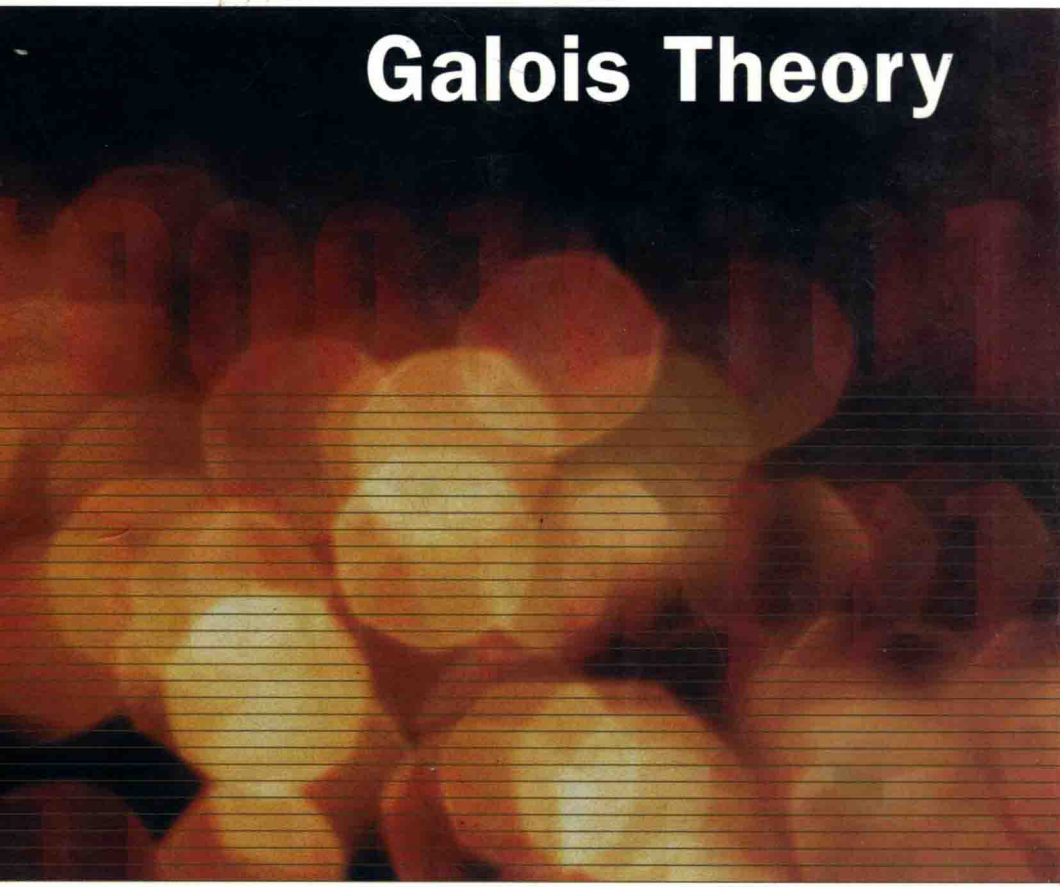
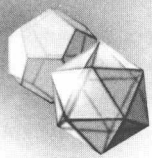
Second Edition

Groups, Rings and Galois Theory



Victor P Snaith



Groups, Rings and Galois Theory

Second Edition

Victor P Snaith

University of Southampton, UK

World Scientific

New Jersey • London • Singapore • Hong Kong

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: Suite 202, 1060 Main Street, River Edge, NJ 07661

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

The first edition was published in 1998.

GROUPS, RINGS AND GALOIS THEORY
Second Edition

ISBN 981-238-576-2
ISBN 981-238-600-9 (pbk)

Printed in Singapore.

Groups, Rings and Galois Theory

Second Edition

Preface

This book was tailor-made for the third-year algebra course at McMaster University. There is very little that is special about the course — every university must have one like it — except perhaps for the fact that it comes in two halves, permitting the disenchanted student to bail out midway through the material.

Those who leave at that point come away with an introductory course on group theory and, it seems to me, are entitled to see groups in action as something other than self-fulfilling exercise fodder. Accordingly — and not very originally — I included a little material on error-correcting codes and on Rubik's cube for them.

Students soldiering on into the second term of the course are treated to an introduction to the theory of rings. For them, I thought it appropriate to present enough material so that they could see how the two subjects — rings and groups — eventually joined forces in a major undertaking. In this book that example is Galois theory — the jewel in the crown of algebra.

