# GROUP THEORY

A Physicist's Survey

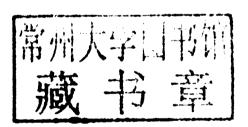
PIERRE RAMOND

# **Group Theory**

# A Physicist's Survey

## PIERRE RAMOND

Institute for Fundamental Theory, Physics Department University of Florida





# CAMBRIDGE UNIVERSITY PRESS Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521896030

© P. Ramond 2010

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2010

Printed in the United Kingdom at the University Press, Cambridge

A catalog record for this publication is available from the British Library

ISBN 978-0-521-89603-0 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party Internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

### GROUP THEORY

### A Physicist's Survey

Group theory has long been an important computational tool for physicists, but, with the advent of the Standard Model, it has become a powerful conceptual tool as well. This book introduces physicists to many of the fascinating mathematical aspects of group theory, and mathematicians to its physics applications.

Designed for advanced undergraduate and graduate students, this book gives a comprehensive overview of the main aspects of both finite and continuous group theory, with an emphasis on applications to fundamental physics. Finite groups are extensively discussed, highlighting their irreducible representations and invariants. Lie algebras, and to a lesser extent Kac–Moody algebras, are treated in detail, including Dynkin diagrams. Special emphasis is given to their representations and embeddings. The group theory underlying the Standard Model is discussed, along with its importance in model building. Applications of group theory to the classification of elementary particles are treated in detail.

PIERRE RAMOND is Distinguished Professor of Physics at the University of Florida and Director of the Institute for Fundamental Theory. He has held positions at FermiLab, Yale University and Caltech. He has made seminal contributions to supersymmetry, superstring theory and the theory of neutrino masses, and is a Member of the American Academy of Arts & Sciences.

To Richard Slansky Who would have written this book

# Contents

1	Preia	ice: the j	pursuit of symmetries	page 1
2	Finite groups: an introduction		4	
	2.1	Group	5	
	2.2	Finite	6	
	2.3	Permu	ntations	19
	2.4	Basic	concepts	22
		2.4.1	Conjugation	22
		2.4.2	Simple groups	25
		2.4.3	Sylow's criteria	27
		2.4.4	Semi-direct product	28
		2.4.5	Young Tableaux	31
3	Finite groups: representations			33
	3.1	1 Introduction		33
	3.2	Schur's lemmas		35
	3.3	The $\mathcal A$	41	
	3.4	as section of the sec		44
	3.5	Real a	nd complex representations	46
	3.6	Embed	ddings	48
	3.7	$\mathcal{Z}_n$ cha	52	
	3.8	$\mathcal{D}_n$ cha	53	
	3.9	$Q_{2n}$ ch	naracter table	56
	3.10	Some	semi-direct products	58
	3.11	1 Induced representations		61
	3.12	2. Invariants		64
	3.13	Coveri	ngs	67
4	Hilbe	ert space	S	69
	4.1	Finite 1	Hilbert spaces	69

viii Contents

	4.2	Fermi oscillators	70	
	4.3	Infinite Hilbert spaces	72	
5	SU(	78		
	5.1	Introduction	78	
	5.2	Some representations	82	
	5.3	From Lie algebras to Lie groups	86	
	5.4	$SU(2) \rightarrow SU(1,1)$	89	
	5.5	Selected $SU(2)$ applications	93	
		5.5.1 The isotropic harmonic oscillator	93	
		5.5.2 The Bohr atom	95	
		5.5.3 Isotopic spin	99	
6	SU(	(3)	102	
	6.1	SU(3) algebra	102	
	6.2	$\alpha$ -Basis	106	
	6.3	$\omega$ -Basis	107	
	6.4	$\alpha'$ -Basis	108	
	6.5	The triplet representation	110	
	6.6	The Chevalley basis	112	
	6.7	SU(3) in physics	114	
		6.7.1 The isotropic harmonic oscillator redux	114	
		6.7.2 The Elliott model	115	
		6.7.3 The Sakata model	117	
		6.7.4 The Eightfold Way	118	
7	Class	123		
	7.1			
	7.2	Simple roots	129	
	7.3	Rank-two algebras	131	
	7.4	Dynkin diagrams	134	
	7.5 Orthonormal bases		140	
8	Lie a	143		
	8.1	Representation basics	143	
	8.2	$A_3$ fundamentals	144	
	8.3	The Weyl group	149	
	8.4	Orthogonal Lie algebras	151	
	8.5	Spinor representations	153	
		8.5.1 $SO(2n)$ spinors	154	
		8.5.2 $SO(2n+1)$ spinors	156	
		8.5.3 Clifford algebra construction	159	
	8.6	Casimir invariants and Dynkin indices	164	
	8.7	Embeddings	168	

