MATH 3GR3 Assignment #3
Due: Friday, October 27, 11:59pm
Upload your solutions to the Avenue to Learn course website.
Detailed instructions will be provided on the course website.

1. Consider the following two elements of S_7:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 5 & 7 & 6 & 2 \end{pmatrix}.$$

   (a) Decompose σ and τ into cycles.
   (b) Compute $\sigma\tau$ and $\tau\sigma$.
   (c) Compute the order of σ, τ, $\sigma\tau$, and $\tau\sigma$.
   (d) Determine the signs of σ, τ, $\sigma\tau$, and $\tau\sigma$, i.e., determine if they are even or odd permutations.

   Solution:

$$\sigma = \begin{pmatrix} 1 & 6 & 5 \end{pmatrix}\begin{pmatrix} 2 & 7 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 2 & 3 & 4 & 5 & 7 \end{pmatrix},$$
$$\sigma\tau = \begin{pmatrix} 1 & 6 & 5 & 2 & 4 \end{pmatrix}, \tau\sigma = \begin{pmatrix} 1 & 6 & 7 & 3 & 5 \end{pmatrix}.$$

   σ has order 6, while the other elements have order 5. σ is the product of a 3-cycle (even) and two transpositions, and so is even. Any 5-cycle can be written as a product of 4 transpositions and so the other elements are also even.

2. Let $\sigma = (a_1, a_2, \ldots, a_m)$ and $\tau = (b_1, b_2, \ldots, b_n)$ be cycles of length m and n respectively in the group S_X for some set X. Suppose that

   - $\{a_1, a_2, \ldots, a_m\} \neq \{b_1, b_2, \ldots, b_n\}$ and that
   - $\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots, b_n\} \neq \emptyset$.

   So σ and τ are not disjoint, but the sets of elements that they permute are different.

   Show that $\sigma\tau \neq \tau\sigma$.

HINT: Since the elements being permuted are elements of some set X, you may assume that X is just $\{1, 2, \ldots, k\}$ for some large enough k (bigger than $n + m$), that $\sigma = (1, 2, \ldots, m)$, that the element 1 is equal to one of the b_i's and that τ is of the form $(1, b_2, \ldots, b_n)$ with $b_2 > m$. To use this hint, you should provide a justification for why this reduction of the general case to this specific case is valid.

Solution:

It is not essential to make use of the hint, but here is a justification for the reduction stated in the hint.

- Setting
$$X' = \{a_1, \ldots, a_m, b_1, \ldots, b_n\},$$
we see that for $x \in X \setminus X'$, $\sigma(x) = \tau(x) = x$ and so $\sigma\tau(x) = \tau\sigma(x)$. Also, for $x \in X'$, $\sigma(x)$, $\tau(x) \in X'$. So, whether or not σ and τ commute will depend on whether or not their restrictions to X' do so. So, we may assume that $X = X'$, which is a finite set, by considering the permutations $\sigma|_{X'}$ and $\tau|_{X'}$ in place of σ and τ.
We can assume that X is equal to the finite set $\{1, 2, \ldots, k\}$ for a natural number k that is big enough. Implicitly we are using that if two sets U and V are in bijective correspondence, then the groups S_U and S_V are isomorphic.
- The elements $a_1, a_2, \ldots, a_m$ are distinct integers between 1 and k, as are the elements $b_1, b_2, \ldots, b_n$. Since these two sets have at least one common element, and are different, then by rearranging the elements of these cycles, we may assume that $a_1 = b_1$ and $b_2 \notin \{a_1, a_2, \ldots, a_m\}$.
- By symmetry, we may assume that the m distinct elements a_i, $1 \leq i \leq m$ are just the elements $1, 2, \ldots, m$. (To fully justify this, we could use Exercise #30 from Chapter 5 of the textbook.) So we have that $\sigma = (1, 2, \ldots, m)$ and $\tau = (1, b_2, \ldots, b_n)$, where $b_2 > m$. Note that this part of the reduction isn't all that useful, since the conclusion that $\sigma\tau$ and $\tau\sigma$ are different can be derived just by knowing that b_2 is not equal to any of the a_i's.
- Then $\sigma\tau(1) = \sigma(b_2) = b_2$ and $\tau\sigma(1) = \tau(2) \neq b_2$, since τ is one-to-one and since $\tau(1) = b_2$ we can't have that $\tau(2) = b_2$ as well. This shows that the functions $\sigma\tau$ and $\tau\sigma$ are different, as required.

