Garret Sobczyk

New Foundations in Mathematics

The Geometric Concept of Number

Birkhäuser

New Foundations in Mathematics

Garret Sobczyk

New Foundations in Mathematics

The Geometric Concept of Number

Birkhäuser

Garret Sobczyk
Departamento de Física y Matemáticas
Universidad de Las Américas
Puebla, Mexico

ISBN 978-0-8176-8384-9 ISBN 978-0-8176-8385-6 (eBook)
DOI 10.1007/978-0-8176-8385-6
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2012948769

Mathematics Subject Classification (2010): 11A05, 15A16, 15A18, 15A21, 15A63, 15A63, 15A66, 15A69, 15A75, 17B45, 22E60, 51N10, 51N15, 53A04, 53A05, 53A30, 58A05, 65D05, 83A05, 20B30

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.birkhauser-science.com)

I dedicate this book to those who search for truth and beauty no matter how treacherous and narrow that path may be.

Preface

This book provides an introduction to geometric algebra and its application to diverse areas of mathematics. It maintains the spirit of its predecessor, *Clifford Algebra to Geometric Calculus: A Unified Language for Mathematics and Physics*, and as such it has many unique features not seen in any other undergraduate textbook. It provides many innovative ways of looking at geometrical ideas and topics for student research and thesis projects.

The material has been developed over the many years that the author has taught undergraduate courses at the Universidad de Las Américas-Puebla, Mexico, in linear algebra, vector calculus, differential geometry, numerical analysis, modern algebra, and number theory. Whereas this book cannot be considered a textbook for all of these different subjects, there is a common theme they all share: they can all be efficiently formulated using the unified geometric number system advocated here. Geometric algebra, which has undergone extensive development in the second half of the twentieth Century, has its origins in the seminal works of Grassmann, Hamilton, and Clifford in the nineteenth century.

The book begins with the introduction of the spectral basis in modular number systems and in modular polynomials. This often overlooked concept provides insight into and greatly simplifies the proofs of many basic theorems in number theory and the corresponding closely related structure theorems of a linear operator. Since geometric numbers obey exactly the same algebraic rules as square matrices of real numbers, the languages are completely compatible and structure theorems that are valid for one are equally valid for the other.

The concept of a matrix as an array of numbers with an unintuitive multiplication rule hardly provides a geometric way of looking at things. Nevertheless, matrices have proven to be an extremely effective computational tool and have played a major role in the development of diverse areas of mathematics. Geometric algebra rectifies this defect by providing a geometric perspective, and many new algebraic tools. Combining both of these powerful systems by simply considering matrices whose elements are geometric numbers adds much needed geometric content and flexibility to both languages. The author hopes that this book captures both the idea and the

spirit of the powerful geometric number system that has kept him going since he learned about the subject as a graduate student at Arizona State University many years ago.

We assume readers to have had undergraduate differential and integral calculus, a first course in modern algebra, and the mathematical maturity that an upper-level mathematics or physics undergraduate student might be expected to have. The many topics covered in the book should also appeal to first-year graduate students in mathematics, physics, engineering and computer science. Any unfamiliarity that a reader might have regarding mathematical terminology can be quickly overcome by a quick reference to the unlimited resources on the internet. We also recommend that the reader has knowledge of and access to symbolic mathematical software such as Mathematica or Maple. Such software considerably lightens the computational work required and makes for easy verification of results. A simple Mathematica package is provided for calculating the spectral basis for a modular polynomial.

There are three main groupings of interrelated core chapters:

- Chapters 1–5 introduce the fundamental concepts of a spectral basis of modular numbers and modular polynomials with applications in number theory, numerical analysis, and linear algebra. The hyperbolic numbers, introduced alongside the well-known complex numbers, are used to solve the cubic equation and provide a mathematical foundation for the theory of special relativity. The geometric extension of the real numbers is achieved by introducing new *anticommuting* square roots of plus or minus one which represent orthogonal directions in successively higher dimensions.
- Chapters 7–10 lay down the ideas of linear and multilinear algebra. Matrices of geometric numbers are considered throughout. New proofs of the Cayley–Hamilton Theorem, Gram–Schmidt orthogonalization, and the spectral decomposition of a linear operator are given in geometric algebra, as well as a comprehensive geometric interpretation of complex eigenvalues and eigenvectors in an Hermitian (definite or indefinite) inner product space.
- Chapters 13–16 develop the basic ideas of vector calculus and differential geometry in the context of geometric algebra. The classical integration theorems are derived from a single fundamental theorem of calculus. Manifolds are embedded in Euclidean or pseudo-Euclidean spaces and consequently have both intrinsic and extrinsic curvature, characterized by the projection and shape operators. Highlighted is a special treatment of conformal mappings and the conformal Weyl tensor, which have applications in physics and engineering.

