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.

$$S_1 = \{(i, i+1) \text{ with } 1 \leqslant i < n\}, \quad S_2 = \{(1, i) \text{ with } 1 \leqslant i \leqslant n\}, \quad S_3 = \{(12), (123\cdots n)\}.$$

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?

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 $n = 4$.