MAT301 Groups and Symmetry

Assignment 2 Solutions

Note on grading: Questions 1(a,c,d,e), 2, 3 and 4 were graded. In Question 3(b) only the centres of $GL_2(\mathbb{R})$ and S_n were considered for grading. The assignment was graded out of 38. The numbers in [ ] indicate how many marks each (part of a) question was worth.

1. [12] In each part, a group G and a subset $S \subset G$ are given. Determine if S is a subgroup of G.

(a) [3] $G = D_n$ (the group of symmetries of a regular n-gon), S = the set of all the rotational symmetries in D_n.
(b) $G = GL_n(\mathbb{R})$, $S \subset GL_n(\mathbb{R})$ the subset consisting of all the invertible diagonal matrices.
(c) [3] $G = SL_2(\mathbb{Z})$ (the group of 2×2 matrices of determinant 1 which have integer entries), S the subset consisting of the matrices of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, where $n \in \mathbb{Z}$.
(d) [3] Fix an integer n. Let G be any abelian group with identity denoted by e, and $S = \{g \in G : g^n = e\}$.
(e) [3] G any abelian group, S the set of all elements of finite order.
(f) $G = \mathbb{C}^\times$ (nonzero complex numbers under multiplication), S the unit circle in $\mathbb{C}$ (so $S = \{z \in \mathbb{C} : |z| = 1\}$, where $|z|$ means the norm of the complex number z).

Solution: The given subsets are all subgroups (of the corresponding groups). We check this for each part below.

(a) The identity transformation is a rotation, the composition of two rotations is a rotation (by the sum of the angles and the two rotations), and the inverse of a rotation is also a rotation (inverse of rotation by θ is rotation by $-\theta$). So S is a subgroup of D_n.

(b) The identity matrix is diagonal, hence in S. We have

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 & 0 \\ 0 & a_2 b_2 \end{pmatrix},$$

hence S is closed under matrix multiplication (which is the operation in $GL_2(\mathbb{R})$). Also,

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a_1} & 0 \\ 0 & \frac{1}{a_2} \end{pmatrix}$$

(where a_1 and a_2 are nonzero), so that S is closed under taking inverses.

(c) The identity matrix certainly belongs to S. The following two calculations show that S is closed under the operation and taking inverses:

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

(d) We have $e^n = e$, so that $e \in S$. Let $g, h \in S$. Then $g^n = h^n = e$. Since the group G is abelian, $(gh)^n = g^n h^n = ee = e$. Thus $gh \in S$ and S is closed under the operation. We have $(g^{-1})^n = (g^n)^{-1} = e^{-1} = e$, so that $g^{-1} \in S$ and S is closed under taking inverses.

(e) The identity element e has finite order. Let g and h be two elements of finite order in G. Then there exist positive integers n, m such that $g^n = h^m = e$. Then, since G is abelian, we have

$$(gh)^{nm} = g^{nm} g^{nm} = (g^n)^m (h^m)^n = e,$$

so that gh has finite order. Also, $(g^{-1})^n = (g^n)^{-1} = e$ so that g^{-1} also has finite order.

(f) The identity element of $\mathbb{C}^\times$ is 1. We have $|1| = 1$ (where here as well as everywhere for this part $|\ |$ means absolute value of a complex number), so $1 \in S$. That S is closed under the operation (= multiplication) and taking inverses follow from the following formulas:

$$|zz'| = |z| \cdot |z'|$$

and

$$|z^{-1}| = \frac{1}{|z|}$$

(where in the latter $z \neq 0$).

2. [7] (a) [4] Give an example of a group G and elements $g, h \in G$ such that $|g|$ and $|h|$ are finite, but $|gh|$ is infinite. (Hint: Consider the group of symmetries of a circle.)

(b) [3] Give an example of a group G in which the subset $S = \{g \in G : g^2 = e\}$ is not a subgroup.

Solution: (a) Let G be the set of all the symmetries of a circle, which forms a group under composition of functions. Note that G consists of reflections over lines passing through the centre of the circle O, and rotations around O. The reflections all have order 2. We claim that rotation by θ has finite order if and only if θ/π is a rational number. Indeed, let ρ_θ denote the rotation by θ. If ρ_θ has finite order, there is a positive integer n such that $\rho_{n\theta} = (\rho_\theta) = e$, so that $n\theta = 2\pi k$ for some integer k. Then $\theta/\pi = 2k/n \in \mathbb{Q}$. Conversely, if $\theta/\pi = a/b$ with a and b integer with $b > 0$, then $\rho_\theta^{2b} = \rho_{2a\pi} = e$ and ρ_θ has finite order. This completes the proof of our claim.