3. (a) We have seen that D_3, the group of symmetries of the equilateral triangle, is not abelian. Show that for $n > 2$, the dihedral group D_n is not abelian.

   (b) Find all elements a of the group D_8 that commute with every element of D_8, i.e., find $\{a \in D_8 \colon ax = xa \text{ for all } x \in D_8\}$. Is this set a subgroup of D_8?

Solution:

We have seen that the group D_n contains elements r and s of orders n and 2 respectively such that $srs = r^{-1}$. Since for $n > 2$, $r \neq r^{-1}$, this implies that D_n is not abelian, since if it were, we would conclude that

$$r^{-1} = srs = rss = r(s^2) = r,$$

which is not true. So, D_n is not abelian.

To solve part (b), the following identity will be useful:

$$r^i s = sr^{-i}.$$

To see why this is true, we get from $srs = r^{-1}$ that $sr^i s = r^{-i}$. This is because

$$sr^i s = srr \ldots rrs = (srs)(srs)(srs)(srs) \ldots (srs)(srs)(srs) = r^{-i},$$

where in the above, r occurs i-times and ss is inserted in between each pair of r's. It follows from this that $r^i s = sr^{-i}$.

Let g be an element of D_8 that commutes with every element of D_8. Clearly $g = id$ has this property, and the claim is that the only other element is $g = r^4$. To see that r^4 has this property, there are two types of elements of D_8 to consider: either r^i or sr^i for some i between 0 and 7. In the first case, $r^4 r^i = r^{4+i} = r^i r^4$. Actually, any power of r commutes with all powers of r because $\langle r \rangle$ is a cyclic, and hence abelian, group.

In the second case,

$$(r^4)(sr^i) = sr^{-4} r^i = sr^{4+i} = (sr^i)(r^4),$$

as required. This uses that $r^4 = r^{-4}$. So, as claimed, r^4 has this property.

To show that no other element of D_8 commutes with all elements of the group, consider the element r^j with $j \neq 4$ and with $1 \leq j < 8$. Using the same identities as above, we get that $(r^j)(s) = sr^{-j} \neq (s)(r^j)$, since $j \neq 4$. Similarly, $(sr^j)(s) \neq (s)(sr^j)$.

To conclude, the elements in question form the subset $\{id, r^4\}$. Since this set is closed under the group operation, taking inverses, and contains the identity element, then it is a subgroup of D_8.

You can check that the same sort of result holds for the groups D_{2n} for any $n > 1$.

4. For each pair of group G and subgroup H, describe the left and right cosets of H in G:

   (a) $G = D_n$, $H = \langle s \rangle$.

   Solution: $H = \langle s \rangle = \{id, s\}$ since s has order 2 in D_n. A left coset of H is of the form gH for some $g \in D_n$ and so is equal to $r^k H$ or $sr^k H$ for some $0 \leq k < n$. (Since D_n consists of the $2n$ elements of the form r^k or sr^k, $0 \leq k < n$.)
   The left coset $r^k H = \{r^k, r^k s\} = \{r^k, sr^{-k}\}$ and the left coset $sr^k H = \{sr^k, sr^k s\} = \{sr^k, r^{-k}\}$. So the left cosets of H are of the form $\{r^k, sr^{-k}\}$, for $0 \leq k < n$.
   Similarly, the right cosets of H are of the form $\{r^k, sr^k\}$, $0 \leq k < n$.

   (b) $G = GL_2(\mathbb{Q})$, $H = SL_2(\mathbb{Q})$.

