# Groups - Part 1 (10 pages; 22/10/16)

The various topics of Group Theory are interrelated. Part 1 of this note introduces ideas in the following order: cyclic groups, subgroups & isomorphisms (so that, for example, an idea relating to both cyclic groups and isomorphisms would appear under the latter heading only - although this doesn't apply to the Notation section).

Part 2 contains examples of groups, and summaries of results for the topics mentioned above (as well as some others) - with no restriction as to order of appearance (so that an idea relating to both cyclic groups and isomorphisms would appear under both headings).

## (1) Definition of a group

The group $(S,*)$ has the following properties:

- non-empty set S

- binary operation $*$

- closure: $a * b \in S \ \ \forall\, a, b \in S$ [$\forall$ means "for all"]

- associativity: $(a * b) * c = a * (b * c) \ \ \forall\, a, b, c \in S$

- identity element, $e$

- each $a \in S$ has an inverse $a^{-1}$ such that $a * a^{-1} = a^{-1} * a = e$

## Notes

(a) If the operation is commutative, the group is referred to as abelian (it can also just be referred to as commutative).

For non-abelian groups, the order of the elements in an operation will need to be specified.

(b) Groups may be of finite or infinite order (ie referring to the number of elements of $S$).

(c) Finite groups can be represented by a Cayley table (a Latin square, where every element occurs just once in each row or column).

Example: $\{1, i, -1, -i\}$ under multiplication

| | $1$ | $i$ | $-1$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $i$ | $-1$ | $-i$ |
| $i$ | $i$ | $-1$ | $-i$ | $1$ |
| $-1$ | $-1$ | $-i$ | $1$ | $i$ |
| $-i$ | $-i$ | $1$ | $i$ | $-1$ |

The Cayley table can be used to define the group.

(d) Some books use the term "binary operation" to mean a closed binary operation.

(e) When testing that the necessary conditions apply, associativity is usually the time-consuming one, and is best saved until last (in case one of the other conditions fails).

## (2) Notation

(i) In its complete form, a group is specified by a set and an operation on it: (G,*); but this is often abbreviated to just G, if the operation is understood.

(ii) Other symbols can be used instead of * ( $\circ$ , for example)

(iii) When there is no ambiguity, $a * b$ or $a \circ b$ can be replaced by $ab$

However, when the operation is addition (including modulo addition), $a + b$ is used instead of $ab$.

By convention, if $+$ is used for the group operation, then the group is abelian; if ab is used, it need not be abelian.

(iv) $n(G)$ is sometimes used to denote the order of the group $G$

(v) $\{\mathbb{Z}_4, +mod\ 4\}$ denotes the group with the set $\{0,1,2,3\}$ [rather confusingly] and operation of addition (mod 4)

Alternatively, $+mod\ 4$ can be denoted by $+_4$ (and $\times\ mod\ 4$ by $\times_4$).

[Note that the following terminology is used:

"addition modulo $n$" (or "addition mod $n$");

"modular arithmetic";

$n$ could be referred to as the "modulus" (but you wouldn't say "addition modulus $n$", for example)]

(vi) $\mathbb{Z}_5 - \{0\}$ denotes the set $\{1,2,3,4\}$

(vii) Alternative ways of denoting the real numbers excluding 0:

(a) $\mathbb{R} - \{0\}$

(b) $\mathbb{R}\backslash\{0\}$

(c) $\mathbb{R}^*$ [probably best used when the operator isn't denoted by *]

(viii) $C_n$: cyclic group of order $n$ (see below)

(ix) $\langle g \rangle$: cyclic group generated by $g$ (see below)

(x) $S_n$: the group of permutations of $(1,2,3, \ldots, n)$ (see below)

(xi) $D_n$: the symmetry group of a regular $n$-sided polygon (see Part 2)

## (3) Basic Results

(i) Cancellation law: if $a * x = a * y$, then $x = y$

(ii) If $a * a^{-1} = e$, then $a^{-1} * a = e$

(iii) $(a * b)^{-1} = b^{-1} * a^{-1}$

(iv) $(a^m)^{-1} = (a^{-1})^m$

(v) A group in which every element is its own inverse is abelian.

