Group Theory Exercise Solutions

Chapter 3: Finite Groups; Subgroups

Exercise 2: Let Q be the group of rational numbers under addition and let Q^* be the group of nonzero rational numbers under multiplication. In Q, list the elements in $\langle\frac{1}{2}\rangle$. In Q^*, list the elements in $\langle 2\rangle$.

Solution:

In Q under addition:

$$\langle\frac{1}{2}\rangle = \{n \cdot \frac{1}{2} \mid n \in \mathbb{Z}\} = \{\ldots, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, 2, \ldots\}$$

In Q^* under multiplication:

$$\langle\frac{1}{2}\rangle = \{(\frac{1}{2})^n \mid n \in \mathbb{Z}\} = \{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\}$$

Exercise 3: Let Q and Q^* be as in Exercise 2. Find the order of each element in Q and in Q^*

Solution:

In Q (addition):

- Order of 0: $|0| = 1$ (identity element)
- Order of any nonzero rational r: $|r| = \infty$

  Proof: If $nr = 0$ for some positive integer n, then $r = 0$, contradiction.

In Q^* (multiplication):

- Order of 1: $|1| = 1$ (identity element)
- Order of -1: $|-1| = 2$ (since $(-1)^2 = 1$)
- Order of any other rational r: $|r| = \infty$

  Proof: For $r \neq 1, -1$, if $r^n = 1$ for some positive n, then r would be a root of unity, but the only rational roots of unity are ± 1.

Exercise 14: How many subgroups of order 4 does D_4 have?

Solution:

$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ where $|D_4| = 8$.

Subgroups of order 4:

1. $\{R_0, R_{90}, R_{180}, R_{270}\}$ - the rotation subgroup
2. $\{R_0, R_{180}, H, V\}$ - Klein 4-group structure
3. $\{R_0, R_{180}, D, D'\}$ - Klein 4-group structure

Verification: Each has order 4 and satisfies closure, associativity, identity, and inverses.

Answer: D_4 has exactly **3 subgroups** of order 4.

Exercise 15: Determine all elements of finite order in $\mathbb{R}^*$, the group of nonzero real numbers under multiplication.

Solution:

Let $r \in \mathbb{R}^*$ have finite order n, so $r^n = 1$.

Case 1: $r > 0$

- Taking logarithms: $n \ln(r) = 0$
- Since $n > 0$, we need $\ln(r) = 0$
- Therefore $r = 1$

Case 2: $r < 0$

- We can write $r = -s$ where $s > 0$
- Then $r^n = (-s)^n = (-1)^n s^n = 1$
- If n is odd: $-s^n = 1 \Rightarrow s^n = -1$ (impossible for $s > 0$)
- If n is even: $s^n = 1 \Rightarrow s = 1 \Rightarrow r = -1$

Answer: The elements of finite order in $\mathbb{R}^*$ are exactly $\{1, -1\}$.

Exercise 27: Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. Is $U(14) = \langle 11 \rangle$? Show that $U(20) \neq \langle k \rangle$ for any $k \in U(20)$.

Solution:

First, $U(14) = \{1, 3, 5, 9, 11, 13\}$ and $|U(14)| = 6$.

Part 1: Show $U(14) = \langle 3 \rangle$

- $3^1 = 3$
- $3^2 = 9$
- $3^3 = 27 \equiv 13 \pmod{14}$
- $3^4 = 39 \equiv 11 \pmod{14}$
- $3^5 = 33 \equiv 5 \pmod{14}$
- $3^6 = 15 \equiv 1 \pmod{14}$

Therefore $\langle 3 \rangle = \{1, 3, 5, 9, 11, 13\} = U(14)$.

Part 2: Show $U(14) = \langle 5 \rangle$

- $5^1 = 5$
- $5^2 = 25 \equiv 11 \pmod{14}$
- $5^3 = 55 \equiv 13 \pmod{14}$
- $5^4 = 65 \equiv 9 \pmod{14}$
- $5^5 = 45 \equiv 3 \pmod{14}$
- $5^6 = 15 \equiv 1 \pmod{14}$

Therefore $\langle 5 \rangle = U(14)$.

Part 3: Is $U(14) = \langle 11 \rangle$?

- $11^1 = 11$
- $11^2 = 121 \equiv 9 \pmod{14}$
- $11^3 = 99 \equiv 1 \pmod{14}$

So $\langle 11 \rangle = \{1, 9, 11\}$ which has order 3, not 6.

Answer: $U(14) \neq \langle 11 \rangle$.

Part 4: Show $U(20) \neq \langle k \rangle$ for any k

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and $|U(20)| = 8$.

Computing orders:

- $|1| = 1$, $|3| = 4$, $|7| = 4$, $|9| = 2$
- $|11| = 2$, $|13| = 4$, $|17| = 4$, $|19| = 2$

Since no element has order 8, $U(20)$ is not cyclic.

