NOTE. I use $\subseteq$ to mean “is a not necessarily proper subset of” and $\subsetneq$ to mean “is a proper subset of.”

A.

Exercise 1

Let $x$ be a nilpotent element of a ring $A$. Show that $1 + x$ is a unit of $A$. Deduce that the sum of a nilpotent element and a unit is a unit.

Since $x$ is nilpotent, $x$ lies in every prime ideal. *A fortiori*, $x$ lies in every maximal ideal. By the properties of ideals, $-x$ therefore also lies in every maximal ideal. No proper ideal may contain 1—since otherwise that ideal contains all of $(1) = A$—and every maximal ideal is proper, so no maximal ideal may contain $1 = (1 + x) + (-x)$.

Since every maximal ideal contains $-x$, it follows that no maximal ideal contains $1 + x$. By Corollary 1.5, every non-unit of $A$ is contained in a maximal ideal. By contraposition, every element contained in no maximal ideal is a unit. We conclude that $1 + x$ is a unit.

Now suppose that $u$ is a unit of $A$. Then $u^{-1}x$ is a nilpotent (since the nilradical of $A$ is an ideal of $A$). So by the preceding result, $1 + u^{-1}x$ is a unit. But then

$$u + x = u(1 + u^{-1}x)$$

is the product of two units, hence a unit.
Exercise 2

Let $A$ be a ring and let $A[x]$ be the ring of polynomials in an indeterminate $x$, with coefficients in $A$. Let $f = a_0 + a_1 x^1 + \cdots + a_n x^n \in A[x]$. Prove that

(i) $f$ is a unit in $A[x] \iff a_0$ is a unit in $A$ and $a_1, \ldots, a_n$ are nilpotent. [If $b_0 + b_1 x + \cdots + b_m x^m$ is the inverse of $f$, prove by induction on $r$ that $a_n^{r+1} b_{m-r} = 0$. Hence show that $a_n$ is nilpotent, and then use Ex. 1.]

(ii) $f$ is nilpotent $\iff a_0, a_1, \ldots, a_n$ are nilpotent.

(iii) $f$ is a zero-divisor $\iff$ there exists $a \neq 0$ in $A$ such that $af = 0$. [Choose a polynomial $g = b_0 + b_1 x + \cdots + b_m x^m$ of least degree $m$ such that $fg = 0$. Then $a_n b_m = 0$, hence $a_n g = 0$ (because $a_n g$ annihilates $f$ and has degree $< m$). Now show by induction that $a_{n-r} g = 0$ ($0 \leq r \leq n$).]

(iv) $f$ is said to be primitive if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then $fg$ is primitive $\iff f$ and $g$ are primitive.

(i) Suppose that $a_0$ is a unit in $A$ (hence in $A[x]$) and that $a_1, \ldots, a_n$ are nilpotent. Let $g = 0 + a_1 x + \cdots + a_n x^n$. Then by part (ii) of this exercise, $g$ is nilpotent. But then $f = a_0 + g$ is the sum of a unit and a nilpotent, hence a unit by Exercise 1.

Conversely, suppose that $f$ is a unit in $A[x]$. Let $\mathfrak{N}$ denote the nilradical of $A$, and for each prime ideal $\mathfrak{p} \subset A$ let

$$\phi_\mathfrak{p} : A[x] \to (A/\mathfrak{p})[x]$$

be the reduction homomorphism mod $\mathfrak{p}$ (i.e. the ring homomorphism such that the $i^{th}$ coefficient of $\phi_\mathfrak{p}(h)$ is the reduction mod $\mathfrak{p}$ of the $i^{th}$ coefficient of $h$). Since ring homomorphisms take units to units, it follows from our hypothesis that $\phi_\mathfrak{p}(f)$ is a unit of $(A/\mathfrak{p})[x]$. But $A/\mathfrak{p}$ is an integral domain, so the only units of $(A/\mathfrak{p})[x]$ are the units of $A/\mathfrak{p}$ (under the canonical identification of $A/\mathfrak{p}$ with degree zero polynomials in $(A/\mathfrak{p})[x]$).\footnote{For a proof of this fact, consider that since $A/\mathfrak{p}$ has no zero divisors, if $f, g \in (A/\mathfrak{p})[x]$ then $\text{deg}(fg) = \text{deg}(f) + \text{deg}(g)$. Thus if $fg = 1$, $\text{deg}(f) = \text{deg}(g) = \text{deg}(fg) = 0$, and the rest follows immediately.} Thus

