

Note: I am accustomed to writing “The element $g \in G$ acting on the element $x \in S$ ” as $g.x$ instead of gx . I use the stated notation, as I feel it is clearer.

Problem 1:

Let G be a finite abelian group, with $n \in \mathbb{N}$ and $n \mid |G|$.

We know that for each $n \in \mathbb{N}$, n has a unique prime factorization; that is, $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$ for some $p_1, p_2 \dots p_k$ each prime, and $a_1, a_2 \dots a_k$ each positive and nonzero.

Proceed as follows:

For each p_i , there is an element with order p_i in G :

We proceed by induction. If $|G| = 1$, then $|G|$ has no prime divisors, so there is vacuously an element of order p in G if $p \mid |G|$.

Now, assume that there is an element of order p (with p prime) in G if $p \mid |G|$ for all G with order less than N . Let G be a group of order N , and let $p \mid N$ be a prime number. Pick an element of G , call it g , other than the identity. It has some order, $m > 1$. Either $p \mid m$ or not. If so, then take $g^{m/p}$; this element clearly has order p . If not, then consider $G/\langle a \rangle$ (this is well defined; G is abelian, so $\langle a \rangle$ is normal, because all subgroups are normal in abelian groups). We know that $p \mid |G/\langle a \rangle|$; $p \mid |G| = |G/\langle a \rangle| |a|$, so because p is prime, we know that $p \mid |G/\langle a \rangle|$. So there's an element, b , of order p in $G/\langle a \rangle$. So there is an element with $\bar{c} = b$. Now, $c^p \in \langle a \rangle$;

$$c = ba^x \text{ for some } x \in \mathbb{Z}, \text{ because } \bar{c} = b$$

$$c^p = b^p a^{px}$$

$$c^p = a^y \text{ for some } y \in \mathbb{Z}, \text{ because } \bar{b}^p = e$$

$$c^p \in \langle a \rangle$$

So, $c^p = a^l$ for some $l \in \mathbb{N}$. We know that a^l has a finite order, $|a^l|$. So clearly $c^{|a^l|}$ has order p .

So in either case, there is an element of order p in G if p is prime and $p \mid |G|$.

Thus, there is a subgroup, H_1 , with order p_1 in G . This subgroup is normal, because G is abelian.

Consider the new group $G_1 = G/H_1$, along with $n_1 = n/p_1$. Note that $|G_1| = |G|/p_1$; this follows from the theorem that says $|G/H| = |G|/|H|$ if H is normal.

We know that G_1 is abelian:

So by similar logic as above, if $a_1 > 1$, then there is a subgroup of order p_1 in G . Otherwise, we know that there is a subgroup of order p_2 in G .

Either way, there is a subgroup, $H'_2 < G_1$, with order p_1 (or p_2) in G_1 . This subgroup is normal in G_1 , because G_1 is abelian. Now, there's a subgroup of G containing H_1 that corresponds to H'_2 : call this subgroup H_2 . We know that H_2 is normal, because G is abelian.

Consider the group $G_2 = G_1/H'_2$. Note that $G_2 \cong G/H_2$, by the third isomorphism theorem. Moreover, $|G_2| = |G|/p_1^2$ (or $|G_2| = |G|/p_1p_2$).

We can proceed in the above manner a_i times for each p_i . Proceed until each prime factor is exhausted.

Consider $G_{a_1+a_2+\dots+a_k}$; it has order $|G|/n$, by the construction above, and is isomorphic to $G/H_{a_1+a_2+\dots+a_k}$ for some $H \leq G$. This means that $|H| = n$ (because $|G/H| = |G|/|H|$...thus, $|H| = |G|/|G/H|$, or in this case, $|H| = |G|/(|G|/n) = n$.)

So G has a normal subgroup of order n if G is a finite abelian group with $n \mid |G|$.

Problem 2:

Let $H < G$ with $[G : H]$ finite.

Problem 3:

Let G be a group acting transitively on a finite set, S , with $|S| > 1$.

