CH4: Cyclic Groups Selected Exercise Solutions

Exercise 1: Find all generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

Solution: For a cyclic group $\mathbb{Z}_n$, an element k is a generator if and only if $\gcd(k, n) = 1$.

For $\mathbb{Z}_6$:

- Elements: $\{0, 1, 2, 3, 4, 5\}$
- Check: $\gcd(1, 6) = 1$ ✓, $\gcd(2, 6) = 2$ ✗, $\gcd(3, 6) = 3$ ✗, $\gcd(4, 6) = 2$ ✗, $\gcd(5, 6) = 1$ ✓
- **Generators:** $\{1, 5\}$

For $\mathbb{Z}_8$:

- Elements: $\{0, 1, 2, 3, 4, 5, 6, 7\}$
- Check: $\gcd(1, 8) = 1$ ✓, $\gcd(3, 8) = 1$ ✓, $\gcd(5, 8) = 1$ ✓, $\gcd(7, 8) = 1$ ✓
- **Generators:** $\{1, 3, 5, 7\}$

For $\mathbb{Z}_{20}$:

- Elements: $\{0, 1, 2, ..., 19\}$
- Since $20 = 2^2 \cdot 5$, we need elements not divisible by 2 or 5
- **Generators:** $\{1, 3, 7, 9, 11, 13, 17, 19\}$

Exercise 2: Suppose that $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are cyclic groups of orders 6, 8, and 20, respectively. Find all generators of $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$.

Solution: If $G = \langle g \rangle$ with $|g| = n$, then g^k generates G if and only if $\gcd(k, n) = 1$.

For $\langle a \rangle$ **with** $|a| = 6$: **Generators:** $\{a^1, a^5\}$

For $\langle b \rangle$ **with** $|b| = 8$: **Generators:** $\{b^1, b^3, b^5, b^7\}$

For $\langle c \rangle$ **with** $|c| = 20$: **Generators:** $\{c^1, c^3, c^7, c^9, c^{11}, c^{13}, c^{17}, c^{19}\}$

Exercise 3: List the elements of the subgroups $\langle 20 \rangle$ and $\langle 10 \rangle$ in $\mathbb{Z}_{30}$. Let a be a group element of order 30. List the elements of the subgroups $\langle a^{20} \rangle$ and $\langle a^{10} \rangle$.

Solution: In $\mathbb{Z}_{30}$,

- $\langle 20 \rangle = \{0, 20, 10\}$ (order 3)
- $\langle 10 \rangle = \{0, 10, 20\}$ (order 3)

Note: $\langle 20 \rangle = \langle 10 \rangle$ since $\gcd(20, 30) = \gcd(10, 30) = 10$

For group element a with $|a| = 30$:

- $\langle a^{20} \rangle = \{e, a^{20}, a^{10}\}$ (order 3)
- $\langle a^{10} \rangle = \{e, a^{10}, a^{20}\}$ (order 3)

Exercise 4: List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$. Let a be a group element of order 18. List the elements of the subgroups $\langle a^3 \rangle$ and $\langle a^{15} \rangle$.

Solution: In $\mathbb{Z}_{18}$,

- $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$ (order 6)
- $\langle 15 \rangle = \{0, 15, 12, 9, 6, 3\}$ (order 6)

Note: $\langle 15 \rangle = \langle 3 \rangle$ since $15 \equiv -3 \pmod{18}$

For group element a with $|a| = 18$:

- $\langle a^3 \rangle = \{e, a^3, a^6, a^9, a^{12}, a^{15}\}$ (order 6)
- $\langle a^{15} \rangle = \{e, a^{15}, a^{12}, a^9, a^6, a^3\}$ (order 6)

Exercise 5: List the elements of the subgroups $\langle 3 \rangle$ and $\langle 7 \rangle$ in $U(20)$.

Solution: $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

For $\langle 3 \rangle$**:**

- $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 7 \pmod{20}$, $3^4 = 21 \equiv 1 \pmod{20}$
- $\langle 3 \rangle = \{1, 3, 9, 7\}$ (order 4)

For $\langle 7 \rangle$**:**

- Since $3 \cdot 7 \equiv 1 \pmod{20}$, we have $7 = 3^{-1}$
- $\langle 7 \rangle = \langle 3^{-1} \rangle = \langle 3 \rangle = \{1, 7, 9, 3\}$ (order 4)

Exercise 6: What do Exercises 3, 4, and 5 have in common? Try to make a generalization that includes these three cases.

