Properties of groups

We have met the group axioms of (a) associativity, (b) identity, (c) inverses and (d) closure. From these laws governing the definition and hence formal structure of a group various properties follow. The main properties are now described.

1. **Cancellation laws**

Cancellation Law

In any group, G

if $xa = xb$ then $a = b$ $\qquad \dfrac{xa = xb}{a = b}$

and

if $ax = ab$ then $a = b$ $\qquad \dfrac{ax = ab}{a = b}$

Note that strictly we should write this using the symbol, **o**, or equivalent, for the operation in the group, thus

In any group, $(G, \mathbf{o})$, for all elements a, b

if $x \mathbf{o} a = x \mathbf{o} b$ then $a = b$

and

if $a \mathbf{o} x = a \mathbf{o} b$ then $a = b$

Throughout this section we will drop the use of the sign for the binary operation (for example, **o**) and we will drop other cumbersome notation that obscures the meaning.

In other words, the symbol

ab means $a \mathbf{o} b$ which means, b followed by a

Proof of the cancellation law

Let $xa = xb$

then

$x^{-1}(xa) = x^{-1}(xb)$	inverse property
$(x^{-1}x)a = (x^{-1}x)b$	associativity
$ea = eb$	inverse
$a = b$	indentity

At each stage of the proof we state explicitly the property of the group structure that is being used. In other words, we justify each line.

The proof of the second part of the theorem is almost identical to that of the first part.

2. There is just one identity element in any group.

Proof

Let e be the identity element of G

Suppose $fa = a$ for some element f in G, and for all elements a in G.

Then

$fa = ea$	identity, $ea = a$
$\therefore f = e$	cancellation law

3. In any group each element has just one inverse.

Proof

Suppose $ab = e$ for elements $a,\ b \in G$

Then

$(ab)b^{-1} = eb^{-1}$	
$a(bb^{-1}) = eb^{-1}$	associativity
$ae = eb^{-1}$	inverses
$a = b^{-1}$	identity

Likewise

$b = a^{-1}$

4. In any group *G*, if $a \in G$ then $(a^{-1})^{-1} = a$

Proof.

Let $b^{-1} = a$

then

$b = a^{-1}$	each element has just one inverse
$b^{-1} = \left(a^{-1}\right)^{-1}$	each element has just one inverse

What this says is that taking the inverse twice gets you back to where you started.

5. In any group $(a\,b)^{-1} = b^{-1}\,a^{-1}$

$(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a$	associativity
$= aea^{-1}$	inverse
$= aa^{-1}$	identity
$= e$	inverse
$\therefore \quad (ab)^{-1} = b^{-1}a^{-1}$	definition of inverse

6. For all elements $a, b \in G$ there is another element $x \in G$ such that $xa = b$ and an element $y \in G$ such that $a = y\,b$

Proof

Let $a, b \in G$ then

$a^{-1} \in G$	inverse
$ba^{-1} \in G$	closure
Let $ba^{-1} = x$	binary operation

$\left(ba^{-1}\right)a = xa$	mulitplying both sides by a
$b\left(a^{-1}a\right) = xa$	associativity
$b = xa$	inverse

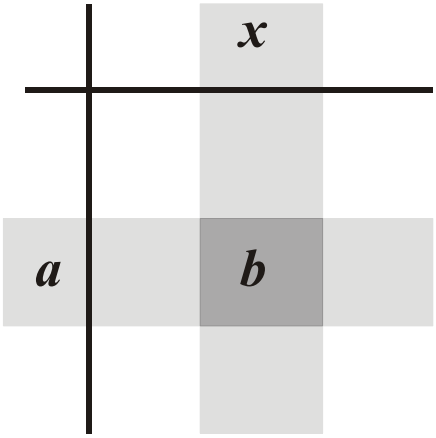
$\therefore$ There exists an $x \in G$ such that $b = xa$

The second part of the proof follows similarly.From this theorem follows:

7. The Latin square property: the combination table for any finite group is such that each row and each column consists of a permutation of the group elements.

Consider the row of the combination table corresponding to element *a.* The table shows the effect of combining *a* with every element of the group under the group operation.

We have just shown that for any element $b \in G$ there is another element $x \in G$ such that $b = a\,x$



This means that every element $b \in G$ appears at least once in the row corresponding to the element *a*. But since there are exactly the same number of entries in a row as there are in a group set, it follows that every row contains all the elements of the set just once. That is, every row is just a permutation of the group elements.

A more formal statement of this theorem and proof is as follows.

Theorem

Let *G* be a group with distinct elements $\{a_1,...,a_n\}$. If $a \in G$ then as *j* varies from 1 to *n* the elements aa_j run through the whole of *G*, each element of *G* occurring exactly once.

Proof

Let $b \in G$, then $a^{-1}b \in a_j$ for some j and $b = aa_j$.

Suppose $aa_i = aa_j$, then

$a_i = a^{-1}aa_j = a^{-1}b = a_j$