THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2022-23
Tutorial 2 Solutions
22nd January 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

1. (a) To show that two permutations are equal, it can be verified by how they act on $\{1, ..., n\}$. Write $\sigma_1 = \sigma(i_1 i_2 \cdots i_k)\sigma^{-1}$ and $\sigma_2 = (\sigma(i_1) \cdots \sigma(i_k))$, let $x \in \{1, ..., n\}$. If $x = \sigma(i_l)$, then $\sigma_1(x) = \sigma(i_1 i_2 \cdots i_k)(i_l) = \sigma(i_{l+1})$, here the subscript is understood as numbers modulo k, i.e. if $l + 1 = k + 1$, then $i_{l+1} = i_1$. Meanwhile $\sigma_2(x) = \sigma(i_{l+1})$ by definition of cycle, so $\sigma_1(x) = \sigma_2(x)$. Otherwise, if $x \notin \{\sigma(i_1), ..., \sigma(i_k)\}$, then $\sigma^{-1}(x) \notin \{i_1, ..., i_k\}$, so it is fixed by the k-cycle, so $\sigma_1(x) = \sigma\sigma^{-1}(x) = x$, while $\sigma_2(x) = x$ for the same reason. So in any case, $\sigma_1 = \sigma_2$.

   In fact, the proposition holds more generally for a product of disjoint cycles.

   (b) By part (a), it suffices to find a permutation σ such that $\sigma(i_l) = j_l$ for $i = 1, ..., l$. This can always be achieved since all i_l's and j_l's are distinct. So it is possible to define $\sigma(i_l) = j_l$ and extend it to a function from $\{1, ..., n\}$ to itself.

   (c) There are $P^n_k = \frac{n!}{(n-k)!}$ many ways of permuting k numbers from $\{1, ..., n\}$. Given any such permutation, one can form a k-cycle, which is not unique since cyclic permuting the entries give the same k-cycle as element in S_n, therefore, each k-cycle is counted k many times. For example, $(1\,2\,3), (2\,3\,1)$ and $(3\,1\,2)$ are there representations of the same 3-cycles. So the number of k-cycles should be $\frac{1}{k}P^n_k = \frac{n!}{(n-k)!k}$.

2. Recall that from the lectures, we have seen that in $\mathbb{Z}_k$, an element i is a generator if and only if $\gcd(i, k) = 1$. Since a k-cycle σ has order k, it follows that $\langle\sigma\rangle = \{\mathrm{id}, \sigma, ..., \sigma^{k-1}\}$. Identifying $\langle\sigma\rangle \cong \mathbb{Z}_k$, the statement now reads, σ^i is a generator if and only if σ^i is a k-cycle.

   ($\Leftarrow$) If σ^i is a k-cycle, then $\langle\sigma^i\rangle$ has cardinality k, and it is clearly a subset of $\langle\sigma\rangle$, which has the same cardinality. Therefore $\langle\sigma^i\rangle = \langle\sigma\rangle$ and so σ^i is a generator.

   ($\Rightarrow$) If σ^i is a generator, then in particular it has order k. Now an element of order k may not necessarily be a k-cycle. If σ^i was not a k-cycle, then it is a product of shorter disjoint cycles whose lengths have least common multiple equals to k (see HW2 Q4). Since σ^i is a generator, $(\sigma^i)^l = \sigma$ is a k-cycle, this gives a contradiction since $(\sigma^i)^l$ is a product of powers of disjoint cycles, so it is itself a product of disjoint cycles whose lengths are smaller than k.

3. By the result of HW2 Q4, by expressing a permutation as disjoint cycles, it has order equal to the lcm of the lengths of the cycles. So an element has order equal to p prime, precisely when this lcm is equal to p. Therefore, only cycles of lengths 1 or p can appear, so it is a product of disjoint p-cycles.

4. For $n = 2k$, since $s^2 = \mathrm{id}$, we have $s = s^{-1}$. We also have $srs^{-1} = r^{-1}$, so inductively $sr^ks^{-1} = r^{-k} = r^k$, so r^k commutes with s. On the other hand, $r^jr^kr^{-j} = r^{j+k-j} = r^k$, so r^k also commutes with r^j for arbitrary j. Finally, for r^is, note that $(r^is)r^k(r^is)^{-1} = r^isr^ks^{-1}r^{-i} = r^ir^{-k}r^{-i} = r^{-k} = r^k$. So r^k commutes with every element in D_{2k}.

5. $r^2sr^6sr^3 = r^2(sr^6)(sr^3) = r^2(r^{-6}s)(sr^3) = r^{-4}s^2r^3 = r^{-1}$.

   $(sr^4)sr^3(sr^2) = (r^{-4}s)sr^3(r^{-2}s) = r^{-4}r^3r^{-2}s = r^{-3}s$.

6. For $n \geq 3$, they are not even abelian. For example, in D_n, $sr = r^{-1}s \neq rs$ since $r \neq r^{-1}$ for $n \geq 3$. And in S_n, $(12)(23) = (312)$ and $(23)(12) = (132)$ are not equal.

   Another reason is that these groups do not contain elements that have the same order as the group. In D_n, elements have orders either dividing n or 2. Meanwhile, in S_n, elements have orders given by lcm of partitions of n, which is nowhere close to $|S_n| = n!$.