# Math 453

Selected Solutions to Assignment 4

**Problem 2:** Give an example of a non-cyclic group all of whose subgroups are cyclic.

**Solution:** Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then the subgroups of $G$ are $\langle e \rangle$, $\langle (1,0) \rangle$, and $\langle (0,1) \rangle$, which are all cyclic, but $G$ is not cyclic.

**Problem 3:** Suppose $(G, *, e)$ is an abelian group of order 35, and that every element $x \in G$ satisfies the equation $x^{35} = e$. Show that $G$ is cyclic.

**Solution:** First, we will need a lemma.

**Lemma.** *Let $H$ be a group, and let $G_1, G_2 \subseteq H$ be cyclic subgroups of order $p$ for some $p \in \mathbb{Z}$ prime. Then either $G_1 \cap G_2 = \langle e \rangle$ or $G_1 = G_1 \cap G_2 = G_2$.*

*Proof.* By the definition of subgroup, we have that $e \in G_1$ and $e \in G_2$, so $e \in G_1 \cap G_2$. Suppose there are no nonidentity elements in $G_1 \cap G_2$; then $G_1 \cap G_2 = \langle e \rangle$.

On the other hand, suppose there exists a nonidentity $g \in G_1 \cap G_2$; then by Theorem 10.5 and the fact that $G_1$ is finite and cyclic, we have that $|g| \mid p$. Since $g \neq e$, $|g| \neq 1$; since $p$ is prime, we have $|g| = p$. Thus, by Theorem 10.3, $g^0, g^1, \ldots, g^{p-1}$ are distinct. Then by definition of subgroup, we have $g^i \in G_1$ and $g^i \in G_2$ for $0 \leq i \leq p-1$. But $|G_1| = |G_2| = p$, so $G_1 = \{g^i | i \in \mathbb{Z}\} = G_2 = G_1 \cap G_2$. $\square$

Now, assume for contradiction that there is no element in $G$ of order 7, and no element in $G$ of order 35. Since $|G| > 1$ and the identity is unique, by Theorem 10.5 and the fact that $G$ is finite, every nonidentity element of $G$ has order 5. Let $g_1, ..., g_{34}$ be the distinct nonidentity elements of $G$, and for each $1 \leq i \leq 34$, define $\mathcal{K}_i = \langle g_i \rangle \setminus \{e\}$, so $|\mathcal{K}_i| = 4$ for each $1 \leq i \leq 34$ by Theorem 10.3. (Note that the $\mathcal{K}_i$ are not subgroups but simply subsets; $|\cdot|$ denotes the cardinality, or size, of each subset.) Then by the Lemma, for each $g_i, g_j$, $1 \leq i, j \leq 34$, either $\langle g_i \rangle \cap \langle g_j \rangle = \langle g_i \rangle = \langle g_j \rangle$ or $\langle g_i \rangle \cap \langle g_j \rangle = \langle e \rangle$. Hence, for each $\mathcal{K}_i, \mathcal{K}_j$, $1 \leq i, j \leq 34$, either $\mathcal{K}_i \cap \mathcal{K}_j = \mathcal{K}_i = \mathcal{K}_j$ or $\mathcal{K}_i \cap \mathcal{K}_j = \emptyset$. Note that $\bigcup_{i=1}^{34} \mathcal{K}_i = G \setminus \{e\}$, so that the subsets $\mathcal{K}_i$ form a partition of $G \setminus \{e\}$. Thus, $4 = |\mathcal{K}_i| \mid |G \setminus \{e\}| = 34$, a contradiction. Hence, $G$ has an element of order 7 or an element of order 35.

By a similar argument (with the contradiction being $6 = |\mathcal{K}_i| \mid |G| = 34$), $G$ has an element of order 5 or an element of order 35.

By the above, $G$ has an element of order 35, or $G$ has both an element of order 5 and an element of order 7 (or all of the above). If $G$ has an element $g$ of order 35, by Theorem 10.3 and the fact that $|G| = 35$, $\langle g \rangle = G$, so $G$ is cyclic. If $G$ has both an element $g_1$ of order 5 and an element $g_2$ of order 7, we have $g_1^5 = e$ and $g_2^7 = e$. Since $G$ is abelian, $(g_1g_2)^{35} = g_1^{35}g_2^{35} = (g_1^5)^7(g_2^7)^5 = e^7 \cdot e^5 = e$, so by Theorem 10.5, $|g_1g_2| \mid 35$. If $|g_1g_2| = 1$, $g_1 = g_2^{-1}$, so $(g_2^{-1})^5 = g_2^{-5} = e$, a contradiction. If $|g_1g_2| = 5$, since $G$ is abelian, $e = (g_1g_2)^5 = g_1^5g_2^5 = eg_2^5 = g_2^5$, so $7 \mid 5$, a contradiction. Similarly, if $|g_1g_2| = 7$, since $G$ is abelian, $e = (g_1g_2)^7 = g_1^7g_2^7 = g_1^7e = g_1^7$, so $5 \mid 7$, a contradiction. Thus, $|g_1g_2| = 35$, so again by Theorem 10.3 and the fact that $|G| = 35$, $\langle g \rangle = G$, so $G$ is cyclic.

**Problem 5:** Prove that a group of order 3 must be cyclic.

**Solution:** Let $G$ be a group with $|G| = 3$. Since the identity is unique, $G$ has exactly two nonidentity elements, so we may write $G = \{e, x, y\}$, where $e$ is the identity of $G$, and $e, x, y$ are distinct. Then we have $xy = e, x$, or $y$. If $xy = x$, $y = e$, a contradiction. If $xy = y$, $x = e$, a contradiction. Hence, $xy = e$.

Now, if $x^2 = x$, we have $x = e$, a contradiction. If $x^2 = e$, by the previous paragraph, we have $x^2 = xy$, so $x = y$, a contradiction. Hence, $x^2 = y$, so $G$ is cyclic.