Problem §1 (6.12) Let G be a group that acts on a set X.

(a) Suppose $|G| = 15$ and $|X| = 7$. Prove there is some element in X that is fixed by every element of G.

(b) What goes wrong if either $X = 6$ or $X = 8$?

Solution:

(a) Suppose $|G| = 15$ and $|X| = 7$. We know from Proposition 6.19 that $|Gx|$ divides $|G|$; furthermore, the distinct orbits $Gx_1, \ldots, Gx_k$ form a disjoint union of X.

From the Orbit-Stabilizer Counting Theorem, we know that

$$|X| = \sum_{i=1}^{k} |Gx_i| = \sum_{i=1}^{k} \frac{|G|}{|G_{x_i}|}.$$

Since $|Gx_i|$ divides $|G| = 15$ for all $1 \le i \le k$ and $\sum_{i=1}^{k} |Gx_i| = |X| = 7$, we must have

$$|Gx_i| = 1, 3, \text{ or } 5 \text{ for all distinct orbits }.$$

With these numbers, there are thus only three possible partitions of X into distinct orbits, up to ordering (each number represents the number of elements in each distinct orbit):

- $7 = 1 + 1 + 5$
- $7 = \underbrace{1 + \ldots + 1}_{7 \text{ times}}$
- $7 = 3 + 3 + 1$

In all cases, there is at least one orbit with only one element; this then implies that

$$1 = |Gx_j| = \frac{|G|}{|G_{x_j}|} = \frac{15}{15}$$

for some orbit Gx_j (from Proposition 6.19c). But then for some $x_j \in X$, its stabilizer has $15 = |G|$ elements; in other words, for some element in X, it is fixed by every element of G.

(b) Suppose instead that $|X| = 6$ or 8. There are then different possible partitions of X; but in either case, there exists a partition of X into distinct orbits that does not consist of any orbit with only 1 element:

- For $|X| = 6$, X can be partitioned into two orbits with 3 elements each (since $|Gx_1| + |Gx_2| = 3 + 3 = 6 = |X|$, as required by the Orbit-Stabilizer Counting Theorem).
- For $|X| = 8$, X can be partitioned into two orbits, one with 3 elements and one with 5 ($|Gx_1| + |Gx_2| = 5 + 3 = 8 = |X|$).

Thus when the group G acts on the set X, it is possible that there doesn't exist any orbit with only one element; then by Proposition 6.19, since

$$1 < |Gx_j| = \frac{|G|}{|G_{x_j}|} = \frac{15}{n},$$

where $1 < n = 3$ or 5. In other words, it is possible that no element in X is fixed by every element in G (since the number of elements in the stabilizer of any x could be less than 15).

Problem §2 (6.14) Let p be a prime. We proved that every group with p^2 elements is Abelian; now let G be a group with p^3 elements.

(a) Mimic the proof of Corollary 6.26 to try to prove that p^3 is Abelian. Where does the proof go wrong?

(b) Give two examples of non-Abelian groups with 2^3 elements.

(c) What sort of information can you deduce about G from the proof in (a) that failed?

Solution:

(a) Let $Z = Z(G)$ as before. Since Z is a subgroup of G, Lagrange's Theorem tells us that the order of Z divides $|G| = p^3$, so
$$|Z| = 1, p, p^2, \text{ or } p^3.$$
Theorem 6.25 tells us that $Z \neq \{e\}$, so $|Z| \neq 1$.

Suppose $|Z| = p^2$. Since the center Z of G is a normal subgroup, we form the quotient subgroup G/Z, with Lagrange telling us that
$$|G/Z| = \frac{|G|}{|Z|} = \frac{p^3}{p^2} = p.$$
Thus G/Z is of prime order, so Proposition 2.43 tells us that it is cyclic. Let hZ be a coset that generates G/Z,
$$G/Z = \{hZ, h^2Z, \ldots, h^{p-1}Z\}.$$
In particular, this implies that
$$G = Z \cup hZ \cup \ldots \cup h^{p-1}Z,$$
since every element is in a coset of Z.