Now, the action has only one orbit; for all $x \in S$, $\bar{x} = S$. In other words, for every $x, y \in S$ there is a $g \in G$ such that $g.x = y$.

Before proceeding, I wish to point out that I use the following freely:

If $g.x = x$, then $g^{-1}.x = x$: This is clear by applying g^{-1} to both sides of the equation.

If $g.x = y$, then $g^{-1}.y = x$: This is clear by applying g^{-1} to both sides of the equation.

Assume that for all $g \in G$, there is an $x \in S$ such that $g.x = x$. We proceed by constructing an infinite set of points in S , by induction.

Because $|S| > 1$, there are at least two distinct points of S : call them x_0 and x_1 .

There is an element, g_2 , such that $g_2.x_0 = x_1$, by transitivity of the action.

There is an x_2 such that $g_2.x_2 = x_2$, by the assumption we made earlier.

Now, $x_2 \neq x_0$, else:

$$\begin{aligned} g_2.x_0 &= g_2.x_2 \\ x_1 &= x_2 = x_0 \end{aligned}$$

which is a contradiction.

Also, $x_2 \neq x_1$, else:

$$\begin{aligned} g_2^{-1}.x_1 &= g_2^{-1}.x_2 \\ x_0 &= x_2 = x_1 \end{aligned}$$

which is also a contradiction.

So x_2 is distinct from x_0 and x_1 .

Now, assume that we have the following: we have defined x_n for each $n \in \mathbb{N}$ such that $n < N$, and g_n for each $n \in \mathbb{N}$ such that $n < N - 1$ and $n \geq 2$, with the following properties: $g_n.x_n = x_n$ and $g_n.x_0 = x_{n-1}$.

Then there is a g_N such that $g_N.x_0 = x_{N-1}$, because the action is transitive.

Also, there is an x_N such that $g_N.x_N = x_N$, by the assumption we made earlier.

Now, $x_N \neq x_0$, else:

$$\begin{aligned} g_N.x_0 &= g_N.x_N \\ x_{N-1} &= x_N = x_0 \end{aligned}$$

which is a contradiction.

Also, $x_N \neq x_{N-1}$, else:

$$\begin{aligned} g_N^{-1}.x_{N-1} &= g_N^{-1}.x_N \\ x_0 &= x_N = x_{N-1} \end{aligned}$$

which is also a contradiction.

Further, $x_N \neq x_i$ for any i between 0 and $N - 1$ (exclusive), else:

$$\begin{aligned} g_N g_i^{-1}.x_i &= g_N.x_i \\ g_n x_0 &= g_N.x_N \\ x_{N-1} &= x_N \end{aligned}$$

which is also a contradiction.

So x_N is distinct from each x_i with $i < N$.

So we have two distinct points, and if we have n distinct points in S , we can make $n + 1$ distinct points in S ; we can make infinitely many distinct points, thus S is infinite.

So, if for all $g \in G$, g has a fixed point, then S is infinite.

Or, in other words, because S is finite, there is a $g \in G$ that has no fixed point.

Problem 4:

Let G be a group such that $G/Z(G)$ is cyclic.

Then there is an $a \in G$ such that for all $\bar{x} \in G/Z(G)$, $\bar{x} = \bar{a}^n$ for some $n \in \mathbb{N}$.

So for all $y \in G$, there is an $n \in \mathbb{N}$ and $b \in Z(G)$ such that $y = a^n b$; the left cosets of $Z(G)$ partition G , and the set of these cosets is $\{a^n Z(G) : n \in \mathbb{N}\}$. So for all $y \in G$, $y \in a^n Z(G)$ for some $n \in \mathbb{N}$.

So for all $y, z \in G$, we have $y = a^n b$ and $z = a^m c$ for some $n, m \in \mathbb{N}$ and $b, c \in Z(G)$.

Now we have:

$$\begin{aligned} yz &= a^n b a^m c \\ &= a^n a^m b c \\ &= a^m a^n b c \\ &= a^m a^n c b \\ &= a^m c a^n b \\ &= z y \end{aligned}$$

Note that this fails if $G/Z(G)$ is only abelian:

Consider $D_8 = \langle r, s \rangle$. We note that the center of D_8 is $\{e, r^2\}$.