Let r and r' be two reflections whose axes form an angle τ with each other (where the angle is measured say from the axis of r to that of r'). Being the composition of two reflections, the element $r \circ r' \in G$ is a rotation. Considering points on the axes we can see that $r' \circ r$ is in fact rotation by 2τ. If we take our lines such that $\tau = \sqrt{2}\pi$ (or any other angle such that τ/π and hence $2\tau/\pi$ is irrational), then $r \circ r'$ has infinite order.

(b) Take $G = D_3$. Then the given subset consists of the identity element and the three reflections. This subset is not closed under the operation (why?) and hence is not a subgroup.

3. [12] For any group G, the *centre* of G (usually denoted by $Z(G)$) is defined as

$$Z(G) := \{g \in G : gh = hg \text{ for every } h \in G\}$$

(i.e. the set of those $g \in G$ which commute with every element of G).

(a) [1] True or false: A group G is abelian if and only if $Z(G) = G$.

(b) [2] Show that in general, $Z(G)$ is a subgroup of G.
(c) [9] Find the centre of each of the groups D_n, S_n, and $GL_2(\mathbb{R})$. (For D_n and S_n assume $n \geq 3$.)

Suggestion: For D_n, it might be useful to think about the following question first: Let r be a reflection and ρ a rotation, with the centre of the rotation on the line of reflection. When is $r \circ \rho = \rho \circ r$? Think about the image of a point on the line of reflection under the two compositions. For $GL_2(\mathbb{R})$, it is easy to see that any matrix of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ commutes with every 2×2 matrix, so that there centre of $GL_2(\mathbb{R})$ certainly contains all such matrices (with $a \neq 0$, of course). Does the centre of $GL_2(\mathbb{R})$ contain any element besides these?)

Solution: (a) true (why?)

(b) The identity element e commutes with every element of the group (as $eh = he = h$ for every $h \in G$), so $e \in Z(G)$. Let $g \in Z(G)$. Given any $h \in G$, we have $gh^{-1} = h^{-1}g$. Taking inverses we get $hg^{-1} = g^{-1}h$. Thus $g^{-1} \in Z(G)$. Now let g' also be in $Z(G)$. Given $h \in G$, since $g \in Z(G)$, we have $g(g'h) = (g'h)g$. Using associativity and the fact that g and g' commute with every element of the group (in particular with each other), we can rewrite this equality as $(gg')h = h(gg')$. Thus $gg' \in Z(G)$.

(c) We claim that the centre of S_n is trivial for $n \geq 3$ (is the trivial subgroup $\{e\}$). Let $f \in S_n$ and $f \neq e$ (where e is the identity element of the group, i.e. the identity function on $\{1, \ldots, n\}$). Then there is $a \in \{1, \ldots, n\}$ such that $f(a) \neq a$. Let $b = f(a)$. Since $n \geq 3$, there is $c \in \{1, \ldots, n\}$ such that $c \neq a, b$. (So the three numbers a, b, c are distinct.) Let $g \in S_n$ be such that $g(a) = a$ and $g(b) = c$. Note that such g certainly exists, as for example we can take g to be the function that sends $b \mapsto c$, $c \mapsto b$, and sends every other element of $\{1, \ldots, n\}$ to itself. Then we have $g \circ f(a) = g(b) = c$, whereas $f \circ g(a) = f(a) = b \neq c$. Thus $g \circ f \neq f \circ g$, so that $f \notin Z(S_n)$. It follows that $Z(S_n) = \{e\}$ (why?).

Now we calculate the centre of $GL_2(\mathbb{R})$. Let H be the set consisting of all the matrices of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI$, where $a \in \mathbb{R} - \{0\}$ and I is the identity matrix. (Matrices of the form aI are called *scalar* matrices.) Note that $H \subset GL_2(\mathbb{R})$. We claim that H is the centre of $GL_2(\mathbb{R})$. Indeed, a straightforward calculation shows that for any 2×2 matrix B, we have $(aI)B = B(aI)$, so that $H \subset Z(GL_2(\mathbb{R}))$. It remains to show that $Z(GL_2(\mathbb{R})) \subset H$. Let $A \in Z(GL_2(\mathbb{R}))$. Write

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then A commutes with every element of $GL_2(\mathbb{R})$. In patricular, it commutes with the matrices

$$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Considering $AB = BA$ we get $b = c = 0$ (write the computation and see). Then considering $AC = CA$ (keeping in mind that we now know $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$) we get $a = d$, so that $A \in H$.

Finally, we find the centre of D_n for $n \geq 3$. We claim that

$$Z(D_n) = \begin{cases} \{e\} & \text{if } n \text{ is odd} \\ \{e, \rho_\pi\} & \text{if } n \text{ is even.} \end{cases}$$

(As before, we denote rotation by θ by ρ_θ. Note that ρ_π is in D_n if and only if n is even.) First note that no reflection will be in the centre: given any reflection $r \in D_n$, let $r' \in D_n$ be a reflection whose axis forms an angle of π/n with the axis of r (in other words, the axis of r' is "next to" the axis of r). Then one easily sees that the two rotations $r \circ r'$ and $r' \circ r$ are not equal (one is rotation by $2\pi/n$ and the other by $-2\pi/n$, and those two are not the same when $n > 2$).

