Tutorial #3.2: Cyclic Group

1 Exercise 1:

All cyclic subgroups of $G = (\mathbb{Z}_7, *)$

$$\begin{aligned}
&< 1 > = \{1\} \\
&< 2 > = \{1, 2, 4\} \\
&< 3 > = \{1, 2, 3, 4, 5, 6\} \\
&< 4 > = \{1, 2, 4\} \\
&< 5 > = \{1, 2, 3, 4, 5, 6\} \\
&< 6 > = \{1, 6\}
\end{aligned}$$

2 Exercise 2:

Let a be the generator of cyclic group G. Thus, $G = < a >$

a) G be a cyclic group of order 6 ($C_6 = \{1, a, a^2, a^3, a^4, a^5\}$). There only a and a^5 generates C_6.

b) G be a cyclic group of order 5 ($C_5 = \{1, a, a^2, a^3, a^4\}$). All elements excepts 1 can generate C_5.

c) G be a cyclic group of order 8 ($C_8 = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7\}$). There are a, a^3, a^5, a^7 generates C_8

d) G be a cyclic group of order 10 ($C_{10} = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}$). There are a, a^3, a^7, a^9 generates C_{10}

3 Exercise 3:

In general, to determines if G is a cyclic group, we must find a generator g such $< g > = G$. g is an element in G and is a co-prime.

For example, to determines whether if Z_6^* is a cyclic group, we only needs to test $g \in \{1, 5\}$

a) $G = \mathbb{Z}_7^* = < 3 >$. Thus, G is cyclic

b) $G = \mathbb{Z}_{12}^*$. Since there exists no such $g \in \{1, 5, 7, 11\}$ that generates $\mathbb{Z}_{12}^*$, G is not cyclic.

4 Exercise 4:

a) $U(18) = \{1, 5, 7, 11, 13, 17\}$. The subgroup generated by 5 in $U(18)$ is $\{1, 5, 7, 11, 13, 17\}$.

b) $U(20) = \{1, 3, 5, 7, 9, 11, 13, 17, 19\}$. The subgroup generated by 3 in $U(20)$ is $\{1, 3, 7, 9\}$

5 Exercise 5:

a) As $< 3 >= \{1, 3, 7, 9\}$, $< 3 >$ is a cyclic subgroup of order 4 in $G = Z_{20}^*$.

b) Let $G_{non-cyclic}$ be $\{1, 2, 3, 4\}$ is a subgroup of Z_{20}^*. While possible generator of $G_{non-cyclic}$ is $g \in \{1, 2, 3, 4\}$, there exist no such g generates $G_{non-cyclic}$. Thus, $G_{non-cyclic}$ is a non-cyclic subgroup of G

6 Exercise 6:

Prove that: b is generator of G. Given that $G = < a >$ and $b \in G$ such that $a = b^k$.
Proof: As $G = < a >$, it's trivial that $G = \{1, a, a^2, ...a^n\}$. While we having $a = b^k$, we can derive G as $G = \{1, b^k, b^{2k}, ..., b^{nk}\}$. Hence, b is a generator of G.