5 Simple Properties of Groups

5.1 Introduction

Now we are starting to gain an understanding of what a group is, it is useful to look at some of their properties which can be proved very easily. We are already familiar with the 4 group axioms and know that if a group is also commutative it is called an Abelian group.

Our original definition used the clumsy notation of G(*) with e as identity and $\bar{a}$ as inverse.

group	G(*)	G(.)	G(+)
	$a*b$	ab	$a+b$
identity	e	1	0
inverse	$\bar{a}$	a^{-1}	$-a$
	$a*a*a*a*a.....*a$	a^{n}	na

We shall in future adopt the multiplicative notation when speaking about groups in general. However when dealing with a specific example we shall use whatever is the most appropriate symbol for the binary operation of that group.

You may also notice when you read other texts that instead of referring to a group as G(.), it is referred to as (G, .); for example $\mathbf{Z}_5(\oplus)$ may be referred to as $(\mathbf{Z}_5 , \oplus)$

5.2 Theorems relating to Groups

We shall now prove some general results about groups. Note that as so many objects and operations can form groups, in order to make sure that anything we prove is true for **all** groups, we must make sure that we only assume properties that we already know are true for **all** groups. At present this is not very much, just the four group axioms in fact. But as we prove a few general results we shall be able to use them to prove other results.

Theorem 5.2.1 Cancellation Law

If G(.) is a group and a, b and $c \in$ G then $ab = ac \quad \Rightarrow \quad b = c$

Proof

$a \in G \quad \Rightarrow \quad a^{-1} \in G$ (iv)

So $ab = ac$

$\Rightarrow \quad a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow \quad (a^{-1}a)\,b = (a^{-1}a)\,c$ (ii)

$\Rightarrow \quad 1\,b = 1\,c$ (iv)

$\Rightarrow \quad b = c$ (iii)

•

Note the above theorem tells us that all entries in any row of the group table are distinct. This means that every row must contain every group element exactly once

	b	c
a	ab	ac

A similar result $ba = ca \Rightarrow b = c$ tells us that all the elements in any column are distinct and so each column must also contain all group elements exactly once.

Theorem 5.2.2

If G(.) is a group and a and $b \in$ G then a) $ax = b$ has a unique solution $x = a^{-1}b$
b) $ya = b$ has a unique solution $y = ba^{-1}$

Proof

a) $a \in$ G $\Rightarrow$ $a^{-1} \in$ G (iv)

So $ax = b$

$\Rightarrow$ $a^{-1}(ax) = a^{-1}b$

$\Rightarrow$ $(a^{-1}a)x = a^{-1}b$ (ii)

$\Rightarrow$ $1x = a^{-1}b$ (iv)

$\Rightarrow$ $x = a^{-1}b$ (iii)

b) is proved similarly

●

Now the definition of a group says that any group must contain an identity and that every group element must have an inverse. But the definition does not say explicitly that each group has exactly one identity (although we have been assuming that there is only one identity when we use the symbol 1) or that each element has exactly one inverse (once again we have been assuming there is only one inverse when we use the symbol a^{-1}). However we shall prove that in fact this is the case.

Theorem 5.2.3

If G(.) is a group then a) G contains a unique identity
b) Every element of G has a unique inverse.

Proof

a) Assume that e_1 and e_2 are both identities of G

So $a\,e_1 = e_1\,a = a$ for all $a \in$ G

and $a\,e_2 = e_2\,a = a$ for all $a \in$ G

Substituting $a = e_2$ in the first equation (since a can be any group element) gives

$$e_2\,e_1 = e_1\,e_2 = e_2$$

and similarly substituting $a = e_1$ in the second equation gives

$$e_1\,e_2 = e_2\,e_1 = e_1$$

Thus

$e_2 = e_1$ ie there is only one identity

b) Assume that an element $a \in$ G has two inverses, b and c.

So we have $ab = ba = 1$ and $ac = ca = 1$

Multiplying the first equation by c gives

$c\,(ab) = c\,(ba) = c\,1$

$(ca)\,b = c\,(ba) = c$ (ii) and (iii)

$1\,b = c\,(ba) = c$ from second equation

$\Rightarrow\quad b = c$

ie a has only one inverse.

