Homework Assignment 7: Solutions

1. Let $n \geq 3$. Show that $Z(S_n) = \{(1)\}$.

   Proof. Recall that an element of a group is in the center if and only if it is the only member of its conjugacy class. (Indeed, fix x, then x is in the center if and only if $gx = xg$ for all g if and only if $gxg^{-1} = x$ for all g.) Therefore, we must show that if $\sigma \in S_n$ is nontrivial, it has a nontrivial conjugacy class. We fix some nontrival permutation σ whose cycle decomposition begins as follows:

   $$\sigma = (a_1\ a_2 \cdots) \cdots .$$

   Since $n \geq 3$, there is some $b \neq a_1, a_2$. Since the conjugacy classes in S_n are classified by cycle type (i.e., the shape of the cycle decomposition), we see that σ is conjugate to

   $$\sigma' = (a_1\ b \cdots) \cdots .$$

   And since $\sigma(a_1) = a_2 \neq b\sigma'(a_1)$, we see that σ has a nontrivial conjugacy class, and therefore cannot be in the center. In this case, it is easy to see how to conjugate σ to get σ'. Let $\tau = (a_2, b)$, then we check directly $\sigma' = \tau\sigma\tau^{-1}$. □

2. Let G be a group. Prove that that $\operatorname{Inn}(G) \trianglelefteq \operatorname{Aut}(G)$. The quotient $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ is called the *outer automorphism group* of G, and is denoted by $\operatorname{Out}(G)$.

   Proof. Let $\sigma_g \in \operatorname{Inn}(G)$ be an inner automorphism associated to $g \in G$, so that $\sigma_g(x) = gxg^{-1}$. Let $\varphi \in \operatorname{Aut}(G)$ be an arbitrary automorphism. We want to show that $\varphi\sigma_g\varphi^{-1}$ is also an inner automorphism. We compute that:

   $$\begin{aligned} (\varphi\sigma_g\varphi^{-1})(x) &= \varphi(\sigma_g(\varphi^{-1}(x))) \\ &= \varphi(g\varphi^{-1}(x)g^{-1}) \\ &= \varphi(g)(\varphi\varphi^{-1}(x))\varphi(g)^{-1} \\ &= \varphi(g)x\varphi(g)^{-1} \\ &= \sigma_{\varphi(g)}(x). \end{aligned}$$

   That is, $\varphi\sigma_g\varphi^{-1} = \sigma_{\varphi(g)}$ is the inner automorphism associated to $\varphi(g)$, and is in particular contained in $\operatorname{Inn}(G)$, as desired. □

3. The converse to Lagrange's theorem holds for groups of prime power order. To prove this we will need to strengthen the fourth isomorphism theorem (HW5#1).

   (a) Let G be a group and $N \trianglelefteq G$. Let $N \leq H \leq K \leq G$, and let $\overline{H}, \overline{K}$ be the corresponding subgroups of G/N as in HW5#1. Show that $|K : H| = |\overline{K} : \overline{H}|$. (*Hint*: There is an obvious map $K/H \to \overline{K}/\overline{H}$. Prove it is bijective. Be careful though, we don't know that K/H is a group, just a set of cosets.)

   Proof. Let $\pi : G \to G/N$ be the natural projection, and consider the map $K/H \to \overline{K}/\overline{H}$ which takes a coset kH to the coset $\pi(k)\overline{H}$.

Well defined: If $kH = k'H$ then $k = k'h$ for some $h \in H$. Thus $\pi(k) = \pi(k')\pi(h)$, and $\pi(h) \in \overline{H}$ so that $\pi(k)\overline{H} = \pi(k')\overline{H}$.

Injectivity: Suppose $\pi(k)\overline{H} = \pi(k')\overline{H}$. This says $\pi(k)\pi(k')^{-1} = \pi(kk'^{-1}) \in \overline{H}$. By HW5#1e(i), this implies that $kk'^{-1} \in H$, so that $kH = k'H$ giving injectivity.

