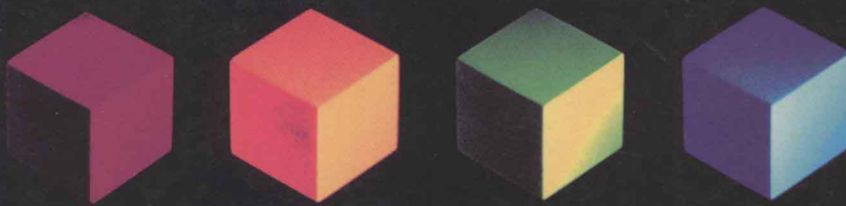
SECOND EDITION



Adventures in Group Theory

RUBIK'S CUBE, MERLIN'S MACHINE & OTHER MATHEMATICAL TOYS

DAVID JOYNER

Adventures in Group Theory

Rubik's Cube, Merlin's Machine, and Other Mathematical Toys

Second Edition

David Joyner

The Johns Hopkins University Press
Baltimore

Printed in the United States of America on acid-free paper
9 8 7 6 5 4 3 2 1

The Johns Hopkins University Press
2715 North Charles Street
Baltimore, Maryland 21218-4363
www.press.jhu.edu

Library of Congress Cataloging-in-Publication Data

Joyner, David, 1959–
Adventures in group theory : Rubik's cube, Merlin's machine, and other mathematical toys / David Joyner—2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-8018-9012-3 (hardcover : alk. paper)
ISBN-13: 978-0-8018-9013-0 (pbk.: alk. paper)
ISBN-10: 0-8018-9012-8 (hardcover : alk. paper)
ISBN-10: 0-8018-9013-6 (pbk.: alk. paper)
1. Group theory. 2. Mathematical recreations. I. Title.
QA 174.2.J69 2008
512′.2—dc22 2008011322

A catalog record for this book is available from the British Library.

Special discounts are available for bulk purchases of this book. For more information, please contact Special Sales at 410-516-6936 or specialsales@press.jhu.edu.

The Johns Hopkins University Press uses environmentally friendly book materials, including recycled text paper that is composed of at least 30 percent post-consumer waste, whenever possible. All of our book papers are acid-free, and our jackets and covers are printed on paper with recycled content.

Adventures in Group Theory

In mathematics you don't understand things.
You just get used to them.

—*Johann von Neumann*

Preface

This book grew out of a combined fascination with games and mathematics, from a desire to marry 'play' with 'work' in a sense. It pursues playing with mathematics and working with games. In particular, abstract algebra is developed and used to study certain toys and games from a mathematical modeling perspective. All the abstract algebra needed to understand the mathematics behind the Rubik's Cube, Lights Out, and many other games is developed here. If you believe in the quote by von Neumann on a previous page, I hope you will enjoy getting used to the mathematics developed here.

Why is it that these games, developed for amusement by non-mathematicians, can be described so well using mathematics? To some extent, I believe it is because many aspects of our experience are universal, crossing cultural boundaries. One can view the games considered in this book, the Rubik's Cube, Lights Out, etc., to be universal in this sense. Mathematics provides a collection of universal analytical methods, which is, I believe, why it works so well to model these games.

This book began as some lecture notes designed to teach discrete mathematics and group theory to students who, though certainly capable of learning the material, had more immediate pressures in their lives than the long-term discipline required to struggle with the abstract concepts involved. My strategy, to tempt them with something irresistible such as the Rubik's Cube, worked and students loved it. Based on my correspondence, my students were not the only ones to enjoy the notes, which have been expanded considerably. I've tried to write the book to be interesting to people with a wider variety of backgrounds, but at the same time I've tried to make it useful as a reference.

This book was truly a labor of love in the sense that I enjoyed every minute of it. I hope the reader derives some fun from it too.

I've tried to ensure no mistakes remain. However, if you find any, I'd appreciate hearing about them so they can be fixed in a possible future edition. My e-mail is `wdjoyner@gmail.com`.

