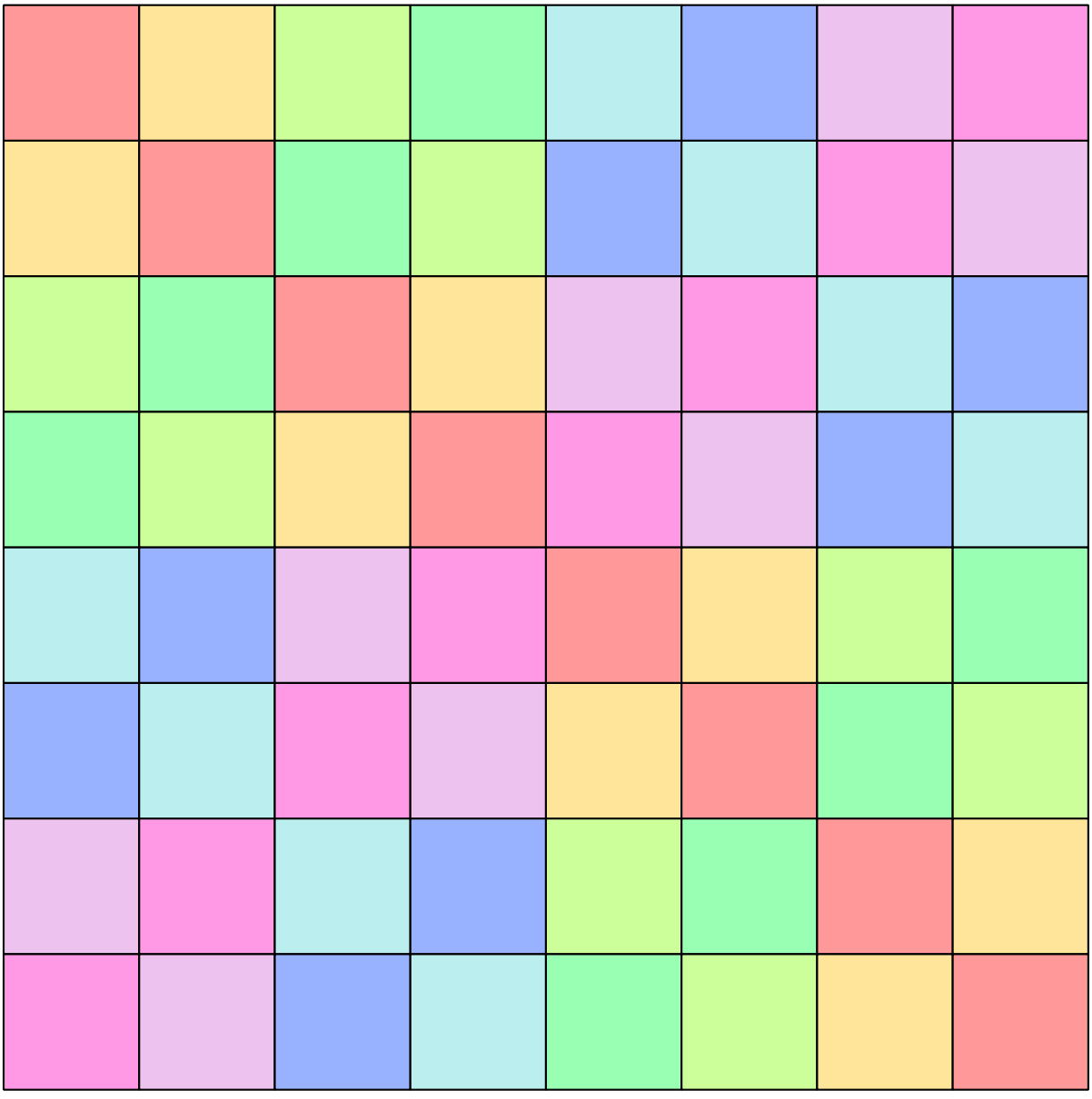
University Undergraduate Lectures in Mathematics
A First Year Course

