421 HW 9 Group

change this to your names

NOTE: Unless stated otherwise, G is a (multiplicative) group with identity element e.
Hint: Some of these problems are related.

Problem (8.1.21)**.** Let H and K, each of prime order p, be subgroups of a group G. If $H \neq K$, prove that $H \cap K = \langle e \rangle$.

Solution.

Problem (8.1.36)**.** Let H and K be subgroups of a finite group G such that $[G : H] = p$ and $[G : K] = q$, with p and q distinct primes. Prove that pq divides $[G : H \cap K]$.

Solution.

Problem (8.1.37)**.** Let G be an abelian group of order n and let k be a positive integer. If $(k, n) = 1$, prove that the function $f : G \to G$ given by $f(a) = a^k$ is an isomorphism. [Hint: To show f is a bijection, find a formula for f^{-1}.]

Solution.

Problem (8.1.40)**.** If a prime p divides the order of a finite group G, prove that the number of elements of order p in G is a multiple of $p-1$. [Cauchy's Theorem says that the number of elements of order p is positive. However, you do not need to prove that or apply it. That is, for this exercise, the proof will work fine if the number of elements of order p is $0(p-1) = 0$.]

Solution.
Outline:
Let $Y = \{a \in G \quad | \quad |a| = p\}$
Let $\sim$ be an equivalence relation on Y such that $a \sim b \Leftrightarrow b \in \langle a \rangle$ (conceptually, this should be equivalent to $a \sim b \Leftrightarrow \langle a \rangle = \langle b \rangle$, but this is not proven).
Each equivalence class is of size $p - 1$ ($[a] = \langle a \rangle \setminus \{e\}$).
Y is the union of these disjoint equivalence classes.
$|Y|$ must be a multiple of $p - 1$.
This depends upon the theorem that any group of size p, where p is prime, is isomorphic to $\mathbb{Z}_p$.
Proof:
To prove $[a] \subseteq \langle a \rangle \setminus \{e\}$

$$b \in [a]$$
$$b \in \langle a \rangle$$
$$[a] \subseteq Y$$
$$|b| = p$$
$$b \neq e$$

$b \in \langle a \rangle \setminus \{e\}$

To prove $\langle a \rangle \setminus \{e\} \subseteq [a]$

$b \in \langle a \rangle \setminus \{e\}$

$$|b| = p$$
$$b \in Y$$
$$b \in \langle a \rangle$$
$$b \in [a]$$

Therefore, $\langle a \rangle \setminus \{e\} = [a]$.

To prove $\forall a \in Y \quad \langle a \rangle \cong \mathbb{Z}_p$

$\sim$ is reflexive: yeah

$\sim$ is symmetric:

$$b \in \langle a \rangle$$

$\exists k \in \mathbb{Z} \quad b = a^k$

$$b^{-k} = a$$
$$a \in \langle b \rangle$$

$\sim$ is transitive:

$$a \sim b$$
$$b \sim c$$

$\exists x, y \in \mathbb{Z} \quad b = a^x, c = a^y$

$$c = a^{xy}$$

x cannot be a multiple of p, since, if it were, $b = e$. y can similarly not be a multiple of p. By Euclid's lemma, $p \nmid xy$. Thus, $a \sim c$.

Each equivalence class is of order $p - 1$:

$e \notin [a]$, so $[a][e] = \langle a \rangle$.

By closure in G, $\langle a \rangle \leq G$.

Since $|a| = p$, $|\langle a \rangle| = p$, so $\langle a \rangle \cong \mathbb{Z}_p$.

Problem (8.1.41)**.** Prove that a group of order 33 contains an element of order 3. [Of course you are not allowed to apply Cauchy's Theorem.]

Solution.

$$\begin{aligned}
\forall g \in G \quad g^{11\cdot 3} &= e \\
(g^{11})^3 &= e \\
|g^{11}| &\mid 3 \\
|g^{11}| = 3 &\text{ or } |g^{11}| = 1 \\
|g^{11}| = 3 &\text{ or } (g^{11} = e) \\
|g^{11}| = 3 &\text{ or } (|g| = 11 \text{ or } g = e) \\
|g^{11}| = 3 &\text{ or } |g| = 11 \text{ or } g = e
\end{aligned}$$

It is unproven, but these are all mutually exclusive things. For any given value of $g \in G$, exactly one of these things must be true.

By 8.1.41, for some $n \in \mathbb{Z}$, the number of elements for which $|g| = 11$ is $10n$.

There is one element for which $g = e$.

Let the number of elements g for which $|g^{11}| = 3$ be denoted by m.

33 is the total number of elements, so

$33 = m + 10n + 1$

$33 - 10n - 1 = m$

$32 - 10n - 1 = m$

Since $m \geq 0$, and $n \geq 0$, the possibilities for m are 32, 22, 12, and 2.

This means there exists $a \in G$ for which $|a^{11}| = 3$.

$|a^{11}|$ is an element of order 3, so this is proven.