MAT 301S - Problem Set 1

Due Wednesday, January 29, 2014

NOTE:

- Students are expected to write up problem sets independently. Please refer to the course information sheet for information about penalties for duplication of other students' solutions.
- Not all of the questions will be marked. Students will not know in advance which questions will be marked and are advised to hand in solutions to all of the questions.
- In order to receive full marks for computational questions, all details of the computation should be included in the solution. Even if the correct final answer is given, marks will be deducted if some details are left out.
- In solving questions involving proofs, *unless the question specifically lists which results may be used*, it is not necessary to reprove facts that have been proved in class, in the sections of the text that have been covered, or on previous problem sets.
- If m and n are integers and $n \geq 2$, then $m (\operatorname{mod} n)$ denotes the remainder after dividing m by n. (In particular, $0 \leq m (\operatorname{mod} n) \leq n-1$.)

1. Let $G = \{ (t, x) \mid t, x \in \mathbb{R},\ t \neq 0 \}$. For (t_1, x_1) and (t_2, x_2) in G, define

$$(t_1, x_1) * (t_2, x_2) = (t_1 t_2, t_1 x_2 + x_1/t_2).$$

   a) Prove that G is a group with respect to the operation $*$.

   b) Find all elements belonging to the centre $Z(G)$ of G. (*Note*: The centre of a group is defined in Chapter 3.)

2. Let $G = D_6$ (the dihedral group of order 12). Let r be a fixed rotation in G such that $|r| = 6$ and let s be a fixed reflection in G.

   a) Let H be the smallest subgroup of G that contains rs and sr^3. List all of the elements in H. (Please explain your answer.)

   b) Find an abelian subgroup H' of D_6 that contains exactly two reflections. (Be sure to list all of the elements of H' and show that H' is an abelian subgroup of D_6.)

3. Determine whether the subset H of the group G is a subgroup of G. If H is a subgroup of G determine whether H is abelian. If H is not a subgroup of G, find elements a and b in H such that ab^{-1} is not in H (be sure to explain why ab^{-1} is not in H).

   a) Let G be the group of functions from $\mathbb{Z}_{15}$ to $\mathbb{Z}_{15}$, under the operation $(f_1 * f_2)(m) = (f_1(m) + f_2(m)) (\operatorname{mod} 15)$, $m \in \mathbb{Z}_{15}$. (You do not need to prove that G is a group.) Let $H = \{ f \in G \mid f(m) \text{ is even for all } m \in \mathbb{Z}_{15} \}$.

b) Let $G = GL(2, \mathbb{R})$ and let $H = \{\ A = \begin{pmatrix} a+b & -2\,b \\ b & a-b \end{pmatrix} \in G \mid a^2 + b^2 = 1\ \}$.

c) Let G be the group of nonzero real numbers under multiplication and let $H = \{\, a + b\sqrt{2} \mid a,\, b \in \mathbb{Z},\ \text{at least one of } a \text{ and } b \text{ is nonzero.}\}$.

4. Let S be a subset of a group G. If $a \in G$, let $aSa^{-1} = \{\, asa^{-1} \mid s \in S\,\}$. (*Note*: Parts a) and b) are independent of each other.)

   a) Prove that S is a subgroup of G if and only if aSa^{-1} is a subgroup of G.

   b) Suppose that $G = D_n$ $(n \geq 3)$ and S is the set of all reflections in G. Prove that $aSa^{-1} = S$ for all $a \in G$.

5. Let $U(16) = \{\, 1, 3, 5, 7, 9, 11, 13, 15\,\}$. This is a group under the binary operation of multiplication modulo 16. That is, $m * n = mn (\text{mod}\, 16)$. (See the example in Chapter 2 where $U(n)$ is defined for each integer $n \geq 2$.)

   a) Find all elements in the cyclic subgroup $\langle 3 \rangle$.

   b) Find an element $m \in U(16)$ such that $|m| = 4$ and $|\langle m \rangle \cap \langle 3 \rangle| = 2$. Is m unique?

   c) Determine whether $U(16)$ is a cyclic group. (*Note*: There is a way to solve this part without computing the order of each element of the group.)

6. Let a and b be elements of a group G Assume that both a and b have finite order.

   a) Prove that if $ab = ba$ and $\gcd(a, b) = 1$, then $|ab| = |a||b|$.

   b) Find an example of elements a and b in a particular group G such that $a \neq e$, $b \neq e$, $\gcd(|a|, |b|) = 1$ and $|ab| = |a|$.

Note: If m and n are nonzero integers, then the *greatest common divisor* of m and n, written $\gcd(m, n)$ is the largest positive integer that divides both m and n. We say that m and n are *relatively prime* whenever $\gcd(m, n) = 1$.