MATH 335 Midterm 2

Chris Camano: ccamano@sfsu.edu

November 3, 2022

Question 1.a

Let $H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \neq 0 \right\}$ be the subset of upper-triangular matrices in GL_2. Show that H is a subgroup.

Proof.
To show that H is a subgroup of GL2 we will satisfy the properties of a subgroup as follows:

1. **Product**
   let $A_1, A_2 \in H$
   $$A_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \quad A_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$$
   $$\left(\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \right) = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix} \in H$$
2. **Identity**
   The identity element is the matrix in H where b=0,a=c=1:
   $$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
3. **Inverses**
   Let h be an element of H then h is of the form :
   $$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$
   The inverse of h can be computed as follows:
   $$h^{-1} = \frac{1}{ac} \begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} = \begin{bmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix}$$
   Which is an element of H. Thus we have shown that $\forall h \in H, h^{-1} \in H$

Since we have proven the properties of a subgroup for H we conclude that H is a subgroup of GL_2 □

Question 1.b

Let G be an abelian group. Prove that $\{g \in G : |g| \text{ is finite}\}$ is a subgroup of G. Give an example where this set is not a subgroup in the case when G is non-abelian. [Hint: Question 5 in Homework 6]

Proof.
Let:

$$H = \{g \in G : |g| \text{ is finite}\}$$

1. **Product**
   let $a, b \in H$ then both elements have finite order meaning:

   $$|a| = n \quad |b| = m$$

   the product of a and b is is the following:

   $$ab^{mn}$$

   but since G is abelian we can distribute these exponents as follows:

   $$a^{mn}b^{mn} = (a^n)^m(b^m)^n = e^m e^n = e$$

   Thus the order of ab is at maximum am, it could be for example something smaller but we have demonstrated the order must be finite So it is an element of H.

Identity
The identity of G has an order of 1 thus it is an element of H since its order is finite.

Inverses
Let $h \in H$ then $|h| = n \rightarrow h^n = e$

$$\begin{aligned}
&h^n = e \\
&h^n h^{-1} = h^{-1} \\
&(h^n h^{-1})^n = (h^{-1})^n \\
&(eh^{-1})^n = (h^{-1})^n \\
&eh^{-n} = (h^{-1})^n \\
&h^n h^{-n} = (h^{-1})^n \\
&e = (h^{-1})^n
\end{aligned}$$

So we have shown that the order of any inverse must be finite and thus for a given element h in H the inverse is also an element of H

□

Proof.
'Give an example where this set is not a subgroup in the case when G is non-abelian.

Let G be GL_2 then H contains the matrices

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

Note that:

$$|A| = 4 \quad |B| = 3$$

but that

$$|AB| = \infty$$

as

$$AB = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

and

$$< AB > = \left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}, k \in \mathbb{Z}^- \right\}$$

□

Question 2

Show that $U(2^n)$ is not a cyclic group for any $n \geq 3$. [Hint: find two distinct subgroups of order 2; remember that in a cyclic group of order m there is a *unique* subgroup of order d for each divisor d of m]

Proof.
Suppose for the sake of contradiction that $U(2^n)$ is in fact cyclic for $n \geq 3$ then we know the order of the group is :

$$\phi(2^n) = 2^{n-1}$$

In a cylic group of order m there is a unique subgroup of order d for each divisor d of m. Here this is to say that for each divisor of 2^n there should be a unique subgroup of order k where $k|2^n$. The divisors of 2^n are:

$$1, 2, 2^2, ..., 2^n$$

So if we can identify two distinct subgroups of order 2 then we can prove that n is not a cylic group.
The smallest case this should hold is the case of $2^3 = 8$

$$U(8) = \{[1], [3], [5], [7]\}$$

Note here that all elements except [1] have order 2! In general it appears that the equivilance class of

$$[2^n - 1]$$

Since:

$$\begin{aligned} &(2^n - 1)^2 \\ &= (2^n)^2 - 2(2^n) + 1 \\ &= 1 \mod 2^n = [1] \end{aligned}$$

will always have an order of 2. Likewise taking element:

$$[2^{n-1}+1]$$

Will also have order 2 since:

$$\begin{aligned}&(2^{n-1}+1)^2\\&=\frac{2^n}{4}+2^n+1\\&=1 \mod 2^n=[1]\end{aligned}$$

So we have shown that there are two identical subgroups in the unit group for values of n greater than or equal to 3 thus we conclude that the group is not cyclic as the subgroup of order 2 is not unique. □

Question 3

Let $G=\langle a\rangle$ be a cyclic group of order n and fix an integer k such that $\gcd(k,n)=1$. Consider the function $\psi: G\longrightarrow G$ where $\psi(g)=g^k$. Show that this function is a bijection (i.e. both surjective and injective).