Let $g_1, g_2 \in G$ be arbitrary elements. Since they're in some coset of Z, we have
$$g_1 = h^{i_1}z_1,\ g_2 = h^{i_2}z_2 \text{ for some } z_1, z_2 \in Z \text{ and } 0 \leq i_1, i_2 \leq p-1.$$
Since $z_1, z_2 \in Z$, we have
$$\begin{aligned} g_1g_2 = (h^{i_1}z_1)(h^{i_2}z_2) = (h^{i_1}h^{i_2})(z_1z_2) &= h^{i_1+i_2}z_2z_1 \\ &= (h^{i_2}h^{i_1})(z_2z_1) = (h^{i_2}z_2)(h^{i_1}z_1) = g_2g_1. \end{aligned}$$
Y I K E S ! ! ! We've shown that every element in G commutes with every other element; this means that $Z = G$, a contradiction of our assumption that $|Z| = p^2 \neq p^3 = |G|$. Thus $|Z| \neq p^2$.

Now, suppose $|Z| = p$. Z normal allows us to form the quotient subgroup G/Z, with Lagrange telling us that
$$|G/Z| = \frac{|G|}{|Z|} = \frac{p^3}{p} = p^2.$$
Thus G/Z has order p^2, so Corollary 6.26 tells us that it is Abelian. That means for two cosets $gZ, hZ \in G/Z$, we have $ghZ = hgZ$.

Like before, since every element is in a coset of Z, and G/Z is a collection of distinct cosets of G, we have
$$G = h_1Z \cup h_2Z \cup \ldots \cup h_{p^2-1}Z,$$
where $h_1, \ldots, h_{p^2-1} \in G$ form distinct cosets of Z.

Let $g_1, g_2 \in G$ be arbitrary elements of G. Then
$$g_1 = h_iz_1,\ g_2 = h_jz_2 \text{ for some } h_1, h_2 \in G \text{ and } 1 \leq i, j \leq j-1.$$
With g_1g_2, we have
$$g_1g_2 = (h_iz_1)(h_jz_2) = (h_ih_j)(z_1z_2),$$
and with g_2g_1, we have
$$g_2g_1 = (h_jz_2)(h_iz_1) = (h_jh_i)(z_2z_1) = (h_jh_i)(z_1z_2).$$
Are these two equal?

Not necessarily. $ghZ = hgZ$ means that for every $ghz \in ghZ$, $ghz \in hgZ$; and for every $hgz' \in hgZ$, $hgz' \in ghZ$. However, this does **not** guarantee that $z = z'$. Indeed, two examples (stated below) illustrate this: $ghZ = hgZ$ does not guarantee that $gh = hg$ for all $g, h \in G$.

Therefore, since not every element necessarily commutes with every other element, it's possible for $|Z| = p$; there is no contradiction.

Thus there exist non-Abelian groups of order p^3.

(b) Two examples of non-Abelian groups of order 2^3 are the dihedral group $\mathcal{D}_4$ (which one can easily verify is not Abelian), and the quaternion group $\mathcal{Q}$ (see Example 2.18; clearly $ji = -ij \neq ij$, and thus is non-commutative). These examples also illustrate that G/Z being Abelian does not necessarily force G to be Abelian; both $\mathcal{D}_4$ and $\mathcal{Q}$ have centers of order 2 ($Z(\mathcal{D}_4) = \{e, f\}$ where f is the flip that fixes the first and third vertices; and $Z(\mathcal{Q}) = \{\pm 1\}$), so G/Z is Abelian (since $|G/Z| = 4 = 2^2$), yet $G = \mathcal{D}_4$ or $\mathcal{Q}$ are not Abelian.

(c) Let G be a group with order p^3. If G is Abelian, then definitionally $Z(G) = G$, so suppose $Z(G) \neq G$ (i.e. G is non-Abelian). Then $|Z(G)| \neq p^3$; and from the proof in (a), we see that $|Z(G)| \neq 1$ and $|Z(G)| \neq p^2$; the only possible value for $|Z(G)|$ is p. Therefore, if G is a non-Abelian group of order p^3, then its center $Z(G)$ has order p.

Problem §3 (6.17) This exercise sketches an alternative proof of a key step in the proof of Corollary 6.26.

(a) Let G be a group, and let $g \in G$ be an element that is not in the center of G. Prove that there is a strict inclusion
$$Z(G) \subsetneq Z_G(g);$$
i.e. prove that the centralizer of g is strictly larger than the center of G.