$$a_1, \ldots, a_n \in \mathfrak{p}.$$
But this holds for every prime ideal \( p \) of \( A \), and so in fact \( a_0, \ldots, a_n \in \mathfrak{m} \). To see that \( a_0 \) is a unit of \( A \), note that if \( a_0 \) were a nonunit, then there would be a maximum ideal \( \mathfrak{m} \) of \( A \) containing \( a_0 \), and then \( \phi_{\mathfrak{m}}(f) \) would have constant term 0.

(ii) Suppose that \( f^n = 0 \) for some \( n > 0 \). Then by Exercise 1, \( 1 + f \) is a unit and hence part (i) of this exercise—specifically and importantly, the second implication of part (i), in which we did not already take part (ii) for granted—implies that \( 1 + a_0 \) is a unit and \( a_1, \ldots, a_n \in \mathfrak{m} \). To see that \( a_0 \in \mathfrak{m} \), consider that ring homomorphisms take nilpotents to nilpotents, and so in particular the evaluation-at-zero homomorphism takes nilpotents to nilpotents. But \( f(0) = a_0 \), so \( a_0 \in \mathfrak{m} \).

(iii) Suppose that for some \( 0 \neq a \in A \), \( af = 0 \). Then trivially, \( f \) is a zero-divisor. Conversely, suppose that there is no \( 0 \neq a \in A \) such that \( af = 0 \) (so \( f \neq 0 \)). We will show that \( f \) is not a zero-divisor. For let \( 0 \neq b_0 + b_1x + \cdots + b_mx^m = g \in A[x] \). We will show by induction on \( \deg(g) \) that \( gf \neq 0 \). If \( \deg(g) = 0 \), then \( gf \neq 0 \) by hypothesis.

Now suppose by way of induction that no nonzero polynomial \( h \) of degree less than \( \deg(g) \) satisfies \( hf = 0 \), and suppose by way of contradiction that \( gf = 0 \). Then in particular the leading term \( b_ma_nx^{m+n} = 0 \), i.e. \( b_ma_n = 0 \). Then \( (a_n)g = a_n(gf) = 0 \), but (since \( a_n b_m x^m = 0 \)) \( a_n g \) has degree less than \( \deg(g) \)—contradicting the inductive hypothesis.

(iv) We will have need of the following fact.

**Lemma.** \( f \) is primitive in \( A[x] \) if and only if \( f \) is nonzero in \( (A/\mathfrak{m})[x] \) for every maximal ideal \( \mathfrak{m} \) of \( A \). (That is, if and only if the polynomial obtained from \( f \) by reducing its coefficients mod \( \mathfrak{m} \) is not the zero polynomial in \( A/\mathfrak{m} \).)

**Proof.** Suppose \( f \equiv 0 \mod \mathfrak{m} \) for some maximal ideal of \( A \). Then every coefficient of \( f \) lies in \( \mathfrak{m} \), so \( (a_0, \ldots, a_n) \subset \mathfrak{m} \subseteq (1) \). So \( f \) is not primitive.

Conversely, suppose that \( f \) is not primitive. Then \( (a_0, \ldots, a_n) \) is proper and hence contained in some maximal ideal \( \mathfrak{m} \) of \( A \). Then \( f \equiv 0 \mod \mathfrak{m} \). ■

Now, suppose that \( f, g \in A[x] \) are primitive and fix a maximal ideal \( \mathfrak{m} \) of \( A \). Because \( A/\mathfrak{m} \) is a field, \( (A/\mathfrak{m})[x] \) is an integral domain. Thus \( fg \neq 0 \).
in \((A/m)[x]\) since \(f, g \neq 0\). Since the choice of \(m\) was arbitrary, \(fg \neq 0\) in \((A/m)[x]\) for any maximal ideal \(m\) of \(A\).

