MATH 335 lecture 14

Chris Camano: ccamano@sfsu.edu

October 13, 2022

Problem 1

Consider the following permutations in S_{15}:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{pmatrix}.$$

Compute σ^2, $\sigma\tau$, $\tau\sigma$, $\tau^2\sigma$, and $\sigma^{-1}\tau$.

1. Derivation of σ^2

   $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix}$$

   σ^2 is the effect of composing the permutation sigma on the identity two consecutive times, for elements of such a large group, it makes sense to consider the effect of manually tracing out the bijection, following the mappings of each corresponding element. The effect of applying sigma a single time is defined by the assignment of the permutation "matrix" above. So to identity the effect of a subsequent composition of this permutation we consider the re mapping of the result of applying sigma.

   $$\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 2 & 8 & 11 & 1 & 6 & 9 & 15 & 14 & 13 & 12 & 4 & 10 & 7 & 3 \end{pmatrix}$$

2. Derivation of $\sigma\tau$
   This composition is equivilant to:

   $$\sigma \circ \tau = \sigma(\tau(i)), i \in [1, 15]$$

   $$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 11 & 4 & 1 & 2 & 9 & 6 & 10 & 7 & 8 & 15 & 3 & 12 & 14 & 13 & 5 \end{pmatrix}$$

3. Derivation of $\tau\sigma$

   $$\tau \circ \sigma = \tau(\sigma(i)), i \in [1, 15]$$

   $$\tau \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix}$$

   $$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 9 & 13 & 1 & 3 & 6 & 7 & 10 & 2 & 14 & 5 & 15 & 12 & 8 & 11 \end{pmatrix}$$

4. Derivation of $\tau^2\sigma$
   We must first find τ^2 which is:

$$\tau \circ \tau = \tau(\tau(i)), i \in [1,15]$$

$$\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 15 & 3 & 9 & 7 & 6 & 12 & 8 & 13 & 10 & 11 & 5 & 2 & 14 & 4 \end{pmatrix}.$$

   Now for:

$$\tau^2 \circ \sigma = \tau^2(\sigma(i)), i \in [1,15]$$

$$\tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 15 & 4 & 14 & 10 & 6 & 5 & 3 & 9 & 1 & 12 & 13 & 7 & 11 & 8 \end{pmatrix}.$$

5. Derivation of $\sigma^{-1}\tau$
   We first define sigma inverse which is the inverse bijection found by manually mapping points back to the identity:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 2 & 8 & 9 & 13 & 6 & 11 & 15 & 12 & 5 & 14 & 7 & 1 & 4 & 3 \end{pmatrix}$$

   now we have that:

$$\sigma^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 12 & 5 & 2 & 7 & 6 & 13 & 14 & 3 & 8 & 15 & 11 & 9 & 10 & 1 \end{pmatrix}$$

Problem 2

Here I will introduce a concept that we will take up very soon. Let G be group and let $g \in G$ be an element of the group. The *order* of g, denoted by $|g|$, is the smallest positive number n such that $g^n = e$. If there is no such n, we say that g has infinite order.

a) In any group, what is $|e|$?
   If the order of an element of a group is the smallest positive number n such that that element composed n times equals the identity then the order of the identity element should always be 1.

b) Compute the order of the elements in $\mathbb{Z}_6$.
   First let us list the elements of $\mathbb{Z}_6$:

$$\mathbb{Z}_6 = \{[0],[1],[2],[3],[4],[5]\}$$

   Here the identity element $[0]$ is of order 1 by (a)

$$|[1]| : [1]+[1]+[1]+[1]+[1]+[1] = [6] \mod 6 = [0] \therefore |[1]| = 6$$

$$|[2]| : [2]+[2]+[2] = [6] \mod 6 = [0] \therefore |[2]| = 3$$

$$|[3]| : [3]+[3] = [6] \mod 6 = [0] \therefore [3] = 2$$

$$|[4]| : [4]+[4]+[4] = [12] \mod 6 = [0] \therefore |[4]| = 3$$

$$|[5]| : [5]+[5]+[5]+[5]+[5]+[5] = [30] \mod 6 = [0] \therefore |[5]| = 6$$

c) Compute the order of the elements in $U(9)$.

$$U_9 = \{[1],[2],[4],[5],[7],[8]\}$$

$$|[1]| = 1 \text{by}(a)$$

$$|[2]| : 2^k \equiv 1 \mod 9, k = 6 \therefore |[2]| = 6$$

$$|[4]| : 4^k \equiv 1 \mod 9, k = 3 \therefore |[4]| = 3$$

$$|[5]| : 5^k \equiv 1 \mod 9, k = 6 \therefore |[5]| = 6$$

$$|[7]| : 7^k \equiv 1 \mod 9, k = 3 \therefore |[7]| = 3$$

$$|[8]| : 9^k \equiv 1 \mod 9, k = 2 \therefore |[8]| = 2$$

d) Compute the order of the elements in S_3.

