MAT301 Groups and Symmetry
Assignment 1 Solutions

Note on grading: Questions 1, 3, 4 and 5 were graded. The assignment was graded out of 25. The numbers in [ ] indicate how many marks each (part of a) question was worth.

1. [10, each part 2] Determine if each of the following is a group.

(a) $\mathbb{Z}$ under $\star$ defined by $x \star y = x + y + xy$
(b) $\mathbb{Q} - \{-1\}$ under $\star$ defined by $x \star y = x + y + xy$ (First make sure that $\star$ is a binary operation on $\mathbb{Q} - \{-1\}$.)
(c) the set $\mathbb{R}_{>0}$ of positive real numbers under $\star$ defined by $x \star y = xy^2$ (So for instance, $2 \star 3 = 18$.)
(d) the set of all invertible 2×2 matrices with entries in $\mathbb{R}$ under matrix multiplication
(e) the set of all invertible 2×2 matrices with entries in $\mathbb{Z}$ under matrix multiplication

Solution:

(a) A straightforward computation shows that 0 satisfies the defining property of the identity element. We claim that -1 does not have an inverse. Indeed,

$$-1 \star x = -1 + x - x = -1,$$

so that $-1 \star x \neq 0$ for any $x \in \mathbb{Z}$. Thus $\mathbb{Z}$ is not a group under $\star$.

(b) First we check that $\star$ is a binary operation on $\mathbb{Q} - \{-1\}$ (the analogous statement for (a) is trivial and that is why we did not mention it). We need to check that if $x, y \neq -1$, then $xy + x + y \neq -1$. This follows from that

$$xy + x + y + 1 = (x + 1)(y + 1),$$

so that if the left hand side is zero, x or y has to be -1.

It is easy to see that the operation is indeed associative and that 0 is the identity (we leave the details to the reader). Let $x \in \mathbb{Q} - \{-1\}$. Set $y = \frac{1}{x+1} - 1$ (note that the denominator is not zero as $x \neq -1$). Then y is a rational number, and moreover $y \neq -1$, as $\frac{1}{x+1} \neq 0$. Now one checks by a direct computation that $x \star y = 0$ (the operation is clearly commutative so $y \star x = 0$ as well). Thus $\mathbb{Q} - \{-1\}$ is a group under $\star$.

(c) The operation is not associative (hence we don't have a group): $1 \star (2 \star 2) = 1 \star 8 = 64$ but $(1 \star 2) \star 2 = 4 \star 2 = 16$.

(d) This is a group (which we will denote by $GL_2(\mathbb{R})$). The product of two invertible matrices is invertible (as if A and B are invertible, $\det(A)$ and $\det(B)$ are nonzero, hence $\det(AB) = \det(A)\det(B)$ is nonzero). It follows that matrix multiplication indeed gives a binary operation on the the set of all invertible 2×2 matrices with entries in $\mathbb{R}$ (that the product of two matrices with real entries has real entries is clear from the definition of matrix multiplication). We know from previous courses that matrix multiplication is associative. The 2×2 identity matrix I satisfies the defining property of the identity element. The inverse of an element $A \in GL_2(\mathbb{R})$ is simply the inverse matrix A^{-1}.

(e) Let us refer to the set given in the question by S. The identity matrix I is the identity element. The element $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ is in S, but there is no element B in S such that $AB = I$. Indeed, the only 2×2 real matrix with this property is $B = \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}$, which does not belong to S. Thus S is not a group under matrix multiplication.

2. Suppose $(G, \star)$ is a group. Let $g, h, h' \in G$.

(a) Show that if $h \star g = h' \star g$, then $h = h'$. (In other words, "right cancellation" holds in a group. One can similarly show that "left cancellation" holds in a group as well, i.e. $g \star h = g \star h'$ implies $h = h'$.)
(b) Suppose $g \star h = h' \star g$. Does it follow that $h = h'$? Suggestion: Look for a counter-example in D_3 (the group of symmetries of an equilateral triangle, which you studied in your tutorial activity).
(c) Now suppose moreover that $(G, \star)$ is abelian. Does $g \star h = h' \star g$ imply $h = h'$?

Solution:
(a) Let $hg = h'g$ (dropping the symbol $\star$ to simplify the notation). Multiply by g^{-1} on the right we get $(hg)g^{-1} = (h'g)g^{-1}$, which in view of associativity gives $h(gg^{-1}) = h'(gg^{-1})$. By the definition of g^{-1}, denoting the identity element by e, the latter equation can be rewritten as $he = h'e$, which in turn, by the definition of the identity element, implies $h = h'$.

