2 Examples

2.3 The permutation group

Cayley's Theorem

Every finite group of order n can be considered as (is isomorphic to) a subgroup of S_n.

To prove this theorem, consider the n group elements of group G as the objects that are being permuted by S_n. We need to demonstrate the correspondence between the group elements of G and that of a subgroup of S_n.

First, notice that left multiplication of an element $g \in G$ on all group elements $\{h\}$ of G corresponds to a permutation of these n objects. This is because, firstly, if $gh_1 = gh_2$, then $h_1 = h_2$, which can be obtained by multiplying g^{-1} on both sides of the first equation. This implies that after left multiplication of g, there are n different elements in $\{gh, h \in G\}$ and they all belong to G. Therefore, left multiplication corresponds to the permutation of the n group elements in G.

Secondly, the permutation operation P_g obtained with left multiplication of $g \in G$ forms a group where the composition of P_{g_1} and P_{g_2} is simply the permutation operation obtained with left multiplication of $g_1 g_2$. The identity operation is P_e. The inverse of P_g is $P_{g^{-1}}$. And it is easy to verify that the composition of P_g's is associative. $\square$

* Note that this embedding of a group of order n into the permutation group S_n is different from the previous embedding of D_4 (which has 8 elements) into S_4.

2.4 The group of integers $\mathbb{Z}$

At the beginning of the class, we mentioned that the set of all integers $\mathbb{Z}$ form a group. The composition rule is addition and the identity element is 0. This group is different from all the previous examples in that there are an infinite number of elements. The group is still discrete but not finite. The $\mathbb{Z}$ group can be thought of as the $n \to \infty$ limit of the $\mathbb{Z}_n$ groups.

To take into account infinite groups like $\mathbb{Z}$, the generating set of a group needs to be more rigorously defined as a subset such that every element of the group can be expressed as the combination (under the group operation) of finitely many elements of the subset and their inverses. Under this definition, we can choose either $\{1\}$ or $\{-1\}$ as the generating set of the group of integers.

2.5 Circle group

The symmetry group of a directed circle.

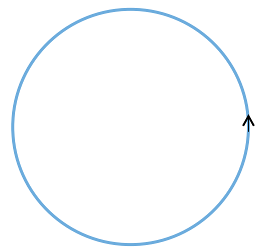

Figure 1: Directed circle

A directed circle has a continuous rotation symmetry. The circle is invariant under rotation by any angle $\theta \in [0, 2\pi)$. The composition of two rotation operations corresponds to the addition of two angles $\theta_1 + \theta_2 (\text{mod } 2\pi)$.

If we use the exponential $e^{i\theta}$ to represent the group element, then the group elements correspond to complex numbers of absolute value 1. The composition rule becomes multiplication $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2) \text{mod } 2\pi}$. The circle group has an infinite number of elements and the elements are continuous. Therefore, the circle group is said to be continuous.

The circle group can be thought of as another $n \to \infty$ limit of the C_n, hence the $\mathbb{Z}_n$, group. This is a different limit than the group of integers $\mathbb{Z}$.

2.6 Matrix group

A set of matrices can form a group.

General Linear Matrix Group: the set of $n \times n$ invertible matrices with matrix multiplication as the composition rule forms a group.

Comments:

(1) If the entries of the matrices are real numbers, the matrix group is said to be over $\mathbb{R}$ and denoted as $GL(n, \mathbb{R})$. If the entries of the matrices are complex numbers, the matrix group is said to be over $\mathbb{C}$ and denoted as $GL(n, \mathbb{C})$.

(2) The identity element in the group is the identity matrix.

(3) The matrix group is in general nonabelian.

(4) If we restrict to the set of matrices with determinant one, we get the special linear group $SL(n, \mathbb{R})$ or $SL(n, \mathbb{C})$.

(5) We can also restrict to orthogonal or unitary matrices and get the orthogonal group $O(n)$ or the unitary group $U(n)$.

3 Basic concepts in group theory

3.1 Conjugacy class

Conjugacy, definition: two elements a and b of a group G are conjugate if there exists an element $g \in G$ such that $a = gbg^{-1}$. The element g is called the conjugating element.