Contents	iX

	8.8	Oscillator representations	178
	8.9	Verma modules	180
		8.9.1 Weyl dimension formula	187
		8.9.2 Verma basis	188
9	Finite	e groups: the road to simplicity	190
	9.1	Matrices over Galois fields	192
		9.1.1 $\mathcal{PSL}_2(7)$	197
		9.1.2 A doubly transitive group	198
	9.2	Chevalley groups	201
	9.3	A fleeting glimpse at the sporadic groups	205
10	Beyo	nd Lie algebras	208
	10.1	Serre presentation	208
	10.2	Affine Kac–Moody algebras	210
	10.3	Super algebras	216
11	The g	groups of the Standard Model	221
	11.1	Space-time symmetries	222
		11.1.1 The Lorentz and Poincaré groups	223
		11.1.2 The conformal group	231
	11.2	Beyond space-time symmetries	235
		11.2.1 Color and the quark model	239
	11.3	Invariant Lagrangians	240
	11.4	Non-Abelian gauge theories	243
	11.5	The Standard Model	244
	11.6	Grand Unification	246
	11.7	Possible family symmetries	249
		11.7.1 Finite $SU(2)$ and $SO(3)$ subgroups	249
		11.7.2 Finite $SU(3)$ subgroups	252
12	Exce	ptional structures	254
	12.1	Hurwitz algebras	254
	12.2	Matrices over Hurwitz algebras	257
	12.3	The Magic Square	259
	Appe	ndix 1 Properties of some finite groups	265
		ndix 2 Properties of selected Lie algebras	277
	Refer	ences	307
	Index		308

# Preface: the pursuit of symmetries

Symmetric objects are so singular in the natural world that our ancestors must have noticed them very early. Indeed, symmetrical structures were given special magical status. The Greeks' obsession with geometrical shapes led them to the enumeration of platonic solids, and to adorn their edifices with various symmetrical patterns. In the ancient world, symmetry was synonymous with perfection. What could be better than a circle or a sphere? The Sun and the planets were supposed to circle the Earth. It took a long time to get to the apparently less than perfect ellipses!

Of course most shapes in the natural world display little or no symmetry, but many are almost symmetric. An orange is close to a perfect sphere; humans are almost symmetric about their vertical axis, but not quite, and ancient man must have been aware of this. Could this lack of exact symmetry have been viewed as a sign of imperfection, imperfection that humans need to atone for?

It must have been clear that highly symmetric objects were special, but it is a curious fact that the mathematical structures which generate symmetrical patterns were not systematically studied until the nineteenth century. That is not to say that symmetry patterns were unknown or neglected, witness the Moors in Spain who displayed the seventeen different ways to tile a plane on the walls of their palaces!

Évariste Galois in his study of the roots of polynomials of degree larger than four, equated the problem to that of a set of substitutions which form that mathematical structure we call a group. In physics, the study of crystals elicited wonderfully regular patterns which were described in terms of their symmetries. In the twentieth century, with the advent of Quantum Mechanics, symmetries have assumed a central role in the study of Nature.

The importance of symmetries is reinforced by the Standard Model of elementary particle physics, which indicates that Nature displays more symmetries in the small than in the large. In cosmological terms, this means that our Universe emerged from the Big Bang as a highly symmetrical structure, although most of its symmetries are no longer evident today. Like an ancient piece of pottery, some

of its parts may not have survived the eons, leaving us today with its shards. This is a very pleasing concept that resonates with the old Greek ideal of perfection. Did our Universe emerge at the Big Bang with perfect symmetry that was progressively shattered by cosmological evolution, or was it born with internal defects that generated the breaking of its symmetries? It is a profound question which some physicists try to answer today by using conceptual models of a perfectly symmetric universe, e.g. superstrings.

