3 Basic concepts in group theory

3.2 Subgroup

Definition: A subgroup H of G is a subset of G which itself forms a group under the composition law of G.

Comments:

(1) The identity element e forms a subgroup by itself.

(2) The whole group G also forms a subgroup according to this definition.

(3) Any subgroup which is different from $\{e\}$ and G is called a proper subgroup.

Example: $C_2 = \{e, b_1\}$ and $C_3 = \{e, c, c^2\}$ are both proper subgroups of D_3.

Coset, definition: given a subgroup $H = \{h_1, h_2, ..., h_r\}$ of a group G, the left coset given by an element $g \in G$, written as gH, is defined as the set of elements obtained by multiplying all elements of H on the left by g:

$$gH := \{gh_1, gh_2, ..., gh_r\} \tag{1}$$

Comments:

(1) Each coset contains r distinct elements. (If $h_1 \neq h_2$, then $gh_1 \neq gh_2$. Because if $gh_1 = gh_2$, then multiplying both sides from the left with g^{-1}, we get $h_1 = h_2$, contradicting the original assumption that h_1 and h_2 are distinct elements).

(2) For any g_1, $g_2 \in G$, g_1H and g_2H either completely overlap or do not overlap with each other at all. (Suppose that the two cosets contain one pair of identical elements $g_1h_1 = g_2h_2$. Any other element in g_1H can be obtained by right multiplication of some $h_k \in H$ with g_1h_1. As $g_2h_2h_k = g_1h_1h_k$ and $g_2h_2h_k$ belongs to g_2H, for every element in g_1H we can find a corresponding element in g_2H and vice verse. Therefore, if g_1H and g_2H overlap, then they are completely the same.)

(3) Because it is possible that g_1H and g_2H completely overlap with each other, the labeling of a coset as gH is not unique.

(4) For $h \in H$, $hH = H$.

(5) Cosets provide a different way to partition a group into disjoint sets. This partition is different from the conjugacy class partition. In particular, each disjoint set contains the same number of elements r.

(6) One can similarly define the right coset Hg which in general gives a different partition than the

left cosets.

(7) A coset other than H itself does not form a group. In particular, it does not contain the identity element.

Lagrange's Theorem:

The order of any subgroup of G must be a divisor of the order of G.

Corollary: Any group of prime order has no proper subgroups (e.g. C_p for p prime).

Example: For the D_3 group of order 6, $H = \{e, b_1\}$ of order 2 forms a subgroup. Using the composition rule $b_1 c = b_2$, $cb_1 = b_3$ etc., we can see that the left cosets are $eH = b_1 H = \{e, b_1\}$, $cH = b_3 H = \{c, b_3\}$, $c^2 H = b_2 H = \{c^2, b_2\}$.

Normal subgroups: A subgroup H of G is said to be normal if it satisfies $gHg^{-1} = H$ for any $g \in G$.

Comments:

(1) H only has to be invariant under conjugation as a group. Each single element of H does not have to be invariant. Instead they can be mapped into each other. But as long as $gh_i g^{-1}$ stays in H, then H is a normal subgroup.

Example: The C_3 subgroup $\{e, c, c^2\}$ of D_3 is a normal subgroup because $b_i c b_i^{-1} = c^2$. But the C_2 subgroup $\{e, b_1\}$ is not a normal subgroup because $cb_1 c^{-1} = b_2$.

(2) An equivalent definition of normal subgroup is that the left coset gH is equal to the right coset Hg.

Quotient group

The normal subgroup is special in that the set of cosets can be endowed with a group structure by a suitable definition of the composition of two cosets. This is called the quotient group and denoted as G/H.

Suppose that H is a normal subgroup of G. The set of disjoint cosets $\{g_i H\}$ forms a group if we define the composition of two cosets $g_1 H$ and $g_2 H$ as $g_1 g_2 H$

$$(g_1 H) \circ (g_2 H) := g_1 g_2 H \tag{2}$$

First we need to show that this is a legitimate definition. When we write gH, we have chosen a particular g to label a coset, but a different g can be chosen to label the same coset. In the definition above, we have used a particular choice of g to define the composition rule. We need to show that the composition rule as defined does not depend on the choice of g.

