Solution Set for Exercise Session No.1

Course: Mathematical Aspects of Symmetries in Physics,
ICFP Master Program (for M1)

13th November, 2014, at Room 235A

Lecture by Amir-Kian Kashani-Poor (email: kashani@lpt.ens.fr)
Exercise Session by Tatsuo Azeyanagi (email: tatsuo.azeyanagi@phys.ens.fr)

1 Some Basics

(1)

1. Let us call the two elements of the group G as e and g (here e is the unit and $g \neq e$). If $g \cdot g = g$, then we can multiply g^{-1} from left to have $g = e$. This is inconsistent with the assumption $g \neq e$. Therefore, it follows that $g \cdot g = e$ (or in other words, $g^{-1} = g$).

   To summarize, the multiplication table is given by

	e	g
e	e	g
g	g	e

   One can confirm from this table that $\{e, g\}$ is a group (associativity, ...).

   This multiplication table (and thus the group of order 2) is of course unique. From this table, it is obvious that this group is Abelian (symmetric under the reflection with respect to the diagonal line).

2. Let us call the three elements of the group G as e, g_1 and g_2 (here e is the unit, and e, g_1 and g_2 are different elements).

   We first notice that $g_1 \cdot g_2 = g_2 \cdot g_1 = e$ (if $g_1 \cdot g_2 = g_1$ or g_2, then we can multiply g_1^{-1} from the left or g_2^{-1} from the right, to get $g_2 = e$ or $g_1 = e$. This is inconsistent with the assumption. Thus we have confirmed that $g_1 \cdot g_2 = e$. A similar argument shows $g_2 \cdot g_1 = e$). This then means that $g_2 = g_1^{-1}$ (and $g_2^{-1} = g_1$).

   Let us next consider $g_1 \cdot g_1$. If $g_1 \cdot g_1 = e$ or g_1, then we can multiply g_1^{-1} from left (or right, whichever is fine) to get $g_1 = g_1^{-1}(= g_2)$ or $g_1 = e$. This is inconsistent with the assumption. Therefore, we conclude that $g_1 \cdot g_1 = g_1^{-1}$. By multiplying g_1^{-1} from left or right, we also get $g_1^{-1} \cdot g_1^{-1} = g_1$.

   To summarize, the multiplication table is written as

	e	g_1	g_1^{-1}
e	e	g_1	g_1^{-1}
g_1	g_1	g_1^{-1}	e
g_1^{-1}	g_1^{-1}	e	g_1

One can confirm from this table that $\{e, g_1, g_2\}$ is a group (associativity, ...).

This multiplication table (and thus the group of order 3) is of course unique. From this table, it is obvious that this group is Abelian (symmetric under the reflection with respect to the diagonal line).

3. Since G is a group, $g_i g \in G$ for elements $g_i, g \in G$. For $g_i, g_j \in G$ $(g_i \neq g_j)$, if $g_i g = g_j g$, then by multiplying g^{-1} from the right, we have $g_i = g_j$. This is inconsistent with the assumption. Thus we conclude that $g_i g \neq g_j g$ for $g_i, g_j \in G$ $(g_i \neq g_j)$. Therefore, $\{g_1 g, g_2 g, \cdots, g g_r g\}$ contains all the elements of G and each element of G appears one and only one time.

4. Let us call the four elements of the group G as e, a, b and c (here e is the unit, and e, a, b and c are all different). It is easy to fill out some part of the multiplication table as

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Let us now focus on $a \cdot a$. If $a \cdot a = a$, then by multiplying a^{-1} from the left, we have $a = e$. This is inconsistent with the assumption. Therefore, it follows that $a \cdot a = e, b$ or c. Without loss of generality, we can take as $a \cdot a = e$ or b.

We first consider the case with $a \cdot a = b$. By noticing that each element of G appears one and only one time in each column/row, we can fill out the table in the following way. First, we have

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c		
c	c	e		

Then we in the end have

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 1: The first case

Let us now consider another case: $a \cdot a = e$. By noticing that each element of G appears only one time in each column/row, we can fill out the table in the following way. First, we have

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

To fill out the rest part, there are two possibilities : (1) $b \cdot b = c \cdot c = e$ and $b \cdot c = c \cdot b = a$ (2) $b \cdot b = c \cdot c = a$ and $b \cdot c = c \cdot b = e$. The second case, however, is the same as Table 1 with a and b exchanged. Thus the second possibility is

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 2: The second case

To summarize, there are two possibilities: Table 1 and 2. One can confirm from these tables that $\{e, a, b, c\}$ is a group (associativity, ...). From these Tables, it is obvious that both of these groups of order 4 are Abelian.

