Name and UCLA ID:

Task 1: Read Sections 10 and 11.

Exercise 1: For all $i \in I$ an indexing set let H_i be a subgroup of G a group. Prove that $\bigcap_{i \in I} H_i$ is a subgroup of G. Is $\bigcup_{i\in I} H_i$ a subgroup of G?

Exercise 2: Let G be a group and W a subset of G. Show that:

$$\langle W \rangle = \{g \in G \mid \exists\, w_1, \ldots, w_r \in W \text{ and } n_1, \ldots, n_r \in \mathbb{Z} \text{ with } g = w_1^{n_1} \cdots w_t^{n_r}\}.$$

Note that the $w_1, \ldots, w_r \in W$ need not be distinct.

Exercise 3: Let G be a group in which $(ab)^2 = a^2b^2$ for all $a, b \in G$. Show that G is abelian.

Exercise 4: Determine all groups up to order 6.

Exercise 5: Let p be a prime. Show that $F = \mathbb{Z}/p\mathbb{Z}$ is a field, namely that every non-zero element in the commutative ring $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. Compute $|G|$ for $G = \mathrm{GL}_n(F)$, $\mathrm{SL}_n(F)$, $\mathrm{T}_n(F)$, $\mathrm{ST}_n(F)$, $\mathrm{D}_n(F)$. Hint: You can first show that F is a domain, namely a commutative ring satisfying that if $ab = 0$ for $a, b \in F$, then $a = 0$ or $b = 0$. You can then show that any domain with finitely many elements is a field.

Exercise 6: Let $m_i \in \mathbb{Z}$, $m_i > 1$, for $i = 1, \ldots, n$, be pairwise relatively prime integers. Let $m = m_1 \cdots m_n$. Let $\varphi(m)$ denote the order of the group $(\mathbb{Z}/m\mathbb{Z})^\times$, recall that by setting $\varphi(1) = 1$ the function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is called the Euler phi function. Show that there exists an isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})^\times$. In particular, we have $\varphi(m) = \varphi(m_1)\cdots\varphi(m_n)$. Compute $\varphi(p^r)$ for p prime and $r \in \mathbb{Z}^+$.

Exercise 7: Prove the Cyclic Subgroup Theorem, that is, let H be a subgroup of the cyclic group $g = \langle g \rangle$, let e be the identity of G, and let $n \in \mathbb{Z}^+$, then prove that:

1. $H = \{e\}$ or $H = \langle g^m \rangle$ where $m \geq 1$ is the least integer such that $g^m \in H$. If G is infinite then $H = \{e\}$ or H is infinite. If G is finite of order n then m divides n.
2. If $|G| = n$ and $m \in \mathbb{Z}$ divides n then $\langle g^m \rangle$ is the unique subgroup of G of order $n/|m|$.
3. If $|G| = n$ and $m \in \mathbb{Z}$ does not divides n then G does not have a subgroup of order m.
4. If $|G| = n$ and then the number of subgroups of G is equal to the number of divisors of $|G|$.
5. If $|G| = p$ prime then the only subgroups of G are $\{e\}$ and G.

Exercise 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 your claim or give a counterexample.

Exercise 9: Let $n_1, \ldots, n_r \in \mathbb{Z}^+$, set $n = n_1 + \cdots + n_r$. Use Lagrange's Theorem to prove that $\binom{n}{n_1, \ldots, n_r} = \frac{n!}{n_1! \cdots n_r!}$ is an integer.