Groups and Symmetry Problem Set 6 — Solutions

Q1: The identity element fixes all of X, so it has more than one fixed point. The orbit counting theorem says that the average number of fixed points is the number of orbits, which is 1. As the identity has more than one fixed point, some other element $g \in G$ must have less than one, so as to bring the average back down to 1. Thus $|\operatorname{Fix}(g)| < 1$ but of course $|\operatorname{Fix}(g)|$ is a nonnegative integer so $|\operatorname{Fix}(g)| = 0$ so $\operatorname{Fix}(g) = \emptyset$.

For a more algebraic presentation, note that $\sum_{g\in G} 1 = |G|$, so $|G|^{-1}\sum_{g\in G} 1 = 1$. The orbit counting theorem tells us that $|G|^{-1}\sum_{g\in G}|\operatorname{Fix}(g)| = \text{ number of orbits } = 1$. By subtracting these equations we find that $\sum_{g\in G}(|\operatorname{Fix}(g)|-1) = 0$. If we move the $g = 1$ term to the other side we get $\sum_{g\neq 1}(|\operatorname{Fix}(g)|-1) = 1-|X|$. The right hand side is less than 0, so at least one of the terms on the left must be less than 0, so $|\operatorname{Fix}(g)| - 1 < 0$ for some g. As before, this means that $\operatorname{Fix}(g) = \emptyset$.

Q2: We can use X to define a homomorphism $G \to S_n$ in the usual way. (In other words, we list the elements of X as $\{x_1, \dots, x_n\}$ say, and then let $\phi(g)$ be the permutation σ such that $gx_i = x_{\sigma(i)}$ for all i.) The kernel of any homomorphism is a normal subgroup, and there are only two normal subgroups of G so either $\ker(\phi) = \{1\}$ or $\ker(\phi) = G$. As the action is nontrivial, we have $gx_i \neq x_i$ for some $g \in G$ and $i \in \{1, \dots, n\}$, so $\phi(g)(i) \neq i$, so $\phi(g) \neq 1$. Thus $g \notin \ker(\phi)$, so $\ker(\phi) \neq G$, so we must have $\ker(\phi) = \{1\}$. This means that ϕ is injective and thus that $|G| = |\phi(G)|$. Moreover, $\phi(G)$ is a subgroup of S_n, so $n! = |S_n|$ is divisible by $|\phi(G)| = |G|$, and $|G|$ is divisible by p, so $n!$ is divisible by p. Now, if $m < p$ then none of the numbers $1, 2, \dots, m$ are divisible by p so $m!$ is not divisible by p. As p divides $n!$ we must have $n \geq p$ as claimed.

Q3: First note that $1225 = 25 \times 49 = 5^2 7^2$, so we will study the Sylow 5-subgroups and 7-subgroups of G. We know that n_5 divides 49 (so $n_5 \in \{1, 7, 49\}$) and $n_5 = 1 \pmod 5$. As $7 = 2 \pmod 5$ and $49 = 4 \pmod 5$ we see that the only possibility is $n_5 = 1$. We therefore have a unique Sylow 5-subgroup, which we call P. Note that P is normal, and also that $|P| = 5^2$, so Proposition 2.8 tells us that P is abelian.

Next, we know that n_7 divides 25 (so $n_7 \in \{1, 5, 25\}$) and $n_7 = 1 \pmod 7$. As $5 = 5 \pmod 7$ and $25 = 4 \pmod 7$, we see that n_7 must be 1. There is thus a unique Sylow 7-subgroup, which we call Q. We again see that Q is normal and abelian.

Using Proposition 2.9 in the notes, we see that $G \simeq P \times Q$. This is abelian, because P and Q are.

Q4: We first claim that any nontrivial subgroup $P \leq G$ contains the element -1. Indeed, we have $G = \{1, -1, i, -i, j, -j, k, -k\}$ and $i^2 = (-i)^2 = j^2 = (-j)^2 = k^2 = (-k)^2 = -1$. As P is nontrivial it must either contain -1 (so there is nothing to say) or some element $x \in \{\pm i, \pm j, \pm k\}$, in which case it also contains $x^2 = -1$, as claimed. By the same argument, Q must contain -1, so $P \cap Q$ contains -1, so $P \cap Q$ is nontrivial.

Q5:

(a) We know that n_3 divides 2 and is congruent to 1 modulo 3; the only possibility is $n_3 = 1$. This means that there is a unique, normal Sylow 3-subgroup, which we call P. We then let Q be any Sylow 2-subgroup. As $|Q| = 2$, it is clear that $Q = \{1, h\}$ for some h with $h^2 = 1$.