   Solution: A left coset of H in G is of the form $A \cdot H$, where A is an invertible 2×2 matrix with rational entries. Let $d = \det(A)$, some non-zero rational number. Since H consists of 2×2 matrices with rational entries having determinant equal to 1, then any matrix in $A \cdot H$ will have determinant equal to $d = \det(A)$. Conversely, if $B \in GL_2(\mathbb{Q})$ and $\det(B) = d$, then we can write B as $A \cdot (A^{-1} \cdot B)$. Since $\det(A^{-1} \cdot B) = 1$, then $A^{-1} \cdot B \in SL_2(\mathbb{Q})$ and so B is in the coset $A \cdot H$. Thus the coset $A \cdot H$ consists of all matrices in $GL_2(\mathbb{Q})$ that have determinant equal to d. Since A is an arbitrary element of $GL_2(\mathbb{Q})$ it follows that the left cosets of H in G are precisely the subsets of G of the form $\{B : \det(B) = d\}$ for some non-zero rational number d.

For similar reasons, it follows that the right cosets of H in G are the same as the left cosets.

(c) $G = A_4$, $H = \{(1), (123), (132)\}$.

Solution: Since the index of H in G is 4 (by Lagrange's Theorem), then there will be 4 left cosets and 4 right cosets of H in G. Here they are: Left Cosets – $\{(1), (123), (132)\}$, $\{(124), (134), (14)(23)\}$, $\{(142), (234), (13)(24)\}$, $\{(143), (243), (12)(34)\}$, and Right Cosets – $\{(1), (123), (132)\}$, $\{(124), (243), (13)(24)\}$, $\{(142), (143), (14)(23)\}$, $\{(234), (134), (12)(34)\}$.

(d) $G = \mathbb{Z}_{12}$, $H = \langle 10 \rangle$.

Solution: $H = \langle 10 \rangle = \{0, 2, 4, 6, 8, 10\}$ and so $[G : H] = 2$ (by Lagrange's Theorem). So, there will be two left cosets. Since G is abelian, then these left cosets will also be right cosets. Since H is one of the cosets, and there are only two of them, then the other coset is just $G \setminus H = \{1, 3, 5, 7, 9, 11\}$.

5. Recall that $GL_2(\mathbb{R})$ is the group of all 2×2 invertible matrices with real entries. Let

- $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in GL_2(\mathbb{R}) \, : \, ac \neq 0 \right\}$
- $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \, : \, x \in \mathbb{R} \right\}$

(a) Show that G is a subgroup of $GL_2(\mathbb{R})$ and that H is a subgroup of G.

Solution: Clearly G and H contain the identity matrix. We need to show that both are closed under matrix multiplication and taking inverses. If $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix} \in G$ then their product is $\begin{pmatrix} au & av + bw \\ 0 & cw \end{pmatrix}$, which is also a member of G (since $aucw \neq 0$), and the inverse of the first matrix is $\begin{pmatrix} 1/a & -b/(ac) \\ 0 & 1/c \end{pmatrix}$, which is also a member of G. Thus G is a subgroup of $GL_2(\mathbb{R})$.

If $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in H$ then their product is $\begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$, which is also a member of H, and the inverse of the first matrix is $\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}$, which is also a member of H. Thus H is a subgroup of G (and hence also of $GL_2(\mathbb{R})$).

(b) Show that every left coset of H in the group G is equal to a right coset of H in G.

Solution: Let $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$ and consider the left coset $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} H$. It consists of all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix},$$

for any number $x \in \mathbb{R}$.

Similarly, the right coset $H \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ consists of all matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & cx+b \\ 0 & c \end{pmatrix},$$

for any number $x \in \mathbb{R}$. Since both a and c are non-zero then any real number can be expressed in the form $ax+b$ and in the form $cx+b$, and so these two sets of matrices are identical, and consist of all matrices of the form $\begin{pmatrix} a & x \\ 0 & c \end{pmatrix}$, for any real number x.

(c) Show that for $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} u & v \\ 0 & w \end{pmatrix} \in G$, the two left cosets $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} H$ and $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix} H$ are equal if and only if $a = u$ and $c = w$.

