ME/SE 740

Lecture 6

Group Theory

Summary from last lecture:
In the planar case we have:

$$T: \begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}, \quad \begin{pmatrix} x \\ y \end{pmatrix}$$

In space (3-D) we have:

$$\underbrace{\begin{pmatrix} n_x & o_x & a_x \\ n_y & o_y & a_y \\ n_z & o_z & a_z \end{pmatrix}}_{R} \underbrace{\begin{pmatrix} p_x \\ p_y \\ p_z \end{pmatrix}}_{\vec{r}}$$

where the rules of composition are:

$$(R,\vec{r}) \circ (S,\vec{s}) = (RS, R\vec{s} + \vec{r})$$
$$(R,\vec{r}) \longleftrightarrow \begin{pmatrix} R & r \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} R & r \\ 0 & 1 \end{pmatrix}\begin{pmatrix} S & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} RS & Rs + r \\ 0 & 1 \end{pmatrix}$$

and the inverse is written as:

$$(R,\vec{r})^{-1} \longleftrightarrow \begin{pmatrix} R^T & -R^T r \\ 0 & 1 \end{pmatrix}$$

Observation: The set of rigid body motions forms a group under the operation of composition.

Definition of Group: A set G together with a binary operation between it elements"$\cdot$" (referred to as multiplication) is said to be group if it has the following properties:

1. Whenever a, b are elements of G, the element $a \cdot b$ is also an element of G.
2. There exists a unique identity element $e \in G$ with the property that $e \cdot a = a \cdot e = a$ for all $a \in G$.
3. For every $a \in G$ there exists a unique corresponding element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$ (existence of inverses).
4. The multiplication operation satisfies an associative law, i. e., for every $a, b, c \in G$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

We now provide a number of examples.

Example 1: The set of all square $n \times n$ invertible matrices is a group under the operation of multiplication $G\ell(n)$ (General Linear Group).

proof: At the most basic level, we must first check that it is closed under matrix multiplication, i.e., check that $G \times G \longrightarrow G$. In particular, if A, B are $n \times n$ invertible matrices it follows that $A \cdot B$ is also invertible, with its inverse given by $B^{-1} \cdot A^{-1}$. In going through the other defining properties, we see that the identity matrix serves as the "identity" element. Group inverses are just matrix inverses and the associative law holds.

Counter example (not a group): The set of invertible, symmetric matrices is not a group under matrix multiplication as one can easily see that the product of symmetric matrices is not necessarily a symmetric matrix for any value of a, b, c, r:

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & r \end{pmatrix} = \begin{pmatrix} a+b & a+2b \\ b+c & b+2c \end{pmatrix}$$

This implies that the product of two elements in the set may not be in the set, thus violating "closure."
Example 2: A square $n \times n$ matrix U is said to be orthogonal (an element of $O(n)$) if $U^T U = I$.
subexamples:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad \begin{pmatrix} n_x & o_x & a_x \\ n_y & o_y & a_y \\ n_z & o_z & a_z \end{pmatrix}$$

Proposition: The set of $n \times n$ orthogonal matrices is a group under matrix multiplication.

Before discussing the proof of this proposition we note that from $U^T U = I$, it follows that $UU^T = I$ since:

$$U^T U = I \quad \Rightarrow \quad U(U^T U) = U \quad \Rightarrow (UU^T)U = U$$

and if we multiply both sides by U^{-1} we have:

$$UU^T = I$$

From the combined $U^T U = UU^T = I$, it follows that $U^{-1} = U^T$. From this fact, the proof that $O(n)$ is a group is easy:

1. The identity in $O(n)$ is just the identity matrix
2. $U^{-1} = U^T$
3. The associative law is inheritted from the associative law of matrix multiplication

It remains to be shown that $O(n)$ is closed under matrix multiplication.

Let $U, V \in O(n)$

$$U^T U = I, \quad V^T V = I$$
$$(UV)^T (UV) = \underbrace{V^T \underbrace{U^T U}_{I} V}_{I} = I$$

Example 3: Let $X_n = \{1, 2, 3, \cdots, n\}$ be a finite set of n elements. The set S_n of all $1-1$ and onto functions mapping $X_n \longrightarrow X_n$ is a group under composition. It is called the symmetric group on n-symbols also called the permutation group on n-symbols. The reason it is called the permutation group is that any function (mapping) in the group permutes the symbols.

$$f : \{1, 2, 3, \cdots n\} \longrightarrow \{s_1, s_2, s_3, \cdots s_n\}, \quad f(k) = s_k$$

Clearly, the number of elements in S_n is $n!$.

Example 4: $(\mathbb{Z}_n, +)$ where $\mathbb{Z}_n$ is the set of positive integers $mod m$ under addition:

$+$	0	1	2	$\cdots$	$m-2$	$m-1$
0	0	1	2	$\cdots$	$m-2$	$m-1$
1	1	2	3	$\cdots$	$m-1$	0
2	2	3		$\cdots$		
$\vdots$						
$m-1$	$m-1$	0	1	$\cdots$		

Example 5: $(\mathbb{Z}_p^+, \cdot)$ where $\{1, 2, 3, \cdots p\}$ with multiplication where p is a prime number. In particular for $p = 3$ we have:

$\cdot$	1	2
1	1	2
2	2	1

Example $5'$: $(\mathbb{Z}_m^+, \cdot)$ where m is a positive integer.

Definition: Given a group $(G, \cdot)$ a subset $H \subset G$ defines a subgroup if $(H, \cdot)$ is a group in its own right.

The verify that a subset H defines a subgroup all we need to check is:

1. closure, i.e., for $a, b \in H$ then $a \cdot b \in H$
2. $a \in H$ implies that $a^{-1} \in H$

Example 6: $(\mathbb{Z}, +)$ the group of all integers under addition.

Example $6'$**:** $(2\mathbb{Z}, +)$ the group of all even integers under addition.

Note: Example $6'$ is a subgroup of Example 6.

Definition: Let $(G_1, \cdot$ and $(G_2, \star)$ be groups. A function $h : G_1 \longrightarrow G_2$ is called a homomorphism if for all $a, b \in G_1, \quad h(a \cdot b) = h(a) \star h(b)$.

Example 1h: Let $h : \quad (\mathbb{Z}, +) \quad \longrightarrow (2\mathbb{Z}, +)$ given by: $h(m) = 2m$ is a homomorphism.

$$h(m+n) \;=\; 2(m+n) \;=\; 2m + 2n = h(m) + h(n)$$

Example 2h: Let $h : \quad (\mathbb{Z}, +) \quad \longrightarrow G\ell(2)$ defined by:

$$h(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

is a homomorphism.

$$h(n+m) = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = h(n) \cdot (m)$$