MATH 3GR3 Assignment #2 Solutions
Due: Friday, October 6, by 11:59pm.

Upload your solutions to the Avenue to Learn course website.

1. Produce the Cayley table for the group $U(16)$, the group of units of $\mathbb{Z}_{16}$. Is this group cyclic?

   Solution: $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$ and its Cayley table is

$\cdot$	1	3	5	7	9	11	13	15
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	9	3	13	7	1	11
7	7	5	3	1	15	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

   By inspection we see that $U(16)$ does not contain an element of order 8, the order of this group, and so it is not cyclic. The elements 3, 5, 11, and 13 all have order 4 and the elements 7, 9, and 15 all have order 2.

2. Let G be a group and S a nonempty subset of G. Define the following relation on G:

   $a \sim b$ if and only if $s_1 a s_2 = b$ for some s_1, $s_2 \in S$.

   (a) Show that if S is a subgroup of G then $\sim$ is an equivalence relation on G.

   (b) Compute the equivalence classes of $\sim$ for the group of symmetries of the equilateral triangle, using the subgroup $S = \{id, \mu_1\}$.

   (c) Show, by example, that if S is not a subgroup, then $\sim$ need not be an equivalence relation.

   Solution: For (a) we need to show that this relation is reflexive, symmetric, and transitive when S is a subgroup of G:

- for $g \in G$, $g \sim g$ since $ege = g$ and $e \in S$,
- if $g \sim h$ then there are s_1, $s_2 \in S$ with $h = s_1 g s_2$. But then s_1^{-1}, $s_2^{-1} \in S$ and $g = s_1^{-1} h s_2^{-1}$, showing that $h \sim g$.
- if $g \sim h$ and $h \sim k$ then there are $s_i \in S$, $1 \leq i \leq 4$ with $h = s_1 g s_2$ and $k = s_3 h s_4$. But then $s_3 s_1$, $s_2 s_4 \in S$ and $k = (s_3 s_1) g (s_2 s_4)$, showing that $g \sim k$ as required.

For part (b), let's compute $[id]_\sim$: an element of the group is $\sim$-related to id if it can be written in the form $s_1 id s_2$ for some s_1, $s_2 \in S = \{id, \mu_1\}$. So, there are four different possibilities for s_1 and s_2. By trying them all we see that

$$[id]_\sim = \{id, \mu_1\}.$$

Since $id \sim \mu_1$, then $[\mu_1]_\sim$ is also equal to $\{id, \mu_1\}$. Using a similar approach, it can be shown that

$$[\mu_2]_\sim = \{\mu_2, \mu_3, \rho_1, \rho_2\}.$$

Since these two equivalence classes partition the entire group (it has exactly 6 elements), then they are the only equivalence classes of this equivalence relation.

For part (c), we can use the same group, but choose S to be a subset that is not a subgroup. For example, if we set $S = \{\mu_1\}$, then the resulting relation $\sim$ is not reflexive (check that $\mu_2 \not\sim \mu_2$) and so it is not an equivalence relation.

3. Let $G = \mathbb{Z} \times \mathbb{Z}$. Define a binary operation $\diamond$ on G as follows:

$$(a, b) \diamond (c, d) = (a + c, (-1)^c b + d).$$

   (a) Show that G with the operation $\diamond$ is a group.

   (b) Is this group cyclic? Justify your answer.

Solution:

First note that the product of two pairs of integers is another pair of integers and so $\diamond$ is a well-defined operation on G. The element $(0, 0)$

can be seen to be the identity element with respect to $\diamond$. The following shows that $\diamond$ is associative:

$$\begin{aligned}(a,b)\diamond((c,d)\diamond(e,f)) &= (a,b)\diamond(c+e,(-1)^e d+f)\\ &= (a+(c+e),(-1)^{(c+e)}b+((-1)^e d+f))\\ &= ((a+c)+e,(-1)^e((-1)^c b+d)+f)\\ &= (a+c,(-1)^c b+d)\diamond(e,f)\\ &= ((a,b)\diamond(c,d))\diamond(e,f)\end{aligned}$$

Finally, it can be checked that the inverse of the element (a,b) is $(-a,-(-1)^{-a}b)$.

We know that every cyclic group is abelian, and so to show that G is not cyclic, it suffices to note that $(0,1)\diamond(1,1)=(1,0)\neq(1,2)=(1,1)\diamond(0,1)$. Alternatively, one can show directly that no pair (a,b) is a cyclic generator of G.

4. Let H and K be subgroups of the group G. Show that $H\cap K$ is a subgroup of G. Provide an example that shows that $H\cup K$ is not necessarily a subgroup of G.

   Solution: Let H and K be subgroups of the group G and let $S=H\cap K$. Since e belongs to both H and K (any subgroup must contain the identity element) then $e\in S$. Suppose that $a,\ b\in S$. Then $a,\ b\in H$ and $a,\ b\in K$. Since H and K are closed under the group operation of G and are also closed under taking inverses, then $ab,\ a^{-1}\in H$ and $ab,\ a^{-1}\in K$. Thus $ab\in S$ and $a^{-1}\in S$. This establishes that S is closed under the group operation of G, is closed under taking inverses and contains the identity element of G. Thus S is a subgroup of G.

