Homework #1, to be submitted by Thursday, September, 3rd

1. Let A be a set and let $f : A \to A$ and $g : A \to A$ be mappings such that $f \circ g = id_A$ (where id_A is the identity mapping on A).
(a) Prove that f is surjective and g is injective
(b) Show by example that f need not be injective and f need not be surjective

2. (a) Let G be a group, and define the relation $\sim$ on G: $x \sim y$ if y is conjugate to x in G, that is, there exists $g \in G$ such that $y = gxg^{-1}$. Prove that $\sim$ is an equivalence relation.
(b) Let G be a group. An equivalence relation $\sim$ on G is called a **congruence** if for any $a, b, c, d \in G$ such that $a \sim b$ and $c \sim d$ we have $ac \sim bd$.
Now let H be a subgroup of G and define the relation $\sim_H$ on G by

$$a \sim_H b \iff a^{-1}b \in H.$$

Prove that $\sim_H$ is a congruence if and only if H is normal in G.

3. Let G be a group. (a) Define $\varphi : G \to G$ by $\varphi(g) = g^2$. Prove that φ is a homomorphism if and only if G is abelian.
(b) Assume that $x^2 = 1$ for any $x \in G$. Prove that G is abelian.

4. Find the minimal n for which the symmetric group S_n contains an element of order 15 (and explain why your n is indeed minimal). *Note:* All you need to know about S_n for this problem is stated in Section 1.3 of DF (pp.29-32).

5. Prove that an element $\bar{a} \in \mathbb{Z}_n$ is invertible if and only if $gcd(a, n) = 1$ where gcd is the greatest common divisor. You may use any standard theorem about integers (e.g. unique factorization), but do not use any theorems about $\mathbb{Z}_n$.
Hint: The forward direction is easy. For the opposite direction either use the theorem about representation of $gcd(a, n)$ as an integral linear combination of a and n or, alternatively, show that the mapping $\varphi_n : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\varphi_n(\bar{x}) = \bar{x}\bar{a}$ is injective whenever $gcd(a, n) = 1$.

6. (a) Prove that every finite group is finitely generated.
(b) Let $\mathbb{Q}$ be the group of rational numbers with addition. Prove that $\mathbb{Q}$ is not finitely generated.
(c) Prove that any finitely generated subgroup of $\mathbb{Q}$ is cyclic.

7. Let G be a group and H a subgroup of G. Let G/H (resp. $H\backslash G$) be the set of left (resp. right) cosets of H in G. Construct an explicit bijection between G/H and $H\backslash G$. **Remark:** This result explains why we can talk about the index $[G : H]$ of a subgroup H of G instead of talking about left and right indices.