To continue the universal theme mentioned above, half the royalties from this book will go directly to support SAGE (`http://www.sagemath.org/`), a free and open-source computer algebra system. SAGE installs on all major platforms (Linux, MacOS and Windows) but is also available for use free over the Internet via a web browser, such as Firefox. The other half of the royalties from this book will go directly to the Earth Island Institute, a nonprofit organization dedicated to environmental projects all over the world; see `http://www.earthisland.org/`. To paraphrase David Brower (1912–2000), the founder of EII, there is but one ocean, one atmosphere, one Earth, and there are no replacements.

Preface to the Second Edition

I've been very gratified by the reception of the first edition and flattered by the many kind e-mails from puzzle enthusiasts and mathematicians who enjoyed the first book. Based on their suggestions, I believe that the time has come for a new edition of the book. Based on popular demand, I have now included material of a more interactive nature, where **SAGE**, a free computer algebra software system, is used to illustrate ideas. I have also taken the opportunity to update and correct all the first edition's typographical, historical, and mathematical errors I'm aware of. I trust that those who read the first edition will welcome the new version—based as it is on the feedback that I've received. I hope that those new to the book will enjoy reading it as much as I've enjoyed writing it.

Acknowledgments

This book owes much to the very interesting books of Christoph Bandelow [B1], Professor of Mathematics at the Ruhr-University Bochum in Germany, and David Singmaster [Si], Professor of Mathematics in the Department of Computing, Information Systems and Mathematics, South Bank University, London. I thank my fine editor at Johns Hopkins University Press, Trevor Lipscombe, for his encouragement and for his many excellent suggestions. Without them as a source of ideas, this book would not exist. This book has benefited greatly from the stimulating discussions, encouraging correspondence, and collaborations with many people. These people include Christoph Bandelow, Dan Hoey, Ann Luers (now Ann Casey—for help with §§13.4, 13.3, and parts of chapter 14), Michael Dunbar (for help with §13.3), Mark Longridge, Jim McShea (for help with §§7.4, 13.5), Justin Montague and G. Gomes (for help with §15.4.2, 13.2), Michael Reid, Andy Southern (for help with §15.3), Dennis Spellman (for help with §10.5.1), Herbert Kociemba (for §15.2.3), several people on the SAGE development team (detailed below), and many others.

Some of the graphs given below were produced with the help of SAGE [S]. Some of the group-theoretical calculations were determined with the help of GAP [Gap] or SAGE. Some of the biographical information included in this book was borrowed from the award-winning Internet site the MacTutor History of Mathematics Archive [MT].

The Rubik's Cube, Pyraminx, Megaminx, Masterball, Lights Out, and other puzzles names mentioned frequently are all trademarked. I shall omit the symbol (TM) after each occurrence for ease of reading. I would also like to thank Hasbro Toys (who market Lights Out) for the opportunity to consult for them.

SAGE credits: SAGE was started in 2005 by William Stein, who is its lead developer. It is open source and can be downloaded and installed without cost by anyone with a good Internet connection. The command-line interface in the examples in this book uses Ipython [Ip], started by Fernando Perez. Most people actually prefer the GUI notebook interface (I'm in the minority), written primarily by Tom Boothby and William Stein. This is in the downloadable version of SAGE but is also available online at `http://www.sagenb.org/`. Most of the commands in this book can be run online there without having to install SAGE. For all the group theoretic constructions, SAGE uses an interface to GAP, a computer algebra system specializing in group theory which goes back to the mid-1980's. For the graph theory illustrated in chapter 7, SAGE uses the graph package NetworkX [N] and some functionality written primarily by Emily Kirkman and Robert Miller. Bobby Moretti and Robert Miller wrote SAGE's Cayley graph construction, whereas GAP's GRAPH package was written by Leonard Soicher [So]. SAGE code to plot and manipulate the Rubik's Cube was written by Robert Bradshaw, Robert Miller, and myself (with help from Tom Boothby, who wrote some of the underlying graphics functions).