I hope that this succinctly explains the ingredients of the book and that the table of contents, the index and some browsing through the text will do the rest.

I am very grateful to my son, Daniel, who typed this manuscript into Latex and to Carolyn, my wife, who proof-read the typescript. They did such a thorough job that any blunders which remain are entirely my responsiblity!

It only remains for me to say a few sentences on why I wrote yet another book on this amply covered material. Usually the "book of the course" for this material would be a rather magnificent, expansive tome. I, on the other hand, have tried to give a rather concise treatment, because I have found that demanding proofs and exercises tend to encourage more profitable discussion between the instructor and class. Making the text more terse, providing one does not attempt to cover too much material, made the course more enjoyable — at least for me! Had I made the pace of the book too leisurely I would have run the risk of rendering the instructor superfluous. Had I made the exercises too easy or repetitious I would have

run the risk of superannuating the students! Learning mathematics at this level seems best accomplished by pondering problems on which one gets stuck rather than repeating finger-exercises with the themes one finds easy. The McMaster students were good-natured enough to indulge me in these whims and I responded by trying to strike a workable compromise vis á vis the exercises. Accordingly, the reader — should there be one — will find this book terse enough here and there that there will be no alternative but to discuss the subject with others, preferably fellow students and the lecturer. The exercises will occasionally be too hard or too few and there will be no alternative but to ask the instructor for suggestions about where to look elsewhere.

This book was used as the basis of my 1995/7 courses at McMaster University during which time I tried to correct as many misprints and errors as I could. I am particularly grateful to Hayssam "Sam" Hulays, who was a student in that class and pointed out a number of errors to me and to Matt Valeriote, who taught the course from this text in 1997/8 and his student, Kee Ip, who kindly corrected a few more misprints en route. I have also added some extra exercises which suggested themselves to me while I was teaching from the "first edition".

Victor Snaith
McMaster University
December 1997

Preface to the Second Edition

The second edition of this book differs from the first only by the addition of two chapters concerned with the modules over rings. In particular, Chapter Four introduces the notion of a module, imitating the classification of finitely generated abelian groups in Chapter One in order to classify finitely generated modules over a principal ideal domain. In Chapter Five, Dedekind domains are introduced and developed to the point where a classification of their finitely generated modules can be given. Chapter Five concludes with the analysis of how the primes of a Dedekind domain behave under a Galois extension of the field of fractions.

Chapters Four and Five take the reader through the first steps beyond undergraduate algebra which are essential in order to study algebraic number theory, for example. Elementary number theory is a very popular undergraduate course at the University of Southampton, which made this material particularly suitable for a graduate course given there in the Autumn of 1998 to a rather heterogeneous audience consisting of fourth year undergraduates, PhD students and staff.

Victor Snaith
University of Southampton
May 2003

Contents

Chapter 1

Group Theory

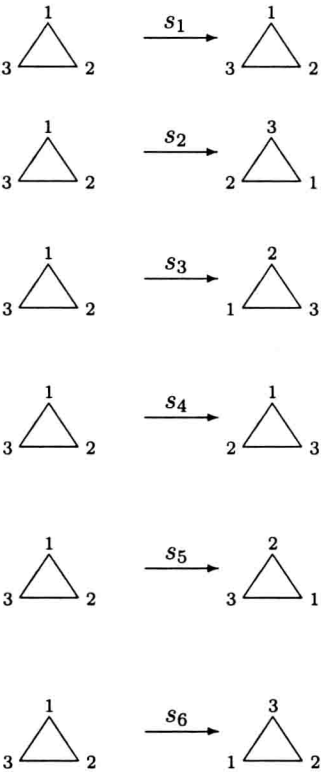
1.1 The concept of a group

The concept of a *group*, which we are about to study in considerable detail, is one of the many axiomatic structures which constitute the area of abstract algebra. As the name suggests, this collection of mathematical gadgets has arisen in response to the desire to construct algebraic abstractions of familiar phenomena. Although groups are used nowadays in a number of applications ranging from vibrations of chemical molecules to error-correcting codes, the fundamental origins of the subject arise from the algebraicisation of the notion of *symmetry*. The following examples will serve to illustrate what this algebraic abstraction is required and expected to do.

