsilon_{0124} & \text{on } j\text{-subscripts}\\ (12)(36)\,\epsilon_{0365} & \text{on } k\text{-subscripts.}\end{array}$$

1	j_0	j_1	j_2	j_3	j_4	j_5	j_6
j_0	-1	i_{52}	i_{34}	$-i_{24}$	i_{61}	$-i_{12}$	$-i_{41}$
j_1	$-i_{52}$	-1	i_{63}	i_{45}	$-i_{35}$	i_{02}	$-i_{23}$
j_2	$-i_{34}$	$-i_{63}$	-1	i_{04}	i_{56}	$-i_{46}$	i_{13}
j_3	i_{24}	$-i_{45}$	$-i_{04}$	-1	i_{15}	i_{60}	$-i_{50}$
j_4	$-i_{61}$	i_{35}	$-i_{56}$	$-i_{15}$	-1	i_{26}	i_{01}
j_5	i_{12}	$-i_{02}$	i_{46}	$-i_{60}$	$-i_{26}$	-1	i_{30}
j_6	i_{41}	i_{23}	$-i_{13}$	i_{50}	$-i_{01}$	$-i_{30}$	-1

1	k_0	k_1	k_2	k_3	k_4	k_5	k_6
k_0	-1	i_{63}	i_{56}	$-i_{61}$	i_{35}	$-i_{34}$	$-i_{52}$
k_1	$-i_{63}$	-1	i_{04}	i_{60}	$-i_{02}$	i_{46}	$-i_{45}$
k_2	$-i_{56}$	$-i_{04}$	-1	i_{15}	i_{01}	$-i_{13}$	i_{50}
k_3	i_{61}	$-i_{60}$	$-i_{15}$	-1	i_{26}	i_{12}	$-i_{24}$
k_4	$-i_{35}$	i_{02}	$-i_{01}$	$-i_{26}$	-1	i_{30}	i_{23}
k_5	i_{34}	$-i_{46}$	i_{13}	$-i_{12}$	$-i_{30}$	-1	i_{41}
k_6	i_{52}	i_{45}	$-i_{50}$	i_{24}	$-i_{23}$	$-i_{41}$	-1

1	k_0	k_1	k_2	k_3	k_4	k_5	k_6
j_0	ω_{00}	i_{01}	i_{02}	$-\omega_{03}$	i_{04}	$-\omega_{05}$	$-\omega_{06}$
j_1	$-\omega_{10}$	ω_{11}	i_{12}	i_{13}	$-\omega_{14}$	i_{15}	$-\omega_{16}$
j_2	$-\omega_{20}$	$-\omega_{21}$	ω_{22}	i_{23}	i_{24}	$-\omega_{25}$	i_{26}
j_3	i_{30}	$-\omega_{31}$	$-\omega_{32}$	ω_{33}	i_{34}	i_{35}	$-\omega_{36}$
j_4	$-\omega_{40}$	i_{41}	$-\omega_{42}$	$-\omega_{43}$	ω_{44}	i_{45}	i_{46}
j_5	i_{50}	$-\omega_{51}$	i_{52}	$-\omega_{53}$	$-\omega_{54}$	ω_{55}	i_{56}
j_6	i_{60}	i_{61}	$-\omega_{62}$	i_{63}	$-\omega_{64}$	$-\omega_{65}$	ω_{66}

Table 11.2. Multiplication tables for the js and ks. For definitions, see Table 11.3.

The action of the group $\mathcal{G}_{\mathsf{K}} \cong L_3(2)\cdot 2$ on various things is easy to see in Table 11.3, which displays the 240 units with respect to the j-frame (using $j_{abcd} = \frac{1}{2}(j_a + j_b + j_c + j_d)$, etc.).

11.4 The Remaining Subrings Modulo 2

This section is devoted to a proof that the only subrings modulo 2 of O^8 are the unit-rings, taken modulo 2, and four others:

$$\mathsf{K}^1 = \langle\lambda\rangle \quad \mathsf{K}^2 = \langle\lambda, i_0\rangle \quad \mathsf{K}^4 = \langle\lambda, i_0, i_1, i_3\rangle \quad \mathsf{K}^8 = \langle\lambda, i_0, \ldots, i_6\rangle,$$

where $\lambda = \frac{-1+i_0+\ldots+i_6}{2}$.