$$S_3 = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}$$

$$\left|\begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix}\right| = 1 \text{ by a}$$
$$\left|\begin{bmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{bmatrix}\right| = 2$$
$$\left|\begin{bmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{bmatrix}\right| = 2$$
$$\left|\begin{bmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{bmatrix}\right| = 2$$
$$\left|\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{bmatrix}\right| = 3$$
$$\left|\begin{bmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{bmatrix}\right| = 3$$

For the second and third and fourth elements of S_3 we obtain an order of two since these permutations represent reflection about a fixed vertex two applications of the function return to identity. The last two elements have order 3 since they represent shifting the elements by one index and it would three compositions to return to the identity.

e) Find an element of GL_2 that has infinite order. Justify your choice. Consider the matrix:

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$$

This matrix is an element of GL2 since it has a determinant of 1 of meaning that for all compositions since $det(A) > 0$ by invertible matrix theorem the matrix is invertible and thus an element of GL2, however note the property that:

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}^n = \begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}$$

as shown in class, so we will never return to the identity meaning that this element has infinte order.

f) Find an element of order 6 in S_5. To find an element of order 6 in S_5 this is to ask which element of S_5 requires 6 compositions with itself to return to the identity element. Given that we have 5 elements we can imagine this problem as a pentagon and moving from vertex to vertex. Clearly the two rotation elements would then have order of 5 since it would require 5 compositions of a single vertex movement to arrive back at the identity. Fixing vertices and reflecting would give order 2 so we are forced to consider which symmetry has the desired property. Consider the following element of S_5:

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}$$

Then we can trace the effect of composig ρ with itself to check whether or not its order is satisfactory:

$$\rho = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{bmatrix}$$
$$\rho^2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$$
$$\rho^3 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{bmatrix}$$
$$\rho^4 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$$
$$\rho^5 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{bmatrix}$$
$$\rho^6 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$

Thus element ρ from S_5 has order 6.

Proof. □

Problem 3

We showed that S_3 is a non-abelian group since we identified two particular elements σ and τ in S_3 such that $\sigma\tau \neq \tau\sigma$. Prove that S_n is non-abelian for all $n \geq 3$. [use σ and τ !]

Proof. Any symmetry group S_n should have elements sigma in tau within them when you fix the values of $n \geq 3$ this is to say that

$$\forall S_n \quad \sigma_n = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 1 & \cdots & n \end{pmatrix} \in S_n$$

Fixing the values afterwards. Because a similar argument can be made for tau:

$$\forall S_n \quad \sigma_n = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix} \in S_n$$

this implies that for any $S_n, n \geq 3$ we have the inclusion of two non commutative elements which then implies that the group as a whole is not abelian. From this observation we conclude that any symmetry group is non abelian by the existence of non commutative elements under the operation of function composition within the set.

□

Problem 4

Exercise 2 in Section 3.5 of our textbook.
Which of the following multiplciation tables defined on the set G=$\{a,b,c,d\}$ form a group? Support your answer in each case.

1. a
   This table cannot be a group since there is not a row and column that read abcd. This row/col is equivilant to composition with the group operator over the identity element. Since there is not a row with this property it cannot be the case that there is an identity element meaning a is not a group/
2. b
   element a is the identity, this multiplication table is associative, ie symmetric meaning associativity is satisifed, every element has another element who once composed returns to a, meaning that every element has an inverse. We have satisifed the properties of a group and thus b is a group.
3. c
   element a is the identity
   the multiplication table is symmetric ie the group operator is associative
   for b,c,d there exist an element who when composed returns a meaning there is an inverse for all elements.
   Thus This is a group
4. d
   note that $b \circ c = b$ but that $c \circ b = c$ meaning the operator is not associative so this cannot be a group.

Problem 5

Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Q}^*$ (i.e. the group of nonzero rational numbers under multiplication).

Proof. To show that H is a subgroup we can check whether or not for some $a,b \in H \quad ab^{-1} \in H$ by the proof provided in class on 10/11/22.
If a,b are in H then we know :

$$a = 2^k, b = 2^l : \quad k,l \in \mathbb{Z}$$

The inverse under multiplication is the element that returns a given element to the multiplicitive identity, in this case 1 or 2^0 so for $b = 2^l$ the inverse is simply $b^{-1} = 2^{-l}$ since we are allowed rationals. Then:

$$ab^{-1} = 2^k 2^{-l} = 2^{k-l}$$
$$\forall k,l \in \mathbb{Z} \quad k-l \in \mathbb{Z}$$

meaning that the resulting element is an element of H. Thus we have proven that H is a subgroup of $\mathbb{Q}^*$ since we have shown that for any element in the nonempty subset of $\mathbb{Q}^*$, H that for any two elements a and b $ab^{-1} \in H$ □