Example 1.1.1 Suppose that we are given a rigid three-dimensional solid which we will fondly call X, for brevity. Imagine X firmly implanted stably in some position; for example, X might be a regular tetrahedron resting on a table. A *symmetry of* X is any operation consisting of picking X up, juggling it around in some manner and then replacing it so as to occupy exactly the same space as before. In abstract algebra it is fashionable (and sensible) to denote things by algebraic symbols; in particular, let us denote the symmetries of X by the symbols $s_1, s_2, \ldots$.

A symmetry of X is not required to return each point of X to the place from which it started. In fact, in order to keep track of what a symmetry of X does, it is a good idea to decorate X in some manner with markers. For example, if X is an equilateral triangle we might number the vertices. Having done this, the six symmetries of the triangle, X, would look as follows:

1.1.2 *Symmetries of an equilateral triangle*



Question: Why is this list complete?

1.1.3 The symmetries of an equilateral triangle, while only a very simple example, can give us some suggestions of what an algebraic abstraction would be needed for and what it should include. Firstly, it should be capable of systematising and simplifying the description of all the possible symmetries of X. Secondly, as part of such a simplification, it should organise what happens when we take several symmetries of X and perform these operations one after another in sequence; the result must, after all, be another in the list of symmetries of X.

In the simple example of §1.1.3 this organisation and description may be accomplished by listing all the possibilities but, for a general X, this process will be prohibitively lengthy. Alternatively, we might express the same symmetry information by tabulating all the symmetries and their pairwise compositions algebraically.

In the following table the entry in the row labelled s_i and column labelled s_j is the symmetry obtained by performing first s_j and then s_i on the equilateral triangle, X, of §1.1.3.

1.1.4 *Compositions of symmetries of an equilateral triangle*

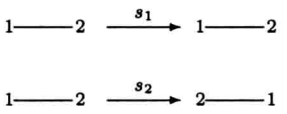
	s_1	s_2	s_3	s_4	s_5	s_6
s_1	s_1	s_2	s_3	s_4	s_5	s_6
s_2	s_2	s_3	s_1	s_5	s_6	s_4
s_3	s_3	s_1	s_2	s_6	s_4	s_5
s_4	s_4	s_6	s_5	s_1	s_3	s_2
s_5	s_5	s_4	s_6	s_2	s_1	s_3
s_6	s_6	s_5	s_4	s_3	s_2	s_1

1.1.5 Notice that the table of compositions given in §1.14 is already a considerable abstraction of the information embodied in the list of §3.1.3. For example, if this table were a little larger we might not be able to guess from it the identity of X, the equilateral triangle, having precisely six symmetries, composing according to §1.1.4.

Let us repeat the process of listing all the symmetries and tabulating their compositions for the case in which X is a line-interval and a square.

1.1.6 *Symmetries of an interval*

There are two symmetries

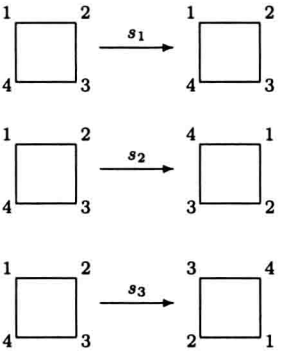


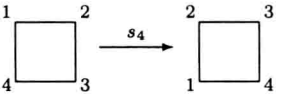
whose compositions yield the following simple table:

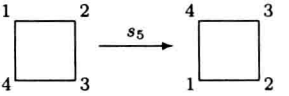
	s_1	s_2
s_1	s_1	s_2
s_2	s_2	s_1

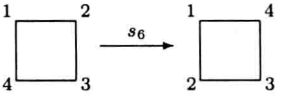
1.1.7 *Symmetries of a square*

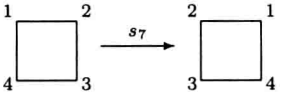
In this case there are eight symmetries.

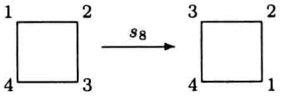












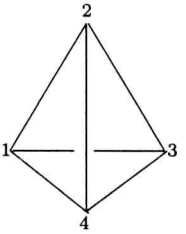
Question: Why is this list complete?
Compositions of these eight symmetries are given by the following table.

