TW 314 Lecture 1 (Mo 30 Jan. 2017)

The definition of a group $(G, *)$

A group $(G, *)$ consists of a set G together with a binary operation $*$ defined on G which satisfies the following axioms.

G1 For all x and y in G, $x * y$ is in G.
— (We then say G is closed under $*$).

G2 For all x, y and z in G, $(x*y)*z = x*(y*z)$.
— ($*$ is associative).

G3 There is an element e in G such that
$e * x = x * e = x$ for all x in G.
— (e is the identity element for $*$).

G4 For each x in G, there is an x' in G such that $x * x' = x' * x = e$.
— (x' is the inverse of x).

If G is a finite set, then $(G, *)$ is called a finite group and the cardinality $|G|$ of G is called the order of the group $(G, *)$.

Examples

- Consider the set $\mathbb{Z}$ of integers together with the binary operation $+$ on $\mathbb{Z}$:

G1 — $\mathbb{Z}$ is closed under $+$

G2 — $+$ is associative

G3 — 0 is the identity element for $+$

G4 — the inverse of an integer x is the integer $-x$

All four group axioms are satisfied; thus $(\mathbb{Z}, +)$ is a group.

- Consider the set $\mathbb{Z}$ together with $\times$:

G1 — $\mathbb{Z}$ is closed under $\times$

G2 — $\times$ is associative

G3 — 1 is the identity element for $\times$

G4 — What is the inverse of 7?
Oh, dear ... $\frac{1}{7}$ is not an integer.

Since axiom G4 is not satisfied,

$(\mathbb{Z}, \times)$ is not a group.

Permutations

Let $\mathbb{N}_n$ denote the set $\{1, 2, \ldots, n\}$.

A permutation r of $\mathbb{N}_n$ is a bijection $r : \mathbb{N}_n \to \mathbb{N}_n$ and we denote the set of all permutations of $\mathbb{N}_n$ by S_n; thus $|S_n| = n!$

Example: S_3 consists of the following $3! = 6$ permutations of $\mathbb{N}_3 = \{1, 2, 3\}$.

$$\text{id}: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{matrix} \qquad r_1: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix} \qquad r_2: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{matrix}$$

$$m_1: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{matrix} \qquad m_2: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{matrix} \qquad m_3: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{matrix}$$

In cycle notation, these permutations are

$$\text{id} \qquad r_1 = (1\ 2\ 3) \qquad r_2 = (1\ 3\ 2)$$

$$m_1 = (2\ 3) \qquad m_2 = (1\ 3) \qquad m_3 = (1\ 2)$$

Note that $r_1 = (1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$

and $m_1 = (2\ 3) = (3\ 2)$, et cetera.