Math 113 **Fall 2015**

Homework #4

Nikhil Unni

1. This problem deals with subgroups of $GL(2, \mathbb{R})$.

   (a) Prove that the set

   $$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R}) : a, b, c, d \in \mathbb{Z} \right\}$$

   is NOT a subgroup of $GL(2, \mathbb{R})$.

   We can disprove by example. Say we have two matrices from H:

   $$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 5 \end{pmatrix}$$

   which are both invertible (both $ad - bc$ are nonzero) and have integer values for every cell.
   Subgroups have the condition where for all $a, b \in H$, ab^{-1} must be in H as well. Given A and B above in H:

   $$AB^{-1} = \begin{pmatrix} \frac{5}{4} & \frac{-1}{4} \\ 1 & 0 \end{pmatrix}$$

   And because AB^{-1} has noninteger cell values, it is not in H, therefore showing that H is not a subgroup of $GL(2, \mathbb{R})$.

   (b) Find an infinite subset of the set H defined in part (a) which is a cyclic subgroup of $GL(2, \mathbb{R})$.

   Let our cyclic subgroup generator be :

   $$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

   Where the inverse is:

   $$A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

   I'll prove that any $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for all $n \in \mathbb{Z}$.

Base Case : for $n = 0$ this is true, since this is just the identity matrix.

$$A^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Recursive Case : Assume the inductive hypothesis (that the integer maps to "b" in the matrix):

$$A^{n-1} = \begin{pmatrix} 1 & n-1 \\ 0 & 1 \end{pmatrix}$$

Then by simple matrix multiplication we see:

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

and

$$A^{n-2} = \begin{pmatrix} 1 & n-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n-2 \\ 0 & 1 \end{pmatrix}$$

Which proves the inductive hypothesis for all $\mathbb{Z}$ (since we can exponentiate forwards or backwards inductively from 0). A generates an infinite subset of H (all A^n are invertible since $ad - bc = 1$, and all cells are in $\mathbb{Z}$). Also, for all A,B in our generated subgroup:

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

And since integer addition and subtraction are closed, every AB^{-1} is also in the subgroup, proving that it's a valid subgroup of H.

(c) Find an infinite subset of H which is a noncyclic subgroup of $GL(2, \mathbb{R})$.

Matrices of the form:

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL(2, \mathbb{R}) : a, b, d \in \mathbb{Z}, ad = \pm 1 \right\}$$

This is a special case of H, as it constrains all 4 elements. But as we can see, it's closed under multiplication:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} m & n \\ 0 & q \end{pmatrix} = \begin{pmatrix} am & an + bq \\ 0 & dq \end{pmatrix}$$

$$(am)(dq) = (ad)(mq) = \pm 1$$

We can also clearly see that the identity element is just the identity matrix, which is also of the same form. And because $ad - bc$ for all matrices in M is nonzero (because it is a subset of invertible matrices, all matrices in M must be invertible as well), every matrix in M has a multiplicative inverse:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \frac{1}{\pm 1} \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}^{-1}$$

And we get matrix multiplication associativity for free. So it is a valid subgroup of $GL(2, \mathbb{R})$. We can also prove by example that it's noncyclic. Since noncyclic subgroups are also commutative (because addition of exponents is commutative), we can just show that our subgroup is noncommutative:

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}$$

So our subgroup is noncyclic.

2. Here we will think about products of groups.

   (a) Prove that if G and H are groups, then $G \times H$, with a componentwise binary operation is a group.

   First we show that $G \times H$ is closed under the componentwise binary operation. For two $a = (g_1, h_1), b = (g_2, h_2) \in G \times H$: $ab = (g_1 g_2, h_1 h_2)$. Since G and H are groups, all $g_1 g_2$ are in G, and all $h_1 h_2$ are in H, so all ab are in $G \times H$.

   Next we show that every element has an identity by which it can multiply with to yield our identity, (e_g, e_h), the tuple of G and H's identities:

   $$ab = (g_1 g_2, h_1 h_2)$$

   Then

   $$(ab)(ab)^{-1} = (g_1 g_2, h_1 h_2)((g_1 g_2)^{-1}, (h_1 h_2)^{-1}) = (e_g, e_h)$$

   Because G and H are groups, then all $g_1 g_2$ and $h_1 h_2$ multiplied by their repsective inverse yields the identity of the group. And the tuple of the identites (which is our new group's identity) is in $G \times H$.

   Next, we can show that any element multiplied by our new identity yields itself:
   $a = (g, h), e = (e_g, e_h)$, so ae should be a.

   $$(g, h)(e_g, e_h) = (ge_g, he_h) = (g, h)$$

Since any element in G multiplied by e_g yields itself, and any element in H multiplied by e_h yields itself, this formulation is correct.

