CS203B, Assignment 3

Prof. Manindra Agarwal

August 2016

1. The Class Equation:
   In this exercise we will use the proof of Burnsides lemma to come up with a very famous equation called as class equation. Define $T(g_1, g_2)$, as group action of G onto G under conjugation, i.e. $T(g_1, g_2) = g_1 * g_2 * g_1^{-1}$. Also $\forall g \in G$ define $C(g) = \{h \in G | h \textit{ commutes with } g\}$. We call $C(g)$ to be a centralizer of g.

   (a) Prove that Centralizer of any element $g \in G$ is a subgroup of G.

   (b) Using the proof of Burnsides lemma prove that

   $$|G| = \sum_{g \in G} |G : C(g)|$$

   This equation is known as the class equation.

   (c) Using the class equation prove that a group of order p^k has more than one element in its center.

   (d) As a corollary of above prove that if $|G| = p^2$ then G is abelian.

2. Sylow's first Theorem.

   (a) Prove that if G is abelian and $p||G|$ where p is a prime number then it has an element of order p.

   (b) Prove that if N is normal in G then any subgroup of $\frac{G}{N}$ is of the form $\frac{H}{N}$ where H is a subgroup of G.

   (c) Now we will prove Sylow's first theorem using induction over $|G|$.

   Let p be a prime such that $p^k||G|$ then G has a subgroup of order p^k.

   Proof: If $|G| = 1$ then its trivial. Assume that this holds for all the groups of order $< |G|$. Now if we have a subgroup H of G such that $p^k||H|$ then we are done using induction hypothesis. Now suppose that this does not hold. Hence prove that following:

   i. p surely divides $|G : C(a)| \forall a \notin Z(G)$ and $|Z(G)|$.

   ii. Now use 2(a), 2(b) to construct a subgroup of order p^k.

   iii. Hence prove the theorem.

   (d) Hence or otherwise prove Cauchy's theorem:

If $p|Ord(G)$ then there is an element of order p in G.

3. This problem will show you the power of all the theory which we have developed throughout the assignments till now. We want to classify all the n's such that Z_n^* has all the elements of order 2. The answer to this problem will be really surprising. First surprise is that the set of all such n's is finite. Lets now try to prove this.

   (a) Prove that $\phi(n) = 2^k$ for all such n's.

   (b) Prove that $n = 3 * 2^l$ for all such n's.(You may like to use the fact $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \oplus \mathbb{Z}_n^*$ iff m and n are coprime).

   (c) Prove that $l \leq 3$ in the above part.

   (d) Hence conclude that the above happens iff $n|24$.

   P.S.: Don't waste your time over internet, you wont find anything (because I also did that fruitless job).

4. We found the units in $\mathbb{Z}[\sqrt(2)]$. Do the similar analysis for $\mathbb{Z}[\sqrt(m)]$ where m is square free integer.

5. A ring R is said to Integral Domain if $ab = 0$ implies $a = 0$ or $b = 0$, $\forall a, b \in R$. Prove that if R is an integral domain so is $R[X]$.