REMARK. For the remaining questions we will be less explicit in our use of the axiom of associativity.
(b) No. Let G be any nonabelian group (e.g. D_3 or $GL_2(\mathbb{R})$). Let $g, h \in G$ be two elements that do not commute. Set $h' = ghg^{-1}$. Then $h'g = ghg^{-1}g = gh$ but $h \neq h'$: if $h = ghg^{-1}$ then multiplying by g on the right we get $hg = gh$, which is not true by our choice of g, h.

(c) Yes, because then $gh = hg$, so that the given equation can be rewritten as $hg = h'g$ and we are in the situation of (a).

3. [5] Let $G = \{e, g\}$ be a group with two elements, with e the identity. Find the Cayley table of G (and provide full justification for your answer).

Solution: By the definition of identity, we have $ee = e$, $eg = g$ and $ge = g$. It remains to find g^2 (i.e. gg). We claim that $g^2 \neq g$. Indeed, if $g^2 = g$, then multiplying by g^{-1} (or writing the equation as say $gg = ge$ and using left cancellation) we get $g = e$, which is absurd. Thus $g^2 = e$. The Cayley table is shown below.

	e	g
e	e	g
g	g	e

4. [5] (a) [4] Let G be a group. Let g be an element of G. Define a function $\phi_g : G \to G$ by $\phi_g(h) = gh$ (i.e ϕ_g sends every $h \in G$ to gh). Show that ϕ_g is a bijection.

(b) [1] True or false: If G is a group, then every element of G appears in every row of the Cayley table of G exactly once.

Solution: (a) We give two solutions.

First solution: First let's check that ϕ_g is injective. Suppose $\phi_g(h) = \phi_g(h')$ for some $h, h' \in G$. This means $gh = gh'$, and multiplying by g^{-1} on the left (or rather by left cancellation) we see $h = h'$. This proves injectivity. Let's turn our attention to surjectivity. Given any $h \in G$, we have

$$\phi_g(g^{-1}h) = gg^{-1}h = eh = h,$$

so that h is in the image of ϕ_g. This proves surjectivity.

Second solution: To show that ϕ_g is a bijection it is enough to show that it has an inverse function. The function $\phi_{g^{-1}} : G \to G$ (sending $h \mapsto g^{-1}h$) is easily seen to be the inverse function to ϕ_g. Indeed, for any $h \in G$,

$$\phi_{g^{-1}} \circ \phi_g(h) = g^{-1}gh = h$$

and

$$\phi_g \circ \phi_{g^{-1}}(h) = gg^{-1}h = h.$$

Thus both $\phi_{g^{-1}} \circ \phi_g$ and $\phi_g \circ \phi_{g^{-1}}$ are identity maps on G (hence ϕ_g and $\phi_{g^{-1}}$ are inverse functions of one another).

(b) True. This is just a restatement of the result of part (a).

5. [5] Let G be a finite group. Denote the identity of G by e. Show that for every element $g \in G$, there is a positive integer n such that $g^n = e$. (In other words, show that every element of a finite group has finite order.)

Solution: Let $|G| = N$. Given $g \in G$, consider the elements

$$g,\ g^2, \ldots,\ g^N,\ g^{N+1}$$

of G. Since G has N elements, two of these must be equal, i.e. there exist $1 \leq i < j \leq N+1$ such that $g^i = g^j$. But $g^j = g^i g^{j-i}$, so that we get

$$g^i = g^i g^{j-i}.$$

Multiplying both sides by the inverse of g^i on the left we get $g^{j-i} = e$. Thus g has finite order (note that $j - i$ is not zero). In fact, $|g| \leq j - i$, which combining with $j - i \leq N$ gives $|g| \leq N$. Thus we have actually proved the order of every element of G is $\leq$ the order of G.

6. Let G be a group with identity element denoted by e. Suppose G has the following property: for every $g \in G$, we have $g^2 = e$. Show that G is abelian. (Suggestion: Let $g, h \in G$. Start with $(gh)(gh) = e$. Now multiply both sides by h on the right. Be sure to carefully justify all steps of your calculation using group axioms.)

Solution: Let $g, h \in G$. We have

$$(gh)(gh) = e.$$

Multiplying by h on the right, we get

$$((gh)(gh))h = eh. \tag{1}$$

By the defining property of e we have $eh = h$. On the other hand, we have

$$((gh)(gh))h \overset{\text{associativity}}{=} (gh)((gh)h) \overset{\text{associativity}}{=} (gh)(g(hh)) \overset{(*)}{=} (gh)(ge) \overset{(**)}{=} (gh)g,$$

where in $(*)$ (resp. $(**)$) we used the hypothesis (resp. definition of the identity element). Thus (1) tells us $(gh)g = h$. Now multiplying by g on the right, in view of $g^2 = e$, we get $gh = hg$ (we leave the detailed and step by step derivation of this using the axioms to the reader). We have shown that every two elements of G commute. Thus G is abelian.