HW 3

Charles Liu
Elementary Modern Algebra - Dr. Ben Clark
February 6th 2025

---

1. Find all the generators of $(\mathbb{Z}, +)$ (integers under regular addition). Let a be a group element in an arbitrary group, that has infinite order. Find all the generators of $\langle a \rangle$.

The generators of $(\mathbb{Z}, +)$ are 1 and -1

If a has infinite order, $\langle a \rangle$ is isomorphic to $(\mathbb{Z}, +)$ so every element in the arbitrary group is a generator of $\langle a \rangle$.

---

2. Solve the following equations for x in the given cyclic group. If multiple solutions exist, be sure to state all solutions.

(a) $x + 5 = 7$, where $G = \mathbb{Z}_{11}$

Since $2 + 5 = 7$ and $2 \in \mathbb{Z}_1 1$, $x = 2$

(b) $2x + 4 = 7$, where $G = \mathbb{Z}_8$

We can solve the equivalent equation $2x = 3$. Since the coefficient of x in the equation is 2, it confines the left-hand side to even numbers although the right-hand side is odd, so x has no solution.

---

3. Prove that an infinite group must have an infinite number of subgroups.

Theorem. There is an infinite number of subgroups in an infinite group.
Proof.
Let G be an infinite group.
If $x \in G$, $\langle x \rangle \in G$

Case 1: An element in G has infinite order, $|x| = \infty$
Since $\langle x \rangle \in G$, if $|x| = \infty$, $\{e, x^1, x^2, x^3, \dots\} \in G$.
Since $\{e, x, \dots x_n\} \leq G$, for $n \in \mathbb{N}$, there is an infinite number of subgroups.
Case 2: All elements in G have finite order; $|x| = n$ where $n \geq 0$ and n is finite.
Since $\langle x \rangle \leq G$, $\{e, x^1, x^2, \dots x^n\} \leq G$. As G has infinite elements, we can find another element $y \in G$ where $y \notin \langle x \rangle$ and the order of y is finite. We can construct a cycle with y as a generator, where $\langle y \rangle \in G$. Similarly, since G has infinite elements, we can find $z \in G$ where $z \notin \langle x \rangle$ and $z \notin \langle y \rangle$. Since $z \in G$, $\langle z \rangle \leq G$ and the order of z is finite. Repeating this logic indefinitely, we can generate infinite subgroups with each new generator in G, but not in previous subgroups.

---

4. Suppose G is a group with more than 1 element. If the only subgroups of G are G and $\{e\}$, prove that G is cyclic and has prime order.

Theorem. For a group G with more than 1 element and subgroups of only G and $\{e\}$, G must be cyclic and have prime order.
Proof.
As G has more than one element, we can find an element $a \in G$ where $a \neq e$. The cyclic subgroup generated by a, $\langle a \rangle \in G$.
We know that $\langle a \rangle$ is a subgroup in G. Since the only subgroups of G are G and $\{e\}$, $\langle a \rangle$ must be $\{e\}$ or G. Since $a \neq e$, $\langle a \rangle \neq \{e\}$. As such, $\langle a \rangle = G$ and G is cyclic.

Let the order of the group G be n. BWOC, assume n is not prime. This means it can be written as $n = xy$ where x, y are integers and $x, y < n$. We can find that

$$a^n = a^{xy} = a^x a^y = e$$

This shows that $a^x = a^y = e$, meaning the order of a is either $x \neq n$ or $y \neq n$, a contradiction as the order of $a = n$.
Thus, the order of G must be prime.

---

5. Prove that no group can have exactly two elements of order 2.

Theorem. No group can have exactly two elements of order 2
Proof.
BWOC, suppose that for a group G, there are exactly two elements $a, b \in G$ of order 2

where $a \neq b$. This means $a^2 = b^2 = e$.
By properties of groups, this means $ab \in G$.
Case 1: $ab = e$
If $ab = e$, this means that $a = b^{-1}$. As b has order 2, $b^{-1} = b$. Substituting into $a = b^{-1}$, we get that $a = b$, a contradiction.
Case 2: $ab \neq e$
Case 2a: $ab = ba$
Since $a^2 = b^2 = e$, if ab is commutative, then
$a^2b^2 = aabb = a(ab)b = abab = (ab)^2 = e$. This means ab has order 2.
Case 2b: $ab \neq ba$.
Take $aba \in G$. We can solve that $(aba)(aba) = ab(a^2)ba = ab^2a = a^2 = e$.
We can find that $aba \neq e$, $aba \neq a$, and $aba \neq b$, and is thus a third element of order 2.
BWOC, assume that $aba = e$. This means that $ab = a^{-1} = a$ which means that $b = e$, a contradiction.
BWOC, assume that $aba = a$. This means that $ba = e$ and $a = b^{-1} = b$, a contradiction.
BWOC, assume that $aba = b$. This means that $ab = ba^{-1} = ba$ which means ab is commutative, a contradiction.
Thus, aba is a third element of order 2 which is not a, b or e, and the statement that there is exactly two elements of order 2 in G is a contradiction.

---

6. Prove that S_n is non-commutative for $n \geq 3$.

Theorem. S_n for $n \geq 3$ is non-commutative.
Proof.
Let $a = (12) \in S_n$ and $b = (23) \in S_n$. We can solve that $ab = (123) \neq ba = (132)$, which means ab, and thus S_n, is not commutative.