Some symmetries of the natural world are so commonplace, that they are difficult to identify. The outcome of an experiment performed by undergraduates should not depend on the time and location of the bench on which it was performed. Their results should be impervious to shifts in time and space, as consequences of time and space translation invariances, respectively. But there are more subtle manifestations of symmetries. The great Galileo Galilei made something of a "trivial" observation: when your ship glides on a smooth sea with a steady wind, you can close your eyes and not "feel" that you are moving. Better yet, you can perform experiments whose outcomes are the same as if you were standing still! Today, you can leave your glass of wine while on an airplane at cruising altitude without fear of spilling. The great genius that he was elevated this to his principle of relativity: the laws of physics do not depend on whether you are at rest or move with constant velocity! However, if the velocity changes, you can feel it (a little turbulence will spill your wine). Our experience of the everyday world appears complicated by the fact that it is dominated by frictional forces; in a situation where their effect can be neglected, simplicity and symmetries (in some sense analogous concepts) are revealed.

According to Quantum Mechanics, physics takes place in Hilbert spaces. Bizarre as this notion might be, we have learned to live with it as it continues to be verified whenever experimentally tested. Surely, this abstract identification of a physical system with a state vector in Hilbert space will eventually be found to be incomplete, but in a presently unimaginable way, which will involve some other weird mathematical structure. That Nature uses the same mathematical structures invented by mathematicians is a profound mystery hinting at the way our brains are wired. Whatever the root cause, mathematical structures which find natural representations in Hilbert spaces have assumed enormous physical interest. Prominent among them are *groups* which, subject to specific axioms, describe transformations in these spaces.

Since physicists are mainly interested in how groups operate in Hilbert spaces, we will focus mostly on the study of their representations. Mathematical concepts will be introduced as we go along in the form of *scholia* sprinkled throughout the text. Our approach will be short on proofs, which can be found in many excellent textbooks. From representations, we will focus on their products and show how

to build group invariants for possible physical applications. We will also discuss the embeddings of the representations of a subgroup inside those of the group. Numerous tables will be included.

This book begins with the study of *finite* groups, which as the name indicates, have a finite number of symmetry operations. The smallest finite group has only two elements, but there is no limit as to their number of elements: the permutations on n letters form a finite group with n! elements. Finite groups have found numerous applications in physics, mostly in crystallography and in the behavior of new materials. In elementary particle physics, only small finite groups have found applications, but in a world with extra dimensions, and three mysterious families of elementary particles, this situation is bound to change. Notably, the sporadic groups, an exceptional set of twenty-six finite groups, stand mostly as mathematical curiosities waiting for an application.

We then consider *continuous* symmetry transformations, such as rotations by arbitrary angles, or open-ended time translation, to name a few. Continuous transformations can be thought of as repeated applications of infinitesimal steps, stemming from generators. Typically these generators form algebraic structures called Lie algebras. Our approach will be to present the simplest continuous groups and their associated Lie algebras, and build from them to the more complicated cases. Lie algebras will be treated à *la Dynkin*, using both Dynkin notation and diagrams. Special attention will be devoted to exceptional groups and their representations. In particular, the Magic Square will be discussed. We will link back to finite groups, as most can be understood as subgroups of continuous groups.

Some non-compact symmetries are discussed, especially the representations of space-time symmetries, such as the Poincaré and conformal groups. Group-theoretic aspects of the Standard Model and Grand Unification are presented as well. The algebraic construction of the five exceptional Lie algebras is treated in detail. Two generalizations of Lie algebras are also discussed, super-Lie algebras and their classification, and infinite-dimensional affine Kac–Moody algebras.

I would like to express my gratitude to the Institute for Advanced Study and the Aspen Center for Physics for their hospitality, where a good part of this book was written. I would like to thank Professors L. Brink and J. Patera, as well as Drs. D. Belyaev, Sung-Soo Kim, and C. Luhn, for their critical reading of the manuscript, and many useful suggestions. Finally, I owe much to my wife Lillian, whose patience, encouragements, and understanding made this book possible.

# Finite groups: an introduction

Symmetry operations can be discrete or continuous. Easiest to describe are the discrete symmetry transformations. In this chapter we lay out notation and introduce basic concepts in the context of finite groups of low order. The simplest symmetry operation is *reflection* (parity):

$$P: x \rightarrow x' = -x.$$

Doing it twice produces the identity transformation

$$I: x \rightarrow x' = x$$

symbolically

$$PP = I$$
.