Solution:

Common Pattern: In each case, $\langle d_1 \rangle = \langle d_2 \rangle$ where d_1 and d_2 are related by:

- Either $d_1 \equiv -d_2 \pmod{n}$, or
- $\gcd(d_1, n) = \gcd(d_2, n)$

General Result: If G is a cyclic group of order n, then $\langle g^a \rangle = \langle g^b \rangle$ if and only if $\gcd(a, n) = \gcd(b, n)$.

Exercise 7: Find an example of a noncyclic group, all of whose proper subgroups are cyclic.

Solution: The Klein 4-group $V_4 = \{e, a, b, ab\}$ where $a^2 = b^2 = e$ and $ab = ba$.

Verification:

- V_4 is not cyclic (no element has order 4)
- All proper subgroups are: $\{e\}$, $\langle a \rangle = \{e, a\}$, $\langle b \rangle = \{e, b\}$, $\langle ab \rangle = \{e, ab\}$
- Each proper subgroup is cyclic (order 1 or 2)

Exercise 9: How many subgroups does $\mathbb{Z}_{20}$ have? List a generator for each of these subgroups. Suppose that $G = \langle a \rangle$ and $|a| = 20$. How many subgroups does G have? List a generator for each of these subgroups.

Solution: The subgroups of $\mathbb{Z}_{20}$ correspond to divisors of 20: $1, 2, 4, 5, 10, 20$. So $\mathbb{Z}_{20}$ has 6 subgroups. **Subgroups and their generators:**

- Order 1: $\langle 0 \rangle = \{0\}$
- Order 2: $\langle 10 \rangle = \{0, 10\}$
- Order 4: $\langle 5 \rangle = \{0, 5, 10, 15\}$
- Order 5: $\langle 4 \rangle = \{0, 4, 8, 12, 16\}$
- Order 10: $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$
- Order 20: $\langle 1 \rangle = \mathbb{Z}_{20}$

For $G = \langle a \rangle$ with $|a| = 20$: G has 6 subgroups with generators $a^{20}, a^{10}, a^5, a^4, a^2, a^1$ respectively.

Exercise 16: Let a be an element of a group.

a. Complete the statement: $|a| = |a^2|$ if and only if $|a|$ ______.
b. Complete the statement: $|a^2| = |a^{12}|$ if and only if ______.

Solution:

Part (a): $|a| = |a^2|$ if and only if $|a|$ **is odd**.

Proof: Let $|a| = n$. Then $|a^2| = \dfrac{n}{\gcd(n,2)}$.

- If n is odd, then $\gcd(n, 2) = 1$, so $|a^2| = n = |a|$
- If n is even, then $\gcd(n, 2) = 2$, so $|a^2| = \dfrac{n}{2} < n = |a|$

Part (b): $|a^2| = |a^{12}|$ if and only if $\gcd(|a|, 10) = \gcd(|a|, 2)$.

Proof: $|a^k| = \dfrac{|a|}{\gcd(|a|, k)}$. So $|a^2| = |a^{12}|$ iff $\gcd(|a|, 2) = \gcd(|a|, 12)$ iff $\gcd(|a|, 10) = \gcd(|a|, 2)$.

Exercise 21: Prove that if G is a group with the property that the square of every element is the identity then G is Abelian.

Proof: Let $a, b \in G$. Since $(ab)^2 = e$, we have: $(ab)^2 = abab = e$. Since $a^2 = b^2 = e$.
From $abab = e$, multiply on the left by a and on the right by b:

$a(abab)b = aeb$
$a^2bab^2 = ab$
$ba = ab$ (since $a^2 = b^2 = e$)

Therefore, G is abelian.

Exercise 27: If a cyclic group has an element of infinite order, how many elements of finite order does it have?

Solution: If a cyclic group has an element of infinite order, then it has exactly one element of finite order.

Proof: Let $G = \langle a \rangle$ where $|a| = \infty$. The elements of G are $\{a^n : n \in \mathbb{Z}\}$. If a^k has finite order for some $k \neq 0$, then $(a^k)^m = a^{km} = e = a^0$ for some positive integer m.

