THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2070A Algebraic Structures 2019-20
Tutorial 4
Date: 30th September 2019

Problems:

1. Let V be the subgroup $\{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ of S_4. Find all the left cosets of V in S_4 and all the right cosets of V in S_4.

Solution. We can list all the elements of S_4 according the cycle pattern. S_4 has 5 cycle patterns: (i) trivial element; (ii) cycles of length 2; (iii) products of two disjoint cycles of length 2; (iv) cycles of length 3; (v) cycles of length 4. A complete list of elements in S_4 (in cycle notation) is

Cycle length	Elements in S_4
(i)	Id
(ii)	$(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$, $(3\ 4)$
(iii)	$(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$
(iv)	$(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$,
	$(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$
(v)	$(1\ 2\ 3\ 4)$, $(1\ 3\ 4\ 2)$, $(1\ 4\ 2\ 3)$,
	$(1\ 2\ 4\ 3)$, $(1\ 4\ 3\ 2)$, $(1\ 3\ 2\ 4)$

We apply a brute-force approach. We may obtain the following $6(=4!/4)$ left cosets:

$$\begin{aligned}
V &= \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}\\
(1,2)V &= \{(1,2), (3,4), (1,3,2,4), (1,4,2,3)\}\\
(1,3)V &= \{(1,3), (1,2,3,4), (2,4), (1,4,3,2)\}\\
(1,4)V &= \{(1,4), (1,2,4,3), (1,3,4,2), (2,3)\}\\
(1,2,3)V &= \{(1,2,3), (1,3,4), (2,4,3), (1,4,2)\}\\
(1,3,2)V &= \{(1,3,2), (2,3,4), (1,2,4), (1,4,3)\}.
\end{aligned}$$

Next we compute (similarly) the right cosets:

$$\begin{aligned}
V &= \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}\\
V(1,2) &= \{(1,2), (3,4), (1,3,2,4), (1,4,2,3)\}\\
V(1,3) &= \{(1,3), (1,2,3,4), (2,4), (1,4,3,2)\}\\
V(1,4) &= \{(1,4), (1,2,4,3), (1,3,4,2), (2,3)\}\\
V(1,2,3) &= \{(1,2,3), (1,3,4), (2,4,3), (1,4,2)\}\\
V(1,3,2) &= \{(1,3,2), (2,3,4), (1,2,4), (1,4,3)\}.
\end{aligned}$$

It is not simply a trial and errors, because we know two (left) cosets are either identical or disjoint. Thus as $(1,2) \notin V$, $(1,2)V$ and V are not identical cosets; as $(1,3) \notin (1,2)V$ and $(1,3) \notin V$, $(1,3)V$ must be different from V and from $(1,2)V$; .... Also you can see that the cosets do partition the whole group. ◀

2. Under what condition a left coset is also a subgroup?

Solution. Let G be a group and $H < G$. Let $g \in G$. The left coset gH is a subgroup if and only if $g \in H$.

Necessity: We first show that $gH = H$. It is clear that $gH \subset H$ as $g \in H$. On the other hand,

$$\forall h \in H, h = g(g^{-1})h \in gH.$$

Sufficiency: As gH is a subgroup, it must contain the identity, so $gh = e$ for some $h \in H$. It follows that $g = h^{-1} \in H$.

Remark; The right coset Hg is a subgroup if and only if $g \in H$. ◀

3. Suppose that $[G : H] = 2$. If a and b are not in H, show that $ab \in H$.

Solution. Let a, b be two elements in G but both not in H. In particular $b^{-1} \notin H$. Consider the partition $\{H, Hb^{-1}\}$. $a \notin H$, so $a \in Hb^{-1}$. Then we can write $a = hb^{-1}$ for some $h \in H$, hence $ab = h \in H$.

◀

4. Find all the subgroups of S_3.

Solution. By Lagrange's Theorem, the order of subgroup should be 1, 2, 3 or 6. First of all, subgroups of order 1 or 6 are $\{Id\}$ and S_3 respectively. For the subgroup of order 2 or 3, it found that it is cyclic by using the corollary of theorem of Lagrange as it is of prime order. We list those subgroups of order 2 or 3 below: $\langle(1\ \ 2)\rangle$, $\langle(1\ \ 3)\rangle$, $\langle(2\ \ 3)\rangle$, and $\langle(1\ \ 2\ \ 3)\rangle$. To conclude, all the subgroups of S_3 are $\{Id\}$, $\langle(1\ \ 2)\rangle$, $\langle(1\ \ 3)\rangle$, $\langle(2\ \ 3)\rangle$,$\langle(1\ \ 2\ \ 3)\rangle$ and S_3.

