Problem Set 2 Solutions

Math 120

1.7.8 (a) For any set $\{a_1, ..., a_k\} \in B$, and any permutations $\sigma, \tau \in S_A$ we have that $\sigma \cdot (\tau \cdot \{a_1, ..., a_k\}) = \sigma \cdot \{\tau(a_1), ..., \tau(a_k)\} = \{\sigma\tau(a_1), ..., \sigma\tau(a_k)\} = (\sigma\tau) \cdot \{a_1, ..., a_k\}$. Also, $1 \cdot \{a_1, ..., a_k\} = \{1(a_1), ..., 1(a_k)\} = \{a_1, ..., a_k\}$, so the given map $S_A \times B \to B$ is a group action.

(b) Merely applying the definition of this action gives us

$$
\begin{gathered}
(1\ 2) \cdot \{1,2\} = \{1,2\} \\
(1\ 2) \cdot \{1,3\} = \{2,3\} \\
(1\ 2) \cdot \{1,4\} = \{2,4\} \\
(1\ 2) \cdot \{2,3\} = \{1,3\} \\
(1\ 2) \cdot \{2,4\} = \{1,4\} \\
(1\ 2) \cdot \{3,4\} = \{3,4\}
\end{gathered}
$$

$$
\begin{gathered}
(1\ 2\ 3) \cdot \{1,2\} = \{2,3\} \\
(1\ 2\ 3) \cdot \{1,3\} = \{1,2\} \\
(1\ 2\ 3) \cdot \{1,4\} = \{2,4\} \\
(1\ 2\ 3) \cdot \{2,3\} = \{1,3\} \\
(1\ 2\ 3) \cdot \{2,4\} = \{3,4\} \\
(1\ 2\ 3) \cdot \{3,4\} = \{1,4\}
\end{gathered}
$$

1.7.16 Let $g, h \in G$. Then for any $a \in G$ we have $g \cdot (h \cdot a) = g \cdot (hah^{-1}) = ghah^{-1}g^{-1} = (gh)a(gh)^{-1} = (gh) \cdot a$. Also, clearly conjgating by the identity fixes any element of G, so the given maps *do* define a left group action of G on itself.

1.7.19 First note that the given map $H \to \mathcal{O}$ defined by $h \mapsto hx$ is surjective by definition, and it is injective because $h_1x = h_2x \Rightarrow h_1xx^{-1} = h_2xx^{-1} \Rightarrow h_1 = h_2$. The map is thus a bijection. Hence, given any $x \in G$, the cardinality of the orbit of x under the action of H is precisely $|H|$. Since the previous exercise implies that the orbits under the action of H partition G, and each of these orbits have the same cardinality, we conclude that $|H|$ divides $|G|$.

1.7.23 Any rotation through an angle of 180° about an axis perpendicular to a face of the cube fixes pairs of opposite faces, so the action is not faithful. One easily checks that the the subgroup of the group of rigid motions generated by such rotations is the kernel of this action.

2.1.5 By Lagrange's theorem (problem 1.7.19 above), if H is a subgroup of G, then the order of H must divide the order of G. But $n - 1$ does not divide n when $n > 2$, so G has no such subgroup.

2.1.12 (a) The subset $B = \{a^n \mid a \in A\}$ is clearly nonempty (it contains the identity), and for any $a, b \in A$ we have $a^n(b^n)^{-1} = a^n b^{-n} = (ab^{-1})^n \in B$, so B is a subgroup.

(b) Again the subset $B = \{a \in A \mid a^n = 1\}$ is nonempty since it contains the identity, and we have for any $a, b \in B$ that $(ab^{-1})^n = a^n(b^n)^{-1} = 1 \cdot 1 = 1$ since A is abelian. B is thus a subgroup.

2.1.14 Given the usual presentation for the dihedral group $D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle$, notice that all elements of the form sr^k have order 2. But $(sr)(sr^2)^{-1} = srr^{-2}s = sr^{-1}s = r$ which has order $n \geq 3$ and is thus not in the subset $\{x \in D_{2n} \mid x^2 = 1\}$. This proves that $\{x \in D_{2n} \mid x^2 = 1\}$ is not a subgroup.

2.2.4 The centralizer of every element of S_3 is a subgroup of S_3, so by Lagrange's theorem, it must have order 1, 2, 3, or 6. Of course the centralizer of the identity element is all of S_3, but notice that, if a, b, and c are distinct, we have $(a\ b)(a\ b\ c) = (b\ c)$ while $(a\ b\ c)(a\ b) = (a\ c)$. Hence since all non-identity elements of S_3 have the form $(a\ b)$ or $(a\ b\ c)$, we conclude the the centralizer of any non-identity element of S_3 is not all of S_3. But certainly the centralizer of any element contains the cyclic subgroup generated by that element, so this observation and Lagrange's theorem imply that the centralizer of any nontrivial element of S_3 is precisely the cyclic subgroup generated by that element. The observations above also imply that the center of S_3 is trivial.