GROUP THEORY

The Mathematics of Symmetry



G R O U P T H E O R Y II

Lecture 1

University Undergraduate Lectures in Mathematics
A First Year Course
Group Theory II

1.1 Introduction

Welcome to Group Theory II, designed to follow on from Group Theory I. There, the focus was on getting an initial feel for the subject. With several key ideas now in place attention shifts to developing slicker notation, and exploring the structure of groups in a more abstract manner. There will still be much that is "hands on". Group Theory II assumes the knowledge of Group Theory I, along with topics taught during a first year at University, such as Matrices and Complex Numbers. Should there be a wish to revisit the earlier ideas, they are presented at;

- Group Theory I : http://www.NumberWonder.co.uk/Pages/Page9108.html

Any reader is welcome to contact me for a set of answers to any exercise in either Group Theory I or II: Martin Hansen : mhh@shrewsbury.org.uk

1.2 Axioms

Four axioms define exactly what a group is;

The Definition of a Group

If G is a set and $\circ$ is a binary operation defined on G, then $(G, \circ)$ is a group if the following four axioms hold:

- **Closure:** For all $g_1, g_2 \in G$, $g_1 \circ g_2 \in G$
- **Identity:** There exists an identity element $e \in G$.
  This is such that, for all $g \in G$, $g \circ e = g = e * g$
- **Inverses:** For each $g \in G$, there exists an inverse element $g^{-1} \in G$
  This is such that $g \circ g^{-1} = e = g^{-1} \circ g$
- **Associativity:** For all $g_1, g_2, g_3 \in G$, $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

Two immediate consequences are that,

- A group can have one, and only one, identity element.
- Each element has one, and only one, inverse.

An Abelian Group

A group is described as being Abelian if the binary operation is commutative.

In other words, if, for all $g_1, g_2 \in G$, $g_1 \circ g_2 = g_2 \circ g_1$

1.3 Subgroups

A subgroup is a group within a group.
A subgroup must inherit the identity element from the parent group and for every other element that is inherited, the inverse of that element must also be inherited.
All groups, *G*, have two "trivial" subgroups, one containing only the identity {e} and the other being a full copy of the group itself.
Subgroups that are not trivial, if any exist, are termed "proper" subgroups.

The Definition and Identification of a Subgroup

A subgroup of a group $(G, \circ)$ is a group $(H, \circ)$ where H is a subset of G.
To show a subset H is a subgroup of G, show the following axioms hold;

- **Closure:** For all $h_1, h_2 \in H$, the composite $h_1 \circ h_2 \in H$
- **Identity:** The identity element, $e_G \in H$
- **Inverses:** For each $h \in H$, the inverse $h^{-1} \in H$

1.4 Order and Generators

The order of a group $(G, \circ)$ is simply the number of elements in the set G.
For example, if $G = \{e, a, c\}$ then $|G| = n\{e, a, c\} = 3$
Each element of a group also has an order associated with it.
To explain how this is determined, first note that, for example, $x \circ x = x^2$ and that, in general,

$$\underbrace{x \circ x \circ x \circ \ldots \circ x}_{k \text{ of these}} = x^k$$

Let x be an element of a finite group G, and let k be the least positive integer such that $x^k = e$. Then the order of the element x is k.

The strategy to find the order k of the element x in the finite group G is to determine the following sequence of composites,

$$x, x^2, x^3, \ldots$$

until an integer k is reached such that $x^k = e$
Then the order of x is k
Furthermore, the sequence of composites will form a (cyclic) subgroup.
It is said that the element x has generated this subgroup and the notation used is,

$$\langle x \rangle = \{e, x^2, x^3, \ldots, x^{k-1}\} \text{ where } x^k = e$$

All cyclic subgroups of a group can be found by using, in turn, each elements of the group as a generator. Non-cyclic subgroups will not be found, however.

1.5 Cyclic Groups

Definition of a Cyclic Group

A group G of finite order k is cyclic if it contains an element x such that,

$G = \{e, x, x^2, x^3, \ldots, x^{k-1}\}$ where $x^k = e$ (e is the identity element)

- In any group, an element and its inverse generate the same cyclic group.
- A group of order p, where p is prime, is cyclic.