(2) By definition, the left and right inverses of g, if exist, need to satisfy (by denoting them by g_1 and g_2)

$$(g_1 \cdot g)(n) = g_1(g(n)) = id(n) = n \,, \qquad (g \cdot g_2)(n) = g(g_2(n)) = id(n) = n \,,$$

respectively, for $\forall n \in \mathbb{N}$. Thus, the left inverse, if it exists, needs to satisfy $g_1(g(n)) = n$ which is equivalent to

$$g_1(n-1) = n \qquad (\text{for } n \geq 2) \,, \qquad g_1(1) = 1 \qquad (\text{for } n = 1) \,,$$

From the first relation, g_1 needs to be taken as $g_1(n) = n+1$ for $n \geq 1$, but this indicates $g_1(1) = 2$ which is obviously inconsistent with the second relation. Therefore there is no left inverse.

On the other hand, the right inverse, if it exists, needs to satisfy $g(g_2(n)) = n$ which is equivalent to

$$g_2(n) - 1 = n \qquad (\text{for } g_2(n) \geq 2)\,, \qquad n = 1 \qquad (\text{for } g_2(n) = 1)\,.$$

Thus we can take g_2 as

$$g_2(n) = \begin{cases} n+1 & (n \geq 2)\,, \\ 1 & (n = 1)\,. \end{cases}$$

Therefore there exists a right inverse.

2 Dihedral Group D_3: Symmetry of Equilateral Triangle

1. We can fill out the multiplication table as follows:

	e	c_3	c_3^{-1}	σ_1	σ_2	σ_3
e	e	c_3	c_3^{-1}	σ_1	σ_2	σ_3
c_3	c_3	c_3^{-1}	e	σ_3	σ_1	σ_2
c_3^{-1}	c_3^{-1}	e	c_3	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	e	c_3	c_3^{-1}
σ_2	σ_2	σ_3	σ_1	c_3^{-1}	e	c_3
σ_3	σ_3	σ_1	σ_2	c_3	c_3^{-1}	e

Table 3: Multiplication table for D_3

Here are some detail of the explicit multiplication. Fist let us call the location of the vertices 1, 2, 3 in the Figure (I mean at the beginning) as the location 1, 2, 3, respectively. Then by (m_1, m_2, m_3), we denote that vertices 1, 2, 3 are located at the location m_1, m_2, m_3, respectively, after transformation(s). Then we can denote the transformations as

- $e\,:\,(1,2,3) \to (1,2,3)$
- $c_3\,:\,(1,2,3) \to (2,3,1)$
- $c_3^{-1}\,:\,(1,2,3) \to (3,1,2)$
- $\sigma_1\,:\,(1,2,3) \to (1,3,2)$
- $\sigma_2\,:\,(1,2,3) \to (3,2,1)$
- $\sigma_3\,:\,(1,2,3) \to (2,1,3)$

Then, as an example, let us consider $c_3 \cdot c_3$, $\sigma_1 \cdot c_3$, $c_3 \cdot \sigma_2$ and $\sigma_1 \cdot \sigma_2$. They move the vertices $1, 2, 3$ as

- $c_3 \cdot c_3 \, : \, (1,2,3) \to (2,3,1) \to (3,1,2)$
- $\sigma_1 \cdot c_3 \, : \, (1,2,3) \to (2,3,1) \to (3,2,1)$
- $c_3 \cdot \sigma_2 \, : \, (1,2,3) \to (3,2,1) \to (1,3,2)$
- $\sigma_1 \cdot \sigma_2 \, : \, (1,2,3) \to (3,2,1) \to (2,3,1)$

Therefore we have

$$c_3 \cdot c_3 = c_3^{-1}\,, \qquad \sigma_1 \cdot c_3 = \sigma_2\,, \qquad c_3 \cdot \sigma_2 = \sigma_1\,, \qquad \sigma_1 \cdot \sigma_2 = c_3\,.$$

One can determine the other entries of the multiplication table in the same way.