Surjectivity: This is immediate, since $\overline{K} = \pi(K)$, so that a coset in the target is automatically $\pi(k)\overline{H}$ for some $k \in K$. □

(b) Suppose $|G| = p^d$ for a prime p and $d \geq 1$. Show that for every $a = 1, 2, \cdots, d$, G has a subgroup of order p^a. (*Hint*: Use what we know about the center of a group of p-power order and proceed by induction using part (a)).

Proof. We proceed by induction on d. If $d = 1$ the $G \cong Z_p$ which has a subgroup of order p^1 given by G itself. For the general case, we use that $1 \neq Z(G) \leq G$. Notice that $Z(G)$ is abelian, and by Lagrange $|Z(G)|$ is a (positive) power of p, and therefore by Cauchy's theorem for abelian groups, contains an element $x \in Z(G)$ of order p. Then x also has order p in G, and so G has a subgroup of order p^1 (in particular, we have established Cauchy's theorem for p groups).

We'd now like to produce a subgroup of order p^a for $a \geq 2$. Since $\langle x \rangle \leq Z(G)$, we know by HW6#2(a) that $\langle x \rangle \trianglelefteq G$, so we consider the quotient $\overline{G} = G/\langle x \rangle$. By induction, $\overline{G}$ has a subgroup $\overline{H}$ of order p^{a-1}. Let H be the preimage of $\overline{H}$ in G (as in HW5#1(a)). Then by part (a):

$$|G|/|H| = [G : H] = [\overline{G} : \overline{H}] = |\overline{G}|/|\overline{H}| = p^{d-1}/p^{a-1} = p^{d-a}.$$

We can then solve for $|H| = p^a$ as desired. □

4. Find all groups with exactly 2 conjugacy classes. (*Hint*: Use the class equation.)

Proof. We know that the trivial group only has 1 conjugacy class. So if G has two conjugacy classes, there exists $g \in G$ not equal to the identity. Since $G * 1 = \{1\}$, this means that $G * g$ must contain everything else. In particular, the class equation degenerates to:

$$|G| = |G * 1| + |G * g| = 1 + [G : C_G(g)].$$

Therefore $[G : C_G(g)] = |G| - 1$, but also it must divide $|G|$ by Lagrange's theorem. But if $n - 1$ divides n, then $n = 2$. Therefore $|G| = 2$ and so $G \cong Z_2$. □

For the next question we remind the reader of the following definitions from linear algebra.

Definition 1. *Let F be a field, with additive identity 0 and multiplicative identity 1. An F-vector space V is an abelian group $(V, +)$ together with a scalar multiplication function $F \times V \to V$ denoted $(\lambda, v) \mapsto \lambda v$ such that for all $u, v \in V$ and $\lambda, \tau \in F$ Notice I had missed an axiom in the first draft, I've added it here in red:*

(1) $0v = 0$.

(2) $1v = v$.

(3) $\lambda(\tau v) = (\lambda\tau)v$.

(4) $\lambda(u + v) = \lambda u + \lambda v$.

(5) $(\lambda + \tau)v = \lambda v + \tau v$

Let V, W be two F-vector spaces. A function $\varphi : V \to W$ is called F-linear if for all $u, v \in V$ and $\lambda \in F$:

(1) $\varphi(u + v) = \varphi(u) + \varphi(v)$.

(2) $\varphi(\lambda v) = \lambda\varphi(v)$.

5. Fix a prime p and let

$$V = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cdots \times \mathbb{Z}/p\mathbb{Z}}_{n \text{ times}}.$$

For $v = (x_1, \cdots, x_n) \in V$, and $\lambda \in \mathbb{F}_p$, define $\lambda v = (\lambda x_1, \cdots, \lambda x_n)$ where multiplication in the coordinates is defined modulo p.

(a) Show that V with scalar multiplication as defined above is an $\mathbb{F}_p$-vector space.