Solution:

We know that in general, two left cosets g_1H and g_2H of a subgroup are equal if and only if $g_1^{-1}g_2 \in H$. In this case,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} \begin{pmatrix} u & v \\ 0 & w \end{pmatrix} = \begin{pmatrix} 1/a & -b/(ac) \\ 0 & 1/c \end{pmatrix} \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$$
$$= \begin{pmatrix} u/a & v/a - (bw)/(ac) \\ 0 & w/c \end{pmatrix}.$$

This matrix will belong to H if and only if $u/a = 1$ and $w/c = 1$, or $u = a$ and $w = c$.

Alternatively, we know from part (b) that the left coset $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} H$ consists of all matrices of the form $\begin{pmatrix} a & x \\ 0 & c \end{pmatrix}$, for any real number x. We also know that $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} H$ and $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix} H$ are equal if and only if $\begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$ belongs to $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} H$. From this it follows that $a = u$ and $c = w$.

(d) H is also a subgroup of $GL_2(\mathbb{R})$ since it has been established in (a) that H is a subgroup of G and G is a subgroup of $GL_2(\mathbb{R})$. Are the left cosets of H in $GL_2(\mathbb{R})$ equal to right cosets of H in $GL_2(\mathbb{R})$?

Solution: No: Just find some matrix $A \in GL_2(\mathbb{R})$ such that $A \cdot H \neq H \cdot A$. For example if $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ then $A \cdot H$ consists of all matrices of the form

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 1 & x+1 \end{pmatrix},$$

and $H \cdot A$ consists of all matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} x+1 & x \\ 1 & 1 \end{pmatrix},$$

for any real number x. Since these two sets of matrices are different, this establishes that the left coset $A \cdot H$ is not equal to the right coset $H \cdot A$.

6. Let G be a group of order $343 = 7^3$. Show that G contains an element of order 7.

   Solution:

   Choose any $g \in G$ with $g \neq e$ and let $H = \langle g \rangle$, the cyclic subgroup of G generated by g. By Lagrange's Theorem, the order of H divides 7^3, the order of G. Since H is a finite cyclic group, then by question #7 on the previous assignment, we know that it contains an element of prime order. But this prime number must divide 7^3 and so is equal to 7, as required.

7. Let G be a finite group that contains elements of order 1 through 10. What is the smallest possible order of G? Provide an example of a group with this property having this order.

   Solution:

   By Lagrange's theorem the order of G must have all numbers less than or equal to 10 as divisors. This is because for all $g \in G$, $|g|$ divides $|G|$. The smallest number with this property is: $5 \times 7 \times 8 \times 9 = 2520$ (the least common multiple of the numbers 1 through 10). The cyclic group $\mathbb{Z}_{2520}$ is an example of such a group.

8. Read over the SageMath tutorials at the ends of Chapters 4, 5, and 6 and perform the following calculations. To submit your calculations, either take a screenshot (or maybe a picture) of the webpage that contains them or include a copy of the link (i.e., URL) that is produced by the SageCell "share" button, or just copy and paste your commands and the results into the document that you upload to Avenue to Learn.

   (a) Produce the alternating group A_7 using the "AlternatingGroup" command and then create and list the elements of the cyclic subgroup of A_7 that is generated by the (even) permutation

   $$(1, 2, 3)(4, 7)(5, 6).$$

   You will need to use the "subgroup" function to create the subgroup.

(b) Produce all of the subgroups of the group A_4 and list all of the orders of these subgroups. Do not list the subgroups, just their orders. Verify that A_4 has no subgroup of order 6 (you don't need to include this in your solution, just look at your list to verify this. We claimed in the lectures that even though $|A_4| = 12$, A_4 doesn't have a subgroup of order 6, a divisor of 12. A description of how to do this can be found in the Subgroups subsection of Section 6.6 of the textbook.

Solution:

For the SageMath question, click on the following link to see a solution: click here

Supplementary problems from the textbook (not to be handed in)

- From Chapter 5, questions 1, 3, 6, 9, 23, 30, 31
- From Chapter 6, questions 3, 5, 10, 16, 17