## (4) Cyclic Groups

(i) Example: $\{\mathbb{Z}_4, +mod(4)\}$

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

General form:

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

Alternative form:

| | $e$ | $a$ | $a^2$ | $a^3$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $e$ |
| $a^2$ | $a^2$ | $a^3$ | $e$ | $a$ |
| $a^3$ | $a^3$ | $e$ | $a$ | $a^2$ |

(ii) The order (or period) of an element (in any group) is the lowest (positive) $k$ such that $x^k = e$.

In the general example above, $a$ and its inverse, $a^3$ both have order 4, whilst $a^2$ has order 2.

Note: In an infinite group, an element can have infinite order.

(iii) A group consisting of powers of a single element $g$ (referred to as a generator of the group) is called a cyclic group - denoted $C_n$ (where $n$ is the order). Thus S can be written as $\{g, g^2, \dots, g^n\}$

For a group of order $n$, $g$ is a generator of the group if $g^n = e$ , and no smaller power of $g$ equals $e$.

Note: The group generated by $g$ is sometimes denoted by $\langle g \rangle$.

In the general example above, $a$ and its inverse, $a^3$ are both generators (with $a^3$, the cycle is now going from right to left).

If $g$ is a generator of a group, then $g^{-1}$ is also a generator.

(iv) Because of associativity, all cyclic groups are abelian.

## (5) Subgroups

(i) Any subset of $S$ that gives rise to a group under the operation $*$ is referred to as a subgroup of $\{S,*\}$.

(ii) Both $\{e\}$ and the whole group are subgroups, but are (usually) referred to as trivial subgroups; any other subgroups are (usually) referred to as proper subgroups.

[Some books define a trivial subgroup as $\{e\}$ only, and a proper subgroup as one that is not the whole group.]

(iii) Example: cyclic group of order 4

| | $e$ | $a$ | $a^2$ | $a^3$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $e$ |
| $a^2$ | $a^2$ | $a^3$ | $e$ | $a$ |
| $a^3$ | $a^3$ | $e$ | $a$ | $a^2$ |

$\{e, a^2\}$ is the only proper subgroup

(iii) Lagrange's theorem: The order of a subgroup of a finite group is a factor of the order of the group.

Note: The converse is not true. If the order of a group has a factor $f$, then there isn't necessarily a subgroup of order $f$.

(iv) Let $a$ be an element of a group G. Then $\{a^n : n \in \mathbb{Z}\}$ is a subgroup of G (referred to as the subgroup generated by $a$).

Note: This applies to both finite and infinite G.

By Lagrange's theorem, the order of an element divides the order of the group.

(v) All groups of prime order are cyclic.

This follows from Lagrange's theorem: Let $a \neq e$ be an element of the group $G$ , where $G$ has prime order $p$. By Lagrange's theorem, the order of $a$ (ie the subgroup generated by $a$) must be a factor of $p$. As the order of $a$ is not 1 (since $a \neq e$), it must be $p$. Hence $a$ is a generator for $G$, which is therefore cyclic.

Note that cyclic groups are not necessarily of prime order. (For example, some groups of order 4 or 6 - discussed later.)

(vi) Every element of a group of prime order is a generator of the group.

(vii) If a group of order 4 is not cyclic, then it contains 3 elements of order 2.

[Were $x$ to be of order 3, then $e, x, x^2$ would be a subgroup, but 3 is not a factor of 4, contradicting Lagrange's Theorem.]

Such a group must therefore be structured as follows:

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | | |
| $b$ | $b$ | | $e$ | |
| $c$ | $c$ | | | $e$ |

There is then only one way of filling in the remaining cells, in order not to duplicate entries in a particular row or column:

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |

| | | | | |
|---|---|---|---|---|
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

This is the so-called Klein 4-group (sometimes denoted [confusingly] by Klein V, where the V is short for vier (German for 4)).

Note that it is abelian.

Also, $ab = c$ (and, by symmetry, $ac = b$ & $bc = a$).