Much of SAGE's development is funded by National Science Foundation grants supporting the number theory research of William Stein, the lead developer and architect of SAGE. The University of Washington, William Stein's home institution, has also been a generous supporter. Many thanks to William Stein (and the entire SAGE development team) for this great piece of software. Credit also must be given to the group-theoretic package GAP, which was originally developed in in the 1980's and has been under continuous active development since then. SAGE uses GAP extensively for its group-theoretic computations.

This version owes much to the careful reading of the following people: Jamie Adams, Lewis Nowitz, David Youd, Roger Johnson, Jaap Scherphuis, Michael Hoy, Tom Davis, John Rood, Trevor Irwin, Stephen Lepp, Mark Edwards, Carl Patterson, Peter Neumann, Bill Zeno, Herbert Kociemba, Alastair Farrugia, Matthew Lewis, Christopher Paul Tuffley, Robert Bradshaw, and Benjamin Weggenmann. I thank them all.

Last, but certainly not least, I thank my wonderful wife, Elva, for more things than I can possibly list here.

Where to begin...

Speaking personally, I am always fascinated to discover that one topic is connected in a surprising way with another completely different topic. The Rubik's Cube, a mechanical toy that has a reasonably efficient solution using pure mathematics (and no 'strategy'), is a case in point. It's difficult to know where to begin to explain this connection: as Wodehouse's character Bertie Wooster said, 'I don't know if you have the same experience, but the snag I come up against when I'm telling a story is the dashed difficult problem of where to begin it'. Let's begin with Rubik himself.

Erno Rubik was born in the air-raid shelter of a Budapest hospital during World War II. His mother was a published poet, his father an aircraft engineer who started a company to build gliders. Rubik himself, far from being a mathematician, studied architecture and design at the Academy of Applied Arts and Design, remaining there as a professor, teaching interior design. In the mid-1970's, he patented a cube-shaped mechanical puzzle that has since captured the imagination of millions of people worldwide. The Rubik's Cube was born. By 1982, 'Rubik's Cube' was a household term, and became part of the Oxford English Dictionary. More than 100 million cubes have been sold worldwide.

About 150 years earlier, in the late 1820's and early 1830's, a French teenager named Evariste Galois developed a new branch of mathematics: group theory was born from his attempts to understand the solvability of polynomial equations. In high school, students learn that

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

are the roots of the quadratic equation $ax^2 + bx + c = 0$. There are similar but more complicated formulas for the cubic and quartic polynomials discovered during the Middle Ages (see, for example, [JKT] for more details). His work on group theory was motivated by what was perhaps the main unsolved mathematical problem of the day: does there exist an analogous algebraic formula involving radicals only in the coefficients for an equation of fifth degree or higher? This problem had remained unsolved for centuries despite the efforts of the best and brightest mathematical minds. Galois' ideas succeeded where others had failed (although one must give credit to Ruffini and Abel here as well). Like Rubik, Galois' life story is also interesting (see, for example, Calinger [Ca] and the article by Rothman [Ro]) and we shall read more of him later in this book.

Groups measure symmetry. (Galois, for example, studied the 'symmetry group' of the roots of a polynomial, now called Galois groups.) As the mathematician Hermann Weyl said in his wonderful book [We], symmetry is 'one idea by which man has tried throughout the ages to comprehend and create order, beauty, and perfection'. Groups play a key role in the study of roots of polynomials, crystallography, elementary particle physics, campanology (or 'bell-ringing'; see chapter 3 below), cryptography, and the Rubik's Cube, among others. Surprisingly enough, it turns out that it is possible to use group theory (and only the 'group-theoretical definition' of the cube—no knowledge of strategy or special moves) to solve the Rubik's Cube (see §10.2 below).

