MATH 31 – HOMEWORK 5 SOLUTIONS!

due **Friday, August 4**

Instructions: This assignment is due at the *beginning* of class. Staple your work together (do not just fold over the corner). Please write the questions in the correct order. If I cannot read your handwriting, you won't receive full credit.

1. (10.8) Let G be a group of order p^2, where p is a prime. Show that G must have a subgroup of order p.

   Proof: Let G be a group of order p^2 for a prime p. Let x be a non-identity element. By Theorem 10.4, the possible orders of x are only p and p^2. If $o(x) = p$, then $\langle x \rangle$ is a subgroup of order p. So, in this case we are done. Otherwise $o(x) = p^2$.

   If $o(x) = p^2$ then we know that $\langle x \rangle = G$, i.e., G is cyclic with x as a generator. It must follow then that $o(x^p) = p$, and $\langle x^p \rangle$ is a subgroup of G of order $p^2/p = p$. □

---

2. (10.21) Prove that every group of order 77 has an element of order 7 and an element of order 11.

   Proof: Let G be a group of order 77 and let x be a non-identity element. As $77 = 7 \cdot 11$ and both 7 and 11 are prime, the only possible orders of x are 7, 11, and 77.

   If G has an element g of order 77, then $G = \langle g \rangle$, and by Theorems from Chapter 4 it follows that $o(g^7) = 11$ and $o(g^{11}) = 7$, proving the result. Hence, we can now assume that every non-identity element of G has order 7 or 11.

   Suppose now toward a contradiction that G has no element of order 7, so that all elements of G have only orders 1 and 11. We will show this is not possible. Any two non-trivial proper subgroups of G have order 11, and if they are not the same subgroup then their intersection is only $\{e\}$. This implies we can write G as the union of a list of subgroups

   $$G = H_1 \cup H_2 \cup \cdots \cup H_k,$$

   such that $|H_i| = 11$ for all i, and $H_i \cap H_j = \{e\}$ for all $i \neq j$. If this is the case, then the size of G can be computed as

   $$|G| = 1 + 10k,$$

   where the 1 counts the identity element and $10k$ counts the ten non-identity elements in each subgroup, which must be different from those in the other subgroups. But, 77 does not have the form $1 + 10k$. So this is not possible. It thus follows that G does have an element of order 7.

   To see that G also has an element of order 11, assume again by contradiction that it does not. The same line of reasoning leads to the statement that

   $$77 = 1 + 6k$$

   for some integer k, which is not possible. □

---

3. (11.29) Show that if $G/Z(G)$ is cyclic then G is abelian.

Proof: Let G be a group and suppose that $G/Z(G)$ is cyclic. The elements of $G/Z(G)$ are right cosets of the form $Z(G)g$, for $g \in G$. If $G/Z(G)$ is cyclic, then there exists an element $Z(G)x \in G/Z(G)$ such that

$$G/Z(G) = \langle Z(G)x \rangle.$$

Note that by the definition of the operation on quotient groups,

$$(Z(G)x)^i = Z(G)x^i,$$

and so we can write that

$$G/Z(G) = \{Z(G)x^i : i \in \mathbb{Z}\}.$$

To show that G is abelian, we pick two arbitrary elements $a, b \in G$, and show that $ab = ba$. Consider the right cosets $Z(G)a$ and $Z(G)b$. By our earlier discussion, there exist m and n in $\mathbb{Z}$ such that

$$Z(G)a = Z(G)x^m \qquad \text{and} \qquad Z(G)b = Z(G)x^n.$$

Therefore, we can write

$$a = z_1 x^m \qquad \text{and} \qquad b = z_2 x^n,$$

where z_1 and z_2 are some elements of $Z(G)$.

Lastly,

$$\begin{aligned} ab &= (z_1 x^m)(z_2 x^n) \\ &= z_1 z_2 x^{m+n} && \text{(because } z_2 \in Z(G)\text{)} \\ &= z_2 z_1 x^{n+m} && \text{(because } z_1, z_2 \in Z(G)\text{)} \\ &= z_2 z_1 x^n x^m \\ &= (z_2 x^n)(z_1 x^m) && \text{(because } z_1 \in Z(G)\text{)} \\ &= ba. \end{aligned}$$

□

---

4. (11.16) Show that $(\mathbb{Q}, +)/(\mathbb{Z}, +)$ is an infinite group every element of which has finite order.

Proof: Let $G = (\mathbb{Q}, +)/(\mathbb{Z}, +)$. For ease of notation, we abbreviate $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$ as $\mathbb{Q}$ and $\mathbb{Z}$. The elements of G are right cosets of the form

$$G = \left\{ \mathbb{Z} + \frac{a}{b} \ : \ \frac{a}{b} \in \mathbb{Q} \right\}.$$

So, we see that two right cosets $\mathbb{Z} + a/b$ and $\mathbb{Z} + c/d$ are the same if and only if a/b and c/d differ by an integer.

This allows us to list the distinct cosets in $\mathbb{Q}/Z$:

$$G = \left\{ \mathbb{Z} + \frac{a}{b} \ : \ \frac{a}{b} \in \mathbb{Q} \cap [0, 1) \right\}.$$

Since there are an infinite number of rational numbers between 0 and 1, the group $\mathbb{Q}/\mathbb{Z}$ is infinite.

What is the order of the coset $\mathbb{Z} + a/b$? Suppose that a/b is written in reduced form. Then,

$$\ell \cdot \left(\mathbb{Z} + \frac{a}{b} \right) = \mathbb{Z} + \left(\ell \cdot \frac{a}{b} \right),$$

and this equals $\mathbb{Z} + 0$ if and only if $\ell \cdot \frac{a}{b}$ is an integer, which is true if and only if ℓ is a multiple of b. The smallest positive integer ℓ for which this is true is $\ell = b$. Therefore, $o(\mathbb{Z} + a/b) = b$, so long as a/b is written in reduced form. □