$abcd$	$j_{\overline{a}bcd}$	$j_{a\overline{b}cd}$	$j_{ab\overline{c}d}$	$j_{abc\overline{d}}$	j_{abcd}	$j_{\overline{a}\overline{b}cd}$	$j_{\overline{a}b\overline{c}d}$	$j_{\overline{a}bc\overline{d}}$
0124	$-k_0$	i_{50}	i_{30}	i_{60}	h_{00}	$-h_{10}$	$-h_{21}$	$-h_{40}$
1235	$-k_1$	i_{61}	i_{41}	i_{01}	h_{11}	$-h_{21}$	$-h_{32}$	$-h_{51}$
2346	$-k_2$	i_{02}	i_{52}	i_{12}	h_{22}	$-h_{32}$	$-h_{43}$	$-h_{62}$
3450	$-k_3$	i_{13}	i_{63}	i_{23}	h_{33}	$-h_{43}$	$-h_{54}$	$-h_{03}$
4561	$-k_4$	i_{24}	i_{04}	i_{34}	h_{44}	$-h_{54}$	$-h_{65}$	$-h_{14}$
5602	$-k_5$	i_{35}	i_{15}	i_{45}	h_{55}	$-h_{65}$	$-h_{06}$	$-h_{25}$
6013	$-k_6$	i_{46}	i_{26}	i_{56}	h_{66}	$-h_{06}$	$-h_{10}$	$-h_{36}$
$\infty653$	ω_{00}	$-\omega_{20}$	$-\omega_{40}$	$-\omega_{10}$	$-\overline{\omega}_{00}$	$\overline{\omega}_{20}$	$\overline{\omega}_{40}$	$\overline{\omega}_{10}$
$\infty064$	ω_{11}	$-\omega_{31}$	$-\omega_{51}$	$-\omega_{21}$	$-\overline{\omega}_{11}$	$\overline{\omega}_{31}$	$\overline{\omega}_{51}$	$\overline{\omega}_{21}$
$\infty105$	ω_{22}	$-\omega_{42}$	$-\omega_{62}$	$-\omega_{32}$	$-\overline{\omega}_{22}$	$\overline{\omega}_{42}$	$\overline{\omega}_{62}$	$\overline{\omega}_{32}$
$\infty216$	ω_{33}	$-\omega_{53}$	$-\omega_{03}$	$-\omega_{43}$	$-\overline{\omega}_{33}$	$\overline{\omega}_{53}$	$\overline{\omega}_{03}$	$\overline{\omega}_{43}$
$\infty320$	ω_{44}	$-\omega_{64}$	$-\omega_{14}$	$-\omega_{54}$	$-\overline{\omega}_{44}$	$\overline{\omega}_{64}$	$\overline{\omega}_{14}$	$\overline{\omega}_{54}$
$\infty431$	ω_{55}	$-\omega_{05}$	$-\omega_{25}$	$-\omega_{65}$	$-\overline{\omega}_{55}$	$\overline{\omega}_{05}$	$\overline{\omega}_{25}$	$\overline{\omega}_{65}$
$\infty542$	ω_{66}	$-\omega_{16}$	$-\omega_{36}$	$-\omega_{06}$	$-\overline{\omega}_{66}$	$\overline{\omega}_{16}$	$\overline{\omega}_{36}$	$\overline{\omega}_{06}$

$h_{mm}=j_m+k_m$	$m=m$	$\omega_{mn}=-j_mk_n$	$m>n$
$h_{mn}=j_m-k_n$	$m>n$	$\omega_{mn}=\pm j_mk_n$	$m\geq n$
$i_{mn}=j_mk_n$	$m<n$	$h_{mn}=j_m\pm k_n$	$m\geq n$
$\omega_{mm}=j_mk_m$	$m=m$	$i_{mn}=j_mk_n$	$m<n$

Table 11.3. As in Table 11.2, we write $j_mk_n=i_{mn}$ when it is an "i"; otherwise, $j_mk_m=\omega_{mm}$, $j_m+k_m=h_{mm}$, $j_mk_n=-\omega_{mn}$, $j_m-k_n=h_{mn}$. The notation is chosen to be invariant (modulo 2) under $L_3(2)$.