This means $km = 0$, which implies $k = 0$ or $m = 0$, contradicting our assumption. Hence, only $a^0 = e$ has finite order (order 1).

Exercise 32: For any element a in any group G, prove that $\langle a \rangle$ is a subgroup of $C(a)$ (the centralizer of a).

Proof: We need to show that every element of $\langle a \rangle$ commutes with a. Let $x \in \langle a \rangle$. Then $x = a^k$ for some integer k. We have:

$$xa = a^k \cdot a = a^{k+1} = a \cdot a^k = ax$$

Therefore, x commutes with a, so $x \in C(a)$. Since this holds for all $x \in \langle a \rangle$, we have $\langle a \rangle \subseteq C(a)$.

Exercise 35: Prove that $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication, has a cyclic subgroup of order n for every positive integer n.

Proof: Consider the nth roots of unity: $\omega_n = e^{2\pi i/n}$. The element ω_n has order n because:

- $(\omega_n)^n = e^{2\pi i} = 1$
- $(\omega_n)^k = e^{2\pi i k/n} \neq 1$ for $0 < k < n$

Therefore, $\langle \omega_n \rangle = \{\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1}\}$ is a cyclic subgroup of order n.

Exercise 43: Show that the group of positive rational numbers under multiplication is not cyclic. Why does this prove that the group of nonzero rationals under multiplication is not cyclic?

Solution: Let $\mathbb{Q}^+$ be the group of positive rational numbers under multiplication is not cyclic. **Proof by contradiction:** Suppose $\mathbb{Q}^+ = \langle r \rangle$ for some $r \in \mathbb{Q}^+$. Write $r = \frac{m}{n}$ where m, n are positive integers. Consider a rational number $\frac{1}{p}$ where p is a prime not appearing in the factorization of neither m nor n. If $r^k = \frac{1}{p}$ for some integer k, then $k \neq 0$.

Case 1: $k > 0$. Then $r^k = (\frac{m}{n})^k = \frac{m^k}{n^k} = \frac{1}{p}$ implies $pm^k = n^k$. This implies $p|n$ a contradiction.

Case 2: $k < 0$. Then $-k > 0$ and $r^{-k} = (\frac{m}{n})^{-k} = \frac{m^{-k}}{n^{-k}} = p$ Similarly leads to a contradiction.

Therefore, $\mathbb{Q}^+$ is not cyclic.

- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ is not cyclic, since if it were, its subgroup $\mathbb{Q}^+$ would also be cyclic.

Exercise 45: Give an example of a group that has exactly 7 subgroups (including the trivial subgroup and the group itself). Generalize to exactly n subgroups for any positive integer n.

Solution: $\mathbb{Z}_{p^{n-1}}$ has exactly n subgroups for any prime p.

For exactly 7 subgroups, we need $n = 7$, so we use $\mathbb{Z}_{p^6}$ for any prime p.

Generalization: For exactly n subgroups, use $\mathbb{Z}_{p^{n-1}}$ for any prime p.

Exercise 51: Suppose that H is a cyclic subgroup of a group G and $|H| = 10$. If a belongs to G and a^6 belongs to H, what are the possibilities for $|a|$?

Solution: Given: H is a cyclic subgroup with $|H| = 10$, and $a^6 \in H$. Since $|a^6| = \frac{|a|}{\gcd(|a|, 6)}$ and the possible orders of elements in H are: 1, 2, 5, 10. **Case analysis:**

- If $|a^6| = 1$: Then $|a|$ divides 6, and $\gcd(|a|, 6) = |a|$, so $|a| = 1, 2, 3$ or 6.
- If $|a^6| = 2$: Then $\frac{|a|}{\gcd(|a|, 6)} = 2$, so $|a| = 4$ or 12.
- If $|a^6| = 5$: Then $\frac{|a|}{\gcd(|a|, 6)} = 5$, so $|a| = 5, 10, 15$ or 30.
- If $|a^6| = 10$: Then $\frac{|a|}{\gcd(|a|, 6)} = 10$, so $|a| = 20, 30,$ or 60.

Possibilities for $|a|$: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

Exercise 61: List all the elements of $\mathbb{Z}_{40}$ that have order 10. Let $|x| = 40$. List all the elements of $\langle x \rangle$ that have order 10.

