Homework Assignment 8

Due Friday, March 18

1. Cayley's theorem says that if $|G| = n$ then G embeds into S_n (that is, is isomorphic to a subgroup of S_n). One could ask if this n is *sharp*, or if perhaps G can embed in some smaller symmetric group.

(a) Give an example to show that Cayley's theorem isn't always sharp. That is, give a group of order n which embeds into S_d for some $d < n$.

Proof. There are many examples. One we have encountered often is the natural embedding $D_{2n} \hookrightarrow S_n$ for $n \geq 3$, given by considering the action of the dihedral group on the vertices of the n-gone (cf. HW3 Problem 3(a)). Since $|D_{2n}| = 2n$, this beats Cayley's theorem which gives an embedding into the larger S_{2n}

A more extreme (in some sense the most extreme) example is the symmetric group S_n itself. Since $|S_n| = n!$ then Cayley's theorem gives an embedding $S_n \hookrightarrow S_{n!}$, but of course the identity map embeds S_n into itself, which is a much smaller symmetric group. □

Nevertheless, we are about to see that for Q_8 the symmetric group given by Cayley's theorem is the smallest. This shows that there can be no strengthening of Cayley's theorem in general.

(b) Let Q_8 act on a set A with $|A| \leq 7$. Let $a \in A$. Show that the stabilizer of a, $(Q_8)_a \leq Q_8$ must contain the subgroup $\{\pm 1\}$. (*Hint:* It might be helpful to use the orbit stabilizer theorem and the lattice from HW6 Problem 5(d).)

Proof. Let $a \in A$, and denote the stabilizer of a by the subgroup $(Q_8)_a \leq Q_8$. Then recall that the index of the stabilizer of a is Q_8 is the same as the size of the orbit of a $Q_8 \cdot a$ which is a subset of A. That is:

$$|Q_8 : (Q_8)_a| = |Q_8 \cdot a| \leq |A| \leq 7 < 8.$$

The left hand size is $8/|(Q_8)_a|$ by Lagrange's theorem, so that $(Q_8)_a$ cannot be the trivial subgroup of Q_8. But in the lattice from HW6 Problem 5(d), we saw that every nontrivial subgroup of Q_8 contains $\{\pm 1\}$, completing the proof. □

(c) Deduce that the kernel of the action of Q_8 on A contains $\{\pm 1\}$.

Proof. $\{\pm 1\}$ is contained in the stabilizer of every element of A by part (b), and so it acts trivially on all of A. This is precisely what it means to be in the kernel. □

(d) Conclude that Q_8 cannot embed into S_n for $n \leq 7$. That is, show there is no injective homomorphisms $Q_8 \hookrightarrow S_n$ for $n \leq 7$.

Proof. Any homomorphism $\varphi : Q_8 \to S_n$ corresponds (by HW4 Problem 6) to an action of Q_8 on the set $A = \{1, 2, \cdots, n\}$, and the kernel of this action is precisely $\ker \varphi$ (by HW4 Problem 7(c)). Since $|A| \leq 7$, part (c) says that this kernel must contain $\{\pm 1\}$, so φ cannot possibly be injective. □

2. Find all finite 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 $G \cong Z_2$. □

3. Compute all the conjugacy classes for the following groups, and verify that the class equation holds in each case.

   (a) S_3

   Proof. One could use that the conjugacy classes of S_n correspond to cycle types, or do it directly. We will take the second approach. Since $g1g^{-1} = 1$ for all $g \in S_3$, we see that the conjugacy class of 1 is itself. Next we compute $S_3 * (12)$ directly. We know that (12) commutes with itself and 1, so conjugating by either of these elements returns (12) itself. What remains is:

   $$\begin{aligned}(13)(12)(13)^{-1} &= (13)(12)(13) = (23)\\ (23)(12)(23)^{-1} &= (23)(12)(23) = (13)\\ (123)(12)(123)^{-1} &= (123)(12)(132) = (23)\\ (132)(12)(132)^{-1} &= (132)(12)(123) = (13),\end{aligned}$$

   In particular, the conjugacy class of (12) are the two cycles $\{(12), (13), (23)\}$. Next we compute $S_3 * (123)$.