Suppose that $g_1 H$ and $g_1' H$ are the same coset, and $g_2 H$ and $g_2' H$ are the same coset. Then we can find a $h_1 \in H$ such that $g_1 h_1 = g_1'$. Similarly we can find a $h_2 \in H$ such that $g_2 h_2 = g_2'$. The composition of $g_1 H$ and $g_2 H$ gives $g_1 g_2 H$. The composition of $g_1' H$ and $g_2' H$ gives $g_1' g_2' H$. $g_1 g_2 H$

and $g_1' g_2' H$ are the same coset because

$$g_1' g_2' H = g_1 h_1 g_2 h_2 H = g_1 h_1 g_2 H = g_1 h_1 H g_2 = g_1 H g_2 = g_1 g_2 H \tag{3}$$

where for the second and fourth $=$ we have used the fact that $h_i H = H$, for the third and fifth $=$ we have used the property of normal subgroup that $gH = Hg$.

Therefore, the composition rule given above is well defined.

One way to calculate the composition of two cosets is to take the two sets of group elements $\{g_1 h_i\}$ and $\{g_2 h_j\}$, and combine them element wise into $\{g_1 h_i g_2 h_j\}$. There are r^2 elements in the combined set but there are repetitions. Only r of them are distinct, which form the resulting coset of $g_1 g_2 H$.

Next, we need to check the closure, associativity, identity and inverse conditions of a group.

(1) closure: if $g_1 H$ and $g_2 H$ are both cosets of H, then $g_1 g_2 H$ is also a coset because $g_1 g_2$ belongs to G if g_1 and g_2 both belong to G.

(2) associativity: this follows from the associativity of G.

$$[(g_1 H) \circ (g_2 H)] \circ (g_3 H) = (g_1 g_2 H) \circ (g_3 H) = (g_1 g_2) g_3 H = g_1 (g_2 g_3) H = g_1 H \circ [(g_2 H) \circ (g_3 H)] \tag{4}$$

(3) identity: $H = eH$ is the identity element in the set of cosets because $(eH) \circ (gH) = gH$ and $(gH) \circ (eH) = gH$.

(4) inverse: the inverse element of gH is $g^{-1}H$ because $(gH) \circ (g^{-1}H) = eH = (g^{-1}H) \circ (gH)$.

Basically, these group properties follow from the group properties of G.

Example: consider $G = \mathbb{Z}_4$, the group of integers with addition mod 4, $G = \{0, 1, 2, 3\}$. It contains a $\mathbb{Z}_2$ subgroup $H = \{0, 2\}$. Since G is an abelian group, the subgroup is normal. The two cosets are $\{0, 2\}$ and $\{1, 3\}$ which corresponds to even and odd numbers in the original set. The quotient group G/H is a $\mathbb{Z}_2$ group.

Example: Let's take G to be D_3 and H to be $C_3 = \{e, c, c^2\}$. H is a normal subgroup as explained above. There are two cosets $H = \{e, c, c^2\}$ and $b_1 H = \{b_1, b_2, b_3\}$. They compose as

$$(H) \circ (H) = H, (H) \circ (b_1 H) = b_1 H, (b_1 H) \circ (H) = b_1 H, (b_1 H) \circ (b_1 H) = H \tag{5}$$

Therefore, the quotient group G/H is isomorphic to the C_2 group.

Counter-example: Consider the $\{e, b_1\}$ subgroup of D_3. There are three left cosets: $H = b_1 H = \{e, b_1\}$, $cH = b_3 H = \{c, b_3\}$ and $c^2 H = b_2 H = \{c^2, b_2\}$. $\{e, b_1\}$ is not a normal subgroup of D_3, therefore the composition of the cosets is not well defined. Indeed we can check that

$$(H) \circ (cH) = cH \tag{6}$$

according to the definition, but

$$(b_1 H) \circ (cH) = b_2 H \neq cH \tag{7}$$

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

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \tag{8}$$

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.