Chapter 6 covers some of the more traditional topics in linear algebra which are not otherwise used in this book. Chapters 11, 12, 17, and 18 provide additional breadth and scope by treating the symmetric group, by giving a novel look at the concept of space-time in special relativity, by laying down the basic ideas of projective geometry, and by giving an introduction to Lie algebras and Lie groups, topics which are not usually covered in an undergraduate course. In the Table of Contents, a "*" is used to indicate those sections which are considerably more technical and may be omitted on first reading.

The author is indebted to many students and collegues from around the world who have contributed much during the many stages of the development of these ideas. Foremost he is indebted to David Hestenes, who first introduced him to geometric algebra many years ago as a graduate student at Arizona State University during the years 1965–1971. The author is indebted to Roman Duda of the Polish Academy of Sciences, Bernard Jancewicz, Jan Łopuszański, and Zbigniew Oziewicz of the Institute of Theoretical Physics in Wrocław, Poland, and Stony Brook University, for encouragement and support during these difficult early years. He wants to thank Rafal Ablamowicz (USA), Timothy Havel (USA), William Baylis (Canada), and Pertti Lounesto (Finland), who contributed in different ways to the writing of this book. In addition, he wants to thank Jaime Keller for inviting him to Mexico, Luis Verde-Star (Mexico), Waldyr Rodrigues (Brazil), Josep Parra (Spain), and Eduardo Bayro-Corrochano (Mexico). Among former students and now sometimes collaborators, he wants to thank José María Pozo (Spain), Marco Antonio Rodríguez (Mexico), Omar Leon Sanchez (Mexico), and Alejandra C. Vicente (Mexico). Graphics design artist Ana Sánchez Stone was a great help with all of the figures in Chap. 11 and in particular Fig. 11.6. The author is greatly indebted to Universidad de Las Américas-Puebla and Sistemas Nacionales de Investigadores de México, for many years of support. This book could not have been written without the constant support and encouragement over the years by my wife, Wanda, my mother and father and is a present for my mother's 100th birthday.

Cholula, México Garret Sobczyk

Contents

Chapter 1
Modular Number Systems

For out of olde feldes, as men seith,
Cometh al this newe corne fro yeere to yere;
And out of olde bokes, in good feith,
Cometh al this new science that men lere.

–Chaucer

We begin by exploring the algebraic properties of the modular numbers, sometimes known as *clock arithmetic*, and the modular polynomials. The modular numbers and modular polynomials are based upon the *Euclidean algorithm*, which is simply the idea of dividing one integer into another or one polynomial into another polynomial, which we first learned in secondary school. Studying the modular number system leads us to introduce the concept of a *spectral basis*. This fundamental concept, which is largely neglected in elementary mathematics, will serve us well in our study of linear algebra and other topics in later chapters.[1]

1.1 Beginnings

In Euclid's *Elements*, Book VII, we find

> **Proposition 2:** *Given two numbers not prime to one another, to find their greatest common measure.*

Then follows what mathematicians refer to as the Euclidean algorithm [32]. We shall need the following consequence of this venerable algorithm. Given r positive

[1]This chapter is based upon an article by the author that appeared in the American Mathematical Monthly [80].

