Chris Hayduk
Math A4900
Homework 6
10/23/2020

1. **Symmetric and alternating groups.**

   (a) In class we showed that S_n is generated by $T = \{(i\ j) \mid 1 \leqslant i < j \leqslant n\}$, the set of transpositions in S_n. Show by induction on $|j - i|$, that for $i < j$,

$$(i\ j) = (i\ i+1)(i+1\ i+2)\cdots(j-2\ j-1)(j-1\ j)(j-2\ j-1)\cdots(i+1\ i+2)(i\ i+1),$$

and conclude S_n is generated by $T' = \{(i\ i{+}1) \mid 1 \leqslant i < n\}$, the set of adjacent transpositions.

Proof. Let us begin with the base case $|j - i| = 1$. Since $i < j$, we have that $j - i > 0$, so we can rewrite our initial equation as,

$$\begin{aligned} |j - i| &= j - i \\ &= 1 \end{aligned}$$

This gives us that $j = i + 1$. Hence, by definition of j, we have $(i\ j) = (i\ i+1)$. Now fix $m \in \mathbb{N}$ such that $m > 1$. Suppose $|j - (i+1)| = m$ and that our desired condition holds for m. Then we have,

$$\begin{aligned} (i+1\ j) = (i+1\ i+2)&(i+2\ i+3)\cdots \\ &\cdots(j-2\ j-1)(j-1\ j)(j-2\ j-1)\cdots \\ &\cdots(i+2\ i+3)(i+1\ i+2) \end{aligned}$$

Let us multiply by $(i\ i+1)$ on the left and right on both sides the equation. This yields,

$$\begin{aligned} (i\ i+1)(i+1\ j)(i\ i+1) = (i\ i+1)&(i+1\ i+2)(i+2\ i+3)\cdots \\ &(j-2\ j-1)(j-1\ j)(j-2\ j-1)\cdots \\ &\cdots(i+2\ i+3)(i+1\ i+2)(i\ i+1) \end{aligned}$$

Now observe that $(i\ i+1)(i+1\ j)(i\ i+1) = (i\ j)$. So we get,

$$\begin{aligned} (i\ j) = (i\ i+1)&(i+1\ i+2)(i+2\ i+3)\cdots \\ &(j-2\ j-1)(j-1\ j)(j-2\ j-1)\cdots \\ &\cdots(i+2\ i+3)(i+1\ i+2)(i\ i+1) \end{aligned}$$

as required. In addition, note that $|j - i| = m + 1$ since $|j - (i+1)| = m$. Hence, the statement being true for $|j - (i+1)| = m$ implies the statement is true for $|j - i| = m + 1$. Thus, by induction this holds for any values i, j with $|j - i| = m \geqslant 1$.

□

(b) Let x, y be distinct 3-cycles in S_n.
[*Hint:* Give their entries names so you can reference them. Like, if $x = (a\ b\ c)$ is a three-cycle, you know a, b, and c are distinct, and you know $x = (b\ c\ a) = (c\ a\ b) \neq (a\ c\ b)$. So you can assume without loss of generality things like a is the smallest of the three, but *not* things like $a < b < c$.]

(i) Set $n = 4$ and assume $x \neq y^{-1}$. Show $\langle x, y\rangle = A_4$.
[*Hint:* $x = (a\ b\ c)$ and $y = (\alpha\ \beta\ \gamma)$, then what does $x \neq y$ and $x \neq y^{-1}$ tell you about $\{a, b, c\} \cap \{\alpha, \beta, \gamma\}$?.]

Proof. Note from the Lecture 12 notes, we have that:

$$\begin{aligned} A_4 = &\{1, (123), (124), (132), (134), (142), (143), \\ &(234), (243), (12)(34), (13)(24), (14)(23)\} \end{aligned}$$

Let $x = (a\, b\, c)$ and $y = (\alpha\, \beta\, \gamma)$. Assume $x \neq y$ and $x \neq y^{-1}$. Then we can assert that at least one object in x and y is different. In addition, since $n = 4$, there are only 4 possible object to permute. Since x contains three distinct objects, we also know at most 1 objects in y can be distinct from x, since if more than 2 objects were distinct we would have that $n > 4$. Hence, these statements together give us that $|\{a, b, c\} \cap \{\alpha, \beta, \gamma\}| = 2$. Assume without loss of generality that $\{a, b, c\} \cap \{\alpha, \beta, \gamma\} = \{a, b\} = \{\alpha, \beta\}$. We thus need to show that x and y generate 1, all possible 3 cycles, and all disjoint 2 cycles from the elements $\{\alpha, \beta, \gamma, c\}$ □