There are many manifestations of this symmetry operation. Consider the isosceles triangle. It is left the same by a reflection about its vertical axis. In geometry this operation is often denoted as  $\sigma$ . It takes place in the x-y plane, and you will see it written as  $\sigma_z$  which denotes a reflection in the x-y plane.

The second simplest symmetry operation is *rotation*. In two dimensions, it is performed about a point, but in three dimensions it is performed about an axis. A square is clearly left invariant by an anti-clockwise rotation about its center by 90°. The inverse operation is a clockwise rotation. Four such rotations are akin to the identity operation. Generally, anti-clockwise rotations by  $(2\pi/n)$  generate the cyclic group  $\mathbb{Z}_n$  when n is an integer. Repeated application of n such rotations is the identity operation. It is only in two dimensions that a reflection is a 180° rotation.

A third symmetry operation is *inversion* about a point, denoted by i. Geometrically, it involves a reflection about a plane together with a  $180^{\circ}$  rotation in the plane. Symbolically

$$i = \sigma_h \operatorname{Rot}(180^\circ).$$

Reflections and inversions are sometimes referred to as *improper* rotations. They are rotations since they require a center of symmetry.

The symmetry operations which leave a given physical system or shape invariant must satisfy a number of properties: (1) a symmetry operation followed by another must be itself a symmetry operation; (2) although the order in which the symmetry operations are performed is important, the symmetry operations must associate; (3) there must be an identity transformation, which does nothing; and (4) whatever operation transforms a shape into itself, must have an inverse operation. These intuitive considerations lead to the group axioms.

### 2.1 Group axioms

A group  $\mathcal{G}$  is a collection of operators,

$$\mathcal{G}: \{a_1, a_2, \ldots, a_k, \ldots\}$$

with a "\*" operation with the following properties.

**Closure**. For every ordered pair of elements,  $a_i$  and  $a_j$ , there exists a unique element

$$a_i \star a_j = a_k, \tag{2.1}$$

for any three i, j, k.

Associativity. The ★ operation is associative

$$(a_i \star a_i) \star a_k = a_i \star (a_i \star a_k). \tag{2.2}$$

**Unit element.** The set  $\mathcal{G}$  contains a unique element e such that

$$e \star a_i = a_i \star e = a_i, \tag{2.3}$$

for all i. In particular, this means that

$$e \star e = e$$
.

**Inverse element**. Corresponding to every element  $a_i$ , there exists a unique element of  $\mathcal{G}$ , the inverse  $(a_i)^{-1}$  such that

$$a_i \star (a_i)^{-1} = (a_i)^{-1} \star a_i = e.$$
 (2.4)

When  $\mathcal{G}$  contains a finite number of elements

$$(\mathcal{G}: a_1, a_2, \ldots, a_k, \ldots, a_n)$$

it is called a finite group, and n is called the *order* of the group.

In the following we will discuss groups with a finite number of elements, but we should note that there are many examples of groups with an infinite number of elements; we now name a few.

• The real numbers, including zero, constitute an infinite group under addition  $(\star \to +)$ . Its elements are the zero, the positive and the negative real numbers. Closure is satisfied: if x and y are real numbers, so is their sum x + y. Each x has an inverse -x, such that

$$x + (-x) = 0,$$
  $x + 0 = 0 + x,$ 

and we see that the zero plays the role of the unit element.

- The real numbers also form a group under multiplication ( $\star \to \times$ ). Indeed xy is a real number. The inverse of x is 1/x, and the unit element is 1. In this case, zero is excluded.
- The rational numbers of the form  $\frac{n}{m}$ , where m and n are non-zero integers also form a group under multiplication, as can easily be checked.

# 2.2 Finite groups of low order

We begin by discussing the finite groups of order less than thirteen (see Ledermann [14]). In the process we will introduce much notation, acquaint ourselves with many useful mathematical concepts, and be introduced to several ubiquitous groups and to the different aspects of their realizations.

# Group of order 2

We have already encountered the unique group, called  $\mathcal{Z}_2$ , with two elements. One element is the identity operation, e, and the second element a must be its own inverse, leading to the following multiplication table.

