colorlinks=true, linkcolor=blue, filecolor=blue, citecolor = black, urlcolor=blue,

MATH 335 Homework 6

Chris Camano:ccamano@sfsu.edu

Question 1

Show that $\mathbb{Q}$ (under addition) is not a cyclic group. [Hint: Suppose it is cyclic, i.e., $\mathbb{Q} = \langle \frac{a}{b} \rangle$]

Proof. Suppose this group is cyclic and lets call it G, i.e., $\mathbb{Q} = \langle \frac{a}{b} \rangle$. Then this implies that there exists integers a and b such that:

$$< \frac{a}{b} >= G$$

where a and b are non zero.

the definition of a generator for a cyclic group is chracterized by the following:

$$< a >= \{a^k, k \in \mathbb{Z}\}$$

Where exponentiation here implies composition over the group operator.
Given this definition we are attempting to say that there exists a rational number acting as a generator for the entirrety of $\mathbb{Q}$ is akin to arguing that :

$$\mathbb{Q} = \{..., \frac{a}{b}, (\frac{a}{b})^2, ...\}$$

However note that here since our group operation picking an arbitrary rational number generates the set:

$$< \frac{a}{b} >= \{..., \frac{a}{b}, \frac{2a}{b}, ..\} = \{\frac{ka}{b}, k \in \mathbb{Z}\}$$

Meaning that the set generated by our selected element would only generate multiples of the generator. This neglects the infinte rational numbers in between multiples of a rational number take for example the case of: $\frac{3a}{2b}$ this value is an element of $\mathbb{Q}$ however it is not an element of $< \frac{a}{b} >$ meaning : $\mathbb{Q} \neq < \frac{a}{b} >$ thus we have shown that $\mathbb{Q}$ is not a cyclic group by contradiction.

addendum: This is equivilant to saying that there does not exist an integer multiple k of our selected rational number $\frac{a}{b}$ such that: $\frac{ka}{b} = \frac{3a}{2b}$ since this implies n $= \frac{3}{2}$ which is not an integer. □

Question 2

List all of the elements in each of the following subgroups.

a) The subgroup of $\mathbb{Z}$ generated by 7.

b) The subgroup of $\mathbb{Z}_{24}$ generated by [15].

c) All subgroups of $\mathbb{Z}_{12}$.

d) The subgroup of $U(20)$ generated by 3.

a) The subgroup of $\mathbb{Z}$ generated by 7.

$$<7>=\{7k, k\in\mathbb{Z}\}$$

b) The subgroup of $\mathbb{Z}_{24}$ generated by [15].

$$<[15]>=\{[0],[3],[6],[9],[12],[15],[18],[21]\}$$

We can find these values by solving the set of linear congruences of the form:

$$15x \equiv k \mod 24, k\in[0,24]$$

Those with solutions are part of the subgroup.

c) All subgroups of $\mathbb{Z}_{12}$. $\phi(12)=4$ the four realtively prime numbers with 12 are 5,7,11,1 meaning those are not subgroups since they just generate $\mathbb{Z}_{12}$ now from the remaining values $\{0,2,3,4,6,8,9,10\}$

$$\{<[0]>,<[1]>,<[2]>,<[3]>,<[4]>,<[6]>,\}$$

Note here we exclude $[10],[9],[8]$ since these are equal to $[2],[3],[4]$ respectivley.

d) The subgroup of $U(20)$ generated by 3. First begin with $U(20)=\{1,3,7,9,11,13,17,19\}$

$$<3>=\{3,9,7,1\}$$

note here that under a modular base of 20 these are the only possible solutions given successive powers of 3.

Question 3

Find the subgroups of GL_2 generated by each of the following matrices.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1/3 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

1. $\left\langle \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

2. $\left\langle \begin{bmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

3. $\left\langle \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

4. $\left\langle \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}, k \in \mathbb{Z}^- \right\} \cup \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

Here my thinking for the last matrix is the effect of exponentiating 0 times gives back the identity.

Question 4

Find all elements of finite order in each of the following groups: $\mathbb{Z}$, $\mathbb{Q}^*$, $\mathbb{R}^*$.