Lemma 3. *The ring $\langle\lambda_1,\lambda_2\rangle$ generated by two λs (with $\langle\lambda_1\rangle\neq\langle\lambda_2\rangle$) is also generated by λ_1 and some i.*

Proof. We can take λ_1 to be $(+\frac{1}{2}^8)$ and λ_2 to have coordinates

$$(\pm\frac{1}{2}^8)\ \text{ or }\ (\pm\frac{1}{2}^4,\pm1,0^3).$$

In the first case, the value is unaffected modulo 2 by changing signs on any quad, which can be used to reduce the number of $-$ signs to at most two, and if exactly two, to put one of them on 1, so that $\lambda_1-\lambda_2$ has the form i or $i+1$. For similar reasons we can suppose, in the second case, that there is at most one "$-$" sign, on a $\frac{1}{2}$, so that $\lambda_1-\lambda_2$ has coordinates

$$(0^4,\pm\frac{1}{2}^4)\ \text{ or }\ (0^3,1,\pm\frac{1}{2}^4)$$

(the coefficient of 1 being 0 or 1). The former is an i, and the latter either a $1+i$ or an $i+i'$ (which is congruent to a $1+i$ modulo 2).

Lemma 4. *The ring generated by a λ and an ω is a unit-ring.*

Proof. We can take

$$\lambda = (\pm\frac{1}{2}^8) \text{ and } \omega = (\pm\frac{1}{2}^4 0^4)$$

and by choosing representatives of λ can control the signs so that $\lambda - \omega$ takes one of the forms

$$(0^4, \pm\frac{1}{2}^4) \text{ or } (0^3, \pm 1, \pm\frac{1}{2}^4),$$

which is either an i or a $1+i$. Then $\langle\lambda, \omega\rangle = \langle\omega, i\rangle$ for this i.

Combining the two lemmas, we obtain

Theorem 2. *Modulo 2, any ring not generated by units is one of the four types* K^1, K^2, K^4, K^8.

Proof. Modulo 2, any non-unit is congruent to a λ or a $1+i$, and so we may suppose all non-unit generators are λs, and then by Lemma 1 that there is only one of them, and by Lemma 2, that there is no "ω." The part of the ring generated by units therefore consists of 1 and some mutually orthogonal "i"s.

Without loss of generality, we can now suppose that one of our generators is the above λ. From the top right-hand entry of Table 11.1, we see that the stabilizer of this λ has three orbits on the "i"s, two of which lead to types K^2 and K^4, while the third can be neglected since it leads to E^4, which contains an ω. So, any remaining ring can be chosen to contain this λ and $1, i_0, i_1, i_3$ together with four "i"s orthogonal to these, which must be either i_2, i_4, i_5, i_6, which leads to K^8, or i'_{2645}, or i''_{2645}, which are equivalent under symmetries.

The Octonion Projective Plane $\mathbb{O}P^2$

This book has been devoted to an internal study of the quaternions and octonions. Our main aim has been to give simple and self-contained presentations of their theory, their most natural arithmetics, and their applications to the geometry of the spaces that contain them. For their many applications to other parts of mathematics and physics, we refer to the works in the bibliography, hoping our book will be of some use in reading them.

In this final chapter, we briefly describe some "external" applications of the octonions.

12.1 The Exceptional Lie Groups and Freudenthal's "Magic Square"

The compact semisimple Lie (that is, continuous) groups over the real and complex numbers have been famously classified: As well as the infinite families (A_n, B_n, C_n, D_n in the Cartan notation) that comprise the families of unitary, orthogonal, and symplectic groups, there are five "exceptional" groups G_2, F_4, E_6, E_7, E_8. It has been realized that these are intimately connected with the octonions—for instance, we have seen that G_2 is their automorphism group.

When Jordan, von Neumann, and Wigner classified "Jordan algebras"[1]

[1] These are defined by the conditions $a \circ b = b \circ a$ and $a \circ (b \circ a^2) = (a \circ b) \circ a^2$, which are satisfied by matrices over an associative ring if $A \circ B$ means $\frac{1}{2}(AB + BA)$. The exceptional one is the only case that cannot be obtained from an associative ring.

in 1934, they found an "exceptional" one consisting of 3×3 "Hermitian" matrices over the octonions, whose automorphism group is F_4.

