**Assignment 11 – Part 1 – Math 412**

Textbook exercises:[1]

**Section 7.3:** 17

**Section 7.4:** 15

Other exercises:

(1) Generators and orders of elements in cyclic groups. Let $n \in \mathbf{Z}_{\geq 2}$.

(a) Let $[a] \in \mathbf{Z}/n\mathbf{Z}$, let $g = \gcd(a, n)$, and let $d = n/g$. Show that $\#[a] = d$. (Hint: first show that $d[a] = 0$ so that $\#[a] \leq d$, then show that if $m[a] = 0$, then $d \mid m$.)

(b) Conclude from part (a) that $[a]$ is a generator of $\mathbf{Z}/n\mathbf{Z}$ if and only if $[a] \in (\mathbf{Z}/n\mathbf{Z})^{\times}$.

(c) Show that 1 and $-1$ are the only generators of $\mathbf{Z}$.

(2) (WI) Subgroups of cyclic groups.

(a) Let $n \in \mathbf{Z}_{\geq 1}$. Show that every subgroup of $\mathbf{Z}/n\mathbf{Z}$ is cyclic. (Hint: let $H \leq \mathbf{Z}/n\mathbf{Z}$. For $H \neq 0$, let $m$ be the least positive integer such that $[m] \in H$. Show that $H = \langle [m] \rangle$, i.e. that for every element $[a] \in H$, $m \mid a$. The Division Algorithm may come in handy.)

(b) Similarly, show that every subgroup of $\mathbf{Z}$ is cyclic.

(3) All the subgroups of cyclic groups. Let $n \in \mathbf{Z}_{\geq 2}$.

(a) Suppose $d \mid n$. Show that there is an element of order $d$ in $\mathbf{Z}/n\mathbf{Z}$.

(b) Let $[a] \in \mathbf{Z}/n\mathbf{Z}$ and let $g = \gcd(a, n)$. Show that $[g] \in \langle [a] \rangle$. (Hint: Bézout's identity.)

(c) In part (b), note that $[a] \in \langle [g] \rangle$ since $g \mid a$. Conclude that $\langle [a] \rangle = \langle [g] \rangle$. (Hint: for any $[b]$, we have that $\langle [b] \rangle = \{m[b] : m \in \mathbf{Z}\}$.)

(d) Conclude from the above parts and Questions (1) and (2) that in a cyclic group of order $n$ there is a unique cyclic subgroup of order $d$ for every $d \mid n$, $d \geq 1$, and that these are the only subgroups of $\mathbf{Z}/n\mathbf{Z}$.

[1] From Hungerford's *Abstract algebra, An introduction, Third edition*