Proof. For all elements in $\mathbb{Z}$ each one has infinite order since under addition composition will increment to the next integer multiple of a selected element. The one exception to this, is simply the identity meaning that 0 is the only element of $\mathbb{Z}$ with finite order having order 1

The group $\mathbb{Q}^*$ is the group of all rationals under multiplication without zero included . This group of course has the identity element with order 1, identity here being 1.
The only other element with finite order is the value -1 which has order of 2. Every other rational when composed with itself will either grow to infinity when the rational is greater than 1 or progressivley grow smaller when the rational is less than one.

For the group $\mathbb{R}^*$ the set of reals under multiplication we will observe a reflection of the behavior of $\mathbb{Q}^*$ with the only elements of finite order being 1 and -1 with order 1 and 2 respectivley. □

Question 5

Let G be an abelian group and let a and b two elements in G such that $|a| = n$ and $|b| = m$. Show that $|ab| \leq \text{lcm}(n,m)$. This shows that in an abelian group the order of the product of two elements of finite order is finite. However, this is not true in a nonabelian group. For instance, consider GL_2 and let

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

Show that A and B have finite order but AB has infinite order

Show that $|ab| \leq \text{lcm}(n,m)$.

Proof. We wish to first show the case of equality

$$ab^{\text{lcm}(n,m)} = e$$

we know that since this is an abelian group that:

$$ab^{\text{lcm}(n,m)} = a^{\text{lcm}(n,m)} b^{\text{lcm}(n,m)}$$

which is really all the same as saying:

$$a^{\text{lcm}(|a|,|b|)}b^{\text{lcm}(|a|,|b|)}$$

In either cases lcm($|a|$,$|b|$) is a multiple of both $|a|$ and $|b|$ meaning that :

$$|a||(lcm(|a|,|b|)) \quad |b||(lcm(|a|,|b|))$$

by definition of lcm. This then gives:

$$lcm|a|,|b|) = |a|k, k \in \mathbb{Z}$$

$$lcm(|a|,|b|) = |b|l, l \in \mathbb{Z}$$

so we have:

$$a^{\text{lcm}(|a|,|b|)}b^{\text{lcm}(|a|,|b|)} = a^{|a|k}b^{|b|l} = (a^{|a|})^k(b^{|b|})^l = e^k e^l = e$$

This ultimatley is a short lemma that:

$$(ab)^{lcm(|a|,|b|)} = e$$

meaning that the order of $|ab|$ is at most $lcm(|a|,|b|)$ in other words:

$$|ab||lcm(|a|,|b|)$$

Note here that it could still be the case that there exists some integer u less than $lcm(|a|,|b|)$ such that :

$$(ab)^u = e$$

Under what circumstances is this true? When could the least common multiple of the order of the two terms be larger than the smallest k that returns us back to the identity? Consider selecting two elements from an abelian group as follows:

$$a = g \in G \quad b = g^{-1} \in G$$

Here

$$|g| = |g^{-1}| = n > 1$$

$$lcm(|g|,|g^{-1}|) = n$$

but for :

$$|gg^{-1}| = |e| = 1$$

So we have a case where $|ab| < lcm(|a|,|b|)$ Together this means that: Given an abelian group $|ab| \leq lcm(|a|,|b|)$ □

Show that A and B have finite order but AB has infinite order.

Proof. $|A|$:

$$< A >= \left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

$|A|$=3
$|B|$:

$$< B >= \left\{ \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

$|B| = 2$
$|AB|$:

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

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

$|AB| = \infty$ □

Question 6

Prove that in a group G an element g and its inverse g^{-1} have the same order [treat the two cases of finite order and infinite order separately].

Case 1: Infinite order

Proof. Suppose that a given element g in G has infinite order. We are then tasked with demonstrating that the inverse is also of infinite order. This is equivilant to demonstrating that the inverse's order cannot be finite. Suppose for the sake of contradiction that the order of g inverse is finite. This is to say that:

$$(g^{-1})^n = e$$

for some integer n. By associativity we can re arrange the exponent giving:

$$(g^n)^{-1} = e$$

This argument states that the inverse of g^n is the identity would only occur in the event that $g^n = e$ but this contradicts the notion that the order of g is infinite proving our property that the inverse must also be of infinite order by contradiction.