In the 1950s, Freudenthal found that four particular "geometries" could all be defined over $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$: the geometries of the elliptic and projective planes, and 5-dimensional symplectic geometry, which were already known, and his new "metasymplectic" geometry. The automorphisms of the four geometries over the four rings form his celebrated "Magic Square" (see [17] and [18]):

	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$	$\mathbb{O}$
elliptic plane	B_1	A_2	C_3	F_4
projective plane	A_2	$A_2 + A_2$	A_5	E_6
5-dimensional symplectic geometry	C_3	A_5	D_6	E_7
metasymplectic geometry	F_4	E_6	E_7	E_8

J. Tits collaborated with Freudenthal in investigating the properties of these geometries.

12.2 The Octonion Projective Plane

The usual definition of a **projective n-space** over a field is that its points are the 1-spaces of an $(n+1)$-dimensional vector space over the field, so can be coordinatized by non-zero $(n+1)$-tuples $(x_0, x_1, \ldots, x_n)$ with the understanding that $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ represents the same point for each $\lambda \neq 0$. Its k-spaces are the $(k+1)$-dimensional vector subspaces under the same identification, so that in particular, its typical hyperplane consists of all points $(x_0, x_1, \ldots, x_n)$ that satisfy some linear equation in the x_i.

In particular, the points of the 2-dimensional complex projective space are coordinatized by non-zero triples (x_0, x_1, x_2) of complex numbers with the understanding that $(\lambda x_0, \lambda x_1, \lambda x_2) = (x_0, x_1, x_2)$ for $\lambda \neq 0$ and the lines specified by linear equations in x_0, x_1, x_2. If the 3-dimensional complex vector space is given an inner product defined by the usual Hermitian form $\overline{x_0}x_0 + \overline{x_1}x_1 + \overline{x_2}x_2$, we can describe the typical line as $x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2} = 0$, the set of all (x_0, x_1, x_2) orthogonal to the particular point (y_0, y_1, y_2).

All of this works up to the quaternions, but not for the octonions. However, there is an alternative, originally suggested by some physical ideas, that does succeed in defining a 2-dimensional projective space, or **projective plane**, over $\mathbb{O}$.

Let us represent a point p of the complex projective plane by the projection operator onto the corresponding 1-space of $\mathbb{C}^3$. For $p = (1, 0, 0)$ this has matrix

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

In general, its matrix will be a **Hermitian** ($e_{ij} = \overline{e_{ji}}$) **idempotent** ($e^2 = e$) **of unit trace** ($e_{00} + e_{11} + e_{22} = 1$). Also, two 1-spaces of $\mathbb{C}^3$ are orthogonal if and only if their projection operators e and f satisfy $e \circ f = 0$, where $e \circ f$ is the **Jordan product** $\frac{1}{2}(ef + fe)$. We can define the line f of the complex projective plane to consist of all the points e for which $e \circ f = 0$.

In fact, this definition generalizes to give projective spaces of all dimensions over $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, but over the octonions $\mathbb{O}$ it produces a projective plane but no higher projective space, because it requires the Jordan algebra property. We therefore define the **octonion projective plane** to have points and lines specified by 3×3 Hermitian idempotents of trace 1 over the octonions, with point e lying on the line f just when $e \circ f = 0$.

This definition is mathematically the most satisfying one, since it makes it immediately clear that the plane has at least the symmetries of the exceptional Jordan algebra (which constitute the Lie group F_4). In fact, it is also invariant under further automorphisms that extend F_4 to the larger Lie group E_6. However, it is cumbrous to work with, so the next section will establish its equivalence to a "coordinate definition" (due to Porteous [35] and Aslaksen [4]) that is less symmetrical but more familiar and more convenient. Our discussion of its equivalence to Freudenthal's definition follows the elegant paper of Allcock [2].

12.3 Coordinates for $\mathbb{O}P^2$

Our first lemma enables us to replace matrices by vectors of octonions.

