EXERCISES

Let R be a subring of the commutative ring S with $1 \in R$.

1. Use the fact that a U.F.D. is integrally closed to prove that the Gaussian integers, $\mathbb{Z}[i]$, is the ring of integers in $\mathbb{Q}(i)$.
2. Suppose k is a field and let $t = \bar{x}/\bar{y}$ in the field of fractions of the integral domain $R = k[x, y]/(x^2 - y^3)$. Prove that $K = k(t)$ is the fraction field of R and $k[t]$ is the integral closure of R in K.
3. Suppose k is a field and i and j are relatively prime positive integers. Find the normalization of the integral domain $R = k[x, y]/(x^i - y^j)$ (cf. Exercise 14, Section 9.1).
4. Suppose k is a field and let P be the ideal $(y^2-x^3-x^2)$ in the polynomial ring $k[x, y]$. Prove that P is a prime ideal and find the normalization of the integral domain $R = k[x, y]/P$. [To prove P is prime, show that $y^2 - x^3 - x^2$ is irreducible in the U.F.D. $k[x, y]$. Then consider $t = \bar{y}/\bar{x} \in R$.]
5. If R is an integral domain with field of fractions F, show that F is a finitely generated R-module if and only if $R = F$.
6. For each of the following give specific rings $R \subseteq S$ and explicit ideals in these rings that exhibit the specified relation:
   (a) an ideal I of R such that $I \neq SI \cap R$ (so the contraction of the extension of an ideal I need not equal I)
   (b) a prime ideal P of R such that there is no prime ideal Q of S with $P = Q \cap R$
   (c) a maximal ideal M of S such that $M \cap R$ is not maximal in R
   (d) a prime ideal P of R whose extension PS to S is not a prime ideal in S
   (e) an ideal J of S such that $J \neq (J \cap R)S$ (so the extension of the contraction of an ideal J need not equal J).
7. Let $\mathcal{O}_K$ be the ring of integers in a number field K.
   (a) Suppose that every nonzero ideal I of $\mathcal{O}_K$ can be written as the product of powers of prime ideals. Prove that an ideal Q of $\mathcal{O}_K$ is P-primary if and only if $Q = P^m$ for some $m \geq 1$. [Show first that since nonzero primes in $\mathcal{O}_K$ are maximal that ${P_1}^{m_1} \subseteq {P_2}^{m_2}$ for distinct nonzero primes P_1, P_2 implies $P_1 = P_2$.]
   (b) Suppose that an ideal Q of $\mathcal{O}_K$ is P-primary if and only if $Q = P^m$ for some $m \geq 1$. Assuming all of Theorem 21, prove that every nonzero ideal I of $\mathcal{O}_K$ can be written uniquely as the product of powers of prime ideals. [Prove that ${P_1}^{m_1}$ and ${P_2}^{m_2}$ are comaximal ideals if P_1 and P_2 are distinct nonzero prime ideals and use the Chinese Remainder Theorem.]
8. Prove that if $s_1, \dots, s_n \in S$ are integral over R, then the ring $R[s_1, \dots, s_n]$ is a finitely generated R-module.
9. Suppose that S is integral over R and that P is a prime ideal in R. Prove that every element s in the ideal PS generated by P in S satisfies an equation $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$ where the coefficients $a_0, a_1, \dots, a_{n-1}$ are elements of P. [If $s = p_1 s_1 + \cdots + p_m s_m \in PS$, show that $T = R[s_1, \dots, s_m]$ satisfies the hypotheses in Proposition 23(3). Follow the proof in Proposition 23 that s is integral, noting that $s \in PT$ so that the a_{ij} are elements of P.]
10. Prove the following generalization of Proposition 28: Suppose R is an integrally closed integral domain with field of fractions k and α is an element of an extension field K of k. Show that α is integral over R if and only if α is algebraic over k and the minimal polynomial $m_{\alpha,k}(x)$ for α over k has coefficients in R. [If α is integral prove the conjugates

of α, i.e., the roots of $m_{\alpha,k}(x)$, are also integral, so the elementary symmetric functions of the conjugates are elements of k that are integral over R.]

11. Suppose R is an integrally closed integral domain with field of fractions k and $p(x) \in R[x]$ is a monic polynomial. Show that if $p(x) = a(x)b(x)$ with monic polynomials $a(x), b(x) \in k[x]$ then $a(x), b(x) \in R[x]$ (compare to Gauss' Lemma, Proposition 5, Section 9.3). [See the previous exercise.]