1.6 Cayley Tables

Given a group $(G, \circ)$ a Cayley Table shows all possible compositions of the elements of the set G. For example, the set $G = \{1, 9, 11\}$ under the binary operation multiplication modulo 14 has the following Cayley table;

$\times_{14}$	1	9	11
1	1	9	11
9	9	11	1
11	11	1	9

1.7 The Latin Square Property

All Cayley Tables have The Latin Square Property.

When the group $(G, \circ)$ is presented as a Cayley table each element occurs

- once and once only in each row
- once and once only in each column

Although all groups when presented as a Cayley table have the Latin square property not all Latin Squares are groups.

1.8 Lagrange's Theorem

When searching for subgroups of a given group, Lagrange's Theorem provides information on the possible orders of the subgroups.

Lagrange's Theorem

If H is a subgroup of a finite group G, the order of H divides the order of G.

- It is also of use to know that the order of an element in a group G must likewise divide the order of G.

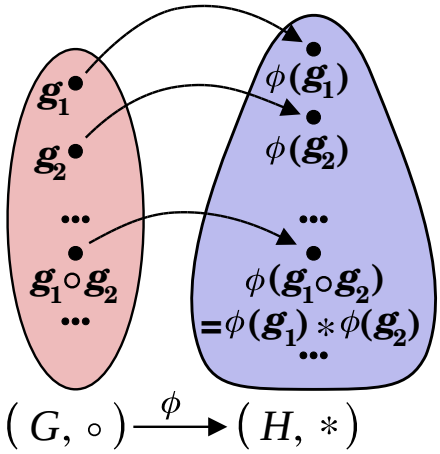
1.9 Isomorphic Groups

Two groups that are isomorphic have the same underlying structure.

Definition of Isomorphism

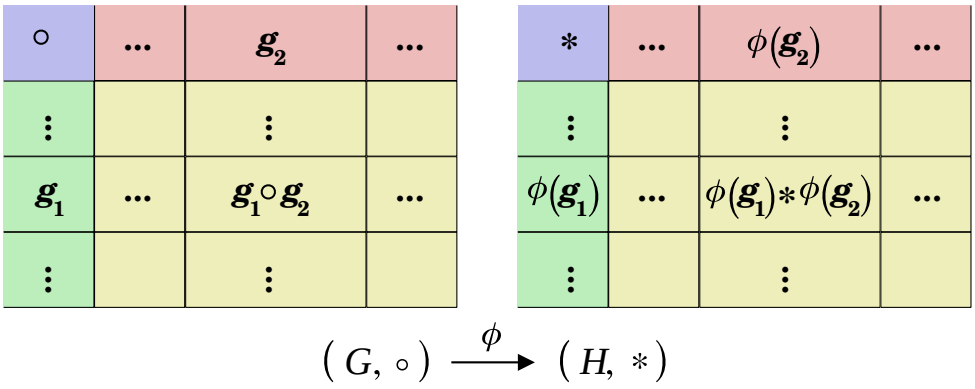
Two groups $(G, \circ)$ and $(H, *)$ are isomorphic, written $G \cong H$, if there exists a mapping ϕ: $G \to H$ such that both of the following statements hold;

- ϕ is one-to-one onto
- For all $g_1,\ g_2 \in G,\ \phi(g_1 \circ g_2) = \phi(g_1) * \phi(g_2)$



It is said that "group isomorphisms preserve identities, inverses, and the order of the groups and subgroups involved". These are all a consequence of the structure preserving relationship, that $\phi(g_1 \circ g_2) = \phi(g_1) * \phi(g_2)$. This key piece of algebra states that "The image of the composite is the composite of the images".