	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
s_1	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
s_2	s_2	s_3	s_4	s_1	s_6	s_7	s_8	s_5
s_3	s_3	s_4	s_1	s_2	s_7	s_8	s_5	s_6
s_4	s_4	s_1	s_2	s_3	s_8	s_5	s_6	s_7
s_5	s_5	s_8	s_7	s_6	s_1	s_4	s_3	s_2
s_6	s_6	s_5	s_8	s_7	s_2	s_1	s_4	s_3
s_7	s_7	s_6	s_5	s_8	s_3	s_2	s_1	s_4
s_8	s_8	s_7	s_6	s_5	s_4	s_3	s_2	s_1

1.1.8 *Observation*
Notice that in each of the tables of §§1.1.4, 1.1.6 and 1.1.7 the entries on each row and column are distinct. In fact, each row and column is a rearrangement (or *permutation*) of the set of all the symmetries of X.

Question: Can you explain this observation?

1.1.9 Consider now the three-dimensional example in which X is a regular tetrahedron whose four vertices are numbered.



Question: What are the symmetries of this tetrahedron?

This example is more complicated than the earlier, two-dimensional examples. However, as a first approximation to an answer, we might at least try to list some symmetries. Looking back at the examples of §§1.1.3 and 1.1.7, one sees that it can be helpful to classify the symmetries into types. For example, in the case of X being a equilateral triangle or a square, half the symmetries flip X onto its back and half of them do not.

Questions: What observations can you make about the behaviour of the 'flips' and 'non-flips' in the tables of §§1.1.4 and 1.1.7? Can you explain these observations?

In the case of the regular tetrahedron some types of symmetries which come to mind are:

(a) clockwise rotations through $\frac{2\pi}{3}$ or $\frac{4\pi}{3}$ about an axis from a vertex to the centroid of the opposite side. There are two such symmetries for each vertex, making eight rotations in all.

(b) the symmetry which leaves every point of the tetrahedron where it is. This is sometimes called *trivial symmetry.*

(c) rotations through π about an axis joining midpoints of two opposite sides. The tetrahedron has six sides but each side has precisely one opposite side, making three pairs of opposite sides in all.

The total number of symmetries listed in (a) to (c) is twelve.

Question: Are these twelve the only symmetries of the regular tetrahedron? (Hint: When studying symmetries of a polyhedron it is sometimes helpful to classify them by how many vertices, edges, etc. remain fixed under the symmetry.)

The following definition of a group is one attempt at an axiomatic algebraic structure that is abstracted from the symmetries of X and their behaviour under composition. The idea is to make an algebraic gadget whose 'multiplication' operation imitates the composing of two symmetries of X to obtain a third.

Definition 1.1.10 A *group* is a set, G, of elements (denoted by lower case letters of the alphabet — a, b, c, ...) together with a *law of composition* (often called the *multiplication* in G) which is a map

$$G \times G \longrightarrow G$$

which sends an ordered pair $(a, b) \in G \times G$ to their *product*, denoted by $ab \in G$. The multiplication in G satisfies the following axioms:

$\underline{G1}$: (Associativity)

Given any three elements belonging to G — $a, b, c \in G$, say — then

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

$\underline{G2}$: (Identity or Neutral element)

There exists an element, $e \in G$, such that $ae = a = ea$ for all $a \in G$.

$\underline{G3}$: (Inverses)

Given any $a \in G$ there exists an element $b \in G$, called the *inverse* of a, such that $ab = e = ba$. (Usually we shall write a^{-1} for the inverse of a, because it is a notationally suggestive and convienient convention.)

Axioms $G1$ - $G3$ are slightly redundant and can be replaced by the equivalent, meaner, leaner Axioms $G1, G'2, G'3$ in which $G'2$ guarantees only a "left neutral" element, e, and $G'3$ guarantees only a "left inverse" for each $a \in G$. Since these axioms are simpler to verify we shall pause to prove this result.

Lemma 1.1.11 Let G be a set with a "product", as in §1.1.10, which satisfies Axiom $G1$ and

$\underline{G'2}$: (left identity)

There exists an element, $e \in G$, such that $ea = a$ for all $a \in G$.

$\underline{G'3}$:

Given any $a \in G$ there exists an element $b \in G$ such that $ba = e$.

With these axioms, the product in G satisfies axioms $G1$ - $G3$ of §1.1.10 and G is a group.

