EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran

Indian Institute of Technology Bombay

Autumn 2010

Assignment 2 : **30 points** — **Due date**: August 17, 2010

Each of the following exercises is worth 3 points. Every nontrivial step in a proof should be accompanied by justification.

1. Prove that a subset H of a group G is a subgroup if it is nonempty, finite and closed under the group operation.
2. Give an example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.
3. Let H and K be subgroups of a group G. Prove that $H \cup K$ is a subgroup of G if and only if H is a subgroup of K or K is a subgroup of H.
4. Prove that if H and K are subgroups of a group G then so is their intersection $H \cap K$.
5. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.
6. Show that every subgroup of $\mathbb{Z}_n$ is cyclic.
7. If $\phi : G \rightarrow H$ is an isomorphism between groups G and H, show that $\phi(0_G) = 0_H$ where 0_G is the additive identity of G and 0_H is the additive identity of H
8. Show that all finite cyclic groups are isomorphic to $\mathbb{Z}_n$.
9. Show that all finite cyclic groups are abelian.
10. Let G be a group. Let $x \in G$ and $m, n \in \mathbb{Z}$. Prove that if $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = \gcd(m, n)$. Using this result, prove that if $x^m = 1$ for some $m \in \mathbb{Z}$, then the order of x divides m.