Fundamentals of Algebra for Computer Science (Home work 2)

October 26, 2006

- Due on Wednesday, November 8, before 4 p.m.
- Late submissions will not be accepted.
- Please give precise arguments for all statements that you write.
- To disprove a fact it is enough to give a counter example.
- Please do not hesitate to contact me if you do not understand the problems.
- Each problem in this homework bear 5 points.

1. An **Automorphism** of a group G is an isomorphism of G onto itself.
   (a) Let G be a group and $\mathcal{A}$ denote the set of all automorphisms of G. Show that $\mathcal{A}$ is a group.
   (b) Let G be a group. For $h \in G$ define $f_h : G \to G$ by $f_h(g) = hgh^{-1}$. Prove that f_h is an automorphism of G.
   (c) Let G be an abelian group. Prove that $f(g) = g^{-1}$ is an automorphism of G.
   (d) Let g be a generator of a cyclic group G and $f : G \to G$ be an automorphism. Show that $f(g)$ is also a generator of G.
2. **Direct products**: Let A, B be groups, then $A \times B = \{(a, b) : a \in A, b \in B\}$ is also a group under the operation defined as $(a_1, b_1)(a_2, b_2) = (a_1b_1, a_2, b_2)$.
   (a) Let $f_1 : G \to A$ and $f_2 : G \to B$ be two group homomorphisms. Let $f : G \to A \times B$ be defined by $f(g) = (f_1(g), f_2(g))$. Show that f is a group homomorphism.
   (b) Show that:
   $$ker(f) = ker(f_1) \cap ker(f_2)$$
3. **Cyclic groups**

(a) Prove that the subgroup of a cyclic group is always cyclic.

(b) Let G be a cyclic group of (finite) order n with a generator g. Show that G is isomorphic to $\mathbb{Z}_n$, by showing that the map $f : G \to \mathbb{Z}_n$ defined by $f(g^i) = i \bmod n$ is such an isomorphism.

(c) Let G be a cyclic group of infinite order, with a generator g. Show that G is isomorphic to $\mathbb{Z}$, by showing that the map $f : G \to \mathbb{Z}$ defined by $f(g^i) = i$ is such an isomorphism.

4. Let G be a finite group and H a subgroup pof G. For A, B subgroups of G, define A to be conjugate to B relative to H, if $B = x^{-1}Ax$ for some $x \in H$. Prove

(a) This defines an equivalence relation on the set of subgroups of G.

(b) The number of subgroups of G conjugate to A relative to H equals the index of $N(A) \cap H$ in H, where $N(A) = \{x \in G | xAx^{-1} = A\}$