We now turn our attention to the rotations in D_n. Let $\rho = \rho_\theta \in D_n$ be any rotation such that $\rho \neq e, \rho_\pi$. We claim that ρ is not in the centre of D_n. Let $r \in D_n$ be any reflection. Then $r \circ \rho \neq \rho \circ r$. (Indeed, let P be one of the two points on the intersection of our polygon and the axis of r. Then $r \circ \rho(P)$ and $\rho \circ r(P)$ are on opposite sides on the axis of r.)

All that remains to show is that if rotation by π is in D_n, then it commutes with every element of D_n (hence is in the centre). Since the rotations all commute with one another, we only need to check that $\rho_\pi \circ r = r \circ \rho_\pi$, where $r \in D_n$ is a reflection. This can easily be checked using plane geometry methods (both compositions are equal to the reflection over the line perpendicular to the axis of r, passing through the centre of the shape). Alternatively, we can choose coordinates for the plane so that the centre of the polygon is the origin, and the axis of r is the x-axis. Then (writing elements of $\mathbb{R}^2$ as column vectors) r and ρ_π are given by

$$r\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

and

$$\rho_\pi\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ -y \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

and the two matrices $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ commute.

4. [7] Let G be a subgroup of S_n. Note that, in particular, each element of G is a bijection $\{1, \ldots, n\} \to \{1, \ldots, n\}$. Define a relation $\sim$ on the set $\{1, \ldots, n\}$ as follows: for any integers $1 \leq a, b \leq n$, set $a \sim b$ if and only if there exists $g \in G$ such that $g(a) = b$.

(a) [4] Show that $\sim$ is an equivalence relation.
(b) [3] Let $n = 5$ and $f \in S_5$ be the function that sends $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 5$, $4 \mapsto 1$, $5 \mapsto 3$. Let $G = \langle f \rangle$ (the subgroup of S_5 generated by f). Calculate the equivalence classes of the relation $\sim$ defined as above.

Solution: (a) Since G is a subgroup of S_n, it contains the identity function e (which is the identity of the group S_n). Given any $a \in \{1, \ldots, n\}$, $e(a) = a$, so that $a \sim a$. We now check that the relation is symmetric. Suppose $a \sim b$. Then there is $f \in G$ such that $f(a) = b$, so that $a = f^{-1}(b)$. Since $G \leq S_n$ is a subgroup, $f^{-1} \in G$. Thus $b \sim a$ as desired. Finally, let us check transitivity. Suppose $a \sim b$ and $b \sim c$. Then there are $f, g \in G$ such that $f(a) = b$ and $g(b) = c$. It follows that $g \circ f(a) = c$. Since G is a subgroup of S_n, it is closed under composition, so that $g \circ f \in G$. Thus we get $a \sim c$.

(b) We calculate the subgroup $G = \langle f \rangle$ first. Let us find powers (i.e. self compositions) of f:

$$f:\ 1 \mapsto 2,\ 2 \mapsto 4,\ 3 \mapsto 5,\ 4 \mapsto 1,\ 5 \mapsto 3$$

$$f^2 : 1 \mapsto 4,\ 2 \mapsto 1,\ 3 \mapsto 3,\ 4 \mapsto 2,\ 5 \mapsto 5$$
$$f^3 : 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 5,\ 4 \mapsto 4,\ 5 \mapsto 3$$
$$f^4 : 1 \mapsto 2,\ 2 \mapsto 4,\ 3 \mapsto 3,\ 4 \mapsto 1,\ 5 \mapsto 5$$
$$f^5 : 1 \mapsto 4,\ 2 \mapsto 1,\ 3 \mapsto 5,\ 4 \mapsto 2,\ 5 \mapsto 3$$
$$f^6 : 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3,\ 4 \mapsto 4,\ 5 \mapsto 5.$$

We see that $f^6 = e$ (and $f^i \neq e$ for $1 \leq i < 6$). Thus $|f| = 6$ and $G = \{e, f, f^2, f^3, f^4, f^5\}$. By definition of our relation and in view of our calculations above, we have

$$[1] = \{g(1) : g \in G\} = \{1, 2, 4\}.$$

(Note that without looking at the calculations we should know that [2] and [4] must also be $\{1, 2, 4\}$. Indeed, by the general properties of equivalence relations $1 \sim 2$ tells us $[1] = [2]$. Say it differently, [2] contains 2, hence intersects [1], hence has to be equal to it, as equivalence classes are either equal or disjoint.) Similarly,

$$[3] = \{3, 5\} = [5].$$

The (distinct) equivalence classes are $\{1, 2, 4\}$ and $\{3, 5\}$.