2. The followings are the subgroups of D_3:

$$H_1 = \{e, c_3, c_3^{-1}\}\,, \qquad H_2 = \{e, \sigma_1\}\,, \qquad H_3 = \{e, \sigma_2\}\,, \qquad H_4 = \{e, \sigma_3\}\,.$$

Here is a one way to derive them. First of all, let us find a subgroup containing e and c_3. Then, it needs to contain c_3^{-1}. Then $H_1 = \{e, c_3, c_3^{-1}\}$ forms a subgroup. Similarly starting with e and c_3^{-1}, one can get H_1. Now we consider a subgroup containing e, c_3, c_3^{-1} as well as σ_1. Then σ_2 and σ_3 need to be included to form a subgroup. This is D_3 itself. The result is the same even when one starts with σ_2 or σ_3 instead of σ_1.

Let us next start with e and σ_1. These two elements form a subgroup $H_2 = \{e, \sigma_1\}$. Once one adds σ_2, σ_3, c_3 or c_3^{-1}, then, to form a subgroup, one needs to add all the elements of D_3. Therefore one always ends up with D_3 itself. The argument is the same when we start with e and σ_2 or σ_3.

Therefore the only nontrivial subgroups are $H_1 = \{e, c_3, c_3^{-1}\}$, $H_2 = \{e, \sigma_1\}, H_3 = \{e, \sigma_2\}$, and $H_3 = \{e, \sigma_3\}$ only.

Note: Here is a little bit quicker way to construct subgroups. In the lecture, it is shown that the order of a subgroup H of a group G divides the order of G. Since the order of S_3 is $3! = 6$, the order of the subgroup should be either 1, 2, 3 or 6. This fact simplifies some steps above. The subgroup of order 1 and 6 are trivial subgroups, $\{e\}$ and D_3, respectively. Thus the nontrivial subgroups have the order either 2 or 3. Therefore, in the above step, once one have to add more than three, one will end up with D_3.

3. We first recall the definition of the left coset decomposition. For a group G and its subgroup H, the left coset decomposition of G is

$$G = Hg_1 + Hg_2 + \cdots Hg_n\,, \qquad (Hg_i \cap Hg_j = \emptyset \text{ for } i \neq j)\,,$$

for some $g_i \in G$ ($i = 1, 2, \cdots n$, and $g_i \neq g_j$ for $i \neq j$). Usually g_1 is set to the unit, $g_1 = e$.

For each subgroup H_i ($i = 1, 2, 3, 4$), $H_i g$ ($g \in D_3$) is computed as

$$H_1 e = \{e, c_3, c_3^{-1}\}\,, \qquad H_1 c_3 = \{c_3, c_3^{-1}, e\}\,, \qquad H_1 c_3^{-1} = \{c_3^{-1}, e, c_3\}\,,$$

$$\begin{aligned}
&H_1\sigma_1 = \{\sigma_1, \sigma_3, \sigma_2\}\,, \qquad H_1\sigma_2 = \{\sigma_2, \sigma_1, \sigma_3\}\,, \qquad H_1\sigma_3 = \{\sigma_3, \sigma_2, \sigma_1\}\,,\\
&H_2e = \{e, \sigma_1\}\,, \qquad H_2c_3 = \{c_3, \sigma_2\}\,, \qquad H_2c_3^{-1} = \{c_3^{-1}, \sigma_3\}\,,\\
&H_2\sigma_1 = \{\sigma_1, e\}\,, \qquad H_2\sigma_2 = \{\sigma_2, c_3\}\,, \qquad H_2\sigma_3 = \{\sigma_3, c_3^{-1}\}\,,\\
&H_3e = \{e, \sigma_2\}\,, \qquad H_3c_3 = \{c_3, \sigma_3\}\,, \qquad H_3c_3^{-1} = \{c_3^{-1}, \sigma_1\}\,,\\
&H_3\sigma_1 = \{\sigma_1, c_3^{-1}\}\,, \qquad H_3\sigma_2 = \{\sigma_2, e\}\,, \qquad H_3\sigma_3 = \{\sigma_3, c_3\}\,,\\
&H_4e = \{e, \sigma_3\}\,, \qquad H_4c_3 = \{c_3, \sigma_1\}\,, \qquad H_4c_3^{-1} = \{c_3^{-1}, \sigma_2\}\,,\\
&H_4\sigma_1 = \{\sigma_1, c_3\}\,, \qquad H_4\sigma_2 = \{\sigma_2, c_3^{-1}\}\,, \qquad H_4\sigma_3 = \{\sigma_3, e\}\,. \qquad (2.1)
\end{aligned}$$