G. Sobczyk, *New Foundations in Mathematics: The Geometric Concept of Number*, DOI 10.1007/978-0-8176-8385-6_1,

integers $h_1, h_2, \ldots, h_r \in \mathbb{N}$ whose *greatest common divisor* (*gcd*) is $1 \in \mathbb{N}$, then there exist integers $b_1, b_2, \ldots, b_r \in \mathbb{Z}$ with the property that

$$b_1 h_1 + b_2 h_2 + \cdots + b_r h_r = 1. \tag{1.1}$$

The justified fame of the Euclidean algorithm arrives from the fact that it has a much larger realm of applicability than just the integers. In particular, Let $\mathbb{K}$ be any *field* and let $\mathbb{K}[x]$ be the corresponding *integral domain* of polynomials over $\mathbb{K}$ [28, p.248, 250]. Given r polynomials $h_1(x), h_2(x), \ldots, h_r(x) \in \mathbb{K}[x]$ whose greatest common divisor (*gcd*) is $1 \in \mathbb{K}$ (no common zeros), then there exist polynomials $b_1(x), b_2(x), \ldots, b_r(x) \in \mathbb{K}[x]$ with the property that

$$b_1(x)h_1(x) + b_2(x)h_2(x) + \cdots + b_r(x)h_r(x) = 1 \tag{1.2}$$

The identities (1.1) and (1.2), and the striking analogy between them, provide the basis for what follows.

Examples

1. $gcd(4, 15) = 1 \implies 4 \cdot 4 + (-1) \cdot 15 = 1,$
2. $gcd(4, 15, 7) = 1 \implies (-24) \cdot 4 + 6 \cdot 15 + (+1) \cdot 7 = 1,$
3. $gcd(x+1, x^2+1) = 1 \implies (-1/2)(x-1)(x+1) + (1/2)(x^2+1) = 1,$
4. $gcd(x+1, x^2+1, x+2) = 1 \implies x^2(x+1) + (x^2+1) - x^2(x+2) = 1.$

1.2 Modular Numbers

Given any integer $n \in \mathbb{Z}$ and any positive integer $h \in \mathbb{N}$, the Euclidean algorithm tells us that there is a unique integer $q \in \mathbb{Z}$ and a nonnegative integer r, $0 \leq r < h$, such that

$$n = qh + r.$$

The set $\mathbb{Z}_h = \{0, 1, 2, \ldots, h-1\}$ of all possible remainders r, after division by h, denotes the *modular number system* modulo(h) where $h \in \mathbb{N}$. The numbers $b \in \mathbb{Z}_h$ represent equivalence classes, and addition, multiplication, and equality in $\mathbb{Z}_h$ are defined modulo(h). We write $b + c \overset{\text{h}}{=} d$ and $bc \overset{\text{h}}{=} d$ to mean that $b + c \equiv d \mod(h)$ and $bc \equiv d \mod(h)$. The modular number system $\mathbb{Z}_h$ is *isomorphic* to the *factor ring* $\mathbb{Z}/ < h >$ for the *ideal*

$$< h >= \{0, \pm h, \pm 2h, \pm 3h, \ldots\} = \{nh\}_{n \in \mathbb{Z}}$$

over the integers $\mathbb{Z}$. In terms of the ideal $< h >$, the equivalence classes of $\mathbb{Z}_h$ are explicitly expressed by

$$\mathbb{Z}_h \overset{\text{h}}{=} \{0+ < h >, 1+ < h >, \ldots, h-1+ < h >\}. \tag{1.3}$$

The technical details, in the framework of modern algebra, can be found in [28, p.261, 262].

For any positive integer $h \in \mathbb{N}$, by *unique prime factorization*, we can write $h = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, where each p_i is a distinct prime factor of h. We can also order the factors $p_i^{m_i}$ so that their multiplicities satisfy $1 \leq m_1 \leq m_2 \leq \cdots \leq m_r$. Now define $h_i = h/p_i^{m_i}$ for $i = 1, \ldots, r$. Since the h_i have no common factor other than 1, (1.1) holds, and we have

$$b_1 h_1 + b_2 h_2 + \cdots + b_r h_r = 1,$$

for an appropriate choice of the integers $b_i \in \mathbb{Z}$. Whereas this equation holds in $\mathbb{Z}$, it is just as valid when interpreted as an identity in $\mathbb{Z}_h$. Defining the numbers $s_i \overset{\text{h}}{=} b_i h_i \in \mathbb{Z}_h$, we can rewrite the above identity as