This book will develop the basics of group theory and create group-theoretical models of Rubik's Cube-like puzzles. On the practical side, I also discuss the solution strategy for the Rubik's Cube in some detail. (For those wanting to see a solution strategy now, see section 15.1.) Some solution strategies are briefly discussed for similar puzzles (the '15 Puzzle', the 'Rubik tetrahedron' or Pyraminx, the 'Rubik dodecahedron' or Megaminx, the Skewb, the 'Hockeypuck', and the 'Masterball') as well.

The important point to remember, though, is that group theory is a powerful tool with many real-world applications. Solving puzzles happens to be just one of them. Because of our Rubik's Cube focus, the approach in this book is different from some texts:

(a) there are a lot of non-standard, though relatively elementary, group theory topics;

(b) I emphasize permutation groups via examples over general theory (such as Sylow theory);

(c) I present some of the basic notions algorithmically (as in [Bu]); and

(d) I include material which is interesting, from both the mathematical and puzzlist's perspective, while keeping the level as low as possible for as long as possible.

Moreover, most group theory texts prove everything. Here a lot of statements are proven; sometimes only a hint or sketch is provided, and the proof is left to the interested reader; other statements are supported only by an example. When a proof is not provided, a reference for a proof in the literature is given. To keep things as clear as possible, the start of a proof is denoted **Proof:** and the end by □. I've used the number system where a result or example in section a.b has a labeling of the form a.b.c.

Chapters 1, 2 and 3 give some basic mathematical background. Chapter 4 introduces some of the puzzles and some notation we use for them. Except for the chapter on solutions, chapter 15, the remaining chapters discuss these puzzles using group theory, graph theory, linear algebra, or automata (finite state machines) theory. While the earlier chapters can probably be followed by a good high school student, chapters 12 and 14 are relatively advanced. They are, in my opinion, the most interesting, and illustrate some remarkable ways in which the Rubik's Cube is connected with other branches of mathematics, which is a continuing source of my fascination with the subject.

The last chapter, chapter 16, gives some indications of directions which weren't pursued and the present state of our, or at least my own, ignorance in this area. As it only gives some of the problems and questions that I don't have the answer to, it is not intended to be complete!

A note to teachers: Based on my experience teaching at the U.S. Naval Academy, a reasonable semester course based on this book could aim for the First Fundamental Theorem of Cube Theory, in chapter 9, with lots of time for 'side trips' and other material. It is possible to cover the Second Fundamental Theorem of Cube Theory, in chapter 11, in one semester but it is a race against time. For example, chapter 6 on 'Merlin's Machine', or any uncovered sections, might be used for some very interesting term projects.

A word about **SAGE**: New in this edition are numerous examples which use **SAGE**, a free and open-source computer algebra system. At the **SAGE** website (`www.sagemath.org`) there is ample documentation (a reference manual, tutorial, e-mail support lists, and so on) but it is worth taking some time here to explain how **SAGE** is used in this book. First, you don't have to know or care about **SAGE** to read the book. You may ignore the **SAGE** boxes if you wish. On the other hand, if you are fairly comfortable with computer software, the examples are added to help you relate to the constructions in a more interactive manner. There are two commonly used interfaces to **SAGE**: one is the command line (you type in a command and hit `Enter` to see the output) and the other is the graphical "notebook" interface (you type a command into a "cell" and hit `Shift-Enter` for the output). Since I prefer the command line, most examples are described that way. To keep publication costs down, **SAGE** plots and graphics are reproduced in greyscale in this book, though of course in **SAGE** they are in color.

Contents

Chapter 1

Elementary, my dear Watson

If logic is the hygiene of the mathematician, it is not his source of food; the great problems furnish the daily bread on which he thrives.

André Weil, 'The future of mathematics', **American Mathematical Monthly**, *May 1950*

Think of a scrambled Rubik's Cube as a car you want to fix on your own. You not only need some tools but you need to know how to use them. This chapter, among others, provides you with some of the tools needed to get the job done. As one of our goals is to discuss the mathematics of the Rubik's Cube, and other games, we start with some fundamentals. The basic purpose of this chapter is to introduce standard set theory notation and some basic notions of mathematical logic.