   The union of two subgroups of a group is not necessarily a subgroup. For example in the group of symmetries of the rectangle, both $H=\{id,s_1\}$ and $K=\{id,s_2\}$ are subgroups (s_1 is reflection along the vertical axis and s_2 is rotation by π radians), but $H\cup K=\{id,s_1,s_2\}$ is not a subgroup since it is not closed under the group operation. This is because $s_1\circ s_2=s_3$, which is not a member of $H\cup K$.

5. Let a and b be integers and define $K=\{na+mb\,|\,n,m\in\mathbb{Z}\}$. Show that K is a subgroup of $\mathbb{Z}$. Since every subgroup of $\mathbb{Z}$ is cyclic, then K also has this property. Find a generator for K, and justify your answer.

Solution: To see that K is a subgroup of $\mathbb{Z}$, we show that $0 \in K$, K is closed under addition, and for any $z \in K$ we have $-z \in K$. $0 \in K$ since $K = \{na + mb \mid n, m \in \mathbb{Z}\}$ and taking $n = m = 0$ we get $0a + 0b = 0 \in K$. Now let $g, h \in K$. Then we have $g = n_1 a + m_1 b$, $h = n_2 a + m_2 b$. Then $g + h = n_1 a + m_1 b + n_2 a + m_2 b = (n_1 + n_2)a + (m_1 + m_2)b \in K$. Also, we have $-g = -(n_1 a + m_1 b) = (-n_1)a + (-m_1)b \in K$. Hence K is a subgroup of $\mathbb{Z}$.

For the second part of this question, there are a few cases to consider. If $a = 0$, then $K = \langle b \rangle$ and if $b = 0$ then $K = \langle a \rangle$. If both a and b are nonzero, then we claim that $d = \gcd(a, b)$ is in K and is a generator for K, that is, for every $z \in K$ we have $z = k \cdot d$ for some $k \in Z$. $d \in K$ since for nonzero integers a and b, $\gcd(a, b)$ can be written in the form $na + mb$ for some n, $m \in \mathbb{Z}$.

To conclude, let $z \in K$. Then $z = na + mb$ for some $m, n \in \mathbb{Z}$. Now since d divides a and b, we can write $a = xd$ and $b = yd$ for some $x, y \in \mathbb{Z}$. Then $z = na + mb = nxd + myd = (nx + my)d$, which is exactly what we wanted to show (with $k = nx + my$).

6. What is the order of the element 9 in the group $\mathbb{Z}_{24}$? Does $\mathbb{Z}_{24}$ contain an element of order 5?

   Solution: The order of 9 in $\mathbb{Z}_{24}$ is the smallest integer $k > 0$ such that $k \cdot 9$ is congruent to 0 modulo 24. We have shown that this is equal to $24/\gcd(9, 24) = 24/3 = 8$. Since the order of an element g in a finite (cyclic) group G must divide into $|G|$, then there can be no element in $\mathbb{Z}_{24}$ of order 5.

7. (a) Let G be a finite **cyclic** group that has at least 2 elements. Prove that there is some $g \in G$ such that $|g|$ is a prime number.

   (b) Let G be a finite group that has at least 2 elements. Prove that there is some $g \in G$ such that $|g|$ is a prime number.

   Solution:

   For part (a), let $a \in G$ with $G = \langle a \rangle$ and let $|a| = n \geq 2$. Let p be a prime divisor of n and let $d = n/p$. Then the element $b = a^d$ has order p, since we know that the order of $a^d = n/\gcd(n, d) = n/d = p$.

   For part (b), let $b \in G$ with $b \neq e$ and let $H = \langle b \rangle$, a finite cyclic subgroup of G. By part (a), H has an element whose order is a prime number, and hence so does G.

8. Suppose that G is a group and let $T = \{g \in G \mid \text{the order of } g \text{ is finite}\}$. Show that if G is abelian, then T is a subgroup of G. Find an example of a non-abelian group G for which T is not a subgroup.

   Solution: We need to show that T contains the identity element e (it does, since the order of e is equal to 1). We also need to show that T is closed under the group operation: let a, $b \in T$. So $|a| = n$ and $|b| = m$ for some natural numbers n and m. But then $(ab)^{nm} = a^{nm}b^{nm}$ since G is assumed to be abelian. We have that $a^{nm} = (a^n)^m = e^m = e$ and $b^{nm} = (b^m)^n = e^n = e$ and so $(ab)^{nm} = e$. This shows that the order of ab is finite and so that $ab \in T$. Finally, we need to show that if $a \in T$ then $a^{-1} \in T$ as well. But if $|a| = n$ then $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$ and so a^{-1} has finite order and hence is a member of T.

   There are several (many) possible non-abelian groups that can be used to show that T is not a subgroup in general. For example, in the group $GL_2(\mathbb{R})$ consider the elements

$$a = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

   It can easily be verified that both a^2 and b^2 are equal to the identity matrix, and so belong to T, but that for any $k > 0$,

$$(ab)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},$$

   showing that (ab) has infinite order, and so does not belong to T. In this case, T is not closed under the group operation and so can't be a subgroup of $GL_2(\mathbb{R})$.

   Another example can be found by using the group of symmetries of the disk (from the previous homework assignment). If we take a and b to be reflections of the disk about different lines through the center of the disk, then $a^2 = b^2 = id$, and so belong to T, but ab will be a rotation of the disk by a certain angle that depends on the angle between the two axes of reflection that determine a and b. In general, the resulting symmetry ab will have infinite order.

9. A solution to the SageMath question can be found by clicking here.