Conversely, suppose that \(fg\) is primitive. Then if either of \(f, g\) is not primitive, say \(f\), then \(f \equiv 0 \mod m\) for some maximal ideal \(m\) of \(A\) and hence \(fg \equiv 0 \mod m\)—but this cannot be, since \(fg\) is primitive. So both \(f\) and \(g\) are primitive. \(\blacksquare\)
Exercise 7

Let \( A \) be a ring in which every element \( x \) satisfies \( x^n = x \) for some \( n > 1 \) (depending on \( x \)). Show that every prime ideal in \( A \) is maximal.

Fix a prime ideal \( p \) of \( A \) and let \( a \) be any ideal of \( A \) strictly containing \( p \). Let \( \phi : A \to A/p \) be the canonical projection and fix \( y \in a \setminus p \) with \( y^n = y \). Then \( y^{n-1} \in a \), so \( \phi(y^{n-1}) \in \phi(a) \). But since \( y \notin p \) and

\[
0 = y - y^n = y(1 - y^{n-1}) \in p
\]

and \( p \) is prime, it follows that \( 1 - y^{n-1} \in p \). But then

\[
0 = \phi(1 - y^{n-1}) = 1 - \phi(y^{n-1}),
\]

i.e. \( \phi(y^{n-1}) = 1 \). So \( 1 \in \phi(a) \), meaning \( \phi(a) = (1) \). By Proposition 1.1, every ideal of \( A/p \) is the image under \( \phi \) of an ideal containing \( p \). But \( \phi(p) = (0) \), and we have just shown that \( \phi(a) = (1) \) for any ideal of \( a \) strictly containing \( p \). Thus the only two ideals of \( A/p \) are \( (0) \) and \( (1) \). So \( A/p \) is a field, which is to say that \( p \) is maximal.

\[\blacksquare\]
Exercise 11

A ring $A$ is Boolean if $x^2 = x$ for all $x \in A$. In a Boolean ring $A$, show that

(i) $2x = 0$ for all $x \in A$;

(ii) every prime ideal $p$ is maximal, and $A/p$ is a field with two elements;

(iii) every finitely generated ideal in $A$ is principal.

(i) Observe that since $A$ is commutative, if $x \in A$ then

$$x + 1 = (x + 1)^2 = x^2 + 2x + 1 = x + 2x + 1,$$

whence

$$0 = 2x.$$

(ii) • Let $p$ be a prime ideal of $A$ and suppose by way of contradiction that there is some proper ideal $a$ of $A$ strictly containing $p$. Observe that for any $x \in A$,

$$x(1 - x) = x - x^2 = 0 \in p,$$

so either $x \in p$ or $1 - x \in p$ since $p$ is prime. Now let $y \in a \setminus p$. Since $y \notin p$, $1 - y \in p$. But then $1 - y \in a$, meaning

$$(1 - y) + y = 1 \in a,$$

contradicting the hypothesis that $a$ is a proper ideal of $A$. We conclude that $p$ is maximal.

• Let $p$ be a prime ideal of $A$ and $\phi : A \to A/p$ be the canonical projection map. Fix $x \in A$. Then there are two cases: either $\phi(x) = 0$ or else $\phi(x) \neq 0$, in which case $x \notin p$. But then $1 - x \in p$, so

$$0 = \phi(1 - x) = 1 - \phi(x),$$

i.e. $\phi(x) = 1$. Thus $\phi(A) = A/p = 2$, the two-element field.\(^2\)

---

\(^2\)This of course proves that $p$ is maximal free of charge. I have left in the separate proof of that fact because I enjoyed the argument.
Let $I$ be an ideal of $A$ with a finite set of generators $X = \{x_1, \ldots, x_n\}$. We will produce a single generator of $I$. In order to find a generator, we observe the correspondence between Boolean rings and Boolean algebras. In brief, the operations of a Boolean algebra and those of a Boolean ring are interdefinable, so that every nonzero Boolean ring $B$ may be regarded as a Boolean algebra $B^*$ and vice versa. Under this translation, $a$ is a ring ideal of a Boolean ring $B$ if and only if $a$ is a lattice ideal of the Boolean algebra $B^*$.