Lemma 1. *Any 3×3 Hermitian idempotent e of trace 1 can be written as $e_{x_0,x_1,x_2} = (\overline{x_i} x_j)$ for a norm 1 vector (x_0, x_1, x_2) with x_0 real.*

Proof. For

$$e = \begin{pmatrix} a & \gamma & \overline{\beta} \\ \overline{\gamma} & b & \alpha \\ \beta & \overline{\alpha} & c \end{pmatrix} \quad \text{and} \quad a + b + c = 1,$$

with $a, b, c \in \mathbb{R}$ and $\alpha, \beta, \gamma \in \mathbb{O}$, the condition $e^2 = e$ is equivalent to the six equations

$$\begin{array}{ll} a = a^2 + [\beta] + [\gamma] & \overline{\gamma}\,\overline{\beta} = (1-b-c)\alpha = a\alpha \\ b = b^2 + [\gamma] + [\alpha] & \overline{\alpha}\,\overline{\gamma} = (1-c-a)\beta = b\beta \\ c = c^2 + [\alpha] + [\beta] & \overline{\beta}\,\overline{\alpha} = (1-a-b)\gamma = c\gamma. \end{array}$$

The three equations on the left imply that $a, b, c \geq 0$, while the three equations on the right imply that

$$[\beta][\gamma] = a^2[\alpha] \qquad [\gamma][\alpha] = b^2[\beta] \qquad [\alpha][\beta] = c^2[\gamma],$$

and so $[\gamma] = ab$ and $[\beta] = ac$ if $\alpha\beta\gamma \neq 0$. It is then easy to verify the lemma upon setting

$$\begin{array}{ll} (x_0, x_1, x_2) = (\sqrt{a}, \frac{\gamma}{\sqrt{a}}, \frac{\overline{\beta}}{\sqrt{a}}) & \text{if } a \neq 0 \\ (x_0, x_1, x_2) = (0, \sqrt{b}, \frac{\alpha}{\sqrt{b}}) & \text{if } a = 0, b \neq 0 \\ (x_0, x_1, x_2) = (0, 0, 1) & \text{otherwise.} \end{array}$$

Of course, we could equally demand that either x_1 or x_2 be real. The conversion is easy—for example:

Lemma 2. *If $(x_0, x_1, x_2) = (r_0, r_1u_1, r_2u_2)$ with $r_i \in \mathbb{R}$ and u_i units, then $e_{x_0,x_1,x_2} = e_{\overline{u_1}x_0, r_1, \overline{u_1}x_2}$.*

Proof. The "inner product" matrices

	r_0	r_1u_1	r_2u_2
r_0	r_0^2	$r_0r_1u_1$	$r_0r_2u_2$
$r_1\overline{u_1}$	$r_0r_1\overline{u_1}$	r_1^2	$r_1r_2\overline{u_1}u_2$
$r_2\overline{u_2}$	$r_0r_2\overline{u_2}$	$r_1r_2\overline{u_2}u_1$	r_2^2

and

	$r_0\overline{u_1}$	r_1	$r_2\overline{u_1}u_2$
$r_0\overline{u_1}$	r_0^2	$r_0r_1u_1$	$r_0r_2u_2$
r_1	$r_0r_1\overline{u_1}$	r_1^2	$r_1r_2\overline{u_1}u_2$
$r_2\overline{u_2}u_1$	$r_0r_2\overline{u_2}$	$r_1r_2\overline{u_2}u_1$	r_2^2

are identical.

Now we show that the coordinate condition for orthogonality works for a point and line that have real coordinates in different places.

Lemma 3. *If x_0 and y_1 are real, then for $e = e_{x_0,x_1,x_2}$ and $f = e_{y_0,y_1,y_2}$ we have*

$$x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2} = 0 \quad \Leftrightarrow \quad e \circ f = 0.$$

Proof. Given that $x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2} = 0$, we see for instance that

$$(ef)_{02} = \overline{x_0}((x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2})y_2) = 0$$

since it is the sum of

$$\overline{x_0}x_0.\overline{y_0}y_2 \qquad \overline{x_0}x_1.\overline{y_1}y_2 \qquad \overline{x_0}x_2.\overline{y_2}y_2,$$

which can be replaced by

$$\overline{x_0}(x_0\overline{y_0}.y_2) \qquad \overline{x_0}(x_1\overline{y_1}.y_2) \qquad \overline{x_0}(x_2\overline{y_2}.y_2),$$

since

x_0 is real	y_1 is real	$\overline{y_2}y_2$ is real and diassociativity.