$$s_1 + s_2 + \cdots + s_r \overset{\text{h}}{=} 1. \tag{1.4}$$

When interpreted as an identity among the numbers $s_i \in \mathbb{Z}_h$, the following additional important properties are easily verified by multiplying (1.4) on both sides by s_i and simplifying modulo h. We find that

$$s_i^2 \overset{\text{h}}{=} s_i \quad \text{and} \quad s_i s_j \overset{\text{h}}{=} 0 \tag{1.5}$$

for $i, j = 1, 2, \ldots, r$, and $i \neq j$. We say that the $s_i \in \mathbb{Z}_h$ are *mutually annihiliating idempotents* that partition unity. The set of numbers $\{s_1, s_2, \ldots, s_r\}$ make up what we call the *spectral basis* of $\mathbb{Z}_h$.

Now suppose that $c \in \mathbb{Z}_h$. Multiplying both sides of the identity (1.4) by c gives

$$cs_1 + cs_2 + \cdots + cs_n \overset{\text{h}}{=} c.$$

Since the s_i are idempotents, they act as *projections* onto the modular numbers $\mathbb{Z}_{p_i^{m_i}}$; this is clear because from the definition of $s_i = b_i h_i$, it follows that $p_i^{m_i} s_i \overset{\text{h}}{=} 0$. Thus, any number $c \in \mathbb{Z}_h$ can be written in the spectral basis as the unique *linear combination*

$$c \overset{\text{h}}{=} \sum_{i=1}^{r} (c \bmod p_i^{m_i}) s_i \ \text{ in } \ \mathbb{Z}_h, \tag{1.6}$$

of the basis elements $s_1, s_2, \ldots, s_r$. This last identity is also known as the famous *Chinese Remainder Theorem*, dating back to the fourth century A.D. The interested reader may check out the web site

http://en.wikipedia.org/wiki/Chinese_remainder_theorem

The modular number systems $\mathbb{Z}_{p^m}$, modulo a power of a prime, play a particularly important role in Number Theory in that most modular problems reduce to problems involving a power of a prime. In dealing with such problems, it is best to represent numbers $a \in \mathbb{Z}_{p^m}$ in terms of the *p-adic number basis*

$$a = (a_{m-1}\, a_{m-2}\, \ldots a_1\, a_0)_p = \sum_{i=0}^{m-1} a_i p^i \tag{1.7}$$

where each digit $a_i \in \mathbb{Z}_p$. Using (1.7) in (1.6), we find that

$$c \overset{\text{h}}{=} \sum_{i=1}^{r} (c \bmod p_i^{m_i}) s_i \overset{\text{h}}{=} \sum_{i=1}^{r} \sum_{j=0}^{m_i-1} c_{i,j}\, q_i^j, \tag{1.8}$$

where $q_i^0 = s_i$ and $q_i^j \overset{\text{h}}{=} p_i^j s_i$ for $i = 1, \ldots, r$ and $j = 1, \ldots, m_i - 1$. The set

$$\cup_{i=1}^{r} \{s_i, q_i, \ldots, q_i^{m_i-1}\}$$

is called the *complete spectral basis* of $\mathbb{Z}_h$.

We are now in a position to directly solve for the idempotents s_i. Multiplying each side of the identity (1.4) by h_i gives

$$h_i s_i \overset{\text{h}}{=} h_i,$$

which can be easily solved in $\mathbb{Z}_h$, getting $s_i = (h_i^{-1} \bmod p_i^{m_i}) h_i$ for each $i = 1, 2, \ldots, r$. The $q_i \overset{\text{h}}{=} p_i s_i$ are *nilpotent* in $\mathbb{Z}_h$, for $i = 1, 2, \ldots, r$. The nilpotents q_i have the *index of nilpotency* m_i, since $q_i^{m_i-1} \neq 0$ but $q_i^{m_i} \overset{\text{h}}{=} 0$ in $\mathbb{Z}_h$.