Considering $I$ as an ideal of $A^*$, we observe that $x \in I$ if and only if $x \leq g$, where the single generator $g$ is $\bigvee X$. Translating this into the language of rings, we see that $x \in I$ if and only if $x = xg$, where the single generator $g$ is

$$\sum_{0 \neq \varepsilon \in 2^n} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}.$$ 

Since we have arrived at this generator by only the sketch of a proof, it remains to show carefully that

$$I = Ag.$$

To that end, fix $x_i \in X$. Without loss of generality we assume $i = n$. Then

$$x_ng = x_n \sum_{0 \neq \varepsilon \in 2^n} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$$

$$= x_n \left[ x_n + \sum_{0 \neq \varepsilon \in 2^{n-1}} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_{n-1}^{\varepsilon_{n-1}} (1 + x_n) \right]$$

$$= x_n^2 + \sum_{0 \neq \varepsilon \in 2^{n-1}} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_{n-1}^{\varepsilon_{n-1}} (x_n + x_n^2)$$

$$= x_n + \sum_{0 \neq \varepsilon \in 2^{n-1}} x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_{n-1}^{\varepsilon_{n-1}} (x_n + x_n)$$

$$= x_n,$$

since $A$ has characteristic 2. Therefore $x_i = x_ig \in Ag$, i.e. $X \subset Ag$. But $g \in I$ so $Ag \subset I$, and $I$ is by definition the smallest ideal containing $X$. Therefore $Ag = I$.  ■
Exercise 12

A local ring contains no idempotent \( \neq 0, 1 \).

Let \( A \) be a local ring and \( m \) its sole maximal ideal, and suppose by way of contradiction that \( x \neq 0, 1 \) is an idempotent element of \( A \). Then since \( x = x^2 \),

\[
0 = x - x^2 = x(1 - x),
\]

and since \( x \neq 0, 1 \), it follows that \( x \) and \( 1 - x \) are each non-zero zero-divisors in \( A \). In particular, \( x \) and \( 1 - x \) are non-units. By Corollary 1.5, every non-unit of \( A \) is contained in a maximal ideal of \( A \). Since \( m \) is the only maximal ideal of \( A \), it follows that \( x, 1 - x \in m \). But then since \( m \) is an additive group,

\[
(1 - x) + x = 1 \in m,
\]

contradicting the fact that \( m \) is a proper subset of \( A \). We conclude that there is no nontrivial idempotent element \( x \in A \). \( \blacksquare \)
Exercise 15

Let $A$ be a ring and $X$ be the set of all prime ideals of $A$. For each subset $E$ of $A$, let $V(E)$ denote the set of all prime ideals of $A$ which contain $E$. Prove that

(i) if $a$ is the ideal generated by $E$, then $V(E) = V(a) = V(r(a))$.

(ii) $V(0) = X$, $V(1) = \emptyset$.

(iii) if $(E_i)_{i \in I}$ is any family of subsets of $A$, then

$$V \left( \bigcup_{i \in I} E_i \right) = \bigcap_{i \in I} V(E_i).$$

(iv) $V(a \cap b) = V(ab) = V(a) \cup V(b)$ for any ideals $a, b$ of $A$.

