Math 541 Spring 2011
Solutions—Homework#8— Orbits,Cosets, Lagrange's Theorem, Fermat's Little Theorem

Remark. Answers should be written in the following format:
0) Statement and/or Result.
i) Main points that will appear in your explanation or proof or computation.
ii) The actual explanation or proof or computation.

1. *Orbits.* Describe the set of orbits (=equivalence classes) $G\backslash X$ in the following cases:

   (a) The set $X = \mathbb{R}^2$, the group $G = SO(2)$ the rotations of the plane, and the action is the natural action, via action of a matrix on a vector.

      1. *Main points.* Geometric meaning.
      2. *Answer.* The geometric meaning of $SO(2)$ is rotations around the origin. So we have that $SO(2)\backslash\mathbb{R}^2 =$ the set of circles around the origin.

   (b) The set $X = \mathbb{R}^2 - \{0\}$, the group $G = \mathbb{R}^* = \mathbb{R} - \{0\}$, and action is the scaling action of G on X via $a \cdot (x, y) = (a \cdot x, a \cdot y)$.

      1. *Main points.* Lines.
      2. *Answer.* Since any line L, through the origin, in the plane is uniquely determined by a non-zero vector $0 \neq v \in L$, and any two such vectors differ by a multiple scalar $a \neq 0$, we deduce that $\mathbb{R}^*\backslash\ (\mathbb{R}^2 - \{0\}) =$ the set of lines in the plane. Mathematicians denote this space by $\mathbb{P}^1(\mathbb{R})$ and call it the 1−dimensional real projective space.

   (c) The set X is the collection of equilateral triangles around the origin in the plane $\mathbb{R}^2$, the group $G = SO(2)$, and the action is the natural one, induced from the action of rotations on the plane.

      1. *Main points.* Clear.
      2. *Answer.* It is clear that two triangles in the same orbit iff they are congruent.

2. *Cosets.* In each of the following compute the set of left cosets G/H, and if G is finite verify Lagrange's Theorem $\#G = [G : H] \cdot \#H$,where $[G : H] = \#(G/H)$, called the index of H in G.

   (a) $G = S_3$, $H = A_3$ the group of even permutations of three letters.

      1. *Main points.* Number of elements.
      2. *Computation.* We have $S_3 = Aut(\{a, b, c\})$. Since $\#S_3 = 6$, $\#A_3 = 3$, and $(a\ b) \notin A_3$, then $S_3 = A_3 \bigsqcup (a\ b) \cdot A_3$. So $S_3/A_3 = \{A_3, (a\ b) \cdot A_3\}$. And indeed, this agrees with Lagrange's theorem.

   (b) $G = S_n$, $H = A_n$.

1. *Main points.* The same as in the case of $n = 3$ above.
2. *Answer.* Change 3 to general n in the answer above for S_3/A_3.

(c) $G = D_3$, $H = C_3$, Where D_3 is the dihedral group of order 3 and C_3 is its subgroup (cyclic of order 3) of rotations.

1. *Main points.* Size.
2. *Answer.* We have $D_3/C_3 = \{C_3, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot C_3\}$.

(d) $G = \mathbb{R}$, $H = \mathbb{Z}$.

1. *Main points.* Direct calculation.
2. Answer. Any two points $x, y \in \mathbb{R}$, are in the same orbit iff $x - y \in \mathbb{Z}$, so we have $\mathbb{R}/\mathbb{Z} = [0, 1) = \{x \in \mathbb{R} |\ 0 \leq x < 1\}$.

(e) $G = O(2)$, $H = SO(2)$.

1. *Main points.* Determinant calculation.
2. *Answer.* Take $A \in O(2)$, with $\det(A) = -1$, then $\det(A \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}) = 1$, so $A \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in S0(2)$. This proves that $O(2) = SO(2) \bigsqcup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot SO(2)$. Hence, $O(2)/SO(2) = \{SO(2), \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot SO(2)\}$.

3. Fermat's little theorem. Let p be a prime number. Denote by $\mathbb{Z}_p^* = \{1, ..., p-1\}$.

(a) Show that $\mathbb{Z}_p^*$ is a groups with operation of multiplication modulo p.

1. *Main points.* Decomposition into prime numbers. Euclid algorithm.
2. Proof. We have
   1. Closure. Let $x, y \in \mathbb{Z}_p^*$. So p doesn't divides $x \cdot y$, which means that $x \cdot y$ is in $\mathbb{Z}_p^*$ modulo p.
   2. Inverse. Let $x \in \mathbb{Z}_p^*$. Then the greatest common deviser of x and p is 1. By Euclid algorithm there exist integers $a, b \in \mathbb{Z}$ with $ax + bp = 1$. In particular, $ax = 1$ modulo p.

(b) Show that for every element $x \in \mathbb{Z}_p^*$ we have $x^{p-1} = 1$ modulo p. Hint: Use Lagrange'sTheorem with the groups $G = \mathbb{Z}_p^*$, and $H =< x >$ the subgroup generated by x.

1. *Main points.* Lagrange's theorem.
2. *Proof.* By Lagrange's theorem $p-1 = k \cdot (\# < x >)$ for some integer d. From this we get
$$x^{p-1} = (x^{\#<x>})^k = 1^k = 1. \tag{1}$$

(c) Conclude with Fermat's little Theorem: For $x \in \mathbb{Z}_p$, we have $x^p = x \bmod(p)$.

1. Main points. Equation (1).
2. *Proof.* If $x = 0$ there is nothing to proof. If $x \in \mathbb{Z}_p^*$ this is what we got in equation (1).

Remarks • I will be happy to help you with any question related to these answers. Please visit me in my office hours.

Good Luck!