This can be pictured for two general finite groups as follows;



Some consequences of the definition of isomorphism are:

If $(G, \circ)$ and $(H, \circ)$ are isomorphic groups with identity elements e_G and e_H respectively, and ϕ: $G \to H$ is an isomorphism from G to H then, for all $g \in G$ and integer values of k,

- $\phi(e_G) = e_H$ identity preserved
- $\phi(g^{-1}) = (\phi(g))^{-1}$ inverses preserved
- $\phi(g^k) = (\phi(g))^k$ orders of elements preserved
- $|G| = |H|$ order of group is preserved
- If G has n elements of order k, so does H
- If G has n subgroups of order k, so does H
- If J is a subgroup of G, then H has a subgroup isomorphic to J

- For groups of order 16 or greater, it is possible to find non-isomorphic groups with exactly the same number of elements of each order.
- A group of order p, for p prime, is isomorphic to the cyclic group of order p.

1.10 Example

Provide an axiomatic proof that the inverse of each element of a group is unique.

Teaching Video: http://www.NumberWonder.co.uk/v9110/1.mp4

[4 marks]

Having proven that each element, g, of a group, G, has a unique inverse it makes sense to talk of **the** inverse of an element.

The unique inverse of an element g is written g^{-1}

1.11 Exercise

Marks Available: 60

Question 1

Here is the first half of a proof that all Cayley group tables are Latin squares.

It begins with the assumption that there exists a row in a group's Cayley table in which the same element occurs twice.
So, given two distinct elements, x and y, in row a the situation is;

$\circ$	...	x	...	y	...
...	...	...	...	...	...
a	...	$a \circ x$	...	$a \circ y$	...
...	...	...	...	...	...

Under the assumption that the same element occurs twice,

$$a \circ x = a \circ y$$

$$a^{-1} \circ (a \circ x) = a^{-1} \circ (a \circ y) \quad \text{Pre-multiply both sides}$$

$$(a^{-1} \circ a) \circ x = (a^{-1} \circ a) \circ y \quad \text{(Associativity)}$$

$$e \circ x = e \circ y \quad \text{(Inverses)}$$

$$x = y \quad \text{(Identity)}$$

But this contradicts the starting assumption that x and y are distinct elements.
$\therefore$ the same element cannot occur twice in any row in a group Cayley table.

Complete the proof by showing that an element cannot occur twice in any column.

[4 marks]

Question 2

Provide an axiomatic proof that the identity element of a group is unique.

[4 marks]

Question 3

If x and y are elements of a group, prove that $(xy)^{-1} = y^{-1}x^{-1}$

[5 marks]

Question 4

An Abelian group $(G, \circ)$ contains elements a and b such that a is self-inverse and b is self-inverse. Prove that $a \circ b$ is also self inverse.
You may use the result proven in Question 3 if you wish.

[5 marks]

Question 5

If x, y are elements of a group G, and if all three of x, y, xy have order 2, prove that the group is Abelian.

[5 marks]

Question 6

Prove that, for a group of order 10, every proper subgroup must be cyclic.

[3 marks]

Question 7

Suppose that a, b are elements of a group and that $a^5 = e,\ b^4 = e,\ ab = b\,a^3$

Prove that,

(i) $a^2 b = ba$

[5 marks]

(ii) $a\,b^3 = b^3 a^2$

[5 marks]

Question 8

Further A-Level Examination Question from June 2018, FP3, Option 4, (OCR)

You are given that the set {1, 2, 4, 7, 8, 11, 13, 14} together with the binary operation of multiplication modulo 15 forms a group G.

(i) Find the order of each element of G.

[4 marks]

(ii) A subgroup of G has order n.
Write down the possible values of n.

[2 marks]

(iii) State all the proper cyclic subgroups of G

[4 marks]

(iv) For each of the following three cases, determine whether the set together with the binary operation forms a group. If the set does form a group, state whether or not it is isomorphic to *G*, justifying your answer. (You may assume associativity in each case)

(a) The set {0, 1, 2, 3, 4, 5, 6, 7} under addition modulo 8

(b) The set {1, 2, 3, 4, 5, 6, 7, 8} under multiplication modulo 9

(c) The set of matrices,

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

together with the binary operation of matrix multiplication
(You may assume that the set is closed under matrix multiplication)

[14 marks]