Solutions to Assignment 3

Cycle decomposition, orders and cyclic groups

MAU22101 — Group Theory

NAME AND SURNAME: .....

STUDENT NUMBER: ..... NUMBER OF PAGES: .....

Note. Solutions to this assignment are **due** by 3:00 pm on Thursday, October 10th. Remember to **fill in** all the information above and **staple** all your sheets together, including this one. All exercises are weighed equally unless otherwise stated.

Recollections. Let G be a group. An element $g \in G$ *has order* $n \in \mathbb{N}$ if this is the least positive integer such that $g^n = 1$. If no such integer exists, we say that g has *infinite order*. We say a subset of elements $S \subseteq G$ *generates* G if every element of G can be written as a product of elements of S and inverses of these elements. A group is *cyclic* if it is generated by a single element. Recall that every permutation in a symmetric group can be written as a disjoint product of cycles, and that the inverse of a cycle is a cycle. Thus, any symmetric group is generated by cycles.

Exercise 1. Show that, in each case, every cycle in S_n can be written as a product of elements or their inverses in the following sets. Explain why this implies that each of these sets of elements generate the symmetric groups.

$$G_1 = \{(i, i+1) \text{ with } 1 \leqslant i < n\}, \quad G_2 = \{(1, i) \text{ with } 1 \leqslant i \leqslant n\}, \quad G_3 = \{(12), (123\cdots n)\}.$$

Solution 1. We begin by observing that if $\gamma = (i_1 \cdot i_t)$ is a cycle and if $\sigma \in S_n$ then $\sigma\gamma\sigma^{-1}$ is the cycle $(\sigma(i_1)\cdots\sigma(i_t))$. We now show that G_2 and G_3 generate G_1, and then that G_1 generates S_n. For the first claim, note that if $\sigma = (123\cdots n)$ then $\sigma(12)\sigma^{-1} = (23)$. Repeating this we obtain $(34), \ldots, (n-1, n)$: these are the elements of G_1. Similarly, note that $(1, i)(1, i+1)(1, i) = (i, i+1)$. We now show that G_1 generates S_n by showing every transposition $(i\,j)$ with $i < j$ is a product of element of G_1. For this, note that when $j = i+1$ there is nothing to prove. For $j > i+1$, we have that $(j-1, j)(i\,j)(j-1, j) = (i, j-1)$, so we can proceed by induction on j. This completes the proof.

Exercise 2. Consider the following two invertible matrices

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Show that $\alpha^4 = \beta^3 = 1$, so both these matrices have finite order, but that the product $\alpha\beta$ has infinite order. Conclude that a group generated by elements with finite order can be infinite.
Bonus: Can you determine the group that α and β generate?

Solution 2. The fact that $\alpha^3 = \beta^4 = 1$ is a computation, which we trust you can carry out. We have $\alpha\beta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and then for any $N \in \mathbb{N}$ we have $(\alpha\beta)^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ which is not the identity.

Exercise 3. Consider the set of integers modulo $n \in \mathbb{N}$, $\mathbb{Z}/n = \{[0], [1], ..., [n-1]\}$. Define addition $+ : \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$ by the formula $[a] + [b] = [a+b]$. Show that:

- The operation + is well-defined: it does not depend on the choice of representatives.
- The element [0] is the identity for + and that every element has an inverse.
- The element [1] generates this group. We say that $\mathbb{Z}/n$ is a *cyclic group of order n*.

Exercise 4. With the notation of the last exercise, show that there is a product $\mathbb{Z}/n \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/n$ such that $[a][b] = [ab]$. This has identity element [1]. Is it true that $\mathbb{Z}/n$ with this product is a group? **Hint:** consider $n = 4$.

Solution 4. Let us solve both exercises at once. The operation is well defined, for if n divides a and b, it divides the sum $a+b$, and similarly, it divides the product ab. It is immediate that the respective identities are the [0] and [1]. Every element $[a]$ has an inverse under addition, namely, the class $[-a]$. Moreover, any element $[a]$ can be written by adding a instances of [1]. It is not true that $\mathbb{Z}/4$ is a group, because, for example, $[2][2] = [0]$, so this element cannot have an multiplicative inverse. Of course, [0] doesn't have a multiplicative inverse either. (We just forgot to exclude it from the set when asking whether this set formed a group.)