(b) Suppose that $P \simeq C_9$. We can then choose an element $g \in P$ that generates P, with $g^9 = 1$. As P is normal, we see that $hgh = g^a$ for some integer a. As $h^2 = 1$, this means that

$$g = h^2 g h^2 = h g^a h = g^{a^2},$$

so $a^2 = 1 \pmod 9$, so the number $a^2 - 1 = (a+1)(a-1)$ is divisible by 9. The following table shows all numbers a mod 9 and their squares:

a	-4	-3	-2	-1	0	1	2	3	4
a^2	-2	0	4	1	0	1	4	0	-2

As $a^2 = 1 \pmod 9$, we must have $a = 1 \pmod 9$ or $a = -1 \pmod 9$, so $hgh = g$ or $hgh = g^{-1}$. If $hgh = g$ then h commutes with g and we find that $G \simeq P \times Q \simeq C_2 \times C_9$. If $hgh = g^{-1}$ we find that $G \simeq D_9$.

(c) Now suppose instead that $P \simeq C_3 \times C_3$.

(i) We have

$$(x_+)^h = hx_+h = h(xxhxxh)h = hxxhxx.$$

Now, xx lies in P and P is normal so $hxxh$ lies in P. Moreover, P is abelian, so xx commutes with $hxxh$. We thus have $hxxhxx = xxhxxh$, or in other words, $(x_+)^h = x_+$. This shows that $x_+ \in P_+$.

Next, we have $xxx = x^3 = 1$ and so

$$(x_-)^h x_- = h(xxhxh)h\, xxhxh = hxxhxxxhxh = hxxhhxh = hxxxh = hh = 1,$$

so $(x_-)^h = (x_-)^{-1}$, so $x_- \in P_-$.

Finally, we have

$$x_+x_- = (xx)(hxxh)\,(xx)(hxh) = (xx)(xx)(hxxh)(hxh) = xhxxxh = xhh = x.$$

(In the second equality, we used the fact that each of the four bracketed terms lies in P, so we can commute them past each other.)

(ii) Clearly $1 \in P_+$ and $1 \in P_-$. If $x, y \in P_+$ we have $x = hxh$ and $y = hyh$, so $xy = hxh\,hyh = hxyh$, so $xy \in P_+$. In particular, we can take $y = x$ to see that the element $x^{-1} = x^2$ lies in P_+. This shows that P_+ is a subgroup of P. Now suppose instead that $x, y \in P_-$, so that $hxh = x^{-1}$ and $hyh = y^{-1}$. As x and y commute we have $x^{-1}y^{-1} = (xy)^{-1}$, so $hxyh = hxh\,hyh = x^{-1}y^{-1} = (xy)^{-1}$, so $xy \in P_-$. It follows that P_- is also a subgroup.

If $x \in P_+ \cap P_-$ then $x^h = x$ and also $x^h = x^{-1}$, so $x = x^{-1}$, so $x^2 = 1$. As $P \simeq C_3 \times C_3$ we also know that $x^3 = 1$, and it follows that $x = x^3(x^2)^{-1} = 1$. This shows that $P_+ \cap P_- = \{1\}$.

(iii) As P_+ and P_- are subgroups of the abelian group P, we see that they commute with each other, so we can define a homomorphism $\phi\colon P_+ \times P_- \to P$ by $\phi(y, z) = yz$. For any $x \in P$ we have $(x_+, x_-) \in P_+ \times P_-$ and $\phi(x_+, x_-) = x_+x_- = x$. This shows that ϕ is surjective. We also have $P_+ \cap P_- = \{1\}$, which implies that ϕ is injective. This means we have an isomorphism $P_+ \times P_- \to P$, and so $|P_+||P_-| = 9$.

(iv) Suppose that $|P_+| = 9$, so $P_+ = P$ and $P_- = \{1\}$. This means that $hxh = x$ for all $x \in P$, so P commutes with Q, so $G \simeq Q \times P \simeq C_2 \times C_3 \times C_3$.

(v) Now suppose instead that $|P_+| = 3$, so $|P_-| = 3$ also. This means that $P_+ \simeq P_- \simeq C_3$, so we can choose $a \in P_+$ and $b \in P_-$ such that $P_+ = \{1, a, a^2\}$ and $P_- = \{1, b, b^2\}$ and $a^3 = b^3 = 1$. We define $\phi\colon C_3 \times D_6 \to G$ by

$$\phi((R^i, R^j)) = a^i b^j$$
$$\phi((R^i, R^j S)) = a^i b^j h.$$

It is easy to check that this is an isomorphism of groups.