380C PROBLEM SET 2

DUE WEDNESDAY, SEPTEMBER 15TH

Problem 1. Show that any subgroup H of $(\mathbb{Z}, +)$ is of the form $m\mathbb{Z} = \{m \cdot n \mid n \in \mathbb{Z}\}$ for some $m \in \mathbb{Z}$.

Problem 2. In this problem, we offer convenient notation for elements of symmetric groups.

Let $(1\,4\,5)(2\,6) \in S_6$ denote the automorphism $\sigma : \{1, \ldots, 6\} \to \{1, \ldots 6\}$ defined by:

$$1 \mapsto 4, 2 \mapsto 6, 3 \mapsto 3, 4 \mapsto 5, 5 \mapsto 1, 6 \mapsto 2.$$

Here a subsequence contained in parentheses is called a *cycle*; the number of elements it contains is its *length*. For example, the above element σ has 3 cycles $(1\,4\,5)$, $(2\,6)$, and (3), and these cycles have length 3, 2, and 1 respectively. An expression of the above type for some $\sigma \in S_n$ is called a *cycle decomposition* of σ.

Some conventions: we typically do not explicitly write cycles of length 1 in a cycle decomposition unless it is needed for clarity; in that case, we would write the element σ above as $(1\,4\,5)(2\,6)(3)$. We write individual cycles with their minimal elements first, and we order cycles according to the minimal element in each cycle.

To be completely explicit: we read a cycle decomposition by sending an element to its rightward neighbor within its cycle, reading a cycle cyclically if we are considering the rightmost element of the cycle.

(a) Show that elements of S_n are in canonical bijection with actions of $\mathbb{Z}$ on $\{1, \ldots, n\}$.

(b) Suppose $\sigma \in S_n$ is fixed. Show that it has a unique cycle decomposition. Show that the cycles in the cycle decomposition are in canonical bijection with the orbits for the corresponding $\mathbb{Z}$ action on $\{1, \ldots, n\}$. Show that the length of a cycle equals the size of the corresponding orbit.

Problem 3. Let $\sigma \in S_n$ be given. Let F_σ denote the set:

$$\mathsf{F}_\sigma = \{(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\} \mid i < j \text{ and } \sigma(j) < \sigma(i)\}.$$

Define the *length*[1] *function* $\ell : S_n \to \mathbb{Z}^{\geqslant 0}$ via:

$$\ell(\sigma) := |\mathsf{F}_\sigma|.$$

For $1 \leqslant i < n$, we let $\tau_i := (i\ \ i{+}1) \in S_n$. A *simple transposition* in S_n is an element of the form τ_i for some i. A *transposition* in S_n is any element of the form $(i\,j)$ for $i \neq j$.

(a) Show that $\ell(1) = 0$ (for $1 \in S_n$ the identity element).
(b) Show that $\ell(\sigma) = 1$ if and only if σ is a simple transposition.
(c) Let $\sigma_0 \in S_n$ be the automorphism $i \mapsto n+1-i$. Show that $\ell(\sigma_0) = \binom{n}{2}$. Show that $\ell(\sigma) \leqslant \ell(\sigma_0)$ for any $\sigma \in S_n$ with equality if and only if $\sigma = \sigma_0$.
(d) For any simple transposition τ_i and any $\sigma \in S_n$, show that $\ell(\tau_i\sigma) = \ell(\sigma) \pm 1$.
(e) For any $\sigma \in S_n$ other than the identity, show that there exists some $1 \leqslant i < n$ such that $\ell(\tau_i\sigma) < \ell(\sigma)$.
(f) Show that $\ell(\sigma)$ is the minimal integer N such that σ can be written as a product of N simple transpositions. (In particular, deduce that any element of S_n can be written as a product of transpositions.)
(g) Define the *sign* map $\mathrm{sgn} : S_n \to \{1, -1\}$ as $\sigma \mapsto (-1)^{\ell(\sigma)}$. Show that sgn is a homomorphism (for $\{1, -1\}$ considered as a group under multiplication).
(h) Show that any (not necessarily simple) transposition has sign -1.

[1]I regret to say that is not related to the notion of *cycle length* from the previous problem. I do not make the rules, I just follow them.