(b) Let G be a finite group of prime power order, say $|G| = p^n$. Prove that if the center of G satisfies $|Z(G)| \geq p^{n-1}$, then $Z(G) = G$, and so G is Abelian.

Solution:

(a) Let $g \in G$ be an element not in the center of G. By definition,
$$Z(G) \subseteq Z_G(g),$$
since $Z_G(g)$ consists of all elements that commute with any element $g^i \in \langle g \rangle \subseteq G$; but every element $z \in Z(G)$ commutes with any element in G. Moreover, since $g \notin Z(G)$, we know $g \neq e$ (g is non-trivial); hence $\langle g \rangle \neq \{e\}$ (and so $\langle g \rangle$ has at least one non-identity element).

Clearly, any $g^i \in \langle g \rangle$ commutes with any element in $\langle g \rangle$. Let $g^i, g^j \in \langle g \rangle$. Then
$$g^i g^j = g^{i+j} = g^{j+i} = g^j g^i.$$
Therefore $\langle g \rangle \subseteq Z_G(g)$.

But $g \notin Z(G)$ and $g \in Z_G(g)$; thus $Z(G) \subsetneq Z_G(g)$, as required.

(b) We start with a lemma (since we didn't do 6.16):

Lemma 1 ($Z_G(g)$ is Subgroup)**.** *Let G be a group, and $g \in G$ an element. Then $Z_G(g)$ is a subgroup of G.*

Proof. Clearly, $eg = ge$ for every $g \in G$; thus $e \in Z_G(g)$.

Let $z_g \in Z_G(g)$. Then $z_g g = g z_g$. Since $z_g \in Z_G(g) \subseteq G$, $z_g^{-1} \in G$ as well. Then
$$z_g g = g z_g \iff z_g^{-1} z_g g = z_g^{-1} g z_g \iff g z_g^{-1} = z_g^{-1} g z_g z_g^{-1} \iff g z_g^{-1} = z_g^{-1} g.$$

Hence $z_g^{-1} \in Z_G(g)$ for any $z_g \in Z_G(g)$.

Finally, suppose $z_g, z_g' \in Z_G(g)$, and consider $z_g z_g'$. Then

$$z_g z_g' g = z_g g z_g' = g z_g z_g',$$

and so $z_g z_g' \in Z_G(g)$ as well. Therefore $Z_G(g)$ is a subgroup of G. $\square$

Suppose G has order p^n for some prime number p, and $|Z(G)| \geq p^{n-1}$. Since $Z(G)$ is a (normal) subgroup of G, Lagrange's Theorem tells us that $|Z(G)|$ must be either p^{n-1} or p^n.

Suppose $Z(G) \neq G$. Then $|Z(G)| = p^{n-1}$, and there exists some $g \in G$ such that $g \notin Z(G)$ (that is, there exists some $g \in G \setminus Z(G)$). From (a), we know that

$$Z(G) \subsetneq Z_G(g);$$

that is, $Z_G(g)$ is strictly larger than $Z(G)$. But we know that $Z_G(g)$ is a subgroup of G from Lemma 1; thus Lagrange tells us that $|Z_G(g)| = p^r$ for some $0 \leq r \leq n$. Since $|Z(G)| = p^{n-1}$, we need $p^{n-1} = |Z(G)| < |Z_G(g)| = p^n$. Hence $Z_G(g) = G$; but since the choice of $g \in G \setminus Z(G)$ was arbitrary, that means every element not in $Z(G)$ commutes with every element in G. In other words, $g \in Z(G)$; a contradiction.

Therefore $|Z(G)|$ must be p^n, and so $Z(G) = G$, and so G is Abelian.

In Corollary 6.26, the above result can be used instead of deriving a contradiction for $|Z(G)| = p$. From Lagrange, we know that $|Z(G)| = 1, p$, or p^2. Theorem 6.25 tells us that $Z(G) \neq \{e\}$, so $|Z(G)| \neq 1$; that is, $|Z(G)| = p$ or p^2. In either case, $|Z(G)| \geq p^{2-1} = p$, so from the result above, we know that G is Abelian.