Math 103A Fall 2012 Exam 1

October 22, 2012

NAME: Solutions

Problem 1 /10	
Problem 2 /10	
Problem 3 /10	
Problem 4 /15	
Total /45	

Problem 1 (10 points)

(1a) (5 pts) Let G be a group and let $a, b, c \in G$. Prove, using only the group axioms, that if $ab = ac$, then $b = c$. (This is the left cancellation law as stated in the text. You are being asked to reproduce the proof of that law.)

By the axioms of a group, a has an inverse a^{-1} with the property that $aa^{-1} = a^{-1}a = e$, where e is the identity element of the group. Multiplying the equation $ab = ac$ on the left by a^{-1}, we get

$$a^{-1}(ab) = a^{-1}(ac).$$

Now by the associativity axiom of a group, this is the same as

$$(a^{-1}a)b = (a^{-1}a)c$$

and so we conclude that $eb = ec$. By the defining property of the identity element e, we now have $b = eb = ec = c$.

(1b) (5 pts). Let G be a finite group. Consider the Cayley table of the group. Recall that the Cayley table has rows and columns indexed by the elements in G, and that the product $g_1 g_2$ is written in the intersection of row g_1 and column g_2 of the table.

Prove that any fixed row of the Cayley table contains every element of the group, each appearing exactly once.

If the row is headed by the element a, and the column headings are $g_1, g_2, \ldots, g_n$ in that order, then the elements in row a are $ag_1, ag_2, \ldots, ag_n$ in that order. By the definition of the Cayley table, the column headings $g_1, \ldots, g_n$ should be a list of the elements of the group, each exactly once.

Now if two different entries in this row are the same, say $ag_i = ag_j$, for two different columns (so $g_i \neq g_j$), then by left cancellation we get $g_i = g_j$, a contradiction. So all of the entries in the row are different.

Now the entries in the row consist of n distinct elements from a finite set G with n elements, and this can only happen if every element of G occurs in the row exactly once.

(Alternatively, one can prove directly that any particular $b \in G$ appears in the row, by looking in the column g_i where $g_i = a^{-1}b$; then $ag_i = aa^{-1}b = b$.)

Problem 2 (10 points)

(2a) (5 pts) Complete the following the Cayley table of the group D_4 of symmetries of the square. Show your work. Remember that R_θ means counterclockwise rotation by θ. Which reflections S_1, S_2, S_3, S_4 correspond to which axes of symmetry of the square is marked in the following diagram: (*on the exam, the diagram indicated that S_1 was reflection about the horizontal axis, S_2 reflection about the vertical axis, S_3 reflection about the diagonal from top left to bottom right, and S_4 reflection about the diagonal from bottom left to top right.*)

	R_0	R_{90}	R_{180}	R_{270}	S_1	S_2	S_3	S_4
R_0	R_0	R_{90}	R_{180}	R_{270}	S_1	S_2	S_3	S_4
R_{90}	R_{90}	R_{180}	R_{270}	R_0	S_4	S_3	S_1	S_2
R_{180}	R_{180}	R_{270}	R_0	R_{90}	S_2	S_1	S_4	S_3
R_{270}	R_{270}	R_0	R_{90}	R_{180}	S_3	S_4	S_2	S_1
S_1	S_1	S_3	S_2	S_4	R_0	R_{180}	$\mathbf{R_{90}}$	$\mathbf{R_{270}}$
S_2	S_2	S_4	S_1	S_3	R_{180}	R_0	$\mathbf{R_{270}}$	$\mathbf{R_{90}}$
S_3	S_3	S_2	S_4	S_1	$\mathbf{R_{270}}$	$\mathbf{R_{90}}$	R_0	R_{180}
S_4	S_4	S_1	S_3	S_2	$\mathbf{R_{90}}$	$\mathbf{R_{270}}$	R_{180}	R_0

The filled-in entries are given above in bold.

To justify your answer, you are allowed to use the fact that every row (and every column) of the table contains each element of G exactly once. Even so, you must do at least two direct calculations, one from each missing square. For example, it suffices to calculate directly that $S_3S_1 = R_{270}$ and $S_1S_3 = R_{90}$. You should have shown your work for those calculations by drawing pictures, but I will not draw any on the solutions here.

(2b) (5 pts) Find, with justification, the center of the group D_4.

The center is $Z(D_4) = \{R_0, R_{180}\}$.

Recall that by definition, $Z(G) = \{x \in G | ax = xa \text{ for all } a \in G\}$. Now note that we can interpret the equation $ax = xa$ for all $a \in G$ as follows: looking at column x and row x of the Cayley table, as we travel across row x and down column x, we get the elements of G in the same order. (This depends on the fact that the rows and columns are labeled in the same order, which we should always do.) From the Cayley table in the previous problem, we see that this happens when x is one of the two elements R_0 or R_{180}, and not for any other x.

