Mathematics 110AH

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
$$\langle W \rangle =$$
$$\{g \in G \mid \exists w_1, \ldots, w_r \in W, \text{not necessarily distinct}, e_1, \ldots, e_r \in \{\pm 1\} \ni g = w_1^{e_1} \ldots w_r^{e_r}\}.$$
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. (You cannot use Lagrange's Theorem.)
5. Let p be a prime. Show that $F = \mathbf{Z}/p\mathbf{Z}$ is a *field* [i.e., in the commutative ring $\mathbb{Z}/p\mathbb{Z}$ every non-zero element has a multiplicative inverse]. Compute $|G|$ if $G =$
$$GL_n(F),\ SL_n(F),\ T_n(F),\ ST_n(F),\ \text{or } D_n(F).$$
[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 $m_i > 1$, $1 \le i \le n$, be pairwise relatively prime integers. Let $m = m_1 \cdots m_n$. Let $\phi(m)$ denote the order of the group $(\mathbb{Z}/m\mathbb{Z})^\times$. The function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is called the *Euler phi function*. [We let $\phi(1) = 1$.] Show that there exists an isomorphism
$$(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}^\times.$$
In particular $\phi(m) = \phi(m_1) \cdots \phi(m_n)$. Compute $\phi(p^r)$ 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 and n be a positive integer. Then
   - (i) $H = \{e\}$ or $H = < g^m >$ where $m \ge 1$ 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 $m \nmid n$, 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.