MTHSC 412 Section 3.1 –Groups

Kevin James

Definition

A *group* is a set G together with a binary operation $*$ on G satisfying the following conditions.

1. $*$ is associative
2. G has an identity element with respect to $*$.
3. For each $g \in G$ there is an inverse g^{-1} of g with respect to $*$.

Definition

Suppose that G is a group with respect to $*$. Then G is an *abelian* or *commutative* group if $*$ is commutative.

Example

1. If A is any set then $\mathcal{S}(A)$ is a group with respect to composition of functions. This group is not abelian.
2. $\mathbb{Z}$ is an abelian group under addition.
3. $M_n(\mathbb{R})$ is an abelian group under addition.
4. $\mathbb{Z}_n$ is an abelian group under addition.

Notation (Cycle notation for S_n)

1. Recall that if $A = \{1, 2, \ldots, n\}$ then we denote by $S_n = \mathcal{S}(A)$.
2. We shall use the notation $\sigma = (a_1, a_2, \ldots, a_k)$ to denote the permutation $\sigma \in S_n$ defined by

$$\sigma(m) = \begin{cases} a_{i+1} & \text{if } m = a_i \text{ where } 1 \leq i \leq k-1, \\ a_1 & \text{if } m = a_k. \\ m & \text{otherwise.} \end{cases}$$

Example

As an element of S_3, $f = (1, 2)$ denotes the function f on $\{1, 2, 3\}$ whose values are $f(1) = 2, f(2) = 1, f(3) = 3$.

Example

The elements of S_3 are $e = (1)$, $(1,2)$, $(1,3)$, $(2,3)$, $(1,2,3)$, $(1,3,2)$.

Note that $(1,2,3)^2 = (1,3,2)$.

The multiplication table for S_3 is

$*$	(1)	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
(1)	(1)	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)$	(1,2)	(1)	$(1,3,2)$	$(1,2,3)$	$(2,3)$	$(1,3))$
$(1,3)$	(1,3)	$(1,2,3)$	(1)	$(1,3,2)$	$(1,2))$	$(2,3)$
$(2,3)$	(2,3)	$(1,3,2)$	$(1,2,3)$	(1)	$(1,3)$	$(1,2)$
$(1,2,3)$	(1,2,3)	$(1,3)$	$(2,3)$	$(1,2)$	$(1,3,2)$	(1)
$(1,3,2)$	(1,3,2)	$(2,3)$	$(1,2)$	$(1,3)$	(1)	$(1,2,3)$

Example

Let $G = \{\pm 1, \pm i\}$ where $i \in \mathbb{C}$ satisfies $i^2 = -1$.
Then G is a group under multiplication of complex numbers.
The multiplication table for G is

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Definition

If a group G has a finite number of elements then we say that G has *finite order* or that G is a *finite group*.
In this case, the number of elements of G is called the *order* of G and is denoted as $o(G)$ or $|G|$ or $\#G$.
If G does not have a finite number of elements then it is said to be an *infinite group*.