10. Assume R is commutative. Prove that if P is a prime ideal of R and P contains no zero divisors then R is an integral domain.

11. Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ (for example, if P contains $I \cap J$). Prove either I or J is contained in P.

12. Assume R is commutative and suppose $I = (a_1, a_2, \ldots, a_n)$ and $J = (b_1, b_2, \ldots, b_m)$ are two finitely generated ideals in R. Prove that the product ideal IJ is finitely generated by the elements $a_i b_j$ for $i = 1, 2, \ldots, n$, and $j = 1, 2, \ldots, m$.

13. Let $\varphi : R \to S$ be a homomorphism of commutative rings.
    (a) Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R.
    (b) Prove that if M is a maximal ideal of S and φ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

14. Assume R is commutative. Let x be an indeterminate, let $f(x)$ be a monic polynomial in $R[x]$ of degree $n \geq 1$ and use the bar notation to denote passage to the quotient ring $R[x]/(f(x))$.
    (a) Show that every element of $R[x]/(f(x))$ is of the form $\overline{p(x)}$ for some polynomial $p(x) \in R[x]$ of degree less than n, i.e.,
    $$R[x]/(f(x)) = \{\overline{a_0} + \overline{a_1 x} + \cdots + \overline{a_{n-1}x^{n-1}} \mid a_0, a_1, \ldots, a_{n-1} \in R\}.$$
    [If $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ then $\overline{x^n} = \overline{-(b_{n-1}x^{n-1} + \cdots + b_0)}$. Use this to reduce powers of $\overline{x}$ in the quotient ring.]
    (b) Prove that if $p(x)$ and $q(x)$ are distinct polynomials in $R[x]$ which are both of degree less than n, then $\overline{p(x)} \neq \overline{q(x)}$. [Otherwise $p(x) - q(x)$ is an $R[x]$-multiple of the monic polynomial $f(x)$.]
    (c) If $f(x) = a(x)b(x)$ where both $a(x)$ and $b(x)$ have degree less than n, prove that $\overline{a(x)}$ is a zero divisor in $R[x]/(f(x))$.
    (d) If $f(x) = x^n - a$ for some nilpotent element $a \in R$, prove that $\overline{x}$ is nilpotent in $R[x]/(f(x))$.
    (e) Let p be a prime, assume $R = \mathbb{F}_p$ and $f(x) = x^p - a$ for some $a \in \mathbb{F}_p$. Prove that $\overline{x - a}$ is nilpotent in $R[x]/(f(x))$. [Use Exercise 26(c) of Section 3.]

15. Let $x^2 + x + 1$ be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$.
    (a) Prove that $\overline{E}$ has 4 elements: $\overline{0}$, $\overline{1}$, $\overline{x}$ and $\overline{x + 1}$.
    (b) Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.
    (c) Write out the 4×4 multiplication table for $\overline{E}$ and prove that $\overline{E}^{\times}$ is isomorphic to the cyclic group of order 3. Deduce that $\overline{E}$ is a field.

16. Let $x^4 - 16$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^4 - 16)$.
    (a) Find a polynomial of degree ≤ 3 that is congruent to $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3$ modulo $(x^4 - 16)$.
    (b) Prove that $\overline{x - 2}$ and $\overline{x + 2}$ are zero divisors in $\overline{E}$.

17. Let $x^3 - 2x + 1$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^3 - 2x + 1)$. Let $p(x) = 2x^7 - 7x^5 + 4x^3 - 9x + 1$ and let $q(x) = (x - 1)^4$.

(a) Express each of the following elements of $\overline{E}$ in the form $\overline{f(x)}$ for some polynomial $f(x)$ of degree ≤ 2: $\overline{p(x)}$, $\overline{q(x)}$, $\overline{p(x)+q(x)}$ and $\overline{p(x)q(x)}$.

(b) Prove that $\overline{E}$ is not an integral domain.

(c) Prove that $\overline{x}$ is a unit in $\overline{E}$.

18. Prove that if R is an integral domain and $R[[x]]$ is the ring of formal power series in the indeterminate x then the principal ideal generated by x is a prime ideal (cf. Exercise 3, Section 2). Prove that the principal ideal generated by x is a maximal ideal if and only if R is a field.

19. Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal.

20. Prove that a nonzero finite commutative ring that has no zero divisors is a field (if the ring has an identity, this is Corollary 3, so do not assume the ring has a 1).

21. Prove that a finite ring with identity $1 \neq 0$ that has no zero divisors is a field (you may quote Wedderburn's Theorem).

22. Let $p \in \mathbb{Z}^+$ be a prime and let the $\mathbb{F}_p$ Quaternions be defined by

$$a + bi + cj + dk \qquad a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$$

where addition is componentwise and multiplication is defined using the same relations on i, j, k as for the real Quaternions.

(a) Prove that the $\mathbb{F}_p$ Quaternions are a homomorphic image of the integral Quaternions (cf. Section 1).

(b) Prove that the $\mathbb{F}_p$ Quaternions contain zero divisors (and so they cannot be a division ring). [Use the preceding exercise.]

23. Prove that in a Boolean ring (cf. Exercise 15, Section 1) every prime ideal is a maximal ideal.

24. Prove that in a Boolean ring every finitely generated ideal is principal.

25. Assume R is commutative and for each $a \in R$ there is an integer $n > 1$ (depending on a) such that $a^n = a$. Prove that every prime ideal of R is a maximal ideal.