Problem 6

Let n be any positive integer and let $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ be the set of all integer multiples of n. Show that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Proof. Let a,b be elements of $n\mathbb{Z}$ then

$$a = nk \quad b = nl$$

We need to show that $ab^{-1} \in n\mathbb{Z}$. Note that for the integers our group operation is addition so we need to first identity the inverse of b with respect to addition as our operator. that is to say solve:

$$nl + b^{-1} = 0$$

Since all enteries of $n\mathbb{Z}$ are multiples of n we can really confine our analysis to the integer being multipied by n to see that the inverse of b is:

$$b^{-1} = -nl$$

as $-nl + nl = 0$ we now show that the composition of a and b inverse is in $n\mathbb{Z}$ as follows:

$$nk - nl = n(k-l), \quad \forall k,l \in \mathbb{Z}, k-l \in \mathbb{Z}$$

so we have shown that the composition of a selected element a and the inverse of a selected element b is an element of the subset $n\mathbb{Z}$ since the resulting term is an integer scaled by n. Thus we conclude that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ □

Problem 7

Prove that the following set of matrices

$$\left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x,y,z \in \mathbb{R} \right\}$$

is a subgroup of GL_3.

Proof. GL3 is the group of invertible three by three matrices. We can leverage properties of the invertible matrix theorem here and investigate the determinant. We will need to this prior to the verification of whether or not this a subgroup because we will need an inverse for the subgroup proof. The determinant of a 3x3 matrix can be found as follows:

$$\det\left(\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\right) = a\det\left(\begin{bmatrix} e & f \\ h & i \end{bmatrix}\right) - b\det\left(\begin{bmatrix} d & f \\ g & i \end{bmatrix}\right) + c\det\left(\begin{bmatrix} d & e \\ g & h \end{bmatrix}\right)$$

in our context this gives:

$$\det\left(\begin{bmatrix}1 & x & y\\ 0 & 1 & z\\ 0 & 0 & 1\end{bmatrix}\right) = \det\left(\begin{bmatrix}1 & z\\ 0 & 1\end{bmatrix}\right) - x\det\left(\begin{bmatrix}0 & z\\ 0 & 1\end{bmatrix}\right) + y\det\left(\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\right)$$

$$\det\left(\begin{bmatrix}1 & x & y\\ 0 & 1 & z\\ 0 & 0 & 1\end{bmatrix}\right) = 1 - 0 + 0$$

so we have shown then that any matrix in this set is invertible and at the very least our set is a subset of GL_3. We now prove subgroup:

let a and b be elements of our set such that.

$$a = \begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix} : a,b,c \in \mathbb{R} \quad b = \begin{pmatrix}1 & x & y\\ 0 & 1 & z\\ 0 & 0 & 1\end{pmatrix} : x,y,z \in \mathbb{R}$$

then to find b inverse we can derive an expression by computing the cofactor matrix and transposing since we have shown that determinant is simply 1. Instead of listing all determinants in the cofactor matrix though I will only really express the non zero ones during the construction of b^{-1} for brevity:

$$b^{-1} = \begin{bmatrix} \left|\begin{bmatrix}1 & z\\ 0 & 1\end{bmatrix}\right| & 0 & 0\\ -\left|\begin{bmatrix}x & y\\ 0 & 1\end{bmatrix}\right| & \left|\begin{bmatrix}1 & y\\ 0 & 1\end{bmatrix}\right| & 0\\ \left|\begin{bmatrix}x & y\\ 1 & z\end{bmatrix}\right| & -\left|\begin{bmatrix}1 & y\\ 0 & z\end{bmatrix}\right| & \left|\begin{bmatrix}1 & 0\\ x & 1\end{bmatrix}\right| \end{bmatrix}^T = \begin{bmatrix}1 & 0 & 0\\ -x & 1 & 0\\ xz-y & -z & 1\end{bmatrix}^T = \begin{bmatrix}1 & -x & xz-y\\ 0 & 1 & -z\\ 0 & 0 & 1\end{bmatrix}$$

$$ab^{-1} = \begin{bmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & -x & xz-y\\ 0 & 1 & -z\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & a-x & -y-az+b+xz\\ 0 & 1 & c-z\\ 0 & 0 & 1\end{bmatrix} \in \left\{\begin{pmatrix}1 & x & y\\ 0 & 1 & z\\ 0 & 0 & 1\end{pmatrix} : x,y,z \in \mathbb{R}\right\}$$

so we have shown that for any two elements from the set that the outcome of composing the first element with the inverse of the second under the group operation is also an element of the set implying that this set forms a subgroup of GL_3 $\square$