HW #3

1. Let H_i, $i \in I$, be a collection of subgroups of G. Prove that $\bigcap H_i$ is a subgroup of G. Is $\bigcup H_i$ a subgroup of G?

2. Let G be a group and W a subset of G. Show that $< W >= \{g \in G \mid \exists w_1, \ldots, w_r \in W,\, n_1, \ldots, n_r \in \mathbf{Z} \ni g = w_1^{n_1} \ldots w_r^{n_r}\}$.

3. Show if G is a group in which $(ab)^2 = a^2b^2$ for all $a, b \in G$ then G is abelian.

4. Determine all groups up to order 6.

5. Let p be a prime. Show that $F = \mathbf{Z}/p\mathbf{Z}$ is a *field* [i.e., in the commutative ring $\mathbf{Z}/p\mathbf{Z}$ every non-zero element has a multiplicative inverse]. Compute $|G|$ if $G = GL_n(F), SL_n(F), T_n(F), ST_n(F)$, or $D_n(F)$.
[Hint: First show that F is a *domain*, i.e., a commutative ring satisfying: if $ab = 0$ in F then $a = 0$ or $b = 0$. Then show that any domain with finitely many elements is a field.]

6.(*) Let $m_i > 1$, $1 \leq i \leq n$, be pairwise relatively prime integers. Let $m = m_1 \cdots m_n$. Let $\varphi(m)$ denote the order of the group $(\mathbf{Z}/m\mathbf{Z})^\times$. The function $\varphi : \mathbf{Z}^+ \to \mathbf{Z}^+$ is called the *Euler phi function.* [We let $\varphi(1) = 1$.] Show that there exists an isomorphism

$$(\mathbf{Z}/m\mathbf{Z})^\times \to (\mathbf{Z}/m_1\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/m_n\mathbf{Z})^\times.$$

In particular $\varphi(m) = \varphi(m_1) \cdots \varphi(m_n)$. Compute $\varphi(p^r)$ when p is a prime and r is a positive integer.

7.(*) Prove the Cyclic Subgroup Theorem which states: Let H be a subgroup of the cyclic group $G =< g >$. Let e be the identity of G. Let n be a positive integer. Then
   (i) $H = \{e\}$ or $H = < g^m >$ where $m \geq 1$ is the least integer such that $g^m \in H$. If G is infinite then H is infinite or $\{e\}$. If G is finite of order n then $m|n$.
   (ii) If $|G| = n$ and $m|n$ then $< g^m >$ is the unique subgroup of G of order $n/|m|$.
   (iii) If $|G| = n$ and $m \not| n$ then G does not have a subgroup of order m.
   (iv) If $|G| = n$ then the number of subgroups of G is equal to the number of divisors of $|G|$.
   (v) If G has prime order then the only subgroups of G are $\{e\}$ and G.

8.(*) Let G be an abelian group. Let $a, b \in G$ have finite order m, n, respectively. Suppose that m and n are relatively prime. Show that ab has order mn. Is this true if G is not abelian? Prove or give a counterexample.