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 $Gx_1, \dots, Gx_k$ 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 $1 \leq i \leq k$ 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.

Problem §4 (6.19) Let p be prime, and let G be a group of order p^n. Prove that for every $0 \leq r \leq n$, there is a subgroup H of G of order p^r.

Solution: We begin with two lemmas.

Lemma 2 (Subgroups of Center are Normal)**.** *Let G be a finite group, and $Z(G)$ its center. If $H \subseteq Z(G)$ is a subgroup of $Z(G)$, then H is a normal subgroup of G.*

Proof. Suppose $H \subseteq Z(G)$ is a subgroup of $Z(G)$ (and thus of G as well). Then for any $h \in H$,

$$hg = gh \text{ for all } g \in G.$$

But then

$$hg = gh \iff g^{-1}hg = h \in H$$

for every $g \in G$; thus $g^{-1}Hg \subseteq H$ for any $g \in G$. Proposition 6.10 then informs us that $g^{-1}Hg$ is a normal subgroup of G. $\square$

Lemma 3. *If G is a finite group with order p^n for some $n \in \mathbb{Z}_{>0}$, G has a normal subgroup of order p.*

Proof. It suffices to prove that an element $z \in Z(G)$ has order p; this thus forms a cyclic subgroup $\langle z \rangle \subseteq Z(G)$ with order p.

Theorem 6.25 tells us that the center of $Z(G) \neq \{e\}$; that is, the center $Z(G)$ of G has non-trivial elements. Precisely, Lagrange tells us that $|Z(G)| = p^i$ for some $1 \leq i \leq n$. Let $z \in Z(G)$; since Corollary 2.42 implies $z^{p^i} = e$, consider $z^{\frac{p^i}{p}} = z^{p^{i-1}}$. Then the order of $z^{p^{i-1}}$ is p, since clearly $k = p$ is the lowest power such that $(z^{p^{i-1}})^k = e$. Thus $z^{p^{i-1}} \in Z(G)$ has order p, and so forms a cyclic subgroup of $Z(G)$, which is a normal subgroup of G with order p (by Lemma 2), as required. $\square$

We now proceed to the main problem by induction on n. If $n = 1$, then $|G| = p$, and $\{e\}$ (with order $p^0 = 1$) and $\{G\}$ (with order p) are clearly subgroups of G; so suppose $n \geq 2$, and that the statement holds for groups of order $p^{n'}$ with $n' < n$.

From Lemma 2, G has a normal subgroup N of G with order p; thus the quotient group G/N is well-defined by Theorem 6.12, and has order

$$|G/N| = \frac{|G|}{|N|} = \frac{p^n}{p} = p^{n-1}.$$

Since $n-1 < n$, the inductive hypothesis says that G/N has subgroups H_r of order p^r for every $0 \leq r \leq n-1$. To complete the proof, we must now show that every $H_r \in G/N$ has an analogous subgroup of G with the same order.

Let $g_1N, g_2N, \ldots, g_{p^{n-1}}N$ denote the elements of G/N (i.e. distinct cosets of N); here $g_i \in G$ are distinct elements of G; i.e. $g_i \neq g_j$ for $i \neq j$ (we can impose a stricter condition on g_i and g_j, since $g_iN \neq g_jN$; but this suffices). Consider the homomorphism

$$\phi : G/N \longrightarrow G, \ \phi(g_iN) = g_i.$$

To see why this is a well-defined function, consider two cosets $gN = g'N \in G/N$. Then $gN = g'N = g_iN$ for one of the cosets above, $g_iN \in G/N$ (since $g_1N, \ldots, g_{p^{n-1}}N$ represent all elements of G/N). So,

$$\phi(gN) = \phi(g_iN) = g_i = \phi(g_iN) = \phi(g'N),$$

and so $\phi(gN) = \phi(g'N)$. Homomorphism properties follow trivially from coset multiplication properties.

We now show that for every $0 \leq r \leq n-1$, the image of the subgroup H_r—denoted $\phi(H_r)$—forms a subgroup in G with order p^r. Let H_r be a subgroup of G/N with order p^r. Clearly, $\phi(H_r)$ is a subset of G, since for every element $g_jN \in H_r \subseteq G/N$, $g_j \in G$, so every element $\phi(g_jN) = g_j \in \phi(H_r)$ is in G as well. Moreover, since there are p^r elements $g_jN \in H_r$ and for different elements g_jN and g_kN, $g_j \neq g_k$, there are necessarily p^r elements in $\phi(H_r)$ as well.