There is just enough associativity to show in a similar way that all other $(ef)_{ij}$ and $(fe)_{ij}$ vanish, except that for the 01 and 10 entries we must first renormalize (x_0, x_1, x_2) to (x_0', x_1', x_2') with x_2' real.

For the converse, we show in this way that the sum of the diagonal entries of $e \circ f$ (given to be 0) is the sum of three real numbers:

$$\textstyle\sum_i[\overline{x_i}((x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2})y_i), 1]$$
$$= \textstyle\sum_i[x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2}, x_i\overline{y_i}] = [x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2}],$$

and so that indeed $x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2}$ vanishes.

Our final lemma justifies the term "projective plane," since it shows that any two distinct lines pass through just one point, and that any two distinct points lie on just one line.

Lemma 4. *If (y_0, y_1, y_2) and (z_0, z_1, z_2) are non-proportional unit vectors with y_1 and z_1 real, then the equations*

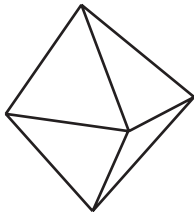
$$x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2} = 0 \quad \text{and} \quad x_0\overline{z_0} + x_1\overline{z_1} + x_2\overline{z_2} = 0$$

and the condition that x_0 be real determine (x_0, x_1, x_2) uniquely up to projectivity.

Proof. The ratio of x_0 to x_2 is found by subtracting

$$(x_0\overline{y_0} + x_1\overline{y_1} + x_2\overline{y_2})\overline{z_1} \quad \text{from} \quad (x_0\overline{z_0} + x_1\overline{z_1} + x_2\overline{z_2})\overline{y_1},$$

and then x_1 can be determined from either equation.



Bibliography

[1] A. A. Albert. Quadratic forms permitting composition. *Annals of Mathematics*, 43:161–177, 1942.

[2] D. Allcock. Identifying models of the octave projective plane. *Geometriae Dedicata*, 65:215–217, 1997.

[3] S. L. Altmann. *Rotations, Quaternions, and Double Groups*. Clarendon Press, Oxford, 1986.

[4] H. Aslaksen. Restricted homogeneous coordinates for the Cayley projective plane. *Geometriae Dedicata*, 40:245–250, 1991.

[5] J. Baez. The octonions. *Bulletin of the American Mathematical Society*, 39:145–205, 2002.

[6] H. F. Blichfeldt. The minimum values of positive quadratic forms in six, seven, and eight variables. *Mathematische Zeitschrift*, 39:1–15, 1935.

[7] H. Brown, R. Bülow, J. Neubüser, H. Wondratschek, and H. Zassenhaus. *Crystallographic groups of four-dimensional space*. John Wiley and Sons, New York, 1978.

[8] R. H. Bruck and E. Kleinfeld. The structure of alternative division rings. *Proceedings of the American Mathematical Society*, 2:878–890, 1951.

[9] A. Cayley. On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions. *Philosophical Magazine*, 26:208–211, 1845.

[10] A. Cayley. On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions (appendix only). In *The Collected Mathematical Papers*, page 127. Johnson Reprint Co., New York, 1963.

[11] H. S. M. Coxeter. Integral Cayley numbers. *Duke Math Journal*, 13:561–578, 1946.

[12] M. J. Crowe. *A History of Vector Analysis*. University of Notre Dame Press, Notre Dame, 1967.

[13] C. W. Curtis. The four and eight square problem and division algebras. In A. Albert, editor, *Studies in Modern Algebra*, pages 100–125. Prentice-Hall, New Jersey, 1963.

[14] L. E. Dickson. On quaternions and their generalization and the history of the eight square theorem. *Annals of Mathematics*, 20:155–171 and 297, 1919.

[15] L. E. Dickson. *Algebras and Their Arithmetics*. University of Chicago Press, 1923.

[16] C. J. Feaux. Divisor matrices in the Cayley ring. *Journal of Number Theory*, 5:502–523, 1973.

[17] H. Freudenthal. Lie groups in the foundations of geometry. *Advances in Mathematics*, 1:145–190, 1964.