(i) Since $a$ is the intersection of all ideals containing $E$, it is in particular the case that every prime ideal containing $E$ contains $a$. Therefore the set of all prime ideals containing $E$ is identical to the set of all prime ideals containing $a$:

$$V(E) = V(a).$$

Now suppose $p \supset a$ is any prime ideal containing $a$. Then, using Exercise 1.13 parts (iii) and (vi),

$$a \subset p \Rightarrow a \cap p = a$$

$$\Rightarrow r(a \cap p) = r(a)$$

$$\Rightarrow r(a) \cap r(p) = r(a)$$

$$\Rightarrow r(a) \cap p = r(a)$$

$$\Rightarrow r(a) \subset p.$$

Likewise, if $p \supset r(a)$, then by Exercise 1.13(i), $p \supset a$. Therefore

$$V(a) = V(r(a)).$$

(ii) Ideals of $A$ are additive subgroups of $A$, hence contain 0. Therefore every prime ideal is a prime ideal containing 0:

$$V(0) = X.$$
By definition, prime ideals are proper, and therefore contain no units. Hence
\[ V(1) = \emptyset. \]

(iii) Suppose that \( p \in V \left( \bigcup_{i \in I} E_i \right) \). Then \( p \) is a prime ideal of \( A \) containing the union of—hence each of—the \( E_i \). Therefore for each \( i \), \( p \) is among the prime ideals containing \( E_i \): \( p \in \bigcap_{i \in I} V(E_i) \).

Conversely, suppose that \( p \in \bigcap_{i \in I} V(E_i) \). Then for each \( i \), \( p \) is a prime ideal containing \( E_i \). Since \( p \) contains \( E_i \) for each \( i \), \( p \) is a prime ideal containing the union of the collection \( \{E_i\}_{i \in I} \): \( p \in V \left( \bigcup_{i \in I} E_i \right) \).

(iv) Using part (i) of this exercise as well as the results of Exercise 1.13, we have
\[ V(a \cap b) = V(r(a \cap b)) = V(r(ab)) = V(ab). \]

Now, suppose on the one hand that \( p \in V(a) \cup V(b) \). Then \( p \) is either a prime ideal containing \( a \) (hence \( a \cap b \)), or else \( p \) is a prime ideal containing \( b \) (hence \( a \cap b \)). Thus in any case, \( p \in V(a \cap b) \).

Conversely, suppose that \( p \in V(a \cap b) \). Then \( p \) is a prime ideal containing \( a \cap b \). By Proposition 1.11(ii), it follows that \( p \) is either a prime ideal containing \( a \) or a prime ideal containing \( b \), and so in either case that \( p \in V(a) \cup V(b) \). \( \blacksquare \)
Exercise 16

Draw pictures of Spec($\mathbb{Z}$), Spec($\mathbb{R}$), Spec($\mathbb{C}[x]$), Spec($\mathbb{R}[x]$), Spec($\mathbb{Z}[x]$).

- Spec($\mathbb{Z}$). $\mathbb{Z}$ is an integral domain, so $(0)$ is prime. And $\mathbb{Z}$ is a PID, so all the remaining prime ideals are of the form $(p)$ for prime $p \in \mathbb{Z}$.

- Spec($\mathbb{R}$). Since $\mathbb{R}$ is a field, it has only one prime ideal: $(0)$.

- Spec($\mathbb{C}[x]$). $\mathbb{C}$ is a field, so $\mathbb{C}[x]$ is a PID. Thus $(0)$ is prime, and all the remaining prime ideals are of the form $(p)$ for prime $p \in \mathbb{C}[x]$. Since $\mathbb{C}[x]$ is a PID, it is a UFD, so the prime polynomials are precisely the irreducible polynomials. Since $\mathbb{C}$ is algebraically closed, the only irreducibles are the linear polynomials $x - z$ for $z \in \mathbb{C}$. In summary: the prime ideals of $\mathbb{C}[x]$ are $(0)$ and $(x - z)$ for $z \in \mathbb{C}$.

