Problem Set 1 Solutions

Math 120

1.1.24 We prove the assertion for positive n first by induction. It is obviously true in the case $n = 1$, so now suppose $(ab)^k = a^k b^k$ for all $k < n$. We then have $(ab)^n = ab(ab)^{n-1} = aba^{n-1}b^{n-1}$ by the inductive hypothesis. But it is easy to see (by induction, for example) that if b commutes with a, then it also commutes with a^k for any positive k. Hence $aba^{n-1}b^{n-1} = aa^{n-1}bb^{n-1} = a^n b^n$, proving the claim when n is positive.

Next note that by the observation above that b commutes with a^k for all positive k, we have that $b^k a^k = b^{k-1}a^k b = b^{k-2}a^k b^2 = ... = a^k b^k$. Hence for any positive n, we have $1 = a^{-n}b^{-n}b^n a^n = a^{-n}b^{-n}a^n b^n = a^{-n}b^{-n}(ab)^n$ where we have used the fact that n is positive and our result above. Multiplying both sides of this equation by $(ab)^{-n}$ proves the assertion for all negative integers $-n$.

1.1.25 Let a and b be two arbitrary elements of a group G with the given property. Then $a^2b^2 = 1 \cdot 1 = 1$. However, we also have $1 = (ab)^2 = abab$, and so $a^2b^2 = abab$. Multiplying both sides of this equation by a^{-1} on the left and then by b^{-1} on the right gives $ab = ba$, and so a and b commute. Since these elements were chosen arbitrarily, we conclude that all pairs of elements in G commute with each other, so G is thus abelian.

1.1.31 As suggested in the hint, we define $t(G) = \{g \in G \mid g \neq g^{-1}\}$. Now if $g \in t(G)$, then we must also have $g^{-1} \in t(G)$, for otherwise we would have $g^{-1} = (g^{-1})^{-1} = g$, contradicting the fact that $g \in t(G)$. Since g and g^{-1} are distinct by assumption, this implies $t(G)$ can be written as a disjoint union of sets of the form $\{g, g^{-1}\}$, so it therefore has an even number of elements. Now if $x \in G$ has order two, this means that x is not the identity and $x^2 = 1 \Rightarrow x = x^{-1}$. Hence either G has an element of order two or $G - t(G)$ consists of a single element (namely the identity). But the latter is impossible since then $G = t(G) \cup \{1\}$ has an odd number of elements, contrary to assumption. We thus conclude that $G - t(G)$ contains some non-identity element which has order two.

1.2.13 The icosahedron I has 20 faces, each of which is an equilateral triangle. Since the group of rigid motions G does not include reflections, the orientation of the vertices of each face is preserved under the action of G. Namely, if A, B, and C are the vertices of some face T of I, listed in the order met as one travels clockwise along the edges of T starting at A, and if $g(A)$ is the image of the vertex A under the action of $g \in G$, then if one traveled clockwise along the edges of $g(T)$ (the image of the face T under the action of g) starting at $g(A)$, the next vertex met would always be $g(B)$ followed by $g(C)$. Now because of this orientation preservation, any rigid motion of the icosahedron is uniquely determined by where it sends the vertices A, B, and C. Since $g(A)$, $g(B)$, and $g(C)$ must be the vertices of some triangular face with clockwise-ordered vertices A', B', and C', if g maps the triangular face with vertices (A, B, C) to the face with vertices (A', B', C'), g is thus uniquely determined by $g(A)$, and there are three possibilities. As there are twenty faces of I, and three possible vertices of each face as the image of A under g, we conclude that there are a total of $20 \cdot 3 = 60$ elements in G.

1.3.2 Finding the cycle decompositions of σ and τ is just a matter of carefully following the arrows: $\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$, $\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$. Finding the cycled decompositions of the other permutations is not much harder. For example, σ sends 1 to 13, and 13 to 5, so σ^2 sends 1 to 5. Similarly, since σ sends 1 to 13, τ sends 13 to 4 and 4 to 2, we conclude that the permutation $\tau^2\sigma$ sends 1 to 2. Continuing this tabulation procedure gives:

$$\sigma^2 = (1\ 5)(13\ 10)(3\ 8\ 15)(4\ 11\ 12)(14\ 7\ 9)$$
$$\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14)$$
$$\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$$
$$\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$$

1.3.18 By the result of exercise 15 in this section (which is straightforward to prove), the order of an element of S_n depends only on the lengths of the cycles in its cycle decomposition. Of course, any n-cycle has order n, so there are elements of S_5 with orders 1, 2, 3, 4, and 5 (for example the cycle $(1\ 2\ ...\ r)$ has order r). Now given an element of S_5 which is not a cycle, we see from its cycle decomposition that it must be the product of two disjoint cycles, one having length 2 and the other having length 2 or 3. This is because the cycles in an element's cycle decomposition are always disjoint, so the sum of the lengths of these cycles must add up to 5 or less. Since 1-cycles are omitted, the question of what type of cycle decomposition a non-cycle in S_5 can have is reduced to the question of how many ways we can write the integers less than 5 as a sum of integers greater than 1. $3 + 2$ is the only possibility for 5, and $2 + 2$ is the only possibility for 4, and there are no possibilities for 3, 2, or 1. Now by exercise 15, an element which is the product of two 2-cycles, such as $(1\ 2)(3\ 4)$, has order 2, while an element which is the product of a 2-cycle and a 3-cycle, such as $(1\ 2)(3\ 4\ 5)$ has order 6. We have thus computed every possible order of elements of S_5.