5. (a) Let G be a group. Let H be a subgroup of G. Define a relation $\sim$ on G as follows: for any $g, g' \in G$, set $g \sim g'$ if and only if there exists $h \in H$ such that $g' = gh$. Show that $\sim$ is an equivalence relation.

(b) Take $G = D_6$ and $H = \langle \rho_{2\pi/3} \rangle$, where ρ_θ denotes counter-clockwise rotation by θ. Calculate the equivalence classes of the relation $\sim$ defined as above.

Solution: (a) For any $g \in G$ we have $g = ge$. Since $e \in H$ (why?) this tells us $g \sim g$.

Let $g \sim g'$. Then $g' = gh$ for some $h \in H$. Then $h^{-1} \in H$ as well, and we have $g = g'h^{-1}$. Thus $g' \sim g$ and the relation is symmetric.

Suppose $g \sim g'$ and $g' \sim g''$. Then there are $h, h' \in H$ such that $g' = gh$ and $g'' = g'h'$, so that $g'' = g(hh')$. Since H is a subgroup, $hh' \in H$. It follows that $g \sim g''$ and our relation is transitive.

(b) By the defintion of $\sim$, for any $g \in G$ we have

$$[g] = \{g' \in G : g \sim g'\} = \{gh : h \in H\}.$$

We use the following notation for the elements of D_6: rotation by $2\pi/6$ is denoted by ρ (so that all the rotations in D_n are $\rho, \rho^2, \ldots, \rho^6 = e\}$). Denote one of the reflections, say one that passes through a vertex, by r_1. Label the other reflections $r_2, \ldots, r_6$ in that order, as we move counter-clockwise from the axis of r_1. Thus the axes of r_1, r_3, r_5 pass through the vertices and the axes of r_2, r_4, r_6 pass through the midpoints of the edges.

Then straightforward calculations using the above formula for $[g]$ give us

$$[e] = H = \{e, \rho^2, \rho^4\}$$
$$[\rho] = \{\rho, \rho^3, \rho^5\},$$
$$[r_1] = \{r_1, r_3, r_5\}$$

and

$$[r_2] = \{r_2, r_4, r_6\}.$$

6. Calculate the order of every element of each of the following groups: (a) $\mathbb{Z}/8$ (= residue classes mod 8 under addition) (b) μ_8 (= the subgroup of $\mathbb{C}^\times$ consisting of the 8th roots of unity) (c) $U(16)$ (Suggestion: Keep the formula $|g^k| = \frac{|g|}{gcd(|g|,k)}$ in mind.)

Solution: (a) We have $|[1]| = 8$.The group $\mathbb{Z}/8$ is generated by [1], so we can use the formula given in the suggestion to find the order of every other element. (Note that the operation is $\mathbb{Z}/8$ is addition.) We have $[2] = 2[1]$ (where 2[1] means [1]+[1]). Thus $|[2]| = \frac{|[1]|}{gcd(2,|[1]|} = 4$. Similarly, we can calculate the order of every other element of $\mathbb{Z}/n$ and see that $|[3]| = |[5]| = |[7]| = 8$,$|[4]| = 2$, $|[6]| = 4$, and of course $|[0]| = 1$.

(b) Let $\alpha = e^{2\pi i/8}$. Then $\mu_8 = \{1, \alpha, \alpha^2, \dots, \alpha^7\}$. We have $|\alpha| = 8$ (where | | means the order, not absolute value of the complex number α). Using the formula given in the suggestion we get the order of every element: $|1| = 1$, $|\alpha^2| = |\alpha^6| = 4$, $|\alpha^4| = 2$, $|\alpha^3| = |\alpha^5| = |\alpha^7| = |\alpha| = 8$.

(c) Note that

$$U(16) = \{[1], [3], [5], [7], [9], [11], [13], [15]\}.$$

We have $|[1]| = 1$. Let us calculate $|[5]|$. Since $U(16)$ has 8 elements, by Lagrange's theorem (or more specefically, by Corollary 2 of the notes) the order of every element of $U(16)$ divides 8. We have

$$[5]^2 = [25] = [9]$$

and

$$[5]^4 = ([5]^2)^2 = [9]^2 = [81] = [1].$$

Thus $|[5]| = 4$. (We did not have to check $[5]^3$ because we knew 3 cannot be the order.)

Now the formula given in the suggestion tells us $[9] = [5]^2$ has order 2, and $[13] = [5]^3$ has order 4. Similarly we easily see $|[3]| = 4$, so that $[3]^3 = [11]$ also has order 4 (why?). It remains to find the orders of [7] and $[-1] = [15]$. We have $[7]^2 = [-1]^2 = [1]$, so $|[7]| = |[-1]| = 2$.