•

Note part (a) of theorem 5.2.3 tells us that exactly one row of the group table is identical to the top heading and exactly one column is identical to the left heading.
Part (b) of the theorem tells us that each row and column contains 1 exactly once.

Theorem 5.2.4

If G(.) is a group then $(a^{-1})^{-1} = a$ for all $a \in$ G

Proof

Since a^{-1} is the inverse of a then by definition

$$a\,a^{-1} = a^{-1}a = 1$$

Since a^{-1} is a group element, it too must have an inverse, let us call this x

So $a^{-1}x = x\,a^{-1} = 1$

Considering $x\,a^{-1} = 1$ and multiplying this by a gives

$$\begin{aligned} & (x\,a^{-1})\,a = 1\,a \\ \Rightarrow\quad & x\,(a^{-1}a) = a \\ \Rightarrow\quad & x\,1 = a \\ \Rightarrow\quad & x = a \end{aligned}$$

hence a is the inverse of a^{-1} ie $(a^{-1})^{-1} = a$

•

Theorem 5.2.5

If G(.) is a group then $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in$ G

Proof

By definition of inverse

$$\begin{aligned} & ab\,(ab)^{-1} = 1 \\ \Rightarrow\quad & a^{-1}\,[ab\,(ab)^{-1}] = a^{-1}\,1 \\ \Rightarrow\quad & (a^{-1}a)\,[b\,(ab)^{-1}] = a^{-1} \\ \Rightarrow\quad & 1\,[b\,(ab)^{-1}] = a^{-1} \\ \Rightarrow\quad & b\,(ab)^{-1} = a^{-1} \\ \Rightarrow\quad & b^{-1}\,[b\,(ab)^{-1}] = b^{-1}a^{-1} \\ \Rightarrow\quad & (b^{-1}b)\,(ab)^{-1} = b^{-1}a^{-1} \\ \Rightarrow\quad & 1\,(ab)^{-1} = b^{-1}a^{-1} \\ \Rightarrow\quad & (ab)^{-1} = b^{-1}a^{-1} \end{aligned}$$

•

Corollary 5.2.6

Similarly, if $a_1, a_2, \ldots\ldots\ldots, a_n$ are all elements of a group G(.)
then $(a_1\,a_2 \ldots\ldots\, a_n)^{-1} = a_n^{-1} \ldots a_2^{-1}\,a_1^{-1}$

Note We shall not in future produce such laborious proofs as the one above. This proof was made lengthy by always showing the application of the associativity law.

Exercise 5.2

1. Show that a group G(.) is abelian if and only if $(ab)^2 = a^2 b^2$ for all $a, b \in$ G (*hint:* prove $ab = ba$)

2. An element x of a group is said to be *idempotent* if $x^2 = x$. Prove that any group contains exactly one idempotent element.

3. Given a group G(.) where $(ab)^{-1} = a^{-1} b^{-1}$ for all $a, b \in$ G. Prove G(.) is abelian

4. Prove if x and y are two elements of G(.) then $x^2 = 1$ if and only if $(yxy^{-1})^2 = 1$.

5. In some group G(.) we have $a^3 b^3 = (ab)^3$ for all $a, b \in$ G.
Prove i) $a^2 b^2 = (ba)^2$ and hence deduce ii) $a^4 b^4 = (ab)^4$

5.3 Groups and Order

Order is a rather problematic word in group theory. It is used to describe two apparently different things.

5.3.1 Definition : the order of a group

The number of elements in a group is called the order of that group.
The order of G is written |G|.

The other use of the word order is somewhat more sophisticated. However before looking at this you should attempt the following

Exercise 5.3A

In each of the following groups G(*),take the element x and evaluate : x; $x{*}x$; $x{*}x{*}x$; $x{*}x{*}x{*}x$; ...., ie x combined with itself an ever increasing number of times **until** you can see a pattern emerging **or** until you are sure that there is no pattern.
Are the patterns the same each time?