Proof. Conditions (1)-(4) are easily verified coordinatewise, as the analogous identities hold for arithmetic mod p (or even mod n). Indeed, (1) holds because multiplication by 0 mod n is 0. (2) holds because 1 is the multiplicative identity mod n. (3) follows from associativity of multiplication mod n and (4) and (5) follow from the distributive law. It is overly pedantic, but we includ the explicit computations:

$$\textbf{(1)}\ 0 \cdot (x_1, \cdots, x_n) = (0x_1, \cdots, 0x_n) = (0, \cdots, 0).$$

$$\textbf{(2)}\ 1 \cdot (x_1, \cdots, x_n) = (1x_1, \cdots, 1x_n) = (x_1, \cdots, x_n).$$

(3) follows from associativity of multiplication mod p.

$$\textbf{(3)}\ \lambda \cdot (\tau \cdot (x_1 \cdots, x_n)) = \lambda \cdot (\tau x_1, \cdots, \tau x_n) = (\lambda\tau x_1, \cdots, \lambda\tau x_n) = \lambda\tau \cdot (x_1, \cdots, x_n).$$

(4) follows from the distributive law.

$$\begin{aligned} \textbf{(4)}\ \lambda((x_1, \cdots, x_n) + (y_1, \cdots, y_n)) &= \lambda(x_1 + y_1, \cdots, x_n + y_n) \\ &= (\lambda(x_1 + y_1), \cdots, \lambda(x_n + y_n)) \\ &= (\lambda x_1 + \lambda y_1, \cdots, \lambda x_n + \lambda y_n) \\ &= (\lambda x_1, \cdots, \lambda x_n) + (\lambda y_1, \cdots, \lambda y_n) \\ &= \lambda \cdot (x_1, \cdots, x_n) + \lambda \cdot (y_1, \cdots, y_n). \end{aligned}$$

$$\begin{aligned} \textbf{(5)}\ (\lambda + \tau) \cdot (x_1, \cdots, x_n) &= ((\lambda + \tau)x_1, \cdots, (\lambda + \tau)x_n) \\ &= (\lambda x_1 + \tau x_1, \cdots, \lambda x_n + \tau x_n) \\ &= (\lambda x_1, \cdots, \lambda x_n) + (\tau x_1, \cdots, \tau x_n) \\ &= \lambda \cdot (x_1, \cdots, x_n) + \tau \cdot (x_1, \cdots, x_n). \end{aligned}$$

□

(b) Show that a function $\varphi : V \to V$ is a group homomorphism if and only if it is $\mathbb{F}_p$-linear.

Proof. Condition (1) of being an $\mathbb{F}_p$-linear map is exactly being a homomorphism, so the left hand direction is immediate, and for the righthand direction we need only verify condition (2). Let φ be a homomorphism, and fix$\lambda = \overline{n} \in \mathbb{F}_p$. Notice that:

$$\overline{n} = \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n\text{-times}}.$$

Therefore for any $v \in V$

$$\overline{n}v = (\underbrace{\overline{1} + \cdots + \overline{1}}_{n\text{-times}}) \cdot v = \underbrace{v + \cdots + v}_{n\text{-times}}.$$

Therefore:

$$\varphi(\overline{n}v) = \varphi(\underbrace{v + \cdots + v}_{n\text{-times}}) = \underbrace{\varphi(v) + \cdots + \varphi(v)}_{n\text{-times}} = \overline{n}\varphi(v).$$

Therefore φ is indeed $\mathbb{F}_p$-linear. □

(c) Show that $\operatorname{Aut}(V) \cong GL_n(\mathbb{F}_p)$. (*Hint:* You may cite Proposition 1 from HW5.)

Proof. By part (b), an automorhpism of V is the same as a linear bijection of V. By Proposition 1, these are in one to one correspondance with elements of $GL_n(\mathbb{F}_p)$. This gives a bijection

$$\operatorname{Aut}(V) \to GL_n(\mathbb{F}_p).$$

Furthermore, the group operation on the left is composition of functions, which corresponds to matrix multiplication on the right (again by Proposition 1), so this bijection commutes with the group operations and is therefore a homomorphism and thus an isomorphism. □

(d) Let p be a prime number and G a group of order p^2. What are the possible values for for $|\operatorname{Aut}(G)|$? (Use the classification of groups of order p^2 and HW#5 3(d).)