Again, the centralizer of the identity in D_8 is all of D_8. The centralizer of r contains $\langle r \rangle$, so it must have order 4 or 8. But r does not commute with s, so the centralizer is not all of D_8 and is therefore the cyclic group $\langle r \rangle$. A nearly identical argument shows that this group is also the centralizer of r^3. r^2, as one may check, commutes with all elements of D_8 so its centralizer is the entire group. Now for an element of the form sr^i, for any $0 \leq i \leq 3$, one easily checks that it does not commute with r, but its centralizer contains 1, sr^i, r^2, and $sr^i \cdot r^2 = sr^{i+2}$. By Lagrange's theorem, this must be the entire centralizer for this element. We have thus computed the centralizer of each element in D_8, and since the center of the group consists exactly of those elements whose center is the entire group, we conclude that the center of D_8 is cyclic and generated by r^2.

The centralizers are a bit easier to calculate in Q_8. Clearly 1 and -1 have centralizer equal to the entire group. On the other hand, the centralizer of i contains the cyclic group of order 4 generated by i, but i does not commute with j, so the centralizer of i can not be the entire group. Lagrange's theorem then guarantees that $\langle i \rangle$ is the entire centralizer. By similar reasoning, the centralizer of each remaining element of Q_8 is given by the cyclic group of order 4 generated by that element. In particular, the center of Q_8 is $\langle -1 \rangle$.

2.2.5 (a) The centralizer of A certainly is contained in the centralizer of the element (1 2 3), which we showed above to be $\langle (1\ 2\ 3) \rangle$. Since each element in this group clearly commutes with (1 3 2), the centralizer of A must contain it and so $C_G(A) = A$. Also, we always have $A \subset N_G(A)$, so by Lagrange's theorem we need only find one element outside of A which normalizes A to show that $N_G(A) = G$. In particular, $(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (1\ 3\ 2)$ and $(1\ 2)(1\ 3\ 2)(1\ 2)^{-1} = (1\ 2\ 3)$, proving the claim.

((b) The element r does not lie in the centralizer of A since it does not commute with s. Hence since one easily checks that $A \subset C_G(A)$, we must have $A = C_G(A)$. Similarly it is easy to see that $A \subset N_G(A)$, so we need only find one element outside of A which normalizes A. r will do:

$$\begin{gathered} r1r^{-1} = 1 \\ rsr^{-1} = r^2 \\ rr^2r^{-1} = r^2 \\ rsr^2r^{-1} = s \end{gathered}$$

which proves $r \in N_G(A) \Rightarrow G = N_G(A)$.

(c) Clearly $A \subset C_G(A)$, so since s does not commute with r, we have from Lagrange's theorem that $A = C_G(A)$. The element $s \notin A$ obviously normalizes A, so again we have $N_G(A) = G$.

2.2.12 (a) This is a straightforward computation:

$$\sigma \cdot p = 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^23x_2^6x_3x_4^3$$

$$\tau \cdot (\sigma \cdot p = (\tau \circ \sigma) \cdot p = 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^23x_3^6x_4^3$$

$$(\sigma \circ \tau) \cdot p = 12x_1x_3^5x_4^7 - 18x_2x_4^3 + 11x_1^23x_2^3x_3^6x_4$$

(b) That $\sigma \cdot (\tau \cdot p) = (\sigma\tau) \cdot p$ and $1 \cdot p = p$ follows directly from the definition of the action, and so this defines a left group action.

(c) The elements of S_4 which stabilize x_4 are precisely those which do not contain a "4" in their cycle decomposition. The map from this subgroup to S_3 given by the homomorphism $(a\ b) \mapsto (a\ b)$ and $(a\ b\ c) \mapsto (a\ b\ c)$ is the obvious isomorphism.

(d) Any element of S_4 which stabilizes x_1+x_2 must either fix both 1 and 2 or send $1 \mapsto 2$ and $2 \mapsto 1$. The former elements are those which do not contain a "1" or a "2" in their cycle decompositions, i.e. the identity element and (3 4). The latter are those which whose cycle decomposition contains the factor (1 2), i.e. the elements (1 2) and (1 2)(3 4). Therefore {1, (1 2), (3 4), (1 2)(3 4)} are all elements which stabilize $x_1 + x_2$. Since this set is easily checked to be an abelian subgroup of S_4, the claim is proved.

(e) Notice that the stabilizer of $x_1x_2 + x_3x_4$ contains all of the elements listed in part (d), and it also contains the cyclic group generated by the cycle (1 3 2 4). Now the group generated by (1 2) and (1 3 2 4) has order 8 ($\langle$(1 2),(1 3 2 4)$\rangle$ = {1, (1 2), (3 4), (1 2)(3 4), (1 3 2 4), (1 4 2 3), (1 4)(2 3), (1 3)(2 4)}), so by Lagrange's theorem the stabilizer is this subgroup or the entire group S_4. Since, for example, (2 3) does not stabilize $x_1x_2 + x_3x_4$, this subgroup is the entire stabilizer. Noting that (1 3 2 4)(1 2) = (1 4)(2 3) = (1 2)(1 3 2 4)$^{-1}$, we may define a homomorphism $D_8 \to \langle$(1 2),(1 3 2 4)$\rangle$ by sending $s \mapsto$ (1 2) and $r \mapsto$ (1 3 2 4). As this map is easily checked to be surjective, since the groups have the same order the map must be an isomorphism.