Logic and set theory are as basic to mathematics as light is to the 'real world'. The background presented here hopefully will make some of the terminology and notation introduced later a little easier to follow for those who either haven't seen or may have forgotten the mathematical notation. In any case, this is not intended to be a 'serious' introduction to mathematical logic nor to set theory.

1.1 You have a logical mind if...

The sentence in the section title, intended to be somewhat whimsical, will be finished later in this section!

A **statement** is an assertion which is either true or false. (Of course we assume that this admittedly circular 'definition' is itself a statement.) Sometimes the truth or falsity of a statement is called its **Boolean value**. One can combine several statements into a single statement using the **connectives** 'and' $\wedge$, 'or' $\vee$, and 'implies' $\Rightarrow$. The Boolean value of a statement is changed using the 'negation' $\sim$. We shall also use 'if and only if' $\Longleftrightarrow$ and 'exclusive or' $\underline{\vee}$ (this is defined in the table below), but these can be defined in terms of negation $\sim$ and the other three connectives ($\vee$, $\wedge$, and $\Rightarrow$).

Example 1.1.1. *Today is Monday if and only if today is the day before Tuesday. An example of 'exclusive or': Either today is Monday or today is not Monday (but not both).*

Ponderable 1.1.1. *Express* $\_\vee$ *and* $\iff$ *in terms of* $\sim$, $\vee$, $\wedge$, *and* $\Rightarrow$.

Solution: The statement $p \iff q$ is the same as $(p \Rightarrow q) \wedge (q \Rightarrow p)$, and $p \_\vee q$ is the same as $\sim (p \iff q)$. □

> LOGIC, n. The art of thinking and reasoning in strict accordance with the limitations and incapacities of the human misunderstanding. The basic of logic is the syllogism, consisting of a major and a minor premise and a conclusion—thus:
>
> Major Premise: Sixty men can do a piece of work sixty times as quickly as one man.
>
> Minor Premise: One man can dig a posthole in sixty seconds; therefore—
>
> Conclusion: Sixty men can dig a posthole in one second.
>
> *Ambrose Bierce,* **The Devil's Dictionary**

Notation: Let p and q be statements.

Statement	Notation	Terminology
p and q	$p \wedge q$	'conjunction'
p or q	$p \vee q$	'disjunction'
p implies q	$p \Rightarrow q$	'conditional'
~q implies ~p	$\sim q \Rightarrow \sim p$	'contrapositive' of $p \Rightarrow q$
negate p	$\sim p$	'negation'
p if and only if q	$p \iff q$	'if and only if'
either p or q (not both)	$p \_\vee q$	'exclusive or'

The contrapositive is part of any 'proof by contradiction', or 'reductio ad absurdum', argument.

Truth tables: Given the Boolean values of the statements p, q, we can determine the values of the statements $p \wedge q$, $p \vee q$, $p \Rightarrow q$, $p \iff q$, $p \_\wedge q$ using the following truth tables:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

p	q	$p \iff q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 1.1.2. *The connectives "and" and "or" are already part of Python (which* SAGE *is built on):*

SAGE

```
sage: True and True
True
sage: True and False
False
sage: False and True
False
sage: False and False
False
```

You can see how these Boolean values agree with those in the truth table for $\wedge$ *above. As an exercise, you can replace* `and` *by* `or` *and check the truth table above for* $\vee$.

Here's a way to implement "implies" as a function in SAGE*:*

SAGE

```
sage: def implies(p,q): return not(p and not(q))
sage: implies(True,True)
True
sage: implies(True,False)
False
sage: implies(False,True)
True
sage: implies(False,False)
True
```

You can see how these Boolean values agree with those in the truth table for $\Longrightarrow$ *above. As an exercise, you can try to implement* $\iff$ *im Python and use it to check the truth table above for* $\iff$.

Note that $\iff$ is analogous to the $=$ sign.

For example, let p be the statement 'I am a millionaire' and q the statement 'I will buy my wife a brand new car.' I claim that 'if p then q' is true. If I were