12. Suppose S is an integral domain that is integral over a ring R as in the previous exercise. If P is a prime ideal in R, let s be any element in the ideal PS generated by P in S. Prove that, with the exception of the leading term, the coefficients of the minimal polynomial $m_{s,k}(x)$ for s over k are elements of P. [By Exercise 10, $m_{s,k}(x) \in R[x]$. Exercise 9 shows that s is a root of a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_0, \ldots, a_{n-1} \in P$. Use the previous exercise to show that $p(x) = m_{s,k}(x)b(x)$ with $b(x)$ in $R[x]$, and consider this equation in the integral domain $(R/P)[x]$.]

The next two exercises extend Exercise 6 in Section 7.5 by characterizing fields that are not fields of fractions of any of their proper subrings.

13. Let K be a field of characteristic 0 and let A be a subring of K maximal with respect to $1/2 \notin A$. (Such A exists by Zorn's Lemma.) Let F be the field of fractions of A in K.
(a) Show that K is algebraic over F. [If t is transcendental over F, show that $1/2 \notin A[t]$.]
(b) Show that A is integrally closed in K. [Show that $1/2$ is not in the integral closure of A in K.]
(c) Deduce from (a) and (b) that $K = F$.

14. Show that a field K is the field of fractions of some proper subring of K if and only if K is not a subfield of the algebraic closure of a finite field. [If K contains t transcendental over $\mathbb{F}_p$ argue as in the preceding exercise with $1/t$ in place of $1/2$ to show that K is the quotient field of some proper subring.]

The next exercise gives a "geometric" interpretation of Noether's Normalization Lemma, showing that every affine algebraic set is a *finite covering* of some affine n-space.

15. Let V be an affine algebraic set over an algebraically closed field k. Prove that for some n there is a surjective morphism from V onto $\mathbb{A}^n$ with finite fibers, and that if V is a variety, then n can be taken to be the dimension of V. [By Noether's Normalization Lemma the finitely generated k-algebra $S = k[V]$ contains a polynomial subalgebra $R = k[x_1, x_2, \ldots, x_n]$ such that S is integral over R. Apply Theorem 6 to the inclusion of R in S to obtain a morphism φ from V to $\mathbb{A}^n$. To see that φ is surjective with finite fibers, apply Corollary 27 to the maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$ of R corresponding to a point $(a_1, \ldots, a_n)$ of $\mathbb{A}^n$.]

16. Let V be an affine algebraic set in $\mathbb{C}^n$. Prove that V is compact in the Euclidean topology (i.e., closed and bounded) if and only if it is finite. [Use Exercise 18 in Section 2, the previous exercise, and the behavior of compact sets with respect to continuous functions.]

17. Let R be a subring of the commutative ring S with $1_S \in R$ and suppose that S is integral over R. This exercise proves that R and S have the same *Krull dimension*, cf. Section 16.1.
(a) If $P_1 \subset P_2 \subset \cdots \subset P_n$ is a chain of distinct prime ideals in R prove that there is a chain $Q_1 \subset Q_2 \subset \cdots \subset Q_n$ of distinct prime ideals in S with $Q_i \cap R = P_i$.
(b) Prove conversely that if $Q_1 \subset Q_2 \subset \cdots \subset Q_n$ is a chain of distinct prime ideals in S and $P_i = Q_i \cap R$ then $P_1 \subset P_2 \subset \cdots \subset P_n$ is a chain of distinct prime ideals in R. [To prove the P_i are distinct, pass to a quotient and reduce the problem to showing that if Q is a nonzero prime ideal in the integral domain S then $Q \cap R$ is a nonzero prime

ideal in R. In this case, if $s \in Q$ is nonzero, show that the constant coefficient of a polynomial of minimal degree in $R[x]$ satisfied by s is a nonzero element in $Q \cap R$.]

18. Let $V = \mathcal{Z}(I)$ and $W = \mathcal{Z}(J)$ where I is the ideal $(uv + v) \subset \mathbb{C}[u, v]$ and J is the ideal $(-2y - y^2 + 2z + z^2, 2x - yz - z^2) \subset \mathbb{C}[x, y, z]$.
  (a) Show that I and J are prime ideals. Conclude that $I = \mathcal{I}(V)$ and $J = \mathcal{I}(W)$ and that V and W are varieties.
  (b) Show that the map $\varphi : V \to W$ defined by $\varphi((a_1, a_2)) = (a_1^2 + a_2, a_1 + a_2, a_1 - a_2)$ is an isomorphism.

19. Let $I = (x^3 + y^3 + z^3, x^2 + y^2 + z^2, (x + y + z)^3) \subset k[x, y, z]$. Use Gröbner bases to show that $x, y, z \in \operatorname{rad} I$ if $\operatorname{ch}(k) \neq 2, 3$.