$\mathcal{Z}_{2}$	e	a
e	e	а
a	a	e

It can serve many functions, depending on the physical situation: a can be the parity operation, the reflection about an axis, a  $180^{\circ}$  rotation, etc.

### Group of order 3

There is only one group of order 3. This is easy to see: one element is the identity e. Let  $a_1$  be its second element. The group element  $a_1 \star a_1$  must be the third element of the group. Otherwise  $a_1 \star a_1 = a_1$  leads to  $a_1 = e$ , or the second possibility  $a_1 \star a_1 = e$  closes the group to only two elements. Hence it must be that  $a_1 \star a_1 = a_2$ , the third element, so that  $a_1 \star a_2 = a_2 \star a_1$ . It is  $\mathcal{Z}_3$ , the *cyclic group* of order three, defined by its multiplication table.

$\mathcal{Z}_3$	e	$a_1$	$a_2$
e	e	$a_1$	$a_2$
$a_1$	$a_1$	$a_2$	e
$a_2$	$a_2$	e	$a_1$

It follows that

$$a_1 \star a_1 \star a_1 = e$$
,

which means that  $a_1$  is an element of *order* three, and represents a 120° rotation.

It should be obvious that these generalize to arbitrary n,  $\mathcal{Z}_n$ , the cyclic group of order n. It is generated by the repeated action of one element a of order n

$$\mathcal{Z}_n$$
: { $e, a, a \star a, a \star a \star a, \ldots, (a \star a \star \cdots a \star a)_{n-1}$ },

with

$$(a \star a \star \cdots a \star a)_{\iota} \equiv a^{\iota}, \qquad a^{\iota} = e.$$

If we write its different elements as  $a_j = a^{j-1}$ , we deduce that  $a_i \star a_j = a_j \star a_i$ . A group for which any two of its elements commute with one another is called *Abelian*. Groups which do not have this property are called *non-Abelian*.

### Groups of order 4

It is equally easy to construct all possible groups with four elements  $\{e, a_1, a_2, a_3\}$ . There are only two possibilities.

The first is our friend  $\mathcal{Z}_4$ , the cyclic group of order four, generated by 90° rotations. We note that the generator of this cyclic group has the amusing realization

$$a: \quad z \to z' = i z, \tag{2.5}$$

where z is a complex number. It is easy to see that a is an element of order four that generates  $\mathcal{Z}_4$ .

The second group of order four, is the *dihedral group*  $\mathcal{D}_2$ , with the following multiplication table.

$\mathcal{D}_{2}$	e	$a_1$	$a_2$	аз
e	e	$a_1$	$a_2$	$a_3$
$a_1$	$a_1$	e	$a_3$	$a_2$
$a_2$	$a_2$	$a_3$	e	$a_1$
$a_3$	$a_3$	$a_2$	$a_1$	e

It is Abelian, since the multiplication table is symmetrical about its diagonal. It is sometimes called *V* (*Vierergruppe*) or Klein's four-group.

It is the first of an infinite family of groups called the dihedral groups of order 2n,  $\mathcal{D}_n$ . They have the simple geometrical interpretation of mapping a plane polygon with n vertices into itself. The case n=2 corresponds to the invariance group of a line: a line is left invariant by two 180° rotations about its midpoint, one about the axis perpendicular to the plane of the line, the other about the axis in the plane of the line. It is trivially invariant under a rotation about the line itself. The multiplication table shows three elements of order two, corresponding to these three 180° rotations about any three orthogonal axes in three dimensions. It has many other realizations, for instance in terms of  $(2 \times 2)$  matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.6}$$

An interesting realization involves functional dependence. Consider the four mappings (functions)

$$f_1(x) = x$$
,  $f_2(x) = -x$ ,  $f_3(x) = \frac{1}{x}$ ,  $f_4(x) = -\frac{1}{x}$ . (2.7)

It is easily verified that they close on  $\mathcal{D}_2$ . These two groups are distinct since  $\mathcal{Z}_4$  has an element of order four and  $\mathcal{D}_2$  does not.