Since H_r has an identity element $eN = N \in H_r$, its image $\phi(N) = e$ has the identity element as well. For two $g = \phi(gN), g' = \phi(g'N) \in \phi(H_r)$, their product

$$\phi(gN \cdot g'N) = \phi(gg'N) = gg' \in \phi(H_r)$$

is in the image as well. Finally, for every $gN \in H_r$, $g^{-1}N \in H_r$ as well, since H_r is itself a subgroup; thus for every $g = \phi(gN) \in \phi(H_r)$, we have

$$\phi(g^{-1}N) = g^{-1} \in \phi(H_r)$$

as well. Therefore $\phi(H_r)$ is a subgroup of G with order p^r.

Since this holds for any H_r with $0 \leq r \leq n-1$, we have thus shown that G has subgroups of order p^r for every $0 \leq r \leq n-1$. Clearly, G is a subgroup of itself; thus G has a subgroup of order p^n as well. Therefore, every group G of order p^n has subgroups of order p^r for every $0 \leq r \leq n$.

Problem §5 (6.20) Give two different proofs of the following stronger version of Sylow's Theorem:

Let G be a finite group, let p prime, and suppose that $|G|$ is divisible by p^r. Prove that G has a subgroup of order p^r. (Note that here, p^r is not required to be the largest power of p that divides $|G|$).

(a) Give a proof that directly mimics the proof of Theorem 6.29 by considering the sets of all subsets of G that contain p^r elements.

(b) Combine the version of Sylow's Theorem that we did prove with Exercise 6.19.

Solution: Let p^n be the largest power of p that divides $|G|$, and suppose $r < n$ (since otherwise, we can just apply Sylow's Theorem). We're given that p^r divides $|G|$, so we can factor

$$|G| = p^r k = p^n m$$

for some integers k and m where $m \nmid p$. The proof is by induction on k. If $k = 1$, then $|G| = p^r$, so G itself is the desired subgroup. Suppose now that $k \geq 2$, and that the stronger theorem holds for groups of order $p^r k'$ with $k' < k$.

Recall that a subset $A \subseteq G$ is a subgroup if and only if $aA = A$ for every $a \in A$. Let's look at the collection of p^r-element subsets of G and let G act on these subsets by left multiplication. Let

$$S = \{A \subseteq G \mid A \text{ has } p^r \text{ elements } \}.$$

Since G has $p^r k$ elements and we need to choose p^r of them, the number of elements of S is equal to

$$|S| = \binom{p^r k}{p^r}.$$

Let $A_1, \dots, A_d \in S$ so that $GA_1, \dots, GA_d$ form distinct orbits. With the Orbit-Stabilizer Counting Theorem, we thus have

$$|S| = \sum_{i=1}^{d} |GA_i| = \sum_{i=1}^{d} \frac{|G|}{|G_{A_i}|}.$$

Observe that

$$|S| = \binom{p^r k}{p^r} = \frac{(p^r k)!}{p^r!(p^r k - p^r)!} = \frac{p^r k(p^r k - 1)\dots(p^r k - p^r + 1)}{p^r(p^r - 1)\dots \cdot 2 \cdot 1}.$$

Unfortunately, we cannot apply Lemma 6.30 here, since $n > r$; that is, the above product is still divisible by p. However, we can glean some information about its divisibility:

Recall that $p^r k = p^n m$, where $p \nmid m$. Thus $k = p^{n-r}m$, and p^{n-r} is the maximal power of p that divides k. It turns out that p^{n-r} is the maximal power of p that divides $|S|$ as well. Since

$$|S| = \prod_{j=0}^{p^r-1} \frac{p^r k - j}{p^r - j},$$

we can inspect each individual fraction. For $j = 0$, the fraction $\frac{p^r k}{p^r} = k$ has maximal p-power p^{n-r}. It remains to show that none of the $1 \leq j \leq p^r - 1$ fractions are divisible by p. Take any j between 1 and $p^r - 1$, and factor it into

$$j = p^i s \text{ with } 0 \leq i < r \text{ and } p \nmid s.$$

Then

$$\frac{p^r k - j}{p^r - j} = \frac{p^r k - p^i s}{p^r - p^i s} = \frac{p^{r-i}k - s}{p^{r-i} - s}.$$

Since $i < r$ and $p \nmid s$, we see that neither the numerator or the denominator is divisible by p. Thus, the maximal power of p that divides $|S|$ is p^{n-r}.

