- **Read:** §6, §9, and §10 through the first paragraph of p. 93 (we will not discuss the remaining content about the "class equation").
- **Suggestion:** Work (or think about) the following problems. Problems marked with a $*$ have answers given at the back of the book.
  - §6 : 1*, 2*
  - §9 : 1*, 7*
  - §10 : 1*, 8, 15

1. Let G, H be groups. Suppose that A is a subgroup of G, and B is a subgroup of H. Prove that $A \times B$ is a subgroup of $G \times H$.
2. Suppose that G, H are groups such that $G \times H$ is cyclic. Prove that G and H are both cyclic.
3. (a) Let G, H be groups. Show that $G \times H$ is abelian if and only if both G and H are abelian.
   (b) Construct a nonablian group of order 16, and one of order 24.
4. Find all subgroups of the group $\mathbb{Z}_2 \times \mathbb{Z}_4$.
5. Suppose that G is a group. Show that if H and K are two subgroups of G such that $(|H|, |K|) = 1$, then $H \cap K = \{e\}$.
6. Let p and q be distinct prime numbers, and suppose that G is a group of order pq.
   (a) Prove that all proper subgroups of G are cyclic (a "proper subgroup" is a subgroup not equal to all of G).
   (b) Give an example to show that G itself need not be cyclic.
7. Suppose that g and h are elements of a group G, such that the following two conditions hold.
   - $gh = hg$ (i.e. "g and h commute").
   - $\langle g \rangle \cap \langle h \rangle = \{e\}$.

   Prove that $o(gh)$ is the least common multiple of $o(g)$ and $o(h)$.

   Hint: try a similar approach to the solution to problem 6 on Problem Set 2, or to problem 1(b) of Problem Set 4. Theorem 6.1(i) in the text is also similar. In fact, the result in this problem can be used to prove each of these three results.
8. Consider the group D_4 (defined with the notation on page 75). Find the right-cosets of the subgroup H in D_4, for:
   (a) $H = \langle f \rangle$,
   (b) $H = \langle f^2 g \rangle$.
9. Let H be a subgroup of a group G. Define a relation ${}_H\equiv$ on G as follows.

$$x \,{}_H\!\equiv y \;\Leftrightarrow x^{-1}y \in H$$

   (Note that this is not exactly the same as the relation $\equiv_H$ defined in the text and in class, although they are equivalent if G is abelian.)

(a) Show that ${}_H\equiv$ is an equivalence relation on G.

(b) Show that the equivalence classes under ${}_H\equiv$ are the left cosets of H in G.

(c) Give an example of a group G and subgroup H to demonstrate that ${}_H\equiv$ is not always the same relation as $\equiv_H$.

10. Suppose that G is a group of order n, and k is an integer such that $(k, n) = 1$.

(a) Prove that there exists an integer ℓ such that for all $g \in G$, $(g^k)^\ell = g$.

(b) Deduce from (a) that the function $f : G \to G$ defined by $f(g) = g^k$ is bijective, and give an explicit description of its inverse function.

(c) Deduce that if G is a finite group of odd order, then every element of G has a unique "square root" (i.e. for every $g \in G$, there exists a unique $h \in G$ such that $h^2 = g$).

Note: One way to phrase this fact is that it is possible to compute unique "kth roots" in a group G, assuming that k is relatively prime to $|G|$. This fact has an important application in the design of the commonly-used RSA cryptosystem.