Math 541 Spring 2011
Solutions–Homework#7, Normal Subgroups, Lagrange's Theorem, Groups of Prime Order

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. *Normal subgroups.* Recall that a subgroup N of a group G is called <u>normal</u> if $g \cdot N \cdot g^{-1} = N$ for every $g \in G$. In this case we denote $N \lhd G$.

   (a) Show that if $\varphi : G \to H$ is an homomorphism of groups, then $N = \ker(\varphi) \lhd G$.

      1. *Main points.* Direct calculation.
      2. *Calculation.* Take $x \in N$, and compute

      $$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \overset{\substack{\varphi \text{ is hom} \\ x \in \ker(\varphi)}}{=} \varphi(g)\varphi(g)^{-1} = 1_H.$$

      So we have proved that $g \cdot N \cdot g^{-1} \subset N$. If $x \in N$, then the same argument $y = g^{-1}xg \in N$ so $x = gyg^{-1}$ i.e., $N \subset gNg^{-1}$.

   (b) Show that the group R of rotations of the plane is a normal subgroup of the group O of orthogonal transformation of $\mathbb{R}^2$.

      1. *Main points.* It is a kernel.
      2. *Proof.* The map $\det : O(2) \to \{\pm 1\}$ is an homomorphism with $\ker(\det) = SO(2) = R$.

   (c) Show that the group A_n of even permutations of $\{1, 2, ..., n\}$ is a normal subgroup S_n.

      1. *Main points.* Kernel.
      2. Proof. We have the homomorphism $sgn : S_n \to \{\pm 1\}$, with kernel $\ker(sgn) = A_n$.

   (d) Find all normal subgroups of S_3.

      1. *Main points.* Direct calculation.
      2. *Calculation.* Lagrange's theorem implies that the subgroups of $S_3 = Aut(\{a, b, c\})$ are of orders $6, 3, 2, 1$. A direct verification shows that they are S_3, $A_3 = \{(a\ b\ c), (a\ c\ b), id\}$, $\{(a\ b), id\}$, $\{(a\ c), id\}$, $\{(b\ c), id\}$, $\{id\}$. A direct calculation shows that the normal subgroups are $\{id\}$, A_3, S_3.

2. Lagrange's Theorem. Recall that if H is a subgroup of a group G, then $\#H$ divides $\#G$.

(a) What is the possible cardinality of subgroups of S_4.

1. *Main points.* Lagrange's theorem.
2. *Computation.* We have $\#S = 24$. The possibilities are $24, 12, 8, 6, 4, 3, 2, 1$.

(b) Can you find for each of the possibilities in (a), a subgroup $H \subset G$ with that cardinality?

1. *Main points.* Just direct verification.
2. *Answer. We have*

$\#G$	$G < S_4$
24	S_4
12	A_4
8	D_4
6	S_3
4	C_4
2	$\{(a\ b),\ id\}$
1	$\{id\}$

3. *Classification of all subgroups of prime order.* Let G be a groups of order (cardinality) $\#G = p$, where p is a prime number. Show that G is cyclic of order p. Use the following steps

(a) Choose a non-trivial element $1 \neq g \in G$, and consider the group $< g >= \{g^k;\ k \in \mathbb{Z}\}$. Show that $< g >= \{1, g, .., g^{d-1}\}$ where d is minimal integer > 0 such that $g^d = 1$. This d is called the order of g, denoted by $d = ord(g)$.

1. *Main points* (Proof of Tim). Euclid algorithm, and minimality of d.
2. *Proof.* By minimality of d all the elements in this set are different. If $g^i = g^j$, for some $0 \leq i < j \leq d-1$, then $g^{j-i} = 1$, contradict the minimality. We need to show that $< g >\subset \{1, g, .., g^{d-1}\}$. Indeed, for $n \in \mathbb{Z}$, write $n = qd + r$, with r integer with $0 \leq r < d$, so $g^n = (g^d)^q \cdot g^r = g^r$.

(b) Since by Lagrange's theorem we have $1 < \# < g > |\#G$, and $\#G = p$, we have that $< g >= G$.

Remark I will be happy to help with any question on these solutions. Please visit me in my office hours.

Good Luck!