Thus we have the following ways of the decomposition of D_3

$$\begin{aligned}
D_3 &= H_1 + H_1\sigma_i \quad (i = 1, 2, 3)\,,\\
D_3 &= H_2 + H_2\sigma_2 + H_2\sigma_3 = H_2 + H_2c_3 + H_2\sigma_3\\
&= H_2 + H_2\sigma_2 + H_2c_3^{-1} = H_2 + H_2c_3 + H_2c_3^{-1}\,,\\
D_3 &= H_3 + H_3\sigma_1 + H_3\sigma_3 = H_3 + H_3c_3^{-1} + H_3c_3\\
&= H_3 + H_3\sigma_1 + H_3c_3 = H_3 + H_3c_3^{-1} + H_3\sigma_3\,,\\
D_3 &= H_4 + H_4\sigma_1 + H_4\sigma_2 = H_4 + H_4c_3 + H_4\sigma_2\\
&= H_4 + H_4\sigma_1 + H_4c_3^{-1} = H_4 + H_4c_3 + H_4c_3^{-1}\,.
\end{aligned}$$

4. We first notice that

$$\begin{aligned}
&eH_1 = \{e, c_3, c_3^{-1}\}\,, \qquad c_3H_1 = \{c_3, c_3^{-1}, e\}\,, \qquad c_3^{-1}H_1 = \{c_3^{-1}, e, c_3\}\,,\\
&\sigma_1H_1 = \{\sigma_1, \sigma_2, \sigma_3\}\,, \qquad \sigma_2H_1 = \{\sigma_2, \sigma_3, \sigma_1\}\,, \qquad \sigma_3H_1 = \{\sigma_3, \sigma_1, \sigma_2\}\,,\\
&eH_2 = \{e, \sigma_1\}\,, \qquad c_3H_2 = \{c_3, \sigma_3\}\,, \qquad c_3^{-1}H_2 = \{c_3^{-1}, \sigma_2\}\,,\\
&\sigma_1H_2 = \{\sigma_1, e\}\,, \qquad \sigma_2H_2 = \{\sigma_2, c_3^{-1}\}\,, \qquad \sigma_3H_2 = \{\sigma_3, c_3\}\,,\\
&eH_3 = \{e, \sigma_2\}\,, \qquad c_3H_3 = \{c_3, \sigma_1\}\,, \qquad c_3^{-1}H_3 = \{c_3^{-1}, \sigma_3\}\,,\\
&\sigma_1H_3 = \{\sigma_1, c_3\}\,, \qquad \sigma_2H_3 = \{\sigma_2, e\}\,, \qquad \sigma_3H_3 = \{\sigma_3, c_3^{-1}\}\,,\\
&eH_4 = \{e, \sigma_3\}\,, \qquad c_3H_4 = \{c_3, \sigma_2\}\,, \qquad c_3^{-1}H_4 = \{c_3^{-1}, \sigma_1\}\,,\\
&\sigma_1H_4 = \{\sigma_1, c_3^{-1}\}\,, \qquad \sigma_2H_4 = \{\sigma_2, c_3\}\,, \qquad \sigma_3H_4 = \{\sigma_3, e\}\,.
\end{aligned}$$

By comparing with (2.1), the normal subgroup (a subgroup H satisfying $gH = Hg$ for arbitrary $g \in D_3$) is $H_1 = \{e, c_3, c_3^{-1}\}$ only.

5. We first recall the definition of the conjugacy class. For a group G, the elements a and b are conjugate when $gag^{-1} = b$, $\exists g \in G$. One can see that this is the equivalence relation (that is, $a \sim b$ is defined by $gag^{-1} = b$, $\exists g \in G$). Then the conjugacy class of $a \in G$ is defined by $C(a) = \{gag^{-1} | g \in G\}$.