20. Let $I = (x^3 + y^3 + z^3, xy + xz + yz, xyz) \subset k[x, y, z]$. Use Gröbner bases to show that $x, y, z \in \operatorname{rad} I$.

21. Let $I = (x^4 + y^4 + z^4, x + y + z) \subset k[x, y, z]$.
  (a) Use Gröbner bases to show that $xy + xz + yz \in \operatorname{rad} I$ if $\operatorname{ch}(k) \neq 2$ and determine the smallest power of $xy + xz + yz$ contained in I. Show that none of x, y or z is contained in $\operatorname{rad} I$.
  (b) If $J = (x^4 + y^4 + z^4, x + y + z, xy + xz + yz)$ show that the reduced Gröbner basis of J relative to the lexicographic ordering $x > y > z$ is $\{x + y + z, y^2 + yz + z^2\}$. Deduce that $k[x, y, z]/J \cong k[y, z]/(y^2 + yz + z^2)$ and that J is radical if $\operatorname{ch}(k) \neq 3$.
  (c) If $\operatorname{ch}(k) \neq 2, 3$, show that $\operatorname{rad} I = J$.
  (d) If $\operatorname{ch}(k) = 3$, show that $\operatorname{rad} I = (x - y, y - z)$.
  (e) If $\operatorname{ch}(k) = 2$, show that $I = (x + y + z)$ is a prime, hence radical, ideal.

22. Let $I = (x^2y + z^3, x + y^3 - z, 2y^4z - yz^2 - z^3) \subset k[x, y, z]$. Use Gröbner bases to show that $x, y, z \in \operatorname{rad} I$ and conclude that $\operatorname{rad} I = (x, y, z)$. Show that x^9, y^7, z^9 are the smallest powers of x, y, z, respectively, lying in I.

23. Let $V = \mathcal{Z}(x^3 - x^2z - y^2z)$ and $W = \mathcal{Z}(x^2 + y^2 - z^2)$ in $\mathbb{C}^3$. Show that $\mathcal{I}(V) = (x^3 - x^2z - y^2z)$ and $\mathcal{I}(W) = (x^2 + y^2 - z^2)$ in $\mathbb{C}[x, y, z]$.

24. Let $V = \mathcal{Z}(x^3 + y^3 + 7z^3) \subset \mathbb{C}^3$. Show that $\mathcal{I}(V) = (x^3 + y^3 + 7z^3)$ in $\mathbb{C}[x, y, z]$.

25. Let $I = (xz + y^2 + z^2, xy - xz + yz - 2z^2)$ and let $K = I + (x^2 - 3y^2 + yz) \subset \mathbb{C}[x, y, z]$.
  (a) By Exercise 46 in Section 1, there is an injective $\mathbb{C}$-algebra homomorphism from $\mathbb{C}[x, y, z]/K$ to $\mathbb{C}[u, v]/(u^3 - uv^2 + v^3)$. Use this together with the example preceding Proposition 34 to prove that K is a radical ideal and deduce that $\operatorname{rad} I \subseteq K$.
  (b) Show that $\operatorname{rad} I \subseteq (y, z)$.
  (c) Show that $K \cap (y, z) = I$ and deduce that I is radical, so that $\mathcal{I}(V) = I$ if $V = \mathcal{Z}(I)$.
  (d) Show that $y(x^2 - 3y^2 + yz)$ and $z(x^2 - 3y^2 + yz)$ are elements of I but none of y, z, or $x^2 - 3y^2 + yz$ is contained in I.

26. Let I be an ideal in $k[x_1, \dots, x_n]$. Prove that the following are equivalent (an ideal satisfying any of these conditions is called a *zero-dimensional ideal* because of (d)):
  (a) The quotient $k[x_1, \dots, x_n]/I$ has finite dimension as a vector space over k.
  (b) $I \cap k[x_i] \neq 0$ for each $i = 1, 2, \dots, n$.
  (c) If G is any reduced Gröbner basis for I then for each $i = 1, \dots, n$, there is a $g_i \in G$ with leading term $x_i^{n_i}$ for some $n_i \geq 1$.
  (d) The set of common zeros $\mathcal{Z}_{\bar{k}}(I)$ of the polynomials in I in an algebraic closure $\bar{k}$ of k is finite.

  [For (a) implies (b) use the injection $k[x_i]/(I \cap k[x_i]) \hookrightarrow k[x_1, \dots, x_n]/I$. For (b) implies (c) note some $LT(g_i)$ divides the leading term of a generator for $I \cap k[x_i]$. For (c) implies (a)