(ii) Set $n = 5$ and assume $x \neq y^{-1}$. Show that either

$$\begin{gathered} x \text{ and } y \text{ both fix some common elements of } [5] \\ (\text{there is some } i \in [5] \text{ such that } x(i) = i \text{ and } y(i) = i) \\ \text{and } \langle x, y\rangle \cong A_4, \end{gathered}$$

or

$$\begin{gathered} x \text{ and } y \text{ do not fix any common elements of } [5] \\ (\text{for all } i \in [5], \text{ if } x(i) = i \text{ then } y(i) \neq i) \\ \text{and } \langle x, y\rangle = A_5. \end{gathered}$$

[*Hint:* Try some examples.]

(iii) Show, for all n, that $\langle x, y\rangle$ is isomorphic to one of Z_3, A_4, A_5, or $Z_3 \times Z_3$.
[*Hint:* If a group is generated by two commuting elements x and y that otherwise satisfy no relations between them, then $\langle x, y\rangle \cong \langle x\rangle \times \langle y\rangle$.]

2. **Group actions.**

(a) Let $G \circlearrowright A$. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$. Deduce that if G acts transitively on A, then the kernel of the action is $\bigcap_{g \in G} gG_ag^{-1}$.

Proof. Recall that $G_a = \{g \in G \mid g \cdot a = a\}$ and $G_b = \{g \in G \mid g \cdot b = b\}$. Now fix $g_1 \in G$ such that $b = g_1 \cdot a$ and fix $g_2 \in G_b$. Then we have, $g_2 \cdot b = g_1 \cdot a$. □

(b) Let S_3 act on the set of ordered triples $A = \{(i, j, k) \mid i, j, k \in [3]\}$.

(i) Find the orbits of $S_3 \circlearrowright A$.
[*Hint*: Break into cases like $i = j = k$, $i = j \neq k$, etc. *Avoid* writing out all the orbits explicitly.]

(ii) For each orbit $\mathcal{O}$, choose one representative $a \in \mathcal{O}$ and calculate G_a. Verify that $|G : G_a| = |\mathcal{O}|$.

(c) Suppose G acts transitively on a finite set A (i.e. $[a] = A$ for all $a \in A$), and let $H \trianglelefteq G$. Note that the action of G on A restricts to an action of H on A, which is not *necessarily* transitive anymore. [*Example*: $G = D_8$ acts transitively on $A = \{1, 2, 3, 4\}$, but $H = \langle r^2 \rangle$ does not. The orbits under the action of H are $\{1, 3\}$ and $\{2, 4\}$.]

Let $\mathcal{O}_1 = [a_1]_H$, $\mathcal{O}_2 = [a_2]_H$, $\ldots$, $\mathcal{O}_r = [a_r]_H$ be the distinct orbits of the action of H on A. [*Hint*: It may be helpful to use set action notation. Namely, if $a \in A$, then the orbit of a under the action of H can be written as $H \cdot a = \{h \cdot a \mid h \in H\}$, whereas $G \cdot a$ is the orbit under the action of G.]

(i) Show that for each $a \in A$, $H_a = G_a \cap H$.

(ii) Prove that G permutes $\mathcal{O}_1$, $\mathcal{O}_2$, $\ldots$, $\mathcal{O}_r$, i.e.

- for each $g \in G$, $i \in [r]$, we have $g \cdot \mathcal{O}_i = \mathcal{O}_j$ for some $j \in [r]$ (where $g \cdot \mathcal{O}_i := \{g \cdot a \mid a \in \mathcal{O}_i\}$); and
- $\sigma_g : \{\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r\} \to \{\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r\}$ defined by $\mathcal{O}_i \mapsto g \cdot \mathcal{O}_i$ is a bijection for each $g \in G$.

(iii) Deduce that G acts on the set $\mathcal{A} = \{\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r\}$. Show that this action is transitive, and deduce that $|\mathcal{O}_i| = |\mathcal{O}_j|$ for all $i, j \in [r]$.

(iv) Fix $\mathcal{O} \in \mathcal{A}$, and let $a \in \mathcal{O}$ (so that $\mathcal{O} = H \cdot a$). Show that $|\mathcal{O}| = |H : H \cap G_a|$ and that $r = |G : HG_a|$ (where $r = |\mathcal{A}|$ as above).