Exercise 32: Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

Solution:

Let G be a group with elements a, b where $|a| = |b| = 2$ and $ab = ba$.

Step 1: Show $H = \{e, a, b, ab\}$ has 4 distinct elements.

- Since $|a| = |b| = 2$, we have $a \neq e$ and $b \neq e$
- If $a = b$, we wouldn't have "two elements"
- If $ab = e$, then $b = a^{-1} = a$ (since $a^2 = e$), contradiction
- If $ab = a$, then $b = e$, contradiction
- If $ab = b$, then $a = e$, contradiction

Step 2: Show H is a subgroup. It is closed under the group operation since

- $a^2 = e \in H$
- $b^2 = e \in H$
- $(ab)^2 = abab = a^2b^2 = e \in H$ (using commutativity)
- All other products are already computed

Step 3: H has identity e, and every element is its own inverse. So H is not empty, closed under multiplication, and inversion.

Conclusion: H is a subgroup of order 4.

Exercise 38: If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G.

Solution:

Step 1: $H \cap K \neq \emptyset$
Since $e \in H$ and $e \in K$, we have $e \in H \cap K$.

Step 2: Closure
Let $x, y \in H \cap K$. Then:

- $x, y \in H \Rightarrow xy \in H$ (since H is a subgroup)
- $x, y \in K \Rightarrow xy \in K$ (since K is a subgroup)
- Therefore $xy \in H \cap K$

Step 3: Inverse property

Let $x \in H \cap K$. Then:

- $x \in H \Rightarrow x^{-1} \in H$
- $x \in K \Rightarrow x^{-1} \in K$
- Therefore $x^{-1} \in H \cap K$

Conclusion: $H \cap K$ is a subgroup of G.

Extension: The same proof shows that the intersection of any collection of subgroups is a subgroup.

$Exercise 46(b)$: In the group $\mathbb{Z}$, find $\langle 8, 13\rangle$ and an integer k such that the subgroup equals $\langle k\rangle$.

Solution:

Method: For $\langle a, b\rangle$ in $\mathbb{Z}$, we have $\langle a, b\rangle = \langle \gcd(a, b)\rangle$.

Step 1: Find $\gcd(8, 13)$ using Euclidean algorithm:

- $13 = 1 \cdot 8 + 5$
- $8 = 1 \cdot 5 + 3$
- $5 = 1 \cdot 3 + 2$
- $3 = 1 \cdot 2 + 1$
- $2 = 2 \cdot 1 + 0$

Therefore $\gcd(8, 13) = 1$.

Step 2: Express 1 as a linear combination: Working backwards:

- $1 = 3 - 1 \cdot 2$
- $1 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5$
- $1 = 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5$
- $1 = 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = 5 \cdot 8 - 3 \cdot 13$

Answer: $\langle 8, 13 \rangle = \langle 1 \rangle = \mathbb{Z}$, so $\boldsymbol{k} = 1$.

Exercise 47: Prove Theorem 3.6.

Solution: See class notes.

Exercise 50: Suppose a belongs to a group and $|a| = 5$. Prove that $C(a) = C(a^3)$. Find an element a from some group such that $|a| = 6$ and $C(a) \neq C(a^3)$.

Solution:

Part 1: Prove $C(a) = C(a^3)$ when $|a| = 5$.

Since $a^5 = e$, then $a^6 = a$.

Show $C(a) \subseteq C(a^3)$:
If $x \in C(a)$, then $xa = ax$, so $xa^3 = xaaa = axaa = aaxa = aaax = a^3x$.

Show $C(a^3) \subseteq C(a)$:
If $x \in C(a^3)$, then $xa^3 = a^3x$, so $x(a^3)^2 = (a^3)^2x$, which gives $xa = ax$.

Therefore $C(a) = C(a^3)$.

Part 2: Find a with $|a| = 6$ and $C(a) \neq C(a^3)$.

Consider $a = R_{60^\circ}$ in D_6 (rotation by 60°).

- $|a| = 6$ and $a^3 = R_{180^\circ}$
- $C(a) = \{R_0, R_{60^\circ}, R_{120^\circ}, R_{180^\circ}, R_{240^\circ}, R_{300^\circ}\}$ (all rotations)
- $C(a^3) = C(R_{180^\circ}) = D_6$ (since R_{180° commutes with all elements)

Since $C(a) \neq D_6$, we have $C(a) \neq C(a^3)$.

Exercise 53: Consider the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $SL(2, \mathbb{R})$. What is the order of A? If we view A as a member of $SL(2, \mathbb{Z}_p)$ (p is prime), what is the order of A?

Solution: Part 1: Order in $SL(2, \mathbb{R})$. Let's compute powers of A:

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$A^3 = A^2 \cdot A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

In general, $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for any positive integer n.