   We can construct the conjugacy class systematically in the following way. In Table 3, (i, j)-element is $g_i \cdot g_j$ (where $g_1 = e, g_2 = c_3, \cdots$). Therefore, if one multiplies g_i^{-1} from the right to (i, j)-element that element turns to $g_i \cdot g_j \cdot g_i^{-1}$ and thus all the elements in the j-th column become conjugate to g_j. Then, the elements in j-th column after multiplied by g_i^{-1} from the right to (i, j)-element form the conjugacy class (corresponding to g_j).

	$e \cdot g_i^{-1}$	$c_3 \cdot g_i^{-1}$	$c_3^{-1} \cdot g_i^{-1}$	$\sigma_1 \cdot g_i^{-1}$	$\sigma_2 \cdot g_i^{-1}$	$\sigma_3 \cdot g_i^{-1}$
e	e	c_3	c_3^{-1}	σ_1	σ_2	σ_3
c_3	e	c_3	c_3^{-1}	σ_2	σ_3	σ_1
c_3^{-1}	e	c_3	c_3^{-1}	σ_3	σ_1	σ_2
σ_1	e	c_3^{-1}	c_3	σ_1	σ_3	σ_2
σ_2	e	c_3^{-1}	c_3	σ_3	σ_2	σ_1
σ_3	e	c_3^{-1}	c_3	σ_2	σ_1	σ_3

Table 4: Table to find the conjugacy classes of D_3

By multiplying g_i^{-1} from the right to (i,j)-element $g_i \cdot g_j$, we obtain Table 4. We recall that

$$e^{-1} = e\,, \qquad c_3 = c_3^{-1}\,, \qquad \sigma_i^{-1} = \sigma_i \quad (\text{for } i = 1,2,3)\,.$$

From this, we have three conjugacy classes for the group D_3:

$$\{e\}\,, \qquad \{c_3, c_3^{-1}\}\,, \qquad \{\sigma_1, \sigma_2, \sigma_3\}\,.$$

——memo——

(i) Here we check that, for $a, b \in G$, "$a \sim b \Leftrightarrow gag^{-1} = b$ for some $g \in G$" is an equivalence relation. First of all, $a \sim a$ (for $a \in G$) is satisfied since $eae^{-1} = a$ for the unit element e of G. Secondly, when $a \sim b$ (for $a, b \in G$), there exists $g \in G$ such that $gag^{-1} = b$ and thus by multiplying g^{-1} from the left and g from the right, we obtain $a = g^{-1}bg = g^{-1}b(g^{-1})^{-1}$. Thus we have $b \sim a$. Finally when $a \sim b$ and $b \sim c$ (for $a, b, c \in G$), there exist $g, h \in G$ such that $gag^{-1} = b$ and $hbh^{-1} = c$. Then we have $c = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}$ and thus $a \sim c$. Therefore we have confirmed that this relation is indeed an equivalence relation.

(ii) Here is a definition of left coset decomposition of a group G. Let us consider a subgroup H of G. Then we the left coset decomposition is given by

$$G = Hg_1 + Hg_2 + \cdots + Hg_n\,,$$

for some $g_i \in G$ $(i = 1, 2, 3, \cdots, n)$ satisfying $Hg_i \cap Hg_j = \emptyset$ for $i \neq j$. Usually g_1 is taken as the unit element e of G. We can carry out the right coset decomposition in a similar way.

We note that for $g, g' \in G$, $Hg = Hg'$ or $Hg \cap Hg' = \emptyset$. This can be checked as follows. If not disjoint, then there exist $h_1, h_2 \in H$ such that $h_1 g = h_2 g'$. This leads to $g = h_1^{-1}h_2 g'$. Since an element of Hg is of the form hg $(h \in H)$, we have $hg = hh_1^{-1}h_2 g' \in Hg'$. Therefore $Hg \subset Hg'$. In the same way, we can show that $Hg \supset Hg'$. Thus we conclude that $Hg = Hg'$.

