Homework #1

Plan for next week: Group actions (§ 4.1-4.3).

Problems, to be submitted by Thursday, September 5th

1. Let G be a group.

(a) Define $\phi : G \to G$ by $\phi(g) = g^2$. 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.

2.

(a) Let G be a cyclic group of order $n < \infty$. Prove that if $k \in \mathbb{Z}$, then the mapping $\phi : G \to G$ defined by $\phi(x) = x^k$ is bijective if and only if k is relatively prime to n.
(b) Let G be an arbitrary finite group of order $n < \infty$. Prove that if $k \in \mathbb{Z}$ is relatively prime to n, then the mapping $\phi : G \to G$ defined by $\phi(x) = x^k$ is bijective. **Hint:** Use one of the corollaries of Lagrange theorem.

3. 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).

4. 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 $\phi_n : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\phi_n(\bar{x}) = \bar{x}\bar{a}$ is injective whenever $gcd(a, n) = 1$.

5. A group G is called *finitely generated* if there exists a finite subset S of G such that $\langle S \rangle = G$.

(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.

6. Let $G = D_8$, the dihedral group of order 8 (that is, the group of isometries of a square). Prove that $|[G,G]| = 2$ and describe $[G,G]$ explicitly without computing every single commutator.

Index of a subgroup. If G is a group and H is a subgroup of G, the index of H in G, denoted by $[G : H]$, is defined to be the cardinality of G/H, that is, the number of left cosets of H in G. It is not hard to show that the sets G/H (the set of left cosets of H) and $H \setminus G$ (the set of right cosets of H) always have the same cardinality, so there is no need to introduce "left index" and "right index".
The full statement of Lagrange theorem asserts that if G is a finite group and H is a subgroup of G, then $[G : H] = \frac{|G|}{|H|}$ (typically one applies not the full statement but its most useful consequence, namely, that the order of H divides the order of G).

7. Let G be a group and let H and K be subgroups of G of finite index (note that G is not assumed to be finite).

(a) Assume that $H \subseteq K$. Prove that $[G : H] = [G : K][K : H]$ (recall that $[A : B]$ denotes the index of a subgroup B in a group A).

(b) Let $m = [G : H]$ and $n = [G : K]$. Prove that $\text{LCM}(m, n) \leq [G : H \cap K] \leq mn$ (where LCM is the least common multiple).

Hint for (a): If A is a group and B a subgroup of A, a subset S of A is called a left transversal of B in A if S contains precisely one element from each left coset of B (an alternative name for a transversal is a system of left coset representatives). Let $\{g_1, \ldots, g_r\}$ be a left transversal of K in G and $\{k_1, \ldots, k_s\}$ a left transversal of H in K. Prove that $\{g_i k_j\}_{1\leq i\leq r, 1\leq j\leq s}$ is a left transversal for H in G. Recall that if B is a subgroup of a group G, then $xB = yB \iff x^{-1}y \in B$ for $x, y \in G$.

8. Let G be a group and H a subgroup of G.

(a) Prove directly from the definitions that the following two statements are equivalent:

(i) $gHg^{-1} = H$ for all $g \in G$

(ii) $gHg^{-1} \subseteq H$ for all $g \in G$

(b) Give an example of a group G, a subgroup H of G and an element $g \in G$ such that gHg^{-1} is a proper subgroup of H.