Example: in the Dihedral group D_3, two reflections b_1 and b_2 are conjugate because $b_2 = cb_1c^{-1}$.

Properties:

(1) every element is conjugate to itself $a = eae^{-1}$.

(2) if a is conjugate to b ($a = gbg^{-1}$), then b is conjugate to a ($b = g^{-1}ag$).

(3) if a is conjugate to b ($a = gbg^{-1}$), and b is conjugate to c ($b = hch^{-1}$), then a is conjugate to c ($a = ghc(gh)^{-1}$).

Conjugacy defines a particular kind of equivalence relation among group elements and conjugate elements are similar to each other in some ways.

For example, if a and b are conjugate to each other, then they have the same order.

To show this, assume the order of a is k_a and the order of b is k_b and $b = gag^{-1}$. Then

$$b^{k_a} = (gag^{-1})^{k_a} = ga^{k_a}g^{-1} = geg^{-1} = e \tag{1}$$

Therefore, k_b is a divisor of k_a. Similarly we can show that k_a is a divisor of k_b. Therefore, $k_a = k_b$. $\square$

Conjugacy class: Elements of a group which are conjugate to each other are said to form a conjugacy class.

Comments:

(1) Each element of a group belongs to one and only one conjugacy class. That is, different conjugacy classes are disjoint. (If a is conjugate with a set of b_i's and also conjugate with a set of c_j's, then the b_i's and c_j's are also conjugate with each other and they belong to the same conjugacy class.)

(2) The identity element forms a class by itself. (For any $g \in G$, $geg^{-1} = e$.)

(3) Each group can be partitioned into a number of disjoint conjugacy classes.

Examples:

(1) Cyclic group C_n

Because $gag^{-1} = a$ for any a and g in C_n, each group element forms a conjugacy class by itself. The number of conjugacy classes is equal to the number of group elements.

This is a result common to all abelian groups.

(2) Dihedral group D_3

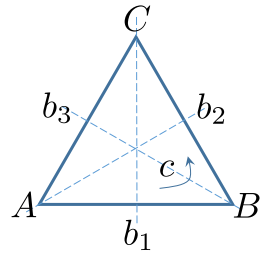

Figure 2: D_3 as the symmetry group of undirected regular triangle

D_3 contains 6 group elements $\{e, c, c^2, b_1, b_2, b_3\}$, where c is rotation by $2\pi/3$ and b_i's are reflection operations. Direct calculation shows

$$b_i c b_i^{-1} = c^2, c b_i c^{-1} = b_{i (\text{mod } 3)+1}, \tag{2}$$

That is, c is conjugate to c^2, and the b_i's are conjugate to each other.

Therefore these 6 elements can be partitioned into three conjugacy classes (e), (c, c^2), (b_1, b_2, b_3). Elements in the same conjugacy class represent similar operations: doing nothing, rotation, reflection.

(3) Dihedral group D_4

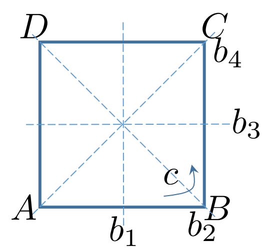

Figure 3: D_4 as the symmetry group of undirected square

The D_4 group contains 8 elements

$$\{e, c, c^2, c^3, b_1, b_2, b_3, b_4\} \tag{3}$$

where c is rotation by $\pi/2$, and b_i is reflection across the corresponding axis.

Direct calculation shows that

$$c b_1 c^{-1} = b_3, c b_3 c^{-1} = b_1, c b_2 c^{-1} = b_4, c b_4 c^{-1} = b_2, b_i c b_i^{-1} = c^3 \tag{4}$$

Therefore, the 8 elements are partitioned into five conjugacy classes (e), (b_1, b_3), (b_2, b_4), (c, c^3), (c_2). Note that while elements in the same conjugacy class have the same order, the reverse is not true. For example, b_2 and b_1 are both order 2 elements, but they are not conjugate to each other.

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.