Thus, since

- $|S|$ is divisible by p^{n-r} (and not divisible for any $\alpha > n - r$);
- $|S| = \sum_{i=1}^{d} |GA_i| = \sum_{i=1}^{d} \frac{|G|}{|G_{A_i}|}$; and
- $\frac{|G|}{|G_{A_i}|}$ is an integer,

every individual summand $\frac{|G|}{|G_{A_i}|}$ is divisible by p^{n-r}; however, does this guarantee that for some G_{A_i}, p^r divides $|G_{A_i}|$?

Suppose that $p^r \nmid |G_{A_i}|$ for every $1 \leq i \leq d$ (that is, p^r does not divide the order of any stabilizer). In other words, $|G_{A_i}|$ is only divisible by a smaller maximal power of p, say p^{r-j_i} for some $1 \leq j_i \leq r$ (and so factors into $|G_{A_i}| = p^{r-j_i}s$, where $p \nmid s$). Then every orbit GA_i would have order

$$|GA_i| = \frac{|G|}{|G_{A_i}|} = \frac{p^n m}{p^{r-j_i}s} = p^{n-r+j_i}\frac{m}{s}.$$

But then every orbit would be divisible by some $p^{n-r+\alpha}$, where $\alpha = \min\{j_1, \ldots, j_d\}$. Since every $j_i \geq 1$, $\alpha \geq 1$, so $n - r + \alpha > n - r$, and so $\sum_{i=1}^{d} |GA_i| = |S|$ is divisible by $ptdn - r + \alpha$, a contradiction of above (since p^{n-r} is the maximal power of p that divides $|S|$). Thus at least one stabilizer G_{A_i} has order $|G_{A_i}|$ divisible by p^r.

In other words, we have shown that there exists a subset $A \subseteq G$ with $|A| = p^r$ such that the stabilizer G_A of A has order

$$|G_A| = p^r k' \text{ with } k'|k,$$

since p^r dividing $|G_A|$ means $|G_A| = p^r k'$ for some integer k'; and $\frac{|G|}{|G_A|} = \beta$ for some integer β means

$$\beta = \frac{p^n m}{p^r k'} = \frac{p^{n-r} m}{k'} \implies k'\beta = p^{n-r} m = k,$$

and so $k'|k$.

We consider two cases. If $k' < k$, then the induction hypothesis says that G_A has a subgroup H with order p^r; but H is thus also a subgroup of G (since G_A is a subgroup of G), so we are done.

Otherwise, suppose $k' = k$. Then $|G_A| = |G|$, so $G_A = G$. By definition of a stabilizer G_A, this means that

$$gA = A \text{ for every element } g \in G.$$

The set has A has p^r elements, so it must be non-empty. Let $a \in A$ be some element of A. Then for every $g \in G$, we have

$$g = (ga^{-1})a \in (ga^{-1})A = A.$$

Thus every element of G is in A, so $G \subseteq A$; and since $A \subseteq G$, $G = A$, so $|G| = |A| = p^r$. But G has order $p^r k$ with $k \geq 2$, a contradiction.

Therefore $k' < k$, and so G has a subgroup of order p^r. □

Alternatively, suppose p^r divides $|G|$ for a prime p and a positive integer r. Let p^n be the highest power of p that divides $|G|$; then $0 \leq r \leq n$ (since r is a positive integer, and any p^r that divides $|G|$ also divides p^n). By Sylow's Theorem, G has a subgroup H of order p^n; and by Exercise 6.19, since H is itself a group, H has a subgroup K of order p^r (since $0 \leq r \leq n$). But H is a subgroup of G, so K is a subgroup of G as well. Thus if $|G|$ is divisible by p^r for some prime p and some positive integer r, G has a subgroup K of order p^r, as required.