(We freely use the identity $sr = r^3s$ in the following).

We know that e commutes with every element, trivially.

Now, r^2 commutes with e , r , r^2 , and r^3 trivially;

Also, r^2 commutes with s , sr , sr^2 , and sr^3 :

$$\begin{aligned}
r^2s &= rsr^3 = sr^3r^3 = sr^2 \\
r^2sr &= r^2r^3s = rs = sr^3 = srr^2 \\
r^2sr^2 &= r^2sr^2 \\
r^2sr^3 &= r^2rs = sr = sr^5 = sr^3r^2
\end{aligned}$$

However, r and s do not commute with each other, and r^3 and s do not commute with each other:

$$rs = sr^3$$

Also, sr , sr^2 , and sr^3 do not commute with r :

$$\begin{aligned}
rsr &= sr^3r = s \neq sr^2 \\
rsr^2 &= sr^3r^2 = sr \neq sr^3 \\
rsr^3 &= sr^3r^3 = sr^2 \neq sr^3r = s
\end{aligned}$$

So every element other than e and r^2 fails to commute with something. So

Also, $D_8/\langle r^2 \rangle$ is abelian:

Observe that this group must have order 4, and that $\{\bar{e}, \bar{r}, \bar{s}, \bar{sr}\}$ are all distinct elements of this group (and thus this represents all elements in the quotient group).

Clearly, \bar{e} commutes with everything. We proceed by exhaustion:

$$\begin{aligned}
\bar{r}\bar{s} &= \bar{s}\bar{r} = \overline{r^3s} = \bar{r}\bar{s} = \bar{r}\bar{s} \\
\overline{rsr} &= \overline{rsr} = \overline{sr^3r} = \bar{s} = \overline{sr^2} = \overline{sr}\bar{r} \\
\overline{ssr} &= \overline{s^2r} = \bar{r} = \overline{r\bar{s}\bar{s}} = \overline{sr^3s} = \overline{sr}\bar{s} = \overline{sr}\bar{s}
\end{aligned}$$

But we know from an earlier homework that D_8 is not abelian. So in general, $G/Z(G)$ being abelian does not imply that G is abelian.

Problem 5:

Let p be prime, and let G be a group of order p^2 . We know that $Z(G)$ is a subgroup of G ; so $Z(G)$ has order 1, p , or p^2 .

We know that $Z(G)$ does not have order 1, from the discussion in class.

If $Z(G)$ has order p , then $G/Z(G)$ is cyclic (as it is a group of order $p^2/p = p$); we know that G is abelian, from problem 4.

If $Z(G)$ has order p^2 , then the center is the entire group; that is, G is abelian.

So in all cases, G is abelian.

Problem 6:

Let p be prime, and let G be a group of order p^n for some $n \in \mathbb{N}$. Let $H \trianglelefteq G$ with $H \neq \{e\}$.

Now, G acts on H by conjugation. By the class equation,

$$\begin{aligned} |H| &= |\{h \in H : \forall g \in G, ghg^{-1} = h\}| + \sum |\overline{x_i}| \\ &= |H \cap Z(G)| + \sum |[G : G_{x_i}]| \text{ Because the order of the orbit is the index of the stabilizer} \end{aligned}$$

We know that $p \mid |H|$, because H is a nontrivial subgroup of a p -group. Also, $p \mid [G : G_{x_i}]$ because each G_{x_i} is a subgroup of G , and none are trivial (because none of those orbits contain only one element; if there was an element whose orbit had only one element, then it would be in the set $\{h \in H : \forall g \in G, ghg^{-1} = h\}$).

So we know that $p \mid |H \cap Z(G)| + \sum |[G : G_{x_i}]|$. So because $p \mid \sum |[G : G_{x_i}]|$, we know that $p \mid |H \cap Z(G)|$.

So because $p \mid |H \cap Z(G)|$, we know that $|H \cap Z(G)| \neq 1$; that is $H \cap Z(G)$ is not the trivial subgroup.