- Spec($\mathbb{R}[x]$). $\mathbb{R}$ is a field, so $\mathbb{R}[x]$ is a PID. Thus $(0)$ is prime, and all the remaining prime ideals are of the form $(p)$ for prime—irreducible, since $\mathbb{R}[x]$ is a UFD—$p \in \mathbb{R}[x]$. Every linear polynomial $x - r$ for $r \in \mathbb{R}$ is irreducible, and the only other irreducibles are the quadratics with two (conjugate) complex roots. In summary: the prime ideals of $\mathbb{R}[x]$ are $(0)$, $(x - r)$ for $r \in \mathbb{R}$, and $(x^2 - 2\alpha x + \alpha^2 + \beta^2)$ for $\alpha, \beta \in \mathbb{R}$.

- Spec($\mathbb{Z}[x]$). $\mathbb{Z}$ is an integral domain, so $\mathbb{Z}[x]$ is an integral domain. Hence $(0)$ is prime. Furthermore, $(p)$ is prime for $p \in \mathbb{Z}$ prime, since if $ab \in (p)$, then $a, b \in \mathbb{Z}$ and the rest follows immediately. Since $\mathbb{Z}$ is a UFD, so is $\mathbb{Z}[x]$; therefore $(p(x))$ is prime for $p(x) \in \mathbb{Z}[x]$ irreducible. Lastly, if $p \in \mathbb{Z}$ is prime and $f \in \mathbb{Z}[x]$ is irreducible and irreducible mod $p$, and if $f_p$ is the reduction of $f$ mod $p$, then $(p, f)$ is prime since

$$\mathbb{Z}[x]/(p, f) \cong (\mathbb{Z}/(p))[x]/(f_p),$$

which is a field.$^3$

---

$^3$Note that I have not proven that these are the only prime ideals of $\mathbb{Z}[x]$, which is somewhat more involved.
B.

Let $A$ be a commutative ring. Show that $A$ is a field iff every ideal of $A$ is prime.

Suppose $A$ is a field. Then its only ideals are the trivial ideals, which are trivially prime. Conversely, suppose that every ideal of $A$ is prime. Then in particular, $(0)$ is prime, wherefore $A$ is an integral domain. Fix any element $x \in A$. By hypothesis, either $(x^2)$ is not proper and so $x$ is a unit, or else $(x^2)$ is prime and so $x \in (x^2)$. Then there is some $a \in A$ such that $x = ax^2$. But because $A$ is an integral domain, we may cancel $x$ to obtain

$$1 = ax.$$

Therefore in any case, $x$ is a unit. We conclude that $A$ is a field. ■
C.

A commutative ring $A$ is called Von Neumann regular (abbreviated VNR) if for every element $a \in A$ there is an element $b \in A$ such that $a^2b = a$. Show that $A$ is VNR iff every ideal $I$ of $A$ is a radical ideal (that is, $I$ is equal to its own radical). [Hint: use Exercise 1.13(iii) on page 9 of your textbook.]

Suppose every ideal of $A$ is radical. Then in particular

$$(a^2) = \{x \in A : x^n \in Aa^2 \text{ for some } n > 0\}.$$ 

Because $a^2 \in (a^2)$, the above implies that $a \in (a^2)$. But this is just to say that there is some $b \in A$ such that $a = ba^2$; i.e. that $A$ is VNR.

Conversely, suppose that $A$ is VNR. Fix $x, a \in A$ and suppose that $x^n \in (a)$ for some $n > 0$. We wish to show that $x \in (a)$.

By hypothesis, there is some $b \in A$ such that $bx^2 = x$. Now suppose by way of induction that $b^k x^{k+1} = x$ for some $k > 0$. Then

$$b^{k+1}x^{k+2} = b(b^k x^{k+1})x = b(x)x = bx^2 = x.$$ 

We conclude by induction that $b^k x^{k+1} = x$ for all $k > 0$—hence in particular that $b^{n-1}x^n = x$.

Since $x^n \in (a)$, there is some $u \in A$ such that $x^n = ua$. Therefore if we denote $b^{n-1}u = v \in A$,

$$x = b^{n-1}x^n = b^{n-1}ua = va,$$

so that $x \in (a)$. This completes the proof. ■

\[ ^4 \text{This will complete the proof, since } \sqrt{(a)} \supset (a) \text{ trivially.} \]