[18] H. Freudenthal. Oktaven, Ausnahmegruppen und Oktavengeometrie. *Geometriae Dedicata*, 19:7–63, 1985.

[19] T. Gosset. On the regular and semi-regular figures in space of n dimensions. *Messenger Math.*, 29:43–48, 1900.

[20] M. E. Goursat. Sur les substitutions orthogonales et les divisions régulières de l'espace. *Annales Scientifiques de L'École Normale Supérieure*, 6:9–102, 1889.

[21] R. P. Graves. *Life of Sir William Rowan Hamilton*. Arno Press, New York, 1975.

[22] R. Guy. Catwalks, sandsteps, and Pascal pyramids. *Journal of Integer Sequences*, 3, 2000. Article 00.1.6.

[23] W. R. Hamilton. *The Mathematical Papers of William Rowan Hamilton, Appendix 3*, volume 3. Cambridge University Press, Cambridge, 1967.

[24] T. L. Hankins. *Sir William Rowan Hamilton*. Johns Hopkins University Press, Baltimore, 1980.

[25] A. C. Hurley. Finite rotation groups and crystal classes in four dimensions. *Proceedings of the Cambridge Philosophical Society*, pages 650–661, 1951.

[26] A. Hurwitz. Über die Komposition der quadratische Formen von beliebig vielen Variabeln. *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, pages 309–316, 1898.

[27] I. Kaplansky. Infinite-dimensional quadratic forms admitting composition. *Proceedings of the American Mathematical Society*, 4:956–960, 1953.

[28] A. Korkine and G. Zolotareff. Sur les formes quadratique positives. *Mathematische Annalen*, 11:242–292, 1877.

[29] J. B. Kuipers. *Quaternions and Rotation Sequences.* Princeton University Press, 2002.

[30] P. J. C. Lamont. Ideals in Cayley's algebra. *Indagationes Mathematicae*, 25:394–400, 1963.

[31] M. Liebeck. The classification of finite simple Moufang loops. *Mathematical Proceedings of the Cambridge Philosophical Society*, 102:33–47, 1987.

[32] K. Mahler. On ideals in the Cayley-Dickson algebra. *Proceedings of the Royal Irish Academy*, 48:123–133, 1942.

[33] R. Moufang. Alternativkörper und der Satz vom vollständigen Vierseit (D_9). *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 9:207–222, 1933.

[34] A. Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. *Inventiones Mathematicae*, 4:229–237, 1967.

[35] I. Porteous. *Topological Geometry.* Cambridge University Press, 1981.

[36] R. A. Rankin. A certain class of multiplicative functions. *Duke Mathematical Journal*, 13:281–306, 1946.

[37] H. P. Rehm. Prime factorization of integral Cayley octaves. *Annales de la Faculté des Sciences de Toulouse*, 2:271–289, 1993.

[38] O. Rodrigues. Des lois géométriques qui régissent les déplacements d'un système solide dans l'espace, et de la variation des coordonnées provenant de ces déplacements considérés indépendamment des causes qui peuvent les produire. *Journal de Mathématiques Pures et Appliquées*, 5:380–440, 1840.

[39] H. J. S. Smith. On the orders and genera of quadratic forms containing more than three indeterminates. *Proceedings of the Royal Society*, 16:197–208, 1867.

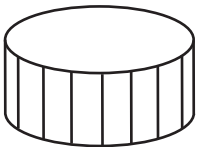
[40] W. Threlfall and H. Seifert. Topologische Untersuchung der Diskontinuitätsbereiche endlicher Bewegungsgruppen des dreidimensionalen sphärischen Raumes. *Mathematische Annalen*, 104:1–70, 1931.

[41] P. Du Val. *Homographies, Quaternions, and Rotations.* Oxford University Press, Oxford, 1964.

[42] F. van der Blij. History of the octaves. *Simon Stevin*, pages 106–125, 1961.

[43] F. van der Blij and T. A. Springer. The arithmetics of octaves and of the group G_2. *Indagationes Mathematicae*, 21:406–418, 1959.

[44] M. Zorn. The automorphisms of Cayley's non-associative algebra. *Proceedings of the National Academy of Sciences*, 21:355–358, 1935.



Index