1.5.1 Clearly the elements 1 and -1 have orders 1 and 2 respectively. Now consider the element i. We have

$$i^2 = -1$$
$$i^3 = i^2 i = -1 \cdot i = -i$$
$$i^4 = (-1)^2 = 1$$

so we thus conclude that the order of i is 4. Similarly, we have

$$(-i)^2 = -1$$
$$(-i)^3 = (-i)^2(-i) = i$$
$$(-i)^4 = (-i)^3(-i) = i(-i) = 1$$

and so $-i$ also has order 4. A nearly identical calculation shows that j, $-j$, k, and $-k$ all have order 4 as well, and this accounts for the orders of each element in Q_8.

1.6.5 By definition, an isomorphism between groups is a bijection of sets, but from elementary set theory we know that there is no bijection between the countable set $\mathbb{Q}$ and the uncountable set $\mathbb{R}$. There is thus no isomorphism between these additive groups.

1.6.6 We argue by contradiction. Suppose that we had an isomorphism of additive groups $\varphi : \mathbb{Z} \to \mathbb{Q}$. Then φ is injective, so $\varphi(1) \neq 0$. Since φ is also surjective, there is some $n \in \mathbb{Z}$ such that $\varphi(n) = \varphi(1)/2$ so that $\varphi(n) + \varphi(n) = \varphi(2n) = \varphi(1)$, where the first equality follows from the fact that φ is a homomorphism. φ is

injective, so this implies $2n = 1$ which clearly has no integer solutions. This contradiction proves that there is no isomorphism $\mathbb{Z} \to \mathbb{Q}$, proving the assertion.

1.6.17 Let φ denote the map from G to itself by $g \mapsto g^{-1}$. First suppose φ is a homomorphism. Then given any $a, b \in G$ we have $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1}$ while $\varphi(a)\varphi(b) = a^{-1}b^{-1}$. Hence $b^{-1}a^{-1} = a^{-1}b^{-1}$, so multiplying both sides of this equation by ab on the right followed by ba on the left yields $ba = ab$. Since a and b were chosen arbitrarily, we conclude that G is abelian.

Now suppose that G is abelian. We then have that $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$ proving that φ is a homomorphism, so the claim follows.

1.6.24 Since x and y generate G and they both have order 2, every element of G must have one of the following forms: $xyxy\cdots x$, $xyxy\cdots y$, $yxyx\cdots x$, or $yxyx\cdots y$. We claim that, in fact, every element of G can be written as $x^{\epsilon}(xy)^k$ where $\epsilon = 0$ or 1 and $0 \leq k \leq n-1$. First note that $(xy)^{-1}x = y = x(xy)$ and so we easily see by induction that $x(xy)^k = (xy)^{-k}x$. We thus deduce that $y(xy)^k = x(xy)(xy)^k = x(xy)^{k+1}$ and $(xy)^k y = (xy)^k x(xy) = x(xy)^{-k}(xy) = x(xy)^{-k+1}$. Hence the first possible form of an element of G that we listed may be written $(xy)^k x = x(xy)^{-k}$. The second form we listed can be written as $(xy)^k$. The third form we listed can be written as $y(xy)^k x = yx(xy)^{-k} = (xy)^{-1}(xy)^{-k} = (xy)^{-1-k}$, while the fourth and final form we listed above can be written as $y(xy)^k = x(xy)(xy)^k = x(xy)^{k+1}$. Since x has order 2 and xy has order n, our preliminary claim follows. Note too that such a representation of an element of G is unique since $x^{\epsilon_1}(xy)^{k_1} = x^{\epsilon_2}(xy)^{k_2} \Rightarrow x^{\epsilon_2-\epsilon_1}(xy)^{k_2-k_1} = 1$. This implies $\epsilon_2 - \epsilon_1 = 0 \pmod 2$ and $k_2 - k_1 = 0 \pmod n$ since no nonzero power of xy is equal to x.

Now define a homomorphism $\varphi : D_{2n} \to G$ by $\varphi(s) = x$ and $\varphi(r) = xy$ (this is possible since $x^2 = (xy)^n = 1$ and $x(xy) = (xy)^{-1}x$). By the uniqueness of the representation for each element of G described above, we conclude that $|G| = 2n$. Hence, since φ is easily seen to be surjective (as $\varphi(s^{\epsilon}r^k) = x^{\epsilon}(xy)^k$), we conclude that the map is injective since the two groups have the same order. φ is thus a bijective homomorphism, and thus an isomorphism, proving the assertion.