Proof

To prove $G2$ we must show that $ae = a$ for all $a \in G$. We, at least, know that this is true for all $a = e$ since, in this case, $ee = e$, is the same equation as that of $G'2$. By $G'3$, we have $ba = e$, so that we may substitute for two of the e's in the equation $ee = e$ to obtain

$$(ba)e = ba.$$

Now choose c such that $cb = e$ (it does not matter that, with our depleted axiom scheme, we do not yet know that $c = a$.). Multiplying on

the left by c yields

$$\begin{aligned} ae &= (ea)e && \text{by } G'2 \\ &= ((cb)a)e && \text{by } G1 \\ &= (c(ba))e && \text{by } G1 \\ &= c((ba)e) && \text{by } G1 \\ &= c(ba) \\ &= (cb)a && \text{by } G1 \\ &= ea \\ &= a && \text{by } G'2. \end{aligned}$$

To verify $G3$ we must show that, if $ba = e$, then $ab = e$. Substituting for e in $eb = b$ we obtain

$$b = (ba)b = b(ab).$$

Now choose c such that $cb = e$ and multiply this equation on the left by c to obtain

$$\begin{aligned} e &= cb \\ &= c(b(ab)) \\ &= (cb)(ab) && \text{by } G1 \\ &= e(ab) \\ &= ab && \text{by } G'2 \end{aligned}$$

which completes the proof of the lemma.□

Remark 1.1.12 (i) Since the definition of §1.1.10 was intended to imitate the set of symmetries, with "multiplication" given by composition, we should verify that axioms $G1$ – $G3$ are true for this example.

Firstly, let us agree that if a and b are symmetries of X then ab is to be the symmetry given by *first performing* b and *then performing* a.

With this convention $(ab)c$ means the symmetry given by first performing c and then performing the composite symmetry called "first b then a". On the other hand, $a(bc)$ means first perform the composite "first c then b" and then follow the result by performing a. Both these recipes are long-winded ways of describing the composite symmetry "first perform c, then b and then a". Therefore the axiom $G1$ is true for the symmetries of X.

Secondly, let e denote the *trivial symmetry*, which leaves every point of X where it is. If a is any symmetry of X then the effect of the symmetry ae is first to move each point of X nowhere and then to perform a. This is merely a tortuous description of the symmetry, a. Similarly ea stands for the symmetry "first perform a and then leave every point of X where it is", which is another roundabout description of a. Therefore the axiom $G2$ is true for symmetries of X.

The verification of $G3$ for symmetries of X is connected with the observation of §1.1.8 and is easily seen in those examples in terms of the "multiplication" tables of §§1.1.4, 1.1.6 and 1.1.7. In each of those examples the row labelled by s_i contains each symmetry just once. In particular the trivial symmetry, s_1, will appear in some column; the one labelled by s_j, say. In terms of "multiplication" of symmetries this is equivalent to the equation

$$s_i s_j = s_1 = e.$$

Now, consulting the entry in the j-th row and i-th column is seen to yield the equation

$$s_j s_i = s_1 = e.$$

In these examples, this process serves to verify axiom $G3$. A closer look at these examples shows that the inverse of the symmetry, a, is nothing more than the symmetry, b, of X which takes each point of X back to the point from which a moved it. For this choice of b it is clear that ba denotes "first move points of X by a and then put them back", which is an elaborate description of the trivial symmetry under which each point of X stays where it is; that is, $ba = e$. Similarly, for this choice of b, ab denotes "take a point of X back to where a found it and then return it to its original position by a"; that is, $ab = e$.

(ii) To tabulate the table of compositions of symmetries of X, as in §§1.1.4, 1.1.6 and 1.1.7, is to tabulate the *multiplication table* of the group of symmetries of X. In general, given a group, G, and a modicum of determination we could depict the group by writing out a similar multiplication table.

(iii) In axioms $G2$ and $G3$ reference is made to *the* identity element of G and *the* inverse of $a \in G$. Before we go any further we should derive from the axioms the fact that those references to unique elements were not merely faux pas. That is, we should convince ourselves that a group does not have several neutral elements and that an element does not have several inverses.

Let us pause to record the result of the discussion of §1.1.12 (i).

Theorem 1.1.13 The set of all symmetries of X, as defined in §1.1.1, with "multiplication" given by composition in the manner of §1.1.12 (i), satisfies the axioms of a group. Henceforth this group will be referred to as the *symmetry group* of X.

Lemma 1.1.14 (i) In axiom $G2$ of §1.1.10 the neutral element is unique.

(ii) In axiom $G3$ of §1.1.10 the inverse of $a \in G$ is uniquely determined by a.