Solutions to select homework problems

September 21, 2018

1. **HW II - Q1. 1.1 v(b):** The set $M_n(k\mathbb{Z})$ is defined by

$$M_n(k\mathbb{Z}) = \{(a_{ij})_{n\times n} : a_{ij} \in k\mathbb{Z}\} = \{kA : A \in M_n(\mathbb{Z})\}.$$

Let $A, B \in M_n(k\mathbb{Z})$. Then $A = kA'$ and $B = kB'$, where $A', B' \in M_n(\mathbb{Z})$. Consequently, we have

$$A - B = kA' - kB' = k(A' - B').$$

As $M_n(\mathbb{Z})$ is a group, we have $A' - B' \in M_n(\mathbb{Z})$, which would imply that $k(A' - B') \in M_n(k\mathbb{Z})$, and so $A - B \in M_n(k\mathbb{Z})$. Therefore, by the subgroup criterion, the assertion follows.

2. **HW II - Q3. 1.3 (ii)(c):** By definition, D_{2n}, for $n \geq 3$, is the group (of order $2n$) comprising the symmetries of a regular n-gon P_n. We know that the rotation r of P_n about its center by $2\pi/n$ generates a cyclic subgroup $\langle r\rangle$ of order n, which contains every other rotational symmetry in D_{2n}. Let $V = \{v_0, \ldots, v_{n-1}\}$ denote the vertices of P_n appearing in counter-clockwise order. Note that the rotation r^k induces a permutation of V that maps

$$v_i \mapsto v_j, \text{ where } j = i + k \pmod{n}, \text{ for } 0 \leq k \leq n-1. \tag{1}$$

Consequently,

No nontrivial rotation can fix any vertex in V. (*)

Now let s be a reflection in D_{2n}. Then s can be of 3 types:

(a) A reflection across a diagonal: This fixes two vertices (i.e. the end points of the diagonal) and swaps the remaining $n-2$ vertices of P_n in pairs.

(b) A reflection across a bisector (joining the midpoints of opposite sides): This swaps all vertices of P_n in pairs.

(c) A reflection across an altitude (from a vertex to the opposite side): This fixes one vertex and and swaps the remaining $n-1$ vertices of P_n in pairs.

If n is even, then s can only be of types (a) or (b), and so by (*), it follows that s cannot be equal to r^k for any k. Moreover, if n is odd, then s has to be a reflection of type (c). This means that there exists a pair v_i, v_{i+1} of adjacent vertices that s swaps (why?). Suppose that $s = r^k$, for some k. Then by (1), we have that $k = n-1$, which would imply that $o(r^k) = n > 2$, which is impossible as $o(s) = 2$. Hence, $s \neq r^k$, for any k, and in conclusion we have that:

$$\text{A reflection can never be realized as a rotation and vice versa.} \qquad (2)$$

Suppose that $sr^j = r^k$, for some $j \neq k$. Then $s = r^{k-j}$, which clearly contradicts (2). Hence, every element of type sr^k (or $r^k s$) has to be reflection. Moreover, if $sr^j = sr^k$, for some $j \neq k$, then $r^{j-k} = 1$, which is impossible, as $o(r) = n$. Therefore, $sr^j \neq sr^k$, when $j \neq k$, and therefore, we have that $D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$.

It remains to show that $sr^k = r^{n-k}s$. It suffices to show that $(s \circ r^k)(v_i) = (r^{n-k} \circ s)(v_i)$, for each $v_i \in V$ (why?). Suppose that s is a reflection about a line that passes through some vertex v_i (i.e a reflection of type (a) or (c)). Then for $j > i$, we have

$$s(v_j) = v_{2i-j \pmod n},$$

which would imply that

$$s(r^k(v_i)) = s(v_{i+k}) = v_{i-k} = r^{n-k}(v_i) = r^{n-k}(s(v_i)),$$

where all the indices are taken modulo n. Now consider v_j, for $j > i$. Then we see that

$$s(r^k(v_j)) = s(v_{j+k}) = v_{2i-j-k} = r^{n-k}(v_{2i-j}) = r^{n-k}(s(v_j)),$$

where the indices are taken modulo n. A similar argument works for the case when $j < i$, and for the case when s is reflection of type (b). (Check!) From these observations, the assertion follows.

3. **HW II - Q3. 1.3 (ii)(d):** We know that each symmetry of $\mathbb{R}^2$ is a finite composition of rotations, translations, and reflections. For $\theta \in \mathbb{R}$, let $f_{\theta,x}$ denote a rotation of $\mathbb{R}^2$ by θ radians about a point $x \in \mathbb{R}^2$. Note that any finite composition of a symmetry of type $f_{\theta,x}$ with translations and reflections yields a symmetry that that has the same magnitude ($|\theta|$) of rotation as $f_{\theta,x}$.

   Now, let us suppose that the group of symmetries of $\mathbb{R}^2$ is generated by a finite set of symmetries S. Then S can contain only finitely many rotations, say $f_{\theta_1,x_1}, \ldots, f_{\theta_n,x_n}$. Now consider any rotation $f_{\theta,x}$, where $\theta \notin \{2k\pi \pm \theta_1, \ldots, 2k\pi \pm \theta_n : k \in \mathbb{Z}\}$. Then by the observations made above, it follows that $f_{\theta,x}$ cannot be written as a finite composition of elements in S. Hence, the group of symmetries of $\mathbb{R}^2$ is not finitely generated.

