Computer Science & Engineering Department

IIT Kharagpur

Computational Number Theory: CS60094

Tutorial III

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1. Let $(G, \cdot, e)$ be a group and $H \subseteq G$ is finite, non-empty, and closed under the group operation.
   Show that H is a subgroup of G.

2. Let $(G, \cdot, e)$ be an *abelian group*. We define $G^m = \{a^m : a \in G\}$, where m is an integer ($a^0 = e$, $a^k = a \cdot a^{k-1}$, and $a^{-k} = (a^{-1})^k$, where k is a positive integer).
   Prove that G^m is a subgroup of G.

3. Let $(G, \cdot, e_G)$ and $(H, *, e_H)$ be two groups. A map $f : G \to H$ is called a *homomorphism* if it is compatible with with the operations i.e. $f(a \cdot b) = f(a) * f(b)$.
   Show that (i) $f(e_G) = e_H$, and (ii) $f(a^{-1}) = f(a)^{-1}$.

4. Let $(G, \cdot, e_G)$ and $(H, *, e_H)$ be two groups. The map $f : G \to H$ is a *homomorphism* and a *bijection*.
   Show that $f^{-1} : H \to G$ is also a *homomorphism*. [Note: a *bijective homomorphism* is called *isomorphism*]

5. An *isomorphism* from $(G, \cdot, e)$ to itself is called an *automorphism*.
   Give an automorphism on G other than identity or the one shown in (7) when the group is commutative.

6. Let $(G, \cdot, e)$ be a group and $Aut(G)$ be the collection of automorphisms on G.
   Prove that $(Aut(G), \circ, 1_G)$ is a group where '$\circ$' is function composition and 1_G is the identity map.

7. Let $(G, \cdot, e)$ be a group and $a \in G$. We define $f_a : G \to G$ as $f : b \mapsto a \cdot b \cdot a^{-1}$.
   Prove that f_a is an automorphism (*inner automorphism*) on G.

8. Let $(G, \cdot, e_G)$ and $(H, *, e_H)$ be two groups and the map $f : G \to H$ be a *homomorphism*. We define $Ker\ f = \{g \in G : f(g) = e_H\}$.
   Prove that $Ker\ f$ is a subgroup of G.

9. Let $(G, \cdot, e_G)$ and $(H, *, e_H)$ be two groups and the map $f : G \to H$ be a *homomorphism*.
Prove that for all $a \in G$ and $b \in Ker\ f$, $aba^{-1} \in Ker\ f$.

10. Let $(G, \cdot, e_G)$ and $(H, *, e_H)$ be two groups; the map $f : G \to H$ be a *homomorphism*.
(a) Let K be a subgroup of G. Is the homomorphic image of K, a subgroup of H?
(b) Let K be a subgroup of H. Is The homomorphic pre-image of K, a subgroup of G?