26. Prove that a prime ideal in a commutative ring R contains every nilpotent element (cf. Exercise 13, Section 1). Deduce that the nilradical of R (cf. Exercise 29, Section 3) is contained in the intersection of all the prime ideals of R. (It is shown in Section 15.2 that the nilradical of R is equal to the intersection of all prime ideals of R.)

27. Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.

28. Prove that if R is a commutative ring and $N = (a_1, a_2, \ldots, a_m)$ where each a_i is a nilpotent element, then N is a nilpotent ideal (cf. Exercise 37, Section 3). Deduce that if the nilradical of R is finitely generated then it is a nilpotent ideal.

29. Let p be a prime and let G be a finite group of order a power of p (i.e., a p-group). Prove that the augmentation ideal in the group ring $\mathbb{Z}/p\mathbb{Z}G$ is a nilpotent ideal. (Note that this ring may be noncommutative.) [Use Exercise 2.]

30. Let I be an ideal of the commutative ring R and define

$$\operatorname{rad} I = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$$

called the *radical* of I. Prove that rad I is an ideal containing I and that $(\operatorname{rad} I)/I$ is the nilradical of the quotient ring R/I, i.e., $(\operatorname{rad} I)/I = \mathfrak{N}(R/I)$ (cf. Exercise 29, Section 3).

31. An ideal I of the commutative ring R is called a *radical ideal* if $\operatorname{rad} I = I$.

(a) Prove that every prime ideal of R is a radical ideal.
(b) Let $n > 1$ be an integer. Prove that 0 is a radical ideal in $\mathbb{Z}/n\mathbb{Z}$ if and only if n is a product of distinct primes to the first power (i.e., n is square free). Deduce that (n) is a radical ideal of $\mathbb{Z}$ if and only if n is a product of distinct primes in $\mathbb{Z}$.

32. Let I be an ideal of the commutative ring R and define

$$\text{Jac } I \text{ to be the intersection of all maximal ideals of } R \text{ that contain } I$$

where the convention is that $\text{Jac } R = R$. (If I is the zero ideal, Jac 0 is called the *Jacobson radical* of the ring R, so $\text{Jac } I$ is the preimage in R of the Jacobson radical of R/I.)
(a) Prove that $\text{Jac } I$ is an ideal of R containing I.
(b) Prove that $\text{rad } I \subseteq \text{Jac } I$, where $\text{rad } I$ is the radical of I defined in Exercise 30.
(c) Let $n > 1$ be an integer. Describe $\text{Jac } n\mathbb{Z}$ in terms of the prime factorization of n.

33. Let R be the ring of all continuous functions from the closed interval [0,1] to $\mathbb{R}$ and for each $c \in [0, 1]$ let $M_c = \{f \in R \mid f(c) = 0\}$ (recall that M_c was shown to be a maximal ideal of R).
(a) Prove that if M is *any* maximal ideal of R then there is a real number $c \in [0, 1]$ such that $M = M_c$.
(b) Prove that if b and c are distinct points in [0,1] then $M_b \neq M_c$.
(c) Prove that M_c is not equal to the principal ideal generated by $x - c$.
(d) Prove that M_c is not a finitely generated ideal.

The preceding exercise shows that there is a bijection between the *points* of the closed interval [0,1] and the set of *maximal ideals* in the ring R of all of continuous functions on [0,1] given by $c \leftrightarrow M_c$. For any subset X of $\mathbb{R}$ or, more generally, for any completely regular topological space X, the map $c \mapsto M_c$ is an *injection* from X to the set of maximal ideals of R, where R is the ring of all bounded continuous real valued functions on X and M_c is the maximal ideal of functions that vanish at c. Let $\beta(X)$ be the set of maximal ideals of R. One can put a topology on $\beta(X)$ in such a way that if we identify X with its image in $\beta(X)$ then X (in its given topology) becomes a subspace of $\beta(X)$. Moreover, $\beta(X)$ is a compact space under this topology and is called the *Stone-Čech compactification* of X.

34. Let R be the ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ and for each $c \in \mathbb{R}$ let M_c be the maximal ideal $\{f \in R \mid f(c) = 0\}$.
(a) Let I be the collection of functions $f(x)$ in R with *compact support* (i.e., $f(x) = 0$ for $|x|$ sufficiently large). Prove that I is an ideal of R that is not a prime ideal.
(b) Let M be a maximal ideal of R containing I (properly, by (a)). Prove that $M \neq M_c$ for any $c \in \mathbb{R}$ (cf. the preceding exercise).

35. Let $A = (a_1, a_2, \ldots, a_n)$ be a nonzero finitely generated ideal of R. Prove that there is an ideal B which is maximal with respect to the property that it does not contain A. [Use Zorn's Lemma.]

36. Assume R is commutative. Prove that the set of prime ideals in R has a minimal element with respect to inclusion (possibly the zero ideal). [Use Zorn's Lemma.]

37. A commutative ring R is called a *local ring* if it has a unique maximal ideal. Prove that if R is a local ring with maximal ideal M then every element of $R - M$ is a unit. Prove conversely that if R is a commutative ring with 1 in which the set of nonunits forms an ideal M, then R is a local ring with unique maximal ideal M.

38. Prove that the ring of all rational numbers whose denominators is odd is a local ring whose unique maximal ideal is the principal ideal generated by 2.

39. Following the notation of Exercise 26 in Section 1, let K be a field, let ν be a discrete