Proof.
Injectivity
To demonstrate injectivity we need to show that: $\psi(a)=\psi(b)$ implies a=b. Since G is cylic all subgroups are cylic as well, so for $g_1,g_2\in G$ we know that a and be are some power of the generator of G

$$g_1=a^i \quad g_2=a^j$$

So :

$$\begin{aligned}&\psi(g_1)=\psi(g_2)\\&\psi(a^i)=\psi(a^j)\\&a^{ik}=a^{jk}\\&g_1^k=g_2^k\\&g_1=g_2\end{aligned}$$

So we have shown injectivity
Surjectivity
To demonstrate Surjectivity we need to show that all elements domain are mapped somewhere in the codomain. Okay so let $g_1\in G$ then we know that since G is cylic with generator a that $g_1=a^i$ for some interger i.$\psi(a^i)=a^{ik}$ Which is guarenteed to be an element of G which happens to be our codomain. Thus we are finished since we have shown there is a surjective relationship under the map ψ □

Question 4.a

Using Lagrange's Theorem list the possible orders of the elements in S_4. Prove that there is no element of order 6 in S_4. Can you answer this *without* enumerating all elements in S_4 and computing their orders?

Proof.
Firstly, S_4 is the set of all bijections regarding four elements. Lagrange's theorem allows us to conclude that the order of any group element divides the order of the original group. Recall that the symmetry group's order is really counting the number of permutations thus the order of the total group is 4!=24. The "possible orders" of the elements of S_4 are then 1,2,3,4,6,8,12,24.
To show there is no element with order 6 we can take a moment to reflect on the nature of S_4. Chapter 5 gives us the tools of cycle notation which state that a cycle of length k generates a set of order k (page 76). Theorem 5.9 says that every permuatiton in Sn can be written as the product of disjoint cycles. This theorem combined with the example on page 79 lead me to the conclusion that the order of a cycle is equal to the the size of the cycle. Since we only have four elements we cant form an order six element with the product of two smaller cycles since the prime decomposition of 6 implies we would need a subcycle of order 3 and a disjoint subcycle of order 2(possible misuse of the word subcycle here) but if we start with a choice of a two cycle we cant form the needed 4 cycle. Then finally we cant just make an order 6 cycle by permuting only 4 elements. So its impossible to form an order 6 element in S$_4$. □

Question 4.b

Let H and K be two subgroups of a group G and g belongs to G. Show that $g(H \cap K) = gH \cap gK$.

Proof.

Suppose x$\in gH \cap gK$, This is to say that $x \in gH$ and $x \in gK$
if x is an element of gK then x=gk , $k \in K$
if x is an element of gH then x=gh , $h \in H$

$$gk = gh = x$$

So x is some element g times an element that is in both H and K which implies:

$$x \in g(H \cap K)$$

So.

$$gH \cap gK \subset g(H \cap K)$$

Suppose that $x \in g(H \cap K)$ Then by definition x=gy,$y \in (H \cap K)$.
Note though that by the definition of set intersection of $y \in (H \cap K)$ implies $y \in H$ and $y \in K$ so gy$\in gH$ and gy$\in gK \rightarrow gH \cap gK$
This implies

$$x \in g(H \cap K) \subset gH \cap gK$$

Thus we have proven set equivilancy by bidirectional set inclusion. □

Question 5

Let G be a group and H and K be subgroups of G. Suppose $[G:H]=m$ and $[G:K]=n$. Prove that $[G:H\cap K]\leq mn$. [Note that we are not assumining that G, H, or K are finite groups].

Proof.
Since we are not assuming that the groups are finite we cannot use Lagranges theorem to leverage properties about the divisibility of the order of G.

The question can be rephrased as: If there are m left distinct left cosets of H in G and n left cosets of K in G prove that that the number of distinct left cosets of $H\cap K$ is less than or equal to mn intuitivley lets think about what this means, Since H and K are never fully disjoint due to the presence of the identity element we know that the number of distinct left cosets of their intersection is at minimum 1.

$$1\leq[G:H\cap K]\leq mn$$

Since we know that the number of distinct left cosets of H and of K are finite then this implies that the number of distinct left cosets of their intersection is inturn finite as well. Other observations. We know that the m left cosets of H in G partition G and so do the n left cosets of K in G. This being said we can interpret the problem as well in the following way:

$$[G:H\cap K]\leq[G:H][G:K]$$

Giving us:

$$[G:H\cap K]\leq[G:H][H:H\cap K]$$

from this we get that $m|[G:H\cap K]$

$$[G:H\cap K]\leq[G:K][K:H\cap K]$$

from this we get that $n|[G:H\cap K]$

If you have two numbers that divide another number the case where their product divides that same number is when they are relativley prime thus : The case where

$$[G:H\cap K]=[G:H][H:H\cap K]$$

Occurs when the number of distinct cosets of H and the number of distinct Cosets of K are relatively prime. so we have proven that it is possible for $[G:H\cap K]=[G:H][H:H\cap K]$ as this happens when m and n are relativley prime. Now we must show that it is possible for $[G:H\cap K]<[G:H][H:H\cap K]$ This occurs when we have less intersections then the maximum which is when the index of H and K are relativley prime. If they are not relativley prime then the index of the intesection would be smaller giving us the other part of the inequality.

□