4. **HW II - Q4:** Let G be a nontrivial group. Then there exists $g \in G$ such that $g \neq 1$. Consider the subgroup $H = \langle g \rangle$ generated by g. Since $g \in G$, it is clear that $H \neq \{1\}$, and as H is generated by a single element, it is cyclic. Hence, the assertion follows. (Note that this argument works both for the case when G is finite and infinite.)

5. **HW II - Q5:** Let m, n be positive integers such that $m < n$. If $D_{2m} < D_{2n}$, then by Lagrange's Theorem, we have that $m \mid n$. So we assume that $m \mid n$, and consider the subgroup H of D_{2n} generated by $\{r^{n/m}, s\}$. Then H will contain precisely m rotations, namely $\{1, r^{n/m}, r^{2n/m}, \ldots, r^{(m-1)n/m}\}$. Moreover, we see that

   $$r^{kn/m}s = sr^{n-(kn/m)} = sr^{(m-k)n/m}.$$

   Consequently, we have that

   $$H = \{1, r^{n/m}, \ldots, r^{(m-1)n/m}, s, sr^{n/m}, \ldots, sr^{(m-1)n/m}\}.$$

   The map

   $$\varphi : D_{2m} = \langle r', s' \rangle \to H : r' \mapsto r^{n/m} \text{ and } s' \mapsto s$$

   extends to monomorphism between the two groups defined by

   $$\varphi((s')^j (r')^i) = s^j r^{in/m}, \text{ for } j = 0, 1 \text{ and } 0 \leq i \leq m-1.$$

   (Verify the claim above!) Therefore, as $\operatorname{Im}\varphi \cong D_{2m}$ and $\operatorname{Im}\varphi < D_{2n}$, an isomorphic copy of D_{2m} lies inside D_{2n}. (This is often written as $D_{2m} \hookrightarrow D_{2n}$.)

6. **HW III - Q3:** (a) We are given that H is both a proper subgroup and a subspace of $\mathbb{R}^2$. Since H is a subspace, by definition it should contain the origin $(0,0)$. Further, we know that any one-dimensional subspace of $\mathbb{R}^2$ is a line through the origin. It remains to show that each such line is also a subgroup of $\mathbb{R}^2$. A typical line L_m of slope m through the origin satisfies the equation $y = mx$, and hence as a set

$$L_m = \{(x, mx) : x \in \mathbb{R}\}.$$

Given points $(x_1, mx_1), (x_2, mx_2) \in L_m$, we see that

$$(x_1, mx_1) - (x_2, mx_2) = (x_1 - x_2, m(x_1 - x_2)) \in L_m.$$

Hence, by the Subgroup Criterion, we have that $L_m < \mathbb{R}^2$.

(b) A left (or right) coset of L_m represented by a vector $(a, b) \in \mathbb{R}^2$ is of the form

$$(a, b) + L_m = \{(x + a, mx + b) : x \in \mathbb{R}\},$$

which is the set of points on a line parallel to L_m satisfying the equation

$$y - b = m(x - a).$$

Moreover, two distinct vectors (a, b) and (c, d) will represent the same coset if, and only if,

$$(a, b) + L_m = (c, d) + L_m \iff (a - c, b - d) \in L_m \iff b - d = m(a - c).$$

7. **HW III - Q4:** Let G be a nontrivial group that has no proper subgroups. Since G is nontrivial, there exists a non-identity element $g \in G$, and so $\langle g \rangle$ is a nontrivial cyclic subgroup of G. Since G has no proper subgroups, this would imply that $G = \langle g \rangle$, or in other words, G is cyclic.

   Suppose that G is of infinite order. Then by assertion 1.4 (iv) of the Lesson Plan, it follows that for every $k \in \mathbb{Z} \setminus \{1\}$, $\langle g^k \rangle$ is a proper subgroup of G. This is impossible, as G does not have any proper subgroups. Therefore, G has to be of finite order.

   Let $|G| = n$. Again, from assertion 1.4 (iv) of the Lesson Plan, we know that for every proper divisor d of n, $\langle g^{n/d} \rangle$ is a proper subgroup of G. Since G has no proper subgroups, n can have no proper divisors. Hence, n has to be a prime.

8. **HW IV - 2.3 (iv)(a):** Let G be a group of order 4. By the Lagrange's Theorem, every non-identity element in G is either of order 2 or 4.

   Suppose that $g \in G$ is a non-identity element of order 4. Then $G = \langle g \rangle$, and so it follows that G is cyclic. Further, this would imply that the remaining two non-trivial element in G are g^2 and g^3, which are or orders 2 and 4, respectively.

   On the other hand, suppose that no non-identity element of G is of order 4. Then G has to be of the form $G = \{1, g_1, g_2, g_3\}$, where $o(g_i) = 2$, and $g_3 = g_1 g_2$. Note that this structure is analogous to the structure of $U_8 = \{[1], [3], [5], [7]\}$, where $o([3]) = o([5]) = o([7]) = 2$, and $[1] \cdot [5] = [7]$. More formally, the map $\varphi : G \to U_8$ defined by

$$1 \overset{\varphi}{\mapsto} [1],\ x_1 \overset{\varphi}{\mapsto} [3],\ x_2 \overset{\varphi}{\mapsto} [5],\ x_3 \overset{\varphi}{\mapsto} [7]$$

   is a isomorphism. (Verify!)