Proof. Since $|G| = p^2$, we know $G \cong Z_{p^2}$ or else $G \cong Z_p \times Z_p$. We know $\operatorname{Aut}(Z_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$. Notice that $\gcd(x, p^2) = 1$ if and only if $p \not| x$. Therefore

$$(\mathbb{Z}/p^2\mathbb{Z})^\times = \{x = 0, \cdots, p^2 - 1 : \gcd(x, p^2) = 1\} = \mathbb{Z}/p^2\mathbb{Z} \setminus \{0, p, 2p, \cdots, (p-1)p\}.$$

Thus $|(\mathbb{Z}/p^2\mathbb{Z})^\times| = p^2 - p$. On the other hand, if $G \cong Z_p \times Z_p$, then $\operatorname{Aut}(G) \cong GL_2(\mathbb{F}_p)$ by part (c), which we know by HW5#3(d) has size $(p^2-1)(p^2-p)$. Therefore:

$$|\operatorname{Aut}(G)| = \begin{cases} p^2 - p & G \cong Z_{p^2} \\ (p^2-1)(p^2-p) & G \cong Z_p \times Z_p \end{cases}$$

□

6. We can apply part (5) as follows. Let G be a group of order $63 = 3^2 * 7$ and suppose that there is a normal subgroup $P \trianglelefteq G$ of order 9. We will show that G is abelian.

(a) Construct an injective map $G/C_G(P) \to \operatorname{Aut} P$. (*Hint:* Since P consider the action of G on P by conjugation).

Proof. Since P is normal, G acts on P by conjugation, and the action is by automorphisms of P. For $g \in G$ we know the associated permutation of P, σ_g, is bijective, and for any $x, y \in P$ we have:

$$\sigma_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \sigma_g(x)\sigma_g(y)$$

Therefore $g \mapsto \sigma_g$ is a homomorphism $G \to \operatorname{Aut}(P)$. The kernel of the homomorphisms is the the action (HW3#4a), which is

$$\{g \in G : gxg^{-1} = x \text{ for all } x \in P\} = C_G(P).$$

Therefore, the first isomorphism theorem provides the desire injective homomorphism. □

(b) Use 5(d) and Lagrange's theorem to show that $C_G(P) = G$. Conclude that G is abelian. (*Hint:* HW6#2b may be helpful).

Proof. By part (a) $G/C_G(P)$ is isomorphic to a subgroup of $\operatorname{Aut}(P)$, so that Lagrange's theorem tells us that $|G/C_G(P)|$ divides $|\operatorname{Aut}(P)|$. Since $|P| = 9 = 3^2$, 5(d) tells us that the order of $\operatorname{Aut}(P)$ is either $3^3 - 3 = 6$ or $3^4 - 3^3 - 3^2 + 3 = 48$.

Let's enumerate the possible values of $|G/C_G(P)|$. By the classification of groups of order p^2, we know P is abelian, so that $P \leq C_G(P) \leq G$ (HW4#3(f)). Therefore 9 divides $|C_G(P)|$ which in turn divides 63. This says that $|C_G(P)|$ is either 9 or 63.

Next we notice that 9 is not a possibility. Indeed, if $|C_G(P)| = 9$ then $|G/C_G(P)| = |G|/|C_G(P)| = 63/9 = 7$. By the first paragraph, this value needs to divide the order of $\operatorname{Aut}(P)$, which is either 6 or 48. But neither of these numbers are divisible by 7. Therefore $|C_G(P)| = 63$ so that $C_G(P) = G$. As a consequence, P is contained in $Z(G)$.

To conclude, notice that we have deduced that $P \leq Z(G) \leq G$. Arguing as above, this means $|Z(G)|$ is 9 or 63. If it is 63, G is abelian and we win. Assume it is 9. Then $|G/Z(G)| = 7$ so that $G/Z(G) \cong Z_7$ (TH1#4(a)). But by HW6#2(b), this implies that G is abelian as well. □

7. Let's finish by computing the automorphism group of a D_8.

(a) For $n \in \mathbb{Z}$, define a homomorphism $\iota : D_{2n} \to D_{4n}$ on the generators of D_{2n} by sending $\iota(r) = r^2$ and $\iota(s) = s$. Show that ι is injective and its image is a normal subgroup of D_{4n}. We abuse notation by saying $D_{2n} \trianglelefteq D_{4n}$.