	G(*)	x
1	$\{\mathbf{Z}_5 - [0]\}(\odot)$	[2]
2	$\{\mathbf{Z}_5 - [0]\}(\odot)$	[4]
3	$\{1, -1, i, -i\}$	i
4	$\{1, -1, i, -i\}$	-1
5	$\mathbf{Z}_6\,(\oplus)$	[2]
6	$\mathbf{Z}_6\,(\oplus)$	[3]

7	$\mathbf{Z}_6\,(\oplus)$	[5]
8	$\left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \right\}\,(.)$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$
9	$\mathbf{Z}\,(+)$	3
10	$[\mathbf{R} - \{0\}]\,(.)$	2

What you should have noticed in all the above examples was that in the last two there was no pattern but in all other cases there was a repeating pattern where each cycle of the pattern ended in the identity.

i.e. $x,\ x^2,\ \ldots\ldots,\ x^{n-1},\ x^n,\ x^{n+1},\ x^{n+2},\ \ldots\ldots,\ x^{2n-1},\ x^{2n},\ x^{2n+1},\ x^{2n+2},\ \ldots\ldots$
$x,\ x^2,\ \ldots\ldots,\ x^{n-1},\ 1,\ x,\ \ x^2,\ \ldots\ldots\ldots,\ x^{n-1},\ 1,\ \ x,\ \ x^2,\ldots\ldots\ldots$

If x^n is the first time that the identity appears in the sequence, we say that the group element x has order n. Or more formally.

5.3.2 Definition : the order of an element

The order of an element a of a group G is the least positive integer n such that $a^n = 1$

Obviously, the identity of a group always has order 1.

Example 5.3.3

In $\mathbf{Z}_6\,(\oplus)$	[2]	=	[2]
	[2] ⊕ [2]	=	[4]
	[2] ⊕ [2] ⊕ [2]	=	[0]

So [2] has order 3

Example 5.3.4

In $\mathbf{Z}_6\,(\oplus)$	[3]	=	[3]
	[3] ⊕ [3]	=	[0]

So [3] has order 2

Example 5.3.5

In $\mathbf{Z}_6\,(\oplus)$	[5]	=	[5]
	[5] ⊕ [5]	=	[4]
	[5] ⊕ [5] ⊕ [5]	=	[3]
	[5] ⊕ [5] ⊕ [5] ⊕ [5]	=	[2]
	[5] ⊕ [5] ⊕ [5] ⊕ [5] ⊕ [5]	=	[1]
	[5] ⊕ [5] ⊕ [5] ⊕ [5] ⊕ [5] ⊕ [5]	=	[0]

So [5] has order 6

Example 5.3.6

In $\{1, -1, i, -i\}(.)$ where $i^2 = -1$

-1 has order 2
i has order 4
$-i$ has order 4

Example 5.3.7

In the permutation group S_3

$$\begin{aligned}
\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} &= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\\
\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} &= \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\\
\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} &= \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}
\end{aligned}$$

So $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ has order 3

Note In groups such as $\mathbf{Z}(+)$ and $[\mathbf{R} - \{0\}]\ (.)$ there are no repeating patterns, so we say that all elements have **infinite order.**

Note also a) If x has order n then $x^{-1} = x^{n-1}$, since $x^{n-1}x = x^n = 1$

b) Elements of order 2 are often called **self-inverse** since if $x^2 = 1$ then $x^{-1} = x$

There is one very useful (but perhaps obvious) theorem to prove about the order of an element. When searching for patterns from repeating multiplication we arrived at something of the form

$$\begin{array}{l}
x,\ x^2,\ \ldots\ldots,\ x^{n-1},\ x^n, x^{n+1}, x^{n+2},\ \ldots\ldots,\ x^{2n-1},\ x^{2n}, x^{2n+1}, x^{2n+2},\ \ldots\ldots\\
x,\ x^2,\ \ldots\ldots,\ x^{n-1},\ 1,\ x,\ \ x^2,\ \ldots\ldots\ldots,\ x^{n-1},\ 1,\ \ x,\ \ x^2, \ldots\ldots\ldots
\end{array}$$

This besides suggesting that $x^n = 1$, also suggests that, $x^{2n} = 1, x^{3n} = 1$ etc. In other words, if $x^k = 1$, then k is some multiple of n where n is the order of the element.

