- **Read:** §17.
- **Suggestion:** Work (or think about) the following problems. Problems marked with a $*$ have answers given at the back of the book.
  - §16 : $1*, 2*, 6*$

1. Let R be a nontrival ring with unity.
   (a) Prove that there are at least two distinct elements $x \in R$ satisfying the equation
   $$x^2 = 5x - 6 \cdot 1_R.$$
   (Follow the same method as the discussion in class of the equation $x^2 = x + 2 \cdot 1_R$.)
   (b) Prove that if R is an integral domain, then there are *exactly* two solutions $x \in R$.
   (c) Give an example of a ring R with unity in which there are more than two solutions to this equation.

2. Suppose that R is a commutative ring with unity, and that R has a *finite* number of elements.
   (a) Prove that if $a \in R$ is not a zero-divisor, then a is a unit (recall from class that this is *not* true for all rings; this is a special feature of finite rings).
   (b) Deduce from part (a) that a finite integral domain is necessarily a field.
   Note: Part (b) is identical to Theorem 16.7 in the text, while part (a) is slightly more general. The proof of 16.7 in the book suggests a solution to (a), however.

3. Let R be an integral domain. Suppose that there exists a positive integer n such that $n \cdot 1_R = 0_R$. Prove that if n is chosen to be the minimum such positive integer, then n is a prime number.
   (This minimum integer n is called the *characteristic* of the domain R. An integral domain where no such positive integer n exists is said to have characteristic 0.)

4. Let $\mathbb{Z}[i]$ denote the ring of Gaussian integers, as defined in class.
   (a) Define the *norm* of an element $r = a + bi$ in $\mathbb{Z}[i]$ to be
   $$N(r) = a^2 + b^2.$$
   Prove that for any two elements $r, s \in \mathbb{Z}[i]$, $N(rs) = N(r)N(s)$.
   (b) Prove that $r \in \mathbb{Z}[i]$ is a unit in $\mathbb{Z}[i]$ if and only if $N(r) = 1$.
   (c) Determine the set of units of $\mathbb{Z}[i]$. The group $\mathbb{Z}[i]^\times$ is isomorphic to a familiar group; which one is it?

5. Let $\mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{6} : \ a, b \in \mathbb{Z}\}$, as in class.
   (a) Show that $\mathbb{Z}[\sqrt{6}]$ is a subring of $\mathbb{R}$ (and therefore a ring in its own right).
   (b) Define the *norm* of an element $r = a + b\sqrt{6}$ by
   $$N(r) = a^2 - 6b^2.$$
   Prove that for all $r, s \in \mathbb{Z}[\sqrt{6}]$, $N(rs) = N(r)N(s)$.

(c) Prove that r is a unit of $\mathbb{Z}[\sqrt{6}]$ if and only if $N(r) = \pm 1$ (in fact, there are no elements of norm -1, but you do not need to prove this).

(d) Prove that $\mathbb{Z}[\sqrt{6}]^\times$ has an infinite number of elements.

(e) Find an element $a + b\sqrt{6} \in \mathbb{Z}[\sqrt{6}]^\times$ with $a > 100$. Use a calculator/computer to approximate a/b as a decimal, and compare it the decimal for $\sqrt{6}$. Explain briefly what you observe.

(The computations involved are a useful way to give highly accurate rational approximations to $\sqrt{6}$, the method generalizes readily to other square roots.)

6. Let R be a ring, and let I be an ideal of R.

(a) Prove that if R is commutative, then so is R/I.

(b) Prove that if R has unity, then so does R/I.

7. Let $I \subseteq \mathbb{Z}[i]$ denote the subset $I = 3\mathbb{Z}[i] = \{3a + 3bi : \ a, b \in \mathbb{Z}\}$. Prove that $\mathbb{Z}[i]/I$ is a field, and that this field has 9 elements. This is the most straightforward way to construct a field with 9 elements (recall that we showed in class how to construct fields with a prime number of elements; together with problem 8 on PSet 8 you have now constructed fields with 4 or 9 elements as well).

8. Let R be a ring, and $I \subseteq R$ an ideal. The ideal I is called a *radical ideal* if it has the property that for all $a \in R$ and $n \in \mathbb{Z}^+$, if $f^n \in I$ then $f \in I$.

(a) Prove that every prime ideal is a radical ideal.

(b) Prove that I is radical if and only if the quotient R/I has no nilpotent elements besides $I + 0_R$.