So an alternative form of the Cayley table is:

| | $e$ | $a$ | $b$ | $ab$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $ab$ |
| $a$ | $a$ | $e$ | $ab$ | $b$ |
| $b$ | $b$ | $ab$ | $e$ | $a$ |
| $ab$ | $ab$ | $b$ | $a$ | $e$ |

The nature of a group of order 4 can quickly be established from its Cayley table: If all of the elements on the leading diagonal (ie from top left to bottom right) are $e$, then it is the Klein 4-group (where every element is its own inverse); otherwise it is the cyclic group.

Note, incidentally, that the elements $a$ & $b$ are said to be the generators for this group (so the term 'generator' doesn't just apply to cyclic groups).

(viii) To establish that a set gives rise to a subgroup:

- The identity will be the same as that of the main group.

- Inverses are defined as before.

- Associativity is inherited from the main group.

- Closure needs to be established.

(ix) Procedure for finding subgroups: consider separately the groups generated by each element.

(x) Commutativity is inherited from the main group. But it is possible for a subgroup of a non-abelian group to be abelian (eg a cyclic group generated by a particular element).

(xi) It can be shown that, if $H$ & $K$ are subgroups of a group $G$, then $H \cap K$ is also a subgroup. $H \cup K$ need not be a subgroup.

(xii) Any subgroup of a cyclic group must also be cyclic.

(xiii) It can be shown that the order of a finite group with at least 2 elements, but no proper subgroups, is prime.

## (6) Isomorphisms

(i) Two groups are isomorphic if they have the same structure.

Formal definition:

The groups $(G,*)$ & $(H,°)$, with the same order, are isomorphic if there exists a function $f: G \to H$ such that

(a) the range of $f$ is $H$

(b) $f$ is 1-1

(c) $f(a * b) = f(a) \circ f(b)$ for all $a, b \in G$

### Notes

(I) If conditions (a) and (b) apply, then $f$ is described as bijective (see "Functions - Miscellaneous").

(II) If the condition that $f(a * b) = f(a) \circ f(b)$ is satisfied, with $f$ being a function, but not necessarily bijective, then $f$ is described as a homomorphism.

(ii) All groups of a particular prime order are cyclic, and therefore isomorphic to each other, and to (for example) $(\mathbb{Z}_n, +)$.

(iii) As seen above, all groups of order 4 are isomorphic to either the cyclic group or the Klein 4-group.

(iv) There are 2 distinct groups of order 6: cyclic groups and groups isomorphic to $D_3$ (see Part 2(C): Groups of order 6).

(v) Cayley's theorem: Any group of order $n$ is isomorphic to a subgroup of $S_n$ (the group of permutations of $(1,2,3, \dots , n)$).

[In the Cayley table for a group of order $n$, each row contains one of each of the elements of the group. As these elements can be relabelled $1,2,3, \dots , n$ , the rows of the table are permutations of $(1,2,3, \dots , n)$]

(vi) If $f: G \to H$ is an isomorphism, then the order of $a \in G$ equals the order of $f(a) \in H$.

(vii) To show that two groups are isomorphic, find a function from one to the other, and show that the function is an isomorphism.

(viii) Ways of proving lack of isomorphism of groups M and N:

(a) Show that one group is abelian and the other isn't.

(b) Establish that the orders of the elements are not the same.

eg consider the number of elements of order 2; ie such that $a^2 = e$ or $a^{-1} = a$

(c) Establish that the orders of the subgroups are not the same.

(ix) See Part 2(A&B) for examples of isomorphisms.

The group of positive real numbers under multiplication is isomorphic to the group of real numbers under addition (consider logarithms).

(x) Properties of isomorphisms (implied by $G$ & $H$ having the same structures)

(a) The identity in $G$ is mapped to the identity in $H$.

(b) $f(g^{-1}) = [f(g)]^{-1}$ for all $g \in G$

(c) $f(g^n) = [f(g)]^n$ for all $g \in G$ & $n \in \mathbb{Z}$

(d) The order of $g \in G$ will always be equal to the order of $f(g) \in H$

(e) $G$ is abelian if and only if $H$ is abelian

(f) If $G = \langle a \rangle$ & $H = \langle b \rangle$ are both cyclic groups of the same order, then there is an isomorphism $f$ such that $f(a^n) = b^n$ for all $n \in \mathbb{Z}$