   $$(12)(123)(12)^{-1} = (12)(123)(12) = (132).$$

   Since we know conjugacy classes form a partition, and the rest of the elements of S_3 are spoken for, we know that this conjugacy class can therefore only be the 3-cycles $\{(123), (132)\}$. In particular, we have shown that the 3 conjugacy classes of S_3 are precisely the 1-cycles, the 2-cycles, and the 3-cycles (confirming that they are indeed the cycle types). The class equation then becomes:

   $$6 = |S_3| = |Z(S_3)| + |S_3 * (12)| + |S_3 * (123)| = 1 + 2 + 3,$$

   and gravity exists! □

   (b) Q_8

   Proof. Since $1, -1 \in Z(Q_8)$, their conjugacy classes are $\{1\}$ and $\{-1\}$ respectively. Next we compute the conjugacy class of i. We can do this directy by conjugating it with every other element, but it is more efficient to use the orbit stabilizer theorem to notice that:

   $$|Q_8 * i| = |Q_8 : (Q_8)_i| = |Q_8 : C_{Q_8}(i)|$$

We certainly have that $\langle i\rangle \leq C_{Q_8}(i) \leq Q_8$, so that the centrailzer is either $\langle i\rangle$ or all of Q_8. But since $i \notin Z(Q_8)$ then the centralizer of i can't be everything, so that $C_{Q_8}(i) = \langle i\rangle$ and therefore

$$|Q_8 * i| = |Q_8|/|\langle i\rangle| = 8/4 = 2.$$

We know i is in its own conjugacy class, so we must find the one remaining member. We check that

$$jij^{-1} = ji(-j) = (-k)(-j) = kj = -i.$$

Thus the conjugacy class of i is $\{\pm i\}$. Similar reasoning says the remaining conjugacy classes are $\{\pm j\}$ and $\{\pm k\}$. Therefore the class equation becomes:

$$8 = |Q_8| = |Z(Q_8)| + |Q_8 : C_{Q_8}(i)| + |Q_8 : C_{Q_8}(j)| + |Q_8 : C_{Q_8}(k)| = 2 + 2 + 2 + 2 = 8.$$

□

For the next problem it may be useful to recall the following fact we proved in class.

Theorem 1 (Cauchy's Theorem for Abelian Groups)**.** *Let G be an abelian group of order n. If p is a prime dividing n, then G has a subgroup of order p.*

This will turn out to be true for all groups, so so far we only have it in the abelian case.

4. 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 (HW7#3).

   (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 HW7#3. 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 HW7#3e(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 G has a normal subgroup of order p. In particular, we have extended Cauchy's theorem to nonabelian p-groups! (*Hint:* What did the class equation say about the center of a p-group?)

Proof. The first application of the class equation in we saw in class was that if $|G| = p^d$ for $d > 0$ then $Z(G)$ is not trivial. Let us revisit the proof, the class equation says:

$$\underbrace{|G|}_{\text{divisible by } p} = |Z(G)| + \underbrace{\sum [G : C_G(g_i)]}_{\text{divisible by } p},$$

so that $|Z(G)|$ must be divisible by p (and therefore cannot be 1). $Z(G)$ is also certainly an abelian group, so by Cauchy's theorem for abelian groups (which we do have!) we know it must contain an element of order p. This is an element of G of order p as well. Further, since $x \in Z(G)$ then $\langle x \rangle \leq Z(G)$ so that $\langle x \rangle \trianglelefteq G$ by HW6 Problem 3(a). □

(c) 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. (Use parts (a) and (b) to proceed by induction).

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'd like to produce a subgroup of order p^a for $a \geq 2$ (for $a = 1$ we are done by part (b)). Consider the normal subgroup $\langle x \rangle \trianglelefteq G$ produced in part (b), so we can 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 HW7#3(b)). 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. □

5. Here we classify all abelian groups of order pq for $p \neq q$ prime.

(a) Let G be a group of finite order and suppose that $x, y \in G$ are commuting elements, i.e., that $xy = yx$. Show that that $|xy|$ divides the least common multiple of x and y.

Proof. Let l be the least common multiple of $|x|$ and $|y|$. Then $x^l = y^l = 1$, so that $(xy)^l = x^l y^l = 1$ Therefore (applying HW2 Problem 8) we see that $|xy|$ divides l. □

(b) Let G be an abelian group of order pq for primes $p \neq q$. Show that $G \cong Z_{pq}$.

Proof. By Cauchy's theorem, we can find $x, y \in G$ with $|x| = p$ and $|y| = q$. Since x and y commute, part (a) shows that $|xy|$ divides pq, so it is one of $1, p, q, pq$. If it is 1 then $y = x^{-1}$ contradiction that their orders are not the same. If it is p then $(xy)^p = y^p = 1$ so that q divides p, which it does not. We can similarly rule out q. Thus $|xy| = pq$ so that $G = \langle xy \rangle \cong Z_{pq}$. □

(c) Classify all groups of order 6 up to isomorphism.

