- **Read:** §16.
- **Suggestion:** Work (or think about) the following problems. Problems marked with a $*$ have answers given at the back of the book.
  - §16 : $2*, 4*, 11*$

1. Let $\operatorname{Aut} G$ denote the set of all automorphisms of a group G, and let $\circ$ denote composition of functions (recall that an automorphism is an isomorphism from a group to itself). Prove that $(\operatorname{Aut} G, \circ)$ is a group. This is called the *automorphism group* of the group G.

2. Let R be a ring with 1_R (ring with unity). Prove that $(-1_R) \cdot a = -a$. Recall: $-a$ denotes the additive inverse of a.

3. Let K denote the set of all real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. Prove that K forms a field, when equippied with the usual addition and multiplication from $\mathbb{R}$.

4. Call an element a of a ring R *idempotent* if $a^2 = a$ (in a ring, a^2 is shorthand for $a \cdot a$). Call a ring *Boolean* if every element is idempotent. Prove that if R is a Boolean ring, then
   (a) for all $a \in R$, $a + a = 0_R$, and
   (b) R is commutative.

   Hint for (a): consider the expression $(r + r)^2$.

5. Prove that in the trivial ring (ring with one element), 0_R is a unit, but that in any other ring it is not a unit. (This shows that for a ring R, $(R, \cdot)$ is never a group, except when R is the trivial ring.)

6. (a) List the elements of the unit group $\mathbb{Z}_{20}^\times$ of the ring $\mathbb{Z}_{20}$.
   (b) Find the inverse and the order of each element in $\mathbb{Z}_{20}^\times$.
   (c) (Bonus, for extra credit) Prove that $\mathbb{Z}_{20}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

7. Let F be a field. Use the notation $\frac{a}{b}$ to denote ab^{-1}, for any $a, b \in F$ with $b \neq 0_F$. Prove that for any $a, b, c, d \in F$ with $b, d \neq 0_F$, the usual addition formula for frations holds:
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

8. Suppose that F is a field with four elements, labeled $\{0, 1, a, b\}$ (here $0 = 0_F$ is the additive identity and $1 = 1_F$ is the multiplicative identity). Fill out the following charts to determine the addition table and multiplication table for F. In your submission, it is not necessary to write a full formal proof that your answer is the only way to do it, but briefly summarize (in a paragraph or so) how you found the tables.

$+$	0	1	a	b
0				
1				
a				
b				

$\cdot$	0	1	a	b
0				
1				
a				
b				

Suggestion: There are many ways to proceed, so just try things out and don't be afraid of a little trial and error. A good way to start is to fill out as much as you can using basic properties of 1 and 0. After that, remember that $F^\times$ is a group, and note that the distributive property will force your hand in a number of places.

9. Let G be a cyclic group of order n. Problem 3 on the previous problem set showed a particular way to construct some automorphisms of G. The purpose of the problem is to show that we have in fact constructed all of them.

   (a) Prove that if $\phi : G \to G$ is *any* automorphism of G, then there exists an integer k such that $\phi(g) = g^k$ for all $g \in G$.

   (b) Prove that if ϕ and k are as in part a, then $(k, n) = 1$. (Ask me for a hint if you are stuck.)

   (c) (Bonus; for extra credit) Prove that $\operatorname{Aut} G \cong \mathbb{Z}_n^\times$ (the unit group of the ring $\mathbb{Z}_n$).