□

Case2: Finite order:

Proof. for some element $g \in G$ if the order of g is finite let this value be referred to as n. This implies:

$$g^n = e$$

By definition of order. Consider the following:

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

thus we have shown that $e = (g^{-1})^n$ meaning g^{-1} is of order n as desired. □

Question 7

Show that in a group $|x| = |g^{-1}xg|$ for any elements x and g. Deduce that in any group $|ab| = |ba|$.

Proof. Let x,g be elements of a group G:
Suppose that x and g have finite order as follows:

$$|x| = n, |g| = m$$

then by extension:

$$x^n = e \quad g^m = e \quad x^n = g^m$$

We wish to show that the order of x is equal to the order of the product of g inverse x g:

$$|x| = |g^{-1}xg|$$

Note by the previous proof that the order of g inverse is also n.
Suppose $|x| = |g^{-1}xg|$ then this implies that :

$$(g^{-1}xg)^n = e$$

since:

$$(g^{-1}xg)^n = (g^{-1}xg) \circ (g^{-1}xg) \circ \ldots \circ (g^{-1}xg)$$

note that for each composition the term of g will cancel out the following g inverse leading to only the first g inverse and last g being preserved. This successive composition increments the exponent of n each time leading to:

$$(g^{-1}xg)^n = g^{-1}x^n g = g^{-1}eg = g^{-1}g = e$$

we have then shown that when $|x| = n$ that $|g^{-1}xg| = n$ proving our argument for the case of finite order

Claim: If $|x|$ is infinite so is $|g^{-1}xg|$

Suppose for the sake of contradiction that: that $|x|$ is infinite and $|g^{-1}xg|$ is finite
This implies that $(g^{-1}xg)^n = e$ for some integer n, However note that $(g^{-1}xg)^n = g^{-1}x^n g$

$$\begin{aligned} &g^{-1}x^n g = e \\ &x^n g = g \\ &x^n = gg^{-1} \\ &x^n = e \end{aligned}$$

Which contradicts our assumption that the order of x is infinite, proving that $|g^{-1}xg|$ must have infinite order by contradiction □

From this proof we can deduce that in any group $|ab| = |ba|$ by constructing one of our elements to resemble that of our earlier proof. Consider the following: Given that:

$$(ab)^n = e$$

Given this fact we wish to show that:

$$(ba)^n = e$$

Below demonstrates how to use our first statement to show this:

$$(ba)^n = b(ab)^{n-1}a$$

Since we can regroup the terms being composed through associativity:

$$\begin{aligned} &b(ab)^{n-1}a \\ &b(ab)^{-1}a \\ &bb^{-1}a^{-1}a \\ &e \end{aligned}$$

So we have shown that by extension : $|ab| = |ba|$

Question 8

Let G be a group and let $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$. In other words $Z(G)$ consists of those elements which commute with every element of G. Show that $Z(G)$ is a subgroup of G.

Proof. let $g_1 \in Z(G), g_2 \in Z(G)$ then this implies g_1 and g_2 commute with all elements of G by def of Z(G). This is to say that:

$$g_1g = gg_1 \quad g_2g = gg_2$$

For some other g ∈ G
Associtivity can be proven rather straight forwardly as follows: $g_1g_2(g) = g_1(g)g_2 = gg_1g_2 = g(g_1g_2)$ leveraging the properties of g_1 and g_2 given by inclusion in Z(G).

We now consider the existence of the identity element in Z(G). If the identity element is in Z(G) this is an argument that the identity element is commutative for all g in G. Of course we know this to be true since composition over the identity is commutative.
To conclude we must now show the existence of inverses for all elements in Z(G). let $g_1 \in Z(G), g \in G$

$$g_1g = gg_1$$

left multiplying by the inverse gives:

$$g_1^{-1}g_1g = g_1^{-1}gg_1 \rightarrow g = g_1^{-1}gg_1$$

right multiplying by the inverse then gives:

$$gg_1^{-1} = g_1^{-1}gg_1g_1^{-1} \mapsto gg_1^{-1} = g_1^{-1}g$$

Which shows that all elements of Z(G) have an inverse in Z(G) as well.

We have shown the properties of a subgroup therefore we conclude that Z(G) is a subgroup of G. □