Problem 3 (10 points)

(a) (10 pts) Let $G = \mathrm{GL}(2, \mathbb{R})$ be the group of all 2×2 matrices with real entries and nonzero determinant, with the operation of multiplication.

Let $H = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| a \in \mathbb{R} \right\}$.

(i) Prove that H is a subgroup of G.

(ii) Is the group H Abelian? Why or why not?

(i). We use the two-step subgroup test. To be truly careful, we should check that $H \neq \emptyset$; but that is obvious in this case.

H is closed under products: for any $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ in H, so $a, b \in \mathbb{R}$, we have

$$AB = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}.$$

Since $a + b \in \mathbb{R}$ also, the product AB is also in H.

H is closed under inverses: for any $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, its inverse in G is equal to $A^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix}$. Since $-a \in \mathbb{R}$ again, $A^{-1} \in H$.

(One way to find the inverse is to remember the formula that if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $A^{-1} = \frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. In this case, you can also find it easily by writing $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and finding what w, x, y, z have to be to make that happen.)

(ii). Taking two arbitrary elements $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ in H as above, we calculate that

$$AB = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b+a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = BA.$$

So H is Abelian.

Problem 3 (15 points)

Consider the group $U(15)$, the units group of integers modulo 15 under multiplication. You are given that $U(15) = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$.

(a) (5 pts). Find the orders of the elements [2], [7], and [11] in this group. Write down two different cyclic subgroups H of $U(15)$ such that $|H| = 4$.

Since $[2]^1 = [2], [2]^2 = [4], [2]^3 = [8], [2]^4 = [16] = [1]$, we have $|[2]| = 4$.

Since $[7]^1 = [7], [7]^2 = [49] = [4], [7]^3 = [4][7] = [28] = [13], [7]^4 = [13][7] = [-2][7] = [-14] = [1]$, we have $|[7]| = 4$.

Since $[11]^1 = [11], [11]^2 = [-4]^2 = [16] = [1]$, we have $|[11]| = 2$.

Since [2] and [7] both have order 4 as elements, the cyclic subgroups they generate also have order 4. So $H_1 = \langle [2] \rangle = \{[1], [2], [4], [8]\}$ and $H_2 = \langle [7] \rangle = \{[1], [7], [4], [13]\}$ are two (obviously different) cyclic subgroups of order 4.

(b) (5 pts) Is $U(15)$ a cyclic group? Justify your answer.

$U(15)$ is not cyclic.

The nicest way to do this (which only a few people noticed) is to quote the theorems on cyclic groups. If G is a cyclic group of order n, then we proved that G has precisely one subgroup of order d, for each positive d dividing n. But $U(15)$ has two different subgroups of order 4, by part (a). So it cannot be cyclic.

Alternatively, you can show directly that $\langle [a] \rangle \neq U(15)$, for all possible $[a] \in U(15)$. In addition to the three already calculated in part (a), there are 5 more $[a]$ to check. (There are other shortcuts that you can use to avoid checking all five of these; for example, since in part (a) you saw that $[4] \in \langle [2] \rangle$, then $\langle [4] \rangle \subseteq \langle [2] \rangle$ and since $\langle [2] \rangle \neq U(15)$, one has $\langle [4] \rangle \neq U(15)$ also. But most people that succeeded on this part just grinded through the five calculations.)

(c) (5 pts) Find a subgroup H of $U(15)$ such that $|H| = 4$ but H is *not* cyclic. You must prove that your answer is a subgroup and that it is not cyclic.

The subgroup is $H = \{[1], [4], [11], [14]\}$. To check it is a subgroup, you can check it is closed under products directly by doing all possible products of pairs of elements (write out the Cayley table), and then check directly also that it is closed under inverses (calculate that $[4]^{-1} = [4]$, $[11]^{-1} = [11]$, $[14]^{-1} = [14]$. To prove H is not cyclic, you can see that the elements [4], [11], and [14] all have order 2 (and [1] has order 1), so H has no element of order 4 and so no generator.

(How would you guess the H above? Here are two possible ways you might have found it.

Way 1: First, if H is to be not cyclic, then H should have no element of order 4, because an element of order 4 will fill up all four elements of H with its powers and then will be a generator for H. However, if you calculate the order of all elements in $U(15)$, $[2], [7], [8], [13]$ all have order 4. So the four remaining elements of $U(15)$ must be the ones in H.

Way 2: You had a homework exercise that if a group G contains different elements a, b both of order 2, then G has a subgroup H of order 4. The solution to the exercise is to take $H = \{e, a, b, ab\}$. Applying this exercise here by taking any two elements of order 2 (for example $[4], [11]$), then you get an order 4 subgroup $H = \{[1], [4], [11], [44] = [14]\}$. It is less obvious maybe why you might have expected this construction to yield a non-cyclic group of order 4, but it does.)