Proof. Let G be a group of order 6. If G is *not* abelian, then by HW6 Problem 4 we know it is isomorphic to S_3. On the other hand, noticing that $6 = 2 * 3$ is a product of distinct primes, we may conclude by part (b) that if G *is* abelian then it is isomorphic to Z_6. So the only groups of order 6 (up to isomorphism) are S_3 and Z_6. □

6. Let V be an abelian group of order p^n for some prime p and $n > 0$. Suppose that every element of V has order $\leq p$. Show by induction on n that:

$$V \cong \underbrace{Z_p \times Z_p \times \cdots Z_p}_{n \text{ times}}.$$

Proof. We proceed by induction on n. The base case where $n = 1$ then V has prime order so it must be cyclic of order p. For the general case, $1 \neq x \in V$. Then $|x| = p$ and $\langle x \rangle \leq V$ is normal since V is abelian. Then $V' = V/\langle x \rangle$ is an elementary abelian group of order p^{n-1}. Therefore by induction:

$$V' \cong \underbrace{Z_p \times Z_p \times \cdots \times Z_p}_{n-1 \text{ times}}$$

Let $e_i = (1, \cdots, 1, g, 1, \cdots, 1)$ be the generator of the ith factor of V' (that is $g \in Z_p$ is a generator placed in the ith position of the tuple). Notice that the e_i form a set of generators for V'. Let $\pi : V \to V'$ be the natural projection, and for each $i = 1, \cdots, n-1$ fix some element of the fiber $y_i \in \pi^{-1}(e_i)$. We now define an isomorphism:

$$\varphi : \underbrace{Z_p \times Z_p \times \cdots \times Z_p}_{n \text{ times}} \to V$$

according to the rule: $\varphi(e_i) = y_i$ for $i \leq n-1$, and $\varphi(e_n) = x$ (since the e_i generate the left hand side, this defines a homomorphism). We now show φ is injective and surjective.

To observe surjectivity, fix some $v \in V$. Then

$$\pi(v) = (g^{r_1}, \cdots, g^{r_{n-1}}).$$

Thus $v \cdot y_1^{-r_1} \ldots y_{n-1}^{-r_{n-1}} \in \ker \pi = \langle x \rangle$, so it is equal to a power of x, say x^{r_n}. In particular:

$$v = y_1^{r_1} \cdots y_{n-1}^{r_{n-1}} \cdot x^{r_n} = \varphi(g^{r_1}, \cdots, g^{r_n}).$$

Since the two groups have the same order, injectivity follows immediatley and we are done. □

We will call such a V the *elementary abelian group of order p^n*. We will see in the following question that these are the same as finite dimensional $\mathbb{F}_p$ vector spaces!

7. Let V be an elementary abelian group of order p^n. And identify it with

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

For $\lambda \in \mathbb{F}_p$ and $v = (v_1, \cdots, v_n) \in V$, we can let:

$$\lambda v = (\lambda v_1, \cdots, \lambda v_n).$$

(a) Explain why the scalar multiplication giving above makes V into an $\mathbb{F}_p$-vector space.

Proof. It is a basic result of linear algebra that for any field k, the set k^n with scalar multiplication given coordinatewise is a vector space (in fact, it is the model example of a vector space). As $V = \mathbb{F}_p^n$, this gives the result. *I don't require this for credit*, but for completeness will include the explicit computations for the 5 axioms of a vector space:

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

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

Using associativity of multiplication mod p.

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

Using 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 homomorphism if and only if it is a linear map of vector spaces.

Proof. Recall that $\varphi : V \to V$ is linear if

(1) $\varphi(v + w) = \varphi(v) + \varphi(w)$ for all vectors $v, w \in V$.

(2) $\varphi(\lambda v) = \lambda\varphi(v)$ for every scalar $\lambda \in \mathbb{F}_p$ and vector $v \in V$.

Condition (1) of being an $\mathbb{F}_p$-linear map is exactly being a homomorphism, so the backward direction is immediate, and for the forward 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) Using Proposition 1 from HW6, identify the set of isomorphisms from V to itself with a group we have already seen.

Proof. By part (b) we know the set of isomorphisms from V to itself is exactly the same as the set of linear bijections from V to itself. By Proposition 1 in HW6, this is precisely the group $GL_n(\mathbb{F}_p)$. □