3 Basic concepts of group theory

Direct Product:

The definition of the quotient group is like dividing the group G by its normal subgroup H. Is there a way to multiply two groups together? The answer is yes.

The direct product of two groups G and H is again a group, with elements $\{(g,h), g \in G, h \in H\}$ and their composition rule is given by

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2) \tag{1}$$

It is straight forward to check that the group axioms are satisfied. The direct product of G with H is denoted as $G \times H$.

Comments about direct product and quotient group:

(1) $G \times H$ contains subgroups $G' = \{(g,e)\}$ and $H' = \{(e,h)\}$ which are isomorphic to G and H respectively.

(2) Every element in G' commute with every element in H'. $(g,e)(e,h) = (g,h) = (e,h)(g,e)$

(3) G' and H' are both normal subgroups of $G \times H$. $((g,h)(g_1,e)(g^{-1},h^{-1}) = (gg_1g^{-1},e)$, $(g,h)(e,h_1)(g^{-1},h^{-1}) = (e, hh_1h^{-1})$.

(4) The quotient group $(G \times H)/G'$ is isomorphic to H and the quotient group $(G \times H)/H'$ is isomorphic to G.

(5) The order of $G \times H$ is the product of the order of G and the order of H.

Example: Take two C_2 groups $G = gp\{a\}, a^2 = e$, $H = gp\{b\}, b^2 = e$. Their direct product $G \times H$ contains four elements $(e,e), (a,e), (e,b), (a,b)$ which forms a D_2 group. Therefore, $D_2 = C_2 \times C_2$.

Example: $C_4 = gp\{a\}, a^4 = e$ also has a C_2 normal subgroup $\{e, a^2\}$ and the quotient group is isomorphic to C_2. However, $C_4 \neq C_2 \times C_2$. (A simple way to see this is to notice that C_4 has an element of order 4.)

Example: D_3 has a C_3 subgroup and $D_3/C_3 = C_2$. However, $D_3 \neq C_2 \times C_3$, because C_2 is not a normal subgroup of D_3. Instead, $C_2 \times C_3 = C_6$ (hint: show that $C_2 \times C_3$ has an element of order 6).

Example: For co-prime integers p_1 and p_2, $C_{p_1} \times C_{p_2} = C_{p_1 \times p_2}$.

Center

Definition: the center of a group, denoted as $Z(G)$, is the set of elements that commute with every element of G.

$$Z(G) = \{a \in G \mid ag = ga, \forall g \in G\} \tag{2}$$

Comments:

(1) $Z(G)$ is a normal subgroup of G. Actually, the requirement of the center is stronger than that of a normal subgroup. Every element of $Z(G)$ is invariant under conjugation.

(2) $Z(G)$ is abelian.

(3) $Z(G) = G$ if and only if G is abelian.

4 Group representations

4.1 Mapping between groups

A group homomorphism from group A to group B, is a mapping from group elements in A to group elements in B, such that the group structure is preserved.

That is, the mapping $f : A \to B$, takes each element $a \in A$ and maps it to a unique element in $b = f(a) \in B$. If $a_1 a_2 = a_3$, then $f(a_1)f(a_2) = f(a_3)$, which implies that the identity element in A is mapped to the identity element in B and $f(a^{-1}) = (f(a))^{-1}$.

Comments:

(1) The set of elements $\{f(a), a \in A\}$ in B is called the image of f. It may happen that not every element in B is in the image of f. The image of f forms a subgroup of B.

(2) Different elements in A can be mapped to the same element in B.

(3) If different elements in A are mapped to different elements in B, then the mapping is said to be faithful.

(4) The set of elements in A that are mapped to the identity in B is said to be the kernel of f. The kernel of f forms a subgroup of A. In fact, it is a normal subgroup of A (how to prove it?) and the image in B form the corresponding quotient group. (we are going to prove this in the homework)

(5) If f is a one to one mapping, then f is said to be an isomorphism. A faithful mapping is not necessarily an isomorphism because it is possible that not all elements in B are in the image of f.

Example: If we choose A to be D_3, what group can the image be? (C_2, D_3 or the trivial group)

4.2 Group Representation: definition

A group is a very abstract concept. The same group can appear in many different ways. For example, we can think of the cyclic group as the rotation symmetry of regular polygons. Or equivalently, we can think of it as integer modulo n. To have a concrete handle when we try to analyze properties of groups, it is useful to choose a nice way to write down the group elements and their composition rules. It turns out to be particularly helpful to use matrices to represent groups and that is what a group representation is.

Definition: a representation of a group G is a group homomorphism from G to $GL(n, \mathbb{C})$, the general linear group of invertible matrices of dimension n over complex numbers $\mathbb{C}$.

Comments:

(1) Apart from $GL(n, \mathbb{C})$, it is often useful to restrict the representation to general linear real matrices $GL(n, \mathbb{R})$, orthogonal matrices $O(n)$ and unitary matrices $U(n)$. The representation is said to be complex, real, orthogonal or unitary respectively.

(2) The set of matrices used as representation can be thought of as linear transformations on an underlying n dimensional vector space. Once we have chosen a basis for the vector space, the linear representation can be written as matrices.

4.3 Examples

Example 1: C_2

The C_2 group has two possible normal subgroups: the identity group $\{e\}$ and C_2 itself. There are hence two possibilities for the kernel group and correspondingly two possibilities for the image group: C_2 and $\{e\}$.

When the image group is C_2, the representation is a faithful one. One possible realization is $D(e) = 1, D(c) = -1$.

When the image group is $\{e\}$, the representation is a trivial one, $D(e) = D(c) = 1$. Every group has a trivial representation like this.

There are also two dimensional representations of C_2. For example, $D(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $D(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.