(f) One verifies directly that the permutations listed in part (e) stabilize the element $(x_1+x_2)(x_3+x_4)$, so again by Lagrange's theorem we conclude that the stabilizer subgroup is either the group

in (e) above or all of S_4. Since, again, (2 3) does not stabilize $(x_1 + x_2)(x_3 + x_4)$, we conclude that the group lised in part (e) is precisely the stabilizer of $(x_1 + x_2)(x_3 + x_4)$, proving the claim.

2.3.10 It is straightforward to compute all elements of $\langle\overline{30}\rangle$ by taking all multiples of 30 and reducing modulo 54, and Proposition 5 in chapter 2 of Dummit and Foote allows us to quickly compute the order of each of these elements:

$$\overline{0} = 0 \cdot \overline{30} \text{ has order } 1$$

$$\overline{30} = 1 \cdot \overline{30} \text{ has order } 54/(54,30) = 9$$

$$\overline{6} = 2 \cdot \overline{30} \text{ has order } 54/(54,6) = 9$$

$$\overline{36} = 3 \cdot \overline{30} \text{ has order } 54/(54,36) = 3$$

$$\overline{12} = 4 \cdot \overline{30} \text{ has order } 54/(54,12) = 9$$

$$\overline{42} = 5 \cdot \overline{30} \text{ has order } 54/(54,42) = 9$$

$$\overline{18} = 6 \cdot \overline{30} \text{ has order } 54/(54,18) = 3$$

$$\overline{48} = 7 \cdot \overline{30} \text{ has order } 54/(54,48) = 9$$

$$\overline{24} = 8 \cdot \overline{30} \text{ has order } 54/(54,24) = 9$$

2.3.16 Suppose that N is the least common multiple of n and m, say $kn = N = pm$. Then since x and y commute, $(xy)^N = x^N y^N = (x^n)^k (y^m)^p = 1^k 1^p = 1$. Proposition 3 of chapter 2 in Dummit and Foote then implies that the order of xy divides N. This certainly needs not be true if x and y do not commute. For example, in S_4 consider the elements (1 2) and (2 3 4). They have orders 2 and 3 respectively, while (1 2)(2 3 4) = (1 2 3 4) has order 4. Next consider $r^2 \in D_8$. Clearly r^2 commutes with itself, and it has order 2, but $r^2 r^2 = 1 \neq 2$.

2.3.21 We have from the binomial theorem that

$$(1+p)^{p^{n-1}} \equiv 1 + \tbinom{p^{n-1}}{1} p + \cdots + \tbinom{p^{n-1}}{n-1} p^{n-1} (\text{mod } p^n)$$

Notice that the coefficient of p above is p^{n-1}, while for $1 \leq k \leq p$ the quantity $(p^{n-1} - k)!k!$ has the same number of p factors. hence every term after the first in the expression above has at least n factors of p, proving that $(1+p)^{p^{n-1}} \equiv 1 (\text{mod } p^n)$ (in particular, since the first term has exactly n factors of p and p is odd, the second term must have $n+1$ factors of p, and so on). Similarly, the binomial theorem gives us

$$(1+p)^{p^{n-2}} \equiv 1 + \tbinom{p^{n-2}}{1} p + \cdots + \tbinom{p^{n-2}}{n-1} p^{n-2} (\text{mod } p^n)$$

and the coefficient of p in the second term is p^{n-2}, we conclude by reasoning similar to that above that all terms in the expression above but the first two have at least n factors of p, so we have that $(1+p)^{p^{n-2}} \equiv (1+p^{n-1}) (\text{mod } p^n)$. Hence since $1+p$ has order dividing p^n in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ by Lagrange's theorem, we conclude that the order of $1+p$ must therefore be p^{n-1}.

2.3.25 Let y be a generator of the cyclic group G. Since k is relatively prime to n, Proposition 5 in chapter 2 of Dummit and Foote implies that the order of y^k is n, which means y^k is a generator of G. Since G is being mapped homomorphically into itself, its image must therefore be all of G. Now let G be any finite group of order n. Let $\varphi : G \to G$ be the given map $g \mapsto g^k$ where k is relatively prime to n. For any $g \in G$, the cyclic group $\langle g \rangle$ is a subgroup of G, so by Lagrange's theorem its order divides n. Say $|g| = m$. Then m is also relatively prime to k, so by the first part of this problem, $\varphi|_{\langle g \rangle}$ is surjective, i.e. g is in the image of φ. But this obviously implies that φ is surjective, so we are done.