◀

5. Prove that the multiplicative group $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \times)$ of nonzero rational numbers is not finitely generated.

Solution.
- We prove by contradiction. Suppose $\mathbb{Q}^*$ is finitely generated.
- Let $x_1, x_2, \ldots, x_n$ be a set of generators of $\mathbb{Q}^*$.
- For each $i = 1, 2, \ldots, n$, write $x_i = \frac{a_i}{b_i}$ where a_i, b_i are nonzero integers.
- Let p be a prime number not dividing $a_1 a_2 \cdots a_n b_1 b_2 \cdots b_n$.
- Consider $p \in \mathbb{Q}^*$.
- More explicitly, there are integers $k_1, k_2, \ldots, k_n$ such that
$$p = \left(\frac{a_1}{b_1}\right)^{k_1} \cdot \left(\frac{a_2}{b_2}\right)^{k_2} \cdots \left(\frac{a_n}{b_n}\right)^{k_n}.$$
- Write
$$\left(\frac{a_1}{b_1}\right)^{k_1} \cdot \left(\frac{a_2}{b_2}\right)^{k_2} \cdots \left(\frac{a_n}{b_n}\right)^{k_n} = \frac{M}{N}.$$
Here M and N are two nonzero integers. They are made of the positive integral powers of a_i and b_i.
- We have $pN = M$.
- Note that $p|M$ while from the contribution of p, $p \nmid M$, hence a contradiction.
- We conclude that $\mathbb{Q}^*$ is not finitely generated.

◀

Optional Part

1. Show that S_n is generated by $\{(1, 2), (1, 2, 3, \ldots, n)\}$.

Solution. Note that

$$\begin{pmatrix}1 & 2 & 3 & \cdots & n\end{pmatrix}^r \begin{pmatrix}1 & 2\end{pmatrix} \begin{pmatrix}1 & 2 & 3 & \cdots & n\end{pmatrix}^{n-r} = \begin{cases} \begin{pmatrix}1 & 2\end{pmatrix} & \text{for } r = 0, \\ \begin{pmatrix}r+1 & r+2\end{pmatrix} & \text{for } r = 1, 2, \ldots, n-2, \\ \begin{pmatrix}n & 1\end{pmatrix} & \text{for } r = n-1. \end{cases}$$

For $r = 0$ or $n-1$, it is trivial. For $r = i$ with $1 \le i \le n-2$, $\begin{pmatrix}1 & 2 & 3 & \cdots & n\end{pmatrix}^{n-i}$ maps $i+1$ to 1, which is then mapped into 2 by $\begin{pmatrix}1 & 2\end{pmatrix}$, which is mapped into $i+2$ by $\begin{pmatrix}1 & 2 & 3 & \cdots & n\end{pmatrix}^{i}$. By a similar manner, $i+2$ maps to $i+1$. For the others, it is unchanged.

Let $\begin{pmatrix}i & j\end{pmatrix}$ be any transposition, written with $i < j$. We observe that
$$\begin{pmatrix}i & j\end{pmatrix} = \begin{pmatrix}i & i+1\end{pmatrix} \cdots \begin{pmatrix}j-2 & j-1\end{pmatrix} \begin{pmatrix}j-1 & j\end{pmatrix} \begin{pmatrix}j-2 & j-1\end{pmatrix} \cdots \begin{pmatrix}i & i+1\end{pmatrix}.$$

Every permutation in S_n can be written as a product of transpositions, which we now see can each be written as a product of the special transpositions $\begin{pmatrix}1 & 2\end{pmatrix}$, $\begin{pmatrix}2 & 3\end{pmatrix}$, …, $\begin{pmatrix}n & 1\end{pmatrix}$. And we have already shown that these in turn can be expressed as products of $\begin{pmatrix}1 & 2 & 3 & \cdots & n\end{pmatrix}$ and $\begin{pmatrix}1 & 2\end{pmatrix}$. The proof follows plainly.

◀