Cyclic Group Exercises: Answers

1. (a) Generators are g^k for $1 \leq k \leq 4$.
   (b) Generators are g^k for $k \in \{1, 3, 7, 9\}$.
   (c) Generators are g^{2k-1} for $1 \leq k \leq 8$.
   (d) Generators are g^k for $k \in \{1, 3, 7, 9, 11, 13, 17, 19\}$.

2. (a) Generators of $\mathbb{Z}_5$ are k for $1 \leq k \leq 4$.
   (b) Generators of $\mathbb{Z}_{10}$ are k for $k \in \{1, 3, 7, 9\}$.
   (c) Generators of $\mathbb{Z}_{16}$ are $2k - 1$ for $1 \leq k \leq 8$.
   (d) Generators of $\mathbb{Z}_{20}$ are k for $k \in \{1, 3, 7, 9, 11, 13, 17, 19\}$.

3. (a) $U(7)$ is cyclic with generator 3.
   (b) $U(12)$ is not cyclic: every nonidentity element has order 2, but $U(12)$ has order 8.
   (c) $U(16)$ is not cyclic: the nonidentity elements have orders 2 or 4, but $U(16)$ has order 8.
   (d) $U(11)$ is cyclic with generator 2.

4. (a) $|g^2| = 10$ (b) $|g^8| = 5$ (c) $|g^5| = 4$ (d) $|g^3| = 20$

5. (a) Subgroups: $H_1 = \langle e \rangle$, $H_2 = \langle g^2 \rangle$, $H_3 = \langle g^4 \rangle$, $H_4 = G$.
   (b) Subgroups: $H_1 = \langle e \rangle$, $H_2 = \langle g^2 \rangle$, $H_3 = \langle g^5 \rangle$, $H_4 = G$.
   (c) Subgroups: $H_1 = \langle e \rangle$, $H_2 = \langle g^2 \rangle$, $H_3 = \langle g^3 \rangle$, $H_4 = \langle g^6 \rangle$, $H_5 = \langle g^9 \rangle$, $H_6 = G$.
   (d) Subgroups $H_1 = \langle e \rangle$, $H_2 = \langle g^p \rangle$, $H_3 = \langle g^{p^2} \rangle$, $H_4 = G$.
   (e) Subgroups $H_1 = \langle e \rangle$, $H_2 = \langle g^p \rangle$, $H_3 = \langle g^q \rangle$, $H_4 = G$.
   (f) Subgroups $H_1 = \langle e \rangle$, $H_2 = \langle g^p \rangle$, $H_3 = \langle g^{p^2} \rangle$, $H_4 = \langle g^q \rangle$, $H_5 = \langle g^{pq} \rangle$, $H_6 = G$.

6. (a) $H = \langle a \rangle$
   (b) $H = \langle a^2 \rangle$
   (c) $H = \langle a^d \rangle$
   (d) $H = G$

Below are detailed solutions to a couple of the exercises.

Exercise 6. Part (c)

Claim: If $G = \langle a \rangle$ and $x = x^m$, $y = a^k$, then the subgroup, generated by x and y, is $H = \langle x, y \rangle = \langle a^d \rangle$, where $d = \gcd(m, k)$.

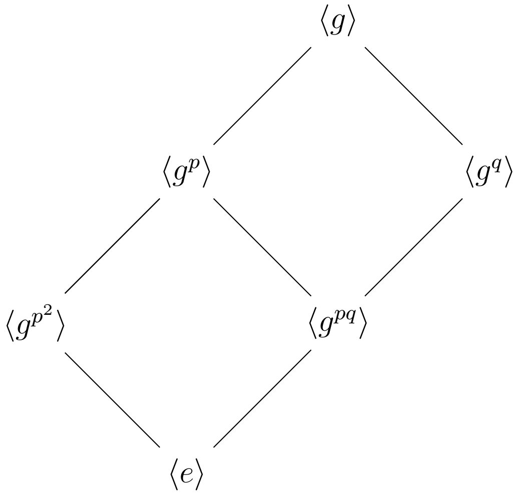
Proof. If $d = \gcd(m, k)$, then there exist integers r, s such that $d = rm + sk$. Therefore, $a^d = a^{rm+sk} = a^{rm+sk} = a^{rm}a^{sk} = x^r y^s$. This proves that $a^d \in \langle x, y \rangle$, so $\langle a^d \rangle \subseteq \langle x, y \rangle$. On the other hand, $d \mid m$, so $m = \alpha d$ and $x = a^m = a^{\alpha d} = (a^d)^\alpha$, so $x \in \langle a^d \rangle$. Similarly, $d \mid k$, so $k = \beta d$ and $y = a^k = a^{\beta d} = (a^d)^\beta$, so $y \in \langle a^d \rangle$. Therefore, $\langle x, y \rangle \subseteq \langle a^d \rangle$. □

Exercise 5. Part (f)

If $|g| = p^2 q$, then the subgroups of $G = \langle g \rangle$ are

$$G, \quad \langle g^p \rangle, \quad \langle g^{p^2} \rangle, \quad \langle g^q \rangle, \quad \langle g^{pq} \rangle, \quad \langle g^{p^2 q} \rangle = \langle e \rangle,$$

and we have $\langle g^m \rangle \leq \langle g^k \rangle$ if and only if $k \mid m$. Therefore, the subgroup lattice is given by the Hasse diagram below.


$\langle g \rangle$
$\langle g^p \rangle$
$\langle g^q \rangle$
$\langle g^{p^2} \rangle$
$\langle g^{pq} \rangle$
$\langle e \rangle$