Let us calculate the complete spectral basis $\{s_1, s_2, q_2\}$ for $\mathbb{Z}_{12}$ where $h = 12 = 3 \cdot 2^2$, so that $p_1 = 3$ and $p_2 = 2$. By (1.4), we must have $s_1 + s_2 \overset{\text{h}}{=} 1$. By multiplying this equation by

$$h_1 = \frac{h}{p_1} = 2^2 \quad \text{and} \quad h_2 = \frac{h}{p_2^2} = 3,$$

we get with the help of (1.6)

$$4s_1 + 4s_2 \overset{\text{h}}{=} 4, \quad \text{or} \quad s_1 = (4 \bmod 3) s_1 \overset{\text{h}}{=} 4,$$

and

$$3s_1 + 3s_2 \overset{\text{h}}{=} 3, \quad \text{or} \quad 3s_2 = (3 \bmod 4) \overset{\text{h}}{=} 3 \implies s_2 \overset{\text{h}}{=} 9,$$

respectively. From $s_2 \overset{\text{h}}{=} 9$, we easily calculate $q_2 = 2s_2 = 18 \overset{\text{h}}{=} 6$, so the complete spectral basis for z_{12} is

$$\{s_1 = 4, s_2 = 9, q_2 = 6\}. \tag{1.9}$$

Much of the power of the spectral basis is a consequence of the simple rules for multiplication of its idempotent and nilpotent elements. We give here the table of multiplication for the spectral basis (1.9) of $\mathbb{Z}_{12}$.

$\cdot \bmod 12$	s_1	s_2	q_2
s_1	s_1	0	0
s_2	0	s_2	q_2
q_2	0	q_2	0

For a second example, consider $h = 360 = 5 \cdot 3^2 \cdot 2^3$ for which $h_1 = 3^2 \cdot 2^3$, $h_2 = 5 \cdot 2^3$ and $h_3 = 5 \cdot 3^2$. The spectral basis satisfying (1.4) and (1.5) is found to be

$$\{s_1 = 216, s_2 = 280, s_3 = 225\},$$

as we now show. To find s_1, multiply $s_1 + s_2 + s_3 = 1$ by $h_1 = 3^2 \cdot 2^3 = 72$, and use (1.6) to get

$$72s_1 = 2s_1 = 72 \text{ in } \mathbb{Z}_{360}$$

or $16s_1 = s_1 = 8 \cdot 72 = 216$. Similar calculations give s_2 and s_3. An arbitrary $c \in \mathbb{Z}_{360}$ can now be written

$$c \overset{\text{h}}{=} cs_1 + cs_2 + cs_3 \overset{\text{h}}{=} (c_1)_5 s_1 + (c_2 c_3)_3 s_2 + (c_4 c_5 c_6)_2 s_3,$$

where $c_1 \in \mathbb{Z}_5$, $c_2, c_3 \in \mathbb{Z}_3$, and $c_4, c_5, c_6 \in \mathbb{Z}_2$. The complete spectral basis of $\mathbb{Z}_{360}$ is

$$\{s_1 = 216, s_2 = 280, q_2 = 120, s_3 = 225, q_3 = 90, q_3^2 = 180\}. \tag{1.10}$$

The multiplication table for spectral basis of $\mathbb{Z}_{360}$ is given below:

$\cdot \bmod 360$	s_1	s_2	q_2	s_3	q_3	q_3^2
s_1	s_1	0	0	0	0	0
s_2	0	s_2	q_2	0	0	0
q_2	0	q_2	0	0	0	0
s_3	0	0	0	s_3	q_3	q_3^2
q_3	0	0	0	q_3	q_3^2	0
q_3^2	0	0	0	q_3^2	0	0

Employing the spectral basis, we also have an easy formula for finding the inverse b^{-1} of $b \in \mathbb{Z}_h$. We have

$$b^{-1} \overset{\text{h}}{=} \sum_{i=1}^{r} (b_{i(m_i-1)} \dots b_{i0})_{p_i}^{-1} s_i,$$

so the problem of finding $b^{-1} \in \mathbb{Z}_h$ is reduced to the problem of finding the inverse in a prime power modular number system $\mathbb{Z}_{p^m}$. For example, using the spectral basis (1.9) for $\mathbb{Z}_{12}$, we can easily calculate the inverse 7^{-1} of $7 \in \mathbb{Z}_{12}$. We first write