Solution: In $\mathbb{Z}_{40}$, an element k has order 10 if and only if $\dfrac{40}{\gcd(40,k)} = 10$, which means $\gcd(40,k) = 4$. Since $40 = 2^3 \cdot 5$ and we need $\gcd(40,k) = 4 = 2^2$, the element k must be divisible by 4 but not by 8, and not divisible by 5.

Elements of order 10: $\{4, 12, 28, 36\}$

For $\langle x \rangle$ with $|x| = 40$: Elements of order 10 are x^k where $\gcd(40,k) = 4$.
Answer: $\{x^4, x^{12}, x^{28}, x^{36}\}$

Exercise 65: If G is an Abelian group and contains cyclic subgroups of orders 4 and 5, what other sizes of cyclic subgroups must G contain? Generalize.

Solution: Let $a, b \in G$ such that $|a| = 4$ and $|b| = 5$. Since $|ab|$ divides $|a||b| = 20$, then $|ab| = 1, 2, 4, 5, 10$ or 20. Since $< a > \cap < b >= \{e\}$ Direct checking shows that $|ab| = 20$. So G contains cyclic subgroups of all sizes dividing 20.

Answer: Orders $1, 2, 4, 5, 10, 20.$

Generalization: If G is abelian and contains cyclic subgroups of relatively prime orders m and n, then G contains cyclic subgroups of all orders dividing mn.

Exercise 66: If G is an Abelian group and contains cyclic subgroups of orders 4 and 6, what other sizes of cyclic subgroups must G contain? Generalize.

Solution: Let $a, b \in G$ such that $|a| = 4$ and $|b| = 6$. Since $|ab|$ divides $|a||b| = 24$, then $|ab| = 1, 2, 3, 4, 6, 8, 12$ or 24. But $(ab)^{12} = a^{12} \cdot b^{12} = (a^4)^3 \cdot (b^6)^2 = e \cdot e = e$ and all lower powers cannot give e. So $|ab| = 12$. **Required subgroup orders:** All divisors of 12: 1, 2, 3, 4, 6, 12.

Generalization: If G is abelian and contains cyclic subgroups of orders m and n, then G contains cyclic subgroups of all orders dividing $\operatorname{lcm}(m, n)$.

Exercise 67: Prove that no group can have exactly two elements of order 2.

Proof: Suppose G has exactly two elements of order 2, say a and b where $a \neq b$ and $a^2 = b^2 = e$. Consider the element ab. We have $(ab)^2 = abab$.

Case 1: $ab = ba$ (elements commute). Then $(ab)^2 = abab = a^2b^2 = e \cdot e = e$. So ab has order 1 or 2.

- If $|ab| = 1$, then $ab = e$, so $a = b^{-1} = b$, contradicting $a \neq b$.
- If $|ab| = 2$, then we have three distinct elements of order 2: a, b, and ab.

Case 2: $ab \neq ba$ (elements don't commute). Then $aba \notin \{e, a, b\}$ has order 2.

Exercise 69: Let a and b be elements of a group. If $|a| = 10$ and $|b| = 21$, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Proof: Let $x \in \langle a \rangle \cap \langle b \rangle$. Then $x = a^i = b^j$ for some integers i, j.

- Since $x \in \langle a \rangle$, the order of x divides $|a| = 10$.
- Since $x \in \langle b \rangle$, the order of x divides $|b| = 21$.

Therefore, $|x|$ divides $\gcd(10, 21) = 1$. Thus $|x| = 1$, which means $x = e$.

Therefore, $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Generalization: If $\gcd(|a|, |b|) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Exercise 76: Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r \rangle \subseteq \langle x^s \rangle$.

Solution: Key Fact: $\langle x^k \rangle = \langle x^{\gcd(n,k)} \rangle$ for any integer k. Therefore:
$\langle x^r \rangle \subseteq \langle x^s \rangle$ iff $\langle x^{\gcd(n,r)} \rangle \subseteq \langle x^{\gcd(n,s)} \rangle$ iff $x^{\gcd(n,r)} \in \langle x^{\gcd(n,s)} \rangle$ iff $|x^{\gcd(n,r)}|$ divides $|x^{\gcd(n,s)}|$ iff $\dfrac{n}{gcd(n,r)}$ divides $\dfrac{n}{gcd(n,s)}$ iff $\gcd(n,s)$ divides $\gcd(n,r)$.