Since $A^n = I$ requires $n = 0$ in the upper right entry, and this never occurs for positive n in $\mathbb{R}$, we have $A^n \neq I$ for all $n > 0$. **Answer:** $|A| = \infty$ in $SL(2, \mathbb{R})$.

Part 2: Order in $SL(2, \mathbb{Z}_p)$

In $\mathbb{Z}_p$, we have $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ where n is computed modulo p.

For $A^n = I$, we need $n \equiv 0 \pmod{p}$.

The smallest positive integer n such that $n \equiv 0 \pmod{p}$ is $n = p$.

Verification: $A^p = \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$ in $\mathbb{Z}_p$.

Answer: $|A| = p$ in $SL(2, \mathbb{Z}_p)$ for any prime p.

Exercise 54: Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbb{R})$. Find $|A|$, $|B|$, and $|AB|$. Does your answer surprise you?

Solution: Find $|A|$:

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^3 = A^2 \cdot A = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$A^4 = A^3 \cdot A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Therefore $|A| = 4$.

Find $|B|$: $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$

$$B^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$$

$$B^3 = B^2 \cdot B = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Therefore $|B| = 3$.

Find $|AB|$:

$$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$(AB)^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$(AB)^3 = (AB)^2 \cdot AB = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

In general, $(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for positive integers n.

Since $(AB)^n \neq I$ for any positive integer n, we have $|AB| = \infty$. **Answer:** $|A| = 4$, $|B| = 3$, $|AB| = \infty$.

Surprising observation: Despite both A and B having finite order, their product AB has infinite order. This demonstrates that the order of a product can behave very differently from the orders of the individual factors, even when both factors have finite order.

Exercise 60: In the group $\mathbb{R}^*$ find elements a and b such that $|a| = \infty$, $|b| = \infty$ and $|ab| = 2$.

Solution:

We need to find $a, b \in \mathbb{R}^*$ with infinite order such that $(ab)^2 = 1$.

Strategy: Let $ab = -1$, so $(ab)^2 = (-1)^2 = 1$, giving $|ab| = 2$.

Example: Let $a = 2$ and $b = -\frac{1}{2}$.

- $|a| = |2| = \infty$ (since $2^n \neq 1$ for any positive integer n)
- $|b| = |-\frac{1}{2}| = \infty$ (since $(-\frac{1}{2})^n \neq 1$ for any positive integer n)
- $ab = 2 \cdot (-\frac{1}{2}) = -1$
- $|ab| = |-1| = 2$ (since $(-1)^2 = 1$)

Answer: $a = 2$, $b = -\frac{1}{2}$ satisfy the conditions.

Exercise 64(b): Compute $|U(5)|$, $|U(7)|$, $|U(35)|$.

Solution: Using Euler's totient function $\phi(n) = |U(n)|$:

$|U(5)|$: Since 5 is prime: $\phi(5) = 5 - 1 = 4$

Verification: $U(5) = \{1, 2, 3, 4\}$, so $|U(5)| = 4$.

$|U(7)|$: Since 7 is prime: $\phi(7) = 7 - 1 = 6$

Verification: $U(7) = \{1, 2, 3, 4, 5, 6\}$, so $|U(7)| = 6$.

$|U(35)|$: Since $35 = 5 \times 7$ where $\gcd(5, 7) = 1$:
$\phi(35) = \phi(5 \times 7) = \phi(5) \times \phi(7) = 4 \times 6 = 24$

Answer: $|U(5)| = 4$, $|U(7)| = 6$, $|U(35)| = 24$.

Conjecture: For $\gcd(r, s) = 1$, we have $|U(rs)| = |U(r)| \times |U(s)|$.

Exercise 77: Let $G = GL(2, \mathbb{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a \textbf{ and } b \textbf{ are nonzero integers} \right\}$ under matrix multiplication. Prove or disprove that H is a subgroup of $GL(2, \mathbb{R})$.

Solution: We need to check if H satisfies the subgroup criteria.

Check 1: Non-empty $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$ since $1, 1$ are nonzero integers.

Check 2: Closure Let $A = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \in H$.

$$AB = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{bmatrix}$$

Since a_1, a_2, b_1, b_2 are nonzero integers, $a_1 a_2$ and $b_1 b_2$ are nonzero integers.
Therefore $AB \in H$. ✓

Check 3: Inverse Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in H$ where a, b are nonzero integers.

$$A^{-1} = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{bmatrix}$$

Problem: $\dfrac{1}{a}$ and $\dfrac{1}{b}$ are not integers unless $a = \pm 1$ and $b = \pm 1$.

Counterexample: Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \in H$.

Then $A^{-1} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{bmatrix} \notin H$.

Conclusion: H is **not** a subgroup of $GL(2, \mathbb{R})$ because it fails the inverse property.