3 Permutation Group

1. There are $3! = 6$ ways of permuting $(1, 2, 3)$. Thus the order of S_3 is 6.

2. We can carry out the multiplication in the following way :

$$\begin{aligned}\pi_1 \cdot \pi_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} .\end{aligned}$$

3. We first recall that the elements of S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

From the elements

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

we can generate the rest of the elements of S_3 as follows :

$$\begin{aligned}\tau_1^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \\ \tau_1^3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \\ \tau_2\tau_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ \tau_1\tau_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.\end{aligned}$$

4. Let us recall Figure in Problem 2. Then the elements of D_3 can be regarded as the permutation of the vertices $(1, 2, 3)$. More precisely, let us denote the location of the vertices 1, 2, 3 at the beginning as the location 1, 2, 3. Then we denote the operation to move the vertices 1, 2, 3 located at the location 1, 2, 3 to the location m_1, m_2, m_3 as

$$\begin{pmatrix} 1 & 2 & 3 \\ m_1 & m_2 & m_3 \end{pmatrix}.$$

Then we can identifies the permutations with the elements of D_3 as

$$\begin{aligned} e &\leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & c_3 &\leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & c_3^{-1} &\leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \\ \sigma_1 &\leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \sigma_2 &\leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & \sigma_3 &\leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{aligned}$$

(2) We first confirm that $H = \{\pi(g) | g \in G\}$ is a subgroup of S_n or S_n itself. Since $\pi(g)$ is a permutation of n-elements, it is obvious that $H \subset S_n$. Then the next step is to show that H is a group:

- For $a, b \in G$, we have

$$\begin{aligned}
\pi(a)\pi(b) &= \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ ag_1 & ag_2 & \cdots & ag_n \end{pmatrix} \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ bg_1 & bg_2 & \cdots & bg_n \end{pmatrix} \\
&= \begin{pmatrix} bg_1 & bg_2 & \cdots & bg_n \\ abg_1 & abg_2 & \cdots & abg_n \end{pmatrix} \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ bg_1 & bg_2 & \cdots & bg_n \end{pmatrix} \\
&= \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ abg_1 & abg_2 & \cdots & abg_n \end{pmatrix} \\
&= \pi(ab) \in H\,. \qquad (3.1)
\end{aligned}$$

- Let us denote the unit element of G as e. Then

$$\pi(e) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ eg_1 & eg_2 & \cdots & eg_n \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 & g_2 & \cdots & g_n \end{pmatrix}.$$

  Thus $\pi(e) \in H$ is the unit of S_n.

- Let us consider $a \in G$ and denote its inverse as $a^{-1} \in G$. Then we have

$$\pi(a^{-1}) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ a^{-1}g_1 & a^{-1}g_2 & \cdots & a^{-1}g_n \end{pmatrix} = \begin{pmatrix} ag_1 & ag_2 & \cdots & ag_n \\ g_1 & g_2 & \cdots & g_n \end{pmatrix} = (\pi(a))^{-1}\,.$$

  Thus we have shown that $\pi(a^{-1}) \in H$ is the inverse of $\pi(a) \in H$.

From these, we conclude that H is a subgroup of S_n or S_n itself.

As a next step, we confirm that π is an isomorphic map from G to H. From (3.1), it is obvious that π is homomorphic. For different two elements $a, b \in G$ $(a \neq b)$, $ag_i \neq bg_i$ since the same element never appears in each column of the multiplication table of G. Thus we conclude that $a \neq b \to \pi(a) \neq \pi(b)$. This means that π is an injection. By construction of π, it is obvious that π is a surjection. Therefore π is an isomorphism from G to H.

From the above results, we conclude that a group G of order n is isomorphic to a subgroup of S_n or S_n itself.

(3) We first notice that

$$\sigma\pi\sigma^{-1} = \sigma(p_1^{(1)}p_2^{(1)}\cdots p_{\lambda_1}^{(1)})\sigma^{-1}\sigma(p_1^{(2)}p_2^{(2)}\cdots p_{\lambda_2}^{(2)})\sigma^{-1}\sigma\cdots\sigma^{-1}\sigma(p_1^{(r)}p_2^{(r)}\cdots p_{\lambda_r}^{(r)})\sigma^{-1}\,.$$

Thus it is enough to show that

$$\sigma(p_1^{(1)}p_2^{(1)}\cdots p_{\lambda_1}^{(1)})\sigma^{-1} = (q_1^{(1)}q_2^{(1)}\cdots q_{\lambda_1}^{(1)})\,,$$

for some $q_1^{(1)}, q_2^{(1)}, \cdots, q^{(1)}$. From now on, we denote $(p_1^{(1)}p_2^{(1)}\cdots p_{\lambda_1}^{(1)})$ as π for simplicity.