Proof. The map ι on a general element $s^i r^j$ for $i = 0, 1$ and $j = 0, \cdots, n-1$ is given by the rule $\iota(s^i r^j) = s^i r^{2j}$. If $s^i r^{2j} = 1$, then $i = 0$. Therefore $r^{2j} = 1$ and, but $0 \leq 2j < 2n$ so that $2j = 0$ and thus $j = 0$. Therefore $s^i r^{2j} = 1$, and injectivity of ι is verified. We identify D_n as the subgroup of D_{4n} given by $s^i r^{2j}$ where the rotation has even exponent. To verify normality we see that $[D_{4n} : D_{2n}] = 4n/2n = 2$ and subgroups of index 2 are always normal. □

(b) Show that $|\operatorname{Aut}(D_8)| \leq 8$. (*Hint*: If $\varphi : D_8 \to D_8$ is an isomorphism, how many options are there for $\varphi(r)$. What about for $\varphi(s)$?)

Proof. Let $\varphi : D_8 \to D_8$. φ is completely determined by its values on the generators, r, and s. We know that $\varphi(r)$ must have order 4, so that it can only be r or r^3. Similarly, $\varphi(s)$ must have order 2, so that it must be one of s, sr, sr^2, sr^3, r^2. But we also know that $\varphi(s)$ cannot be r^2. Indeed, if s and r both map to rotations, the image of φ would be contained in the rotation subgroup, so that φ could not be surjective. This gives 2 options for r and 4 for s, so at most 8 homomorphisms. □

(c) By part (a), D_{16} acts on D_8 by conjugation. Use the associated permutation representation to prove $\operatorname{Aut}(D_8) \cong D_8$. (*Hint:* This last part requires a couple of steps. Rather than have parts (d),(e),(f),..., let's see if you can follow your nose! If you get stuck you can always ask for hints on the discord.)

Proof. The action of D_{16} on D_8 by conjugation has kernel $C_G(D_8)$. Therefore the first isomorphism theorem factors the permutation representation as follows:

$$\begin{tikzcd}
D_{16} \arrow[r] \arrow[d] & \operatorname{Aut} D_8 \\
D_{16}/C_G(D_8) \arrow[ur, hook, "\iota"'] &
\end{tikzcd}$$

Let's compute $C_G(D_8)$. We know that $Z(D_{16}) \leq C_G(D_8)$, and by HW4#4 we know that $Z(D_{16}) = \langle r^4 \rangle$. Furthemore, we know by the same exercise that no other power of r commutes with s, so r^4 is the only rotation in the centralizer. Now fix an arbitrary reflecion sr^i. Then we can compute

$$sr^i(r^2)sr^i = r^{n-2}.$$

Therefore reflection can't centralize D_8. So $C_G(D_8) = \langle r^4 \rangle$. We know that $|D_{16}/r^4| = 16/2 = 8$. Since ι is injective, Lagrange's theorem says 8 divides $|\operatorname{Aut} D_8| \leq 8$. In particular $|\operatorname{Aut} D| = 8$ and so ι is an isomorphism. We finish by computing D_{16}/r^4. We define a map $\pi : D_{16} \to D_8$ by the rule $\pi(s^i r^j) = s^i r^j$. If it is well defined it is certainly a homomorphism. Let $s^i r^j = s^{i'} r^{j'}$ in D_{16}. In particular $s^{i-i'} = r^{j'-j}$, and because $\langle s \rangle \cap \langle r \rangle = 1$, so that they must both be 1 in D_{16}. By HW2#8 this means that $i \equiv i' \mod 2$ and $j \equiv j' \mod 8$, but this imlpies $j \equiv j \mod 4$ so $r^{j-j'} = 1$ in D_8 as well. Therefore $s^i r^j = s^{i'} r^{j'}$ in D_8, and the map is well defined. It is also plainly surjective. Suppose $s^i r^j$ is in the kernel, with $i = 0, 1$ and $j = 0, 1, ..., 7$. Then $i = 0$ and $j \equiv 0 \mod 4$, so $j = 0, 4$. In particular, $\ker \pi = \langle r^4 \rangle$ and thus $D_{16}/r^4 \cong D_8$ by the first isomorphism theorem. Since this is isomorphic to $\operatorname{Aut} D_8$, we win. □