Groups of order four share one feature that we have not yet encountered: a subset of their elements forms a group, in this case  $\mathcal{Z}_2$ . The subgroup within  $\mathcal{Z}_4$  is  $\mathcal{Z}_2$ , generated by  $(e, a^2)$ , expressed as

$$\mathcal{Z}_4 \supset \mathcal{Z}_2$$
.

As for  $\mathcal{D}_2$ , it contains three  $\mathcal{Z}_2$  subgroups, generated by  $(e, a_1)$ ,  $(e, a_2)$ , and  $(e, a_3)$ , respectively. Since  $a_2 \star a_1 = a_1 \star a_2$ , the elements of the first two  $\mathcal{Z}_2$  commute with one another, and we can express  $\mathcal{D}_2$  as the *direct product* of the first two commuting subgroups

$$\mathcal{D}_2 = \mathcal{Z}_2 \times \mathcal{Z}_2. \tag{2.8}$$

This is the first and simplest example of a general mathematical construction.

Scholium. Direct product

Let  $\mathcal{G}$  and  $\mathcal{K}$  be two groups with elements  $\{g_a\}$ ,  $a=1,\ldots,n_g$  and  $\{k_i\}$ ,  $i=1,\ldots,n_k$ , respectively. We assemble new elements  $(g_a,k_i)$ , with multiplication rule

$$(g_a, k_i)(g_b, k_j) = (g_a \star g_b, k_i \star k_j).$$
 (2.9)

They clearly satisfy the group axioms, forming a group of order  $n_g n_k$  called the direct (Kronecker) product group  $\mathcal{G} \times \mathcal{K}$ . Since  $\mathcal{G}$  and  $\mathcal{K}$  operate in different spaces,

they can always be taken to be commuting subgroups, and the elements of the direct product can be written simply as  $g_a k_i$ . This construction provides a simple way to generate new groups of higher order.

Scholium. Lagrange's theorem

This theorem addresses the conditions for the existence of subgroups. Consider a group  $\mathcal{G}$  with elements  $\{g_a\}$ ,  $a=1, 2, \ldots, N$ , that contains a subgroup  $\mathcal{H}$  with n elements  $(h_1, h_2, \ldots, h_n) \equiv \{h_i\}$ ,  $i=1, 2, \ldots, n < N$ ,

$$\mathcal{G}\supset\mathcal{H}.$$

Pick an element  $g_1$  of  $\mathcal{G}$  that is not in the subgroup  $\mathcal{H}$ . The n elements of the form  $g_1 \star h_i$  are of course elements of  $\mathcal{G}$ , but *not* of the subgroup  $\mathcal{H}$ . If any of them were in  $\mathcal{H}$ , we would have for some i and j

$$g_1 \star h_i = h_j$$

but this would imply that

$$g_1 = h_i \star (h_i)^{-1}$$

is an element of  $\mathcal{H}$ , contradicting our hypothesis: the two sets  $\{h_i\}$  and  $\{g_1 \star h_i\}$  have no element in common. Now we repeat the procedure with another element of  $\mathcal{G}$ ,  $g_2$ , not in  $\mathcal{H}$ , nor in  $g_1\mathcal{H}$ . The new set  $\{g_2 \star h_i\}$  is distinct from both  $\{h_i\}$  and  $\{g_1 \star h_i\}$ , for if they overlap, we would have for some i and j

$$g_1 \star h_i = g_2 \star h_i$$
.

This would in turn imply that  $g_2 = g_1 \star h_k$ , contradicting our hypothesis. We proceed in this way until we run out of group elements after forming the last set  $\{g_k \star h_i\}$ . Hence we can write the full  $\mathcal{G}$  as a (right) coset decomposition

$$\mathcal{G} = \{h_i\} + \{g_1 \star h_i\} + \dots + \{g_k \star h_i\}$$
  

$$\equiv \mathcal{H} + g_1 \star \mathcal{H} + \dots + g_k \star \mathcal{H}, \qquad (2.10)$$

in which none of the sets overlap: the order of  $\mathcal{G}$  must therefore be a multiple of the order of its subgroup. Hence we have Lagrange's theorem.

If a group G of order N has a subgroup H of order n, then N is necessarily an integer multiple of n

The integer ratio k = N/n is called the *index* of  $\mathcal{H}$  in  $\mathcal{G}$ . This theorem is about to save us a lot of work.