Let us denote σ as

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ m_1 & m_2 & \cdots & m_n \end{pmatrix} .$$

Let us consider the case in which π is given by

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & \lambda_1 - 1 & \lambda_1 & \lambda_1 + 1 & \cdots & n \\ 2 & 3 & \cdots & \lambda_1 & 1 & \lambda_1 + 1 & \cdots & n \end{pmatrix} ,$$

(that is, when $(p_1^{(1)} p_2^{(1)} \cdots p_{\lambda_1}^{(1)}) = (12 \cdots \lambda_1)$). Then we have

$$\begin{aligned}
&\sigma\pi\sigma^{-1} \\
&= \begin{pmatrix} 1 & 2 & \cdots & n \\ m_1 & m_2 & \cdots & m_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & \lambda_1 - 1 & \lambda_1 & \lambda_1 + 1 & \cdots & n \\ 2 & 3 & \cdots & \lambda_1 & 1 & \lambda_1 + 1 & \cdots & n \end{pmatrix} \begin{pmatrix} m_1 & m_2 & \cdots & m_n \\ 1 & 2 & \cdots & n \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & \cdots & n \\ m_1 & m_2 & \cdots & m_n \end{pmatrix} \begin{pmatrix} m_1 & m_2 & \cdots & m_{\lambda_1 - 1} & m_{\lambda_1} & m_{\lambda_1 + 1} & \cdots & m_n \\ 2 & 3 & \cdots & \lambda_1 & 1 & \lambda_1 + 1 & \cdots & n \end{pmatrix} \\
&= \begin{pmatrix} m_1 & m_2 & \cdots & m_{\lambda_1 - 1} & m_{\lambda_1} & m_{\lambda_1 + 1} & \cdots & m_n \\ m_2 & m_3 & \cdots & m_{\lambda_1} & m_1 & m_{\lambda_1 + 1} & \cdots & m_n \end{pmatrix} \\
&= \begin{pmatrix} m_{\lambda_1} & m_1 & m_2 & \cdots & m_{\lambda_1 - 1} & m_{\lambda_1 + 1} & \cdots & m_n \\ m_1 & m_2 & m_3 & \cdots & m_{\lambda_1} & m_{\lambda_1 + 1} & \cdots & m_n \end{pmatrix} ,
\end{aligned}$$

which is the cycle $(q_1^{(1)} q_2^{(1)} \cdots q_{\lambda_1}^{(1)}) = (m_1 m_2 m_3 \cdots m_{\lambda_1})$. For more general π, we can confirm the statement in a similar way.

Note on cycle decomposition

We can confirm the cycle decomposition of an element $\pi \in S_n$ as follows. We notice that π is a permutation of $\{1, 2, 3, \cdots, n\}$. For $a \in \{1, 2, 3, \cdots, n\}$, we consider the sequence

$$a, \pi(a), \pi^2(a), \cdots .$$

When there exist k and $l < k$ such that $\pi^k(a) = \pi^l(a)$, then we have $\pi^{k-l}(a) = a$. Thus, by taking the smallest $r = k - l$, we obtain a cycle $(a\pi(a) \cdots \pi^{r-1}(a))$. We call this cycle as π_a.

Now we take another element $b \in \{1, 2, 3, \cdots, n\}$ such that $b \notin \{a, \pi(a), \cdots, \pi^{r-1}(a)\}$. We can then similarly construct a cycle $(b\pi(b) \cdots \pi^{s-1}(b))$ for some s. We call this as π_b.

Now we confirm that $\{a, \pi(a), \cdots, \pi^{r-1}(a)\}$ and $\{b, \pi(b), \cdots, \pi^{s-1}(b)\}$ are disjoint. If there exist $p < r$ and $q < s$ such that $\pi^p(a) = \pi^q(b)$, then $b = \pi^{p-q}(a) = \pi^t(a)$ where $t \equiv p-q \pmod r$. This contradicts with the assumption that $b \notin \{a, \pi(a), \cdots, \pi^{r-1}(a)\}$. Thus we have confirmed that $\{a, \pi(a), \cdots, \pi^{r-1}(a)\}$ and $\{b, \pi(b), \cdots, \pi^{s-1}(b)\}$ are disjoint.

By repeating this procedure, we can see that π is decomposed into cycles as $\pi = \pi_a \pi_b \cdots$ where each element of $\{1, 2, \cdots, n\}$ appears one and only one time.