Finally, we have to show associativity, that, for some $a = (g_1, h_1), b = (g_2, h_2), c = (g_3, h_3) \in G \times H$:

$$(ab)c = a(bc)$$

$$(ab)c = (g_1g_2, h_1h_2)(g_3, h_3) = ((g_1g_2)g_3, (h_1h_2)h_3)$$
$$a(bc) = (g_1, h_1)(g_2g_3, h_2h_3) = (g_1(g_2g_3), h_1(h_2h_3))$$

Because binary operations on G and H are both associative, these two end up being the same:

$$(g_1g_2g_3, h_1h_2h_3)$$

proving associativity for the componentwise binary operation on $G \times H$.

(b) Consider the example $\mathbb{C}^* \times \mathbb{C}^*$. Find two subgroups of order 8 in $\mathbb{C}^* \times \mathbb{C}^*$ – one which is cyclic and one which is not.

1. Let our first cyclic subgroup be $U_1 \times U_8$, where the identity is $(1, 1)$, and the generator is $(1, e^{2pi(1/8)})$. The generator generates all 8 elements $(1, e^{2pi(n/8)})$, for $0 \geq n < 7$. And for any $a, b \in U_1 \times U_8$,

$$ab^{-1} = (1, e^{2pi(n/8)})(1, e^{2pi(-m/8)}) = (1, e^{2pi(n-m/8)})$$

which is still in our subgroup.

2. Let our second noncyclic subgroup be $U_2 \times U_4$. We can see that the order of the subgroup is 8, since the order of U_2 and U_4 are 2 and 4 respectively. It is also a valid subgroup of $\mathbb{C}^* \times \mathbb{C}^*$, since for any $a, b \in U_2 \times U_4$:

$$ab^{-1} = (e^{2pi(n/2)}, e^{2pi(m/4)})(e^{2pi(-p/2)}, e^{2pi(-q/4)}) = (e^{2pi(n-p/2)}, e^{2pi(m-q/4)})$$

which is still in our subgroup. We can show that nothing can generate all 8 elements by running through each element and its order:
$(e^{2pi(0/2)}, e^{2pi(0/4)})$, order 1
$(e^{2pi(0/2)}, e^{2pi(1/4)})$, order 4
$(e^{2pi(0/2)}, e^{2pi(2/4)})$, order 2
$(e^{2pi(0/2)}, e^{2pi(3/4)})$, order 4
$(e^{2pi(1/2)}, e^{2pi(0/4)})$, order 2
$(e^{2pi(1/2)}, e^{2pi(1/4)})$, order 4
$(e^{2pi(1/2)}, e^{2pi(2/4)})$, order 2

$(e^{2pi(1/2)}, e^{2pi(3/4)})$, order 4

Since none of the possible elements have order 8, none of them can serve as a generator, meaning that the group is noncyclic.

3. This problem is about cyclic groups and generators.

   (a) Find two choices of n so that Z_n has exactly 4 different generators. Justify your answer.

   1. For n = 5, we can show that our only generators are $\bar{1}, \bar{4}, \bar{2}, \bar{3}$ exhaustively:

   $\bar{0}$, order 1
   $\bar{1}$, order 5
   $\bar{2} \to \{\bar{2}, \bar{4}, \bar{1}, \bar{3}, \bar{0}\}$, order 5
   $\bar{3} \to \{\bar{3}, \bar{1}, \bar{4}, \bar{2}, \bar{0}\}$, order 5
   $\bar{4}$, order 5

   2. For n = 8, we can show that our only generators are $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ exhaustively:

   $\bar{0}$, order 1
   $\bar{1}$, order 8
   $\bar{2}$, order 4
   $\bar{3}, \to \{\bar{3}, \bar{6}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}, \bar{0}\}$, order 8
   $\bar{4}$, order 2
   $\bar{5}, \to \{\bar{5}, \bar{2}, \bar{7}, \bar{4}, \bar{1}, \bar{6}, \bar{3}, \bar{0}\}$, order 8
   $\bar{6}, \to \{\bar{6}, \bar{4}, \bar{2}, \bar{0}$, order 4
   $\bar{7}$, order 8

   (b) Which of the following groups are cyclic groups?

   1. $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic, and is generated by $(\bar{1}, \bar{1})$.

   In order it will generate :

   $$\{(\bar{1}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{2}), (\bar{0}, \bar{0})\}$$

   2. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is noncyclic. Because $\mathbb{Z}_2 \times \mathbb{Z}_4$ is isomorphic to $U_2 \times U_4$, it's the same problem as asking if $U_2 \times U_4$ is cyclic or not. And I already solved this exhaustively on problem 2b. Since $U_2 \times U_4$ is noncyclic, that means $\mathbb{Z}_2 \times \mathbb{Z}_4$ is noncyclic as well.