From example 5.3.6 we could show $i^{12} = 1$, but 12 is not the smallest power of i which gives the identity since $i^8 = 1$ and $i^4 = 1$. The order in this case was 4. However 12, 8 and 4 are all multiples of 4.

Theorem 5.3.8

If a is a group element of order n and k is an integer such that $a^k = 1$, then n|k *(ie n divides k)*

Proof

If a has order n then n is the least integer such that $a^n = 1$.

So $a^k = 1 \Rightarrow k \geq n$

So by the Euclidean Division Algorithm, there exist integers q and r such that

$$k = qn + r \qquad \text{where } 0 \leq r < n$$

So $\qquad a^k = a^{qn+r} = a^{qn}\, a^r = (a^n)^q\, a^r = 1 . a^r = a^r = 1$

But $r < n$ and a has order n, so $r = 0$
Hence $k = qn$ i.e. $n|k$

•

For most of the rest of this course we will mainly be interested in groups of finite order, ie those that contain a finite number of elements. So the following two theorems will be of use.

Theorem 5.3.9

If G has finite order then all the elements of G have finite order.

Proof

If $a \in G$ then by closure a^2, a^3, a^4, ... etc. are all also elements of G.
But this infinite sequence of increasing powers of a cannot have all its terms distinct since G consists of only a finite number of elements. Hence there exists integers i and j such that $a^i = a^j$ and $j < i$

$\Rightarrow$ $a^{i-j} = 1$

$\Rightarrow$ So the order of $a \leq i - j$. i.e. the order of a is finite

•

Theorem 5.3.10

If an element of a group G has order n then $a, a^2, a^3, a^4, \ldots\ldots a^{n-1}, a^n = 1$ are all distinct.

Proof

If there exists integers i and j such that $a^i = a^j$ and $1 \leq j < i \leq n$

$\Rightarrow$ $a^{i-j} = 1$

But $1 \leq i - j < n$ which contradicts the fact that a has order n.

•

Now we have an understanding of both the order of a group and the order of a group element, it is convenient to start expressing groups in terms of the set of elements and some defining relations - when we are given a group in this way we also know all the group axioms hold See following example.

Example 5.3.11

G(.) = {1, a, b, ab} where $a^2 = b^2 = 1$ and $ab = ba$ (note this group is called the Klein 4 group or K_4)

a) Construct the group table b) write down the order of each element

a)

.	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	$\boldsymbol{b}$
b	b	ab	1	a
ab	ab	b	a	1

Notice that when completing the table all elements are expressed in terms of the set elements
So $\boldsymbol{a \,.\, ab = aab = a^2b = 1b = b}$

b) 1 has order 1, a, b and ab all have order 2.
For a and b this is obvious from the defining relations, for ab we see from the table $\boldsymbol{ab.ab = (ab)^2 = 1}$

Exercise 5.3B

1. Find the orders of each of the elements in $\mathbf{Z}_{12}$ ($\oplus$).

2. Find the order of the following elements of S_4

a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$

3. Find the order of the following elements of $\{\mathbf{Z}_7 - [0]\}$ ($\odot$)

a) [2] b) [5]

4. $G(.) = \{1, a, b, ab, ba, aba\}$ where $a^2 = b^2 = 1$ and $aba = bab$

a) Construct the group table
b) Find the order of each element
c) Find the inverse of each element

5. $G(.) = \{ 1, c, c^2, c^3, d, cd, dc, c^2d \}$ where $c^4 = d^2 = 1$ and $dc = c^3d$
Find the order of each element.

6. Show that for any group G(.) and elements a and $b \in$ G
a) a and a^{-1} have the same order. (*Hint* Let the orders of a and a^{-1} be n and m respectively. Prove that $n \leq m$ and $m \leq n$ then because of the fact the relation $\leq$ is anti-symmetric, this will imply that n=m)
b) ab and ba have the same order. (*Hint.* Use a similar approach to a) above)