Debra Griffin
Section 6.1
#6.1, 6.3, 6.4, 6.5, 6.7, 6.16(ii) + Worksheet #2, 3

6.1 (i) *Find all the maximal ideals in $\mathbb{Z}$.*

An ideal I is maximal in $\mathbb{Z} \Leftrightarrow I = (p)$ where p is a prime integer.

Proof:
Let p be a prime integer.
Since, $\mathbb{Z}/(p) = \mathbb{Z}_p$, then $\mathbb{Z}/(p)$ is a field.
$\therefore$ (p) is maximal.
Conversely, if m is a composite integer, then $\mathbb{Z}_m$ is not a field, hence (m) is not maximal by Proposition 6.7 (A proper ideal I in a nonzero commutative ring R is a maximal ideal if and only if R/I is a field.).

(ii) *Find all the maximal ideals in $\mathbb{R}[x]$; that is, describe those $g(x) \in \mathbb{R}[x]$ for which (g) is a maximal ideal.*

An ideal I is maximal in $\mathbb{R}[x] \Leftrightarrow I = (g(x))$ where $g(x)$ is a irreducible in $\mathbb{R}[x]$.

Proof:
Let $g(x) \in \mathbb{R}[x]$ such that $g(x)$ is irreducible.
Note that $g(x)$ is irreducible $\Leftrightarrow$ $\deg(g(x)) = 1$ or $g(x) = ax^2 + bx + c$ and $b^2 - 4ac < 0$.
If $\deg(g(x)) = 1$, then $g(a) = 0$ for some $a \in \mathbb{R}$.
Define φ: $\mathbb{R}[x] \to \mathbb{R}$ by $\varphi(f(x)) = f(a)$. Then φ is a surjection and $\ker \varphi = (g(x))$.
$\therefore$ $\mathbb{R}[x]/(g(x)) \cong \mathbb{R}$, hence $\mathbb{R}[x]/(g(x))$ is a field.
If $g(x) = ax^2 + bx + c$ and $b^2 - 4ac < 0$, then $\exists$ $z \in \mathbb{C}$ such that $g(z) = 0$.
Define φ: $\mathbb{R}[x] \to \mathbb{C}$ by $\varphi(f(x)) = f(z)$. Then φ is a surjection and $\ker \varphi = (g(x))$.
Thus, $\mathbb{R}[x]/(g(x)) \cong \mathbb{C}$, hence $\mathbb{R}[x]/(g(x))$ is a field.
$\therefore$ $(g(x))$ is maximal.
Conversely, assume $g(x)$ is reducible. Let $\deg g(x) = n$.
Then $g(x) = f(x)h(x)$ for some $f(x), h(x) \in \mathbb{R}[x]$ where $\deg f(x) < n$ and $\deg g(x) < n$.
Thus, $(g(x)) \subset (f(x)) \subset \mathbb{R}[x]$, hence $(g(x))$ is not maximal.

(iii) *Find all the maximal ideals in $\mathbb{C}[x]$.*

An ideal I is maximal in $\mathbb{C}[x] \Leftrightarrow I = (g(x))$ where $\deg g(x) = 1$.

Proof:
Let $g(x) \in \mathbb{C}[x]$ such that $\deg(g(x)) = 1$. Then $\exists$ $a \in \mathbb{C}$ such that $g(a) = 0$.
Define φ: $\mathbb{C}[x] \to \mathbb{C}$ by $\varphi(f(x)) = f(a)$. Then φ is a surjection and $\ker \varphi = (g(x))$.
Thus $\mathbb{C}[x]/(g(x)) \cong \mathbb{C}$, hence $\mathbb{C}[x]/(g(x))$ is a field.
$\therefore$ $(g(x))$ is maximal.

6.3 (i) *Give an example of a commutative ring containing two prime ideals P and Q for which $P \cap Q$ is not a prime ideal.*

Example:

If $P = (2)$ and $Q = (3)$ in $\mathbb{Z}$, then $P \cap Q$ is not a prime ideal in $\mathbb{Z}$.

Proof:

Since $6 \in P$ and $6 \in Q$, then $6 \in P \cap Q$.

But $2 \notin P \cap Q$ as $2 \notin Q$, and $3 \notin P \cap Q$ as $3 \notin P$, so $P \cap Q$ is not a prime ideal in $\mathbb{Z}$.

(ii) *If $P_1 \supseteq P_2 \supseteq \cdots \supseteq P_n \supseteq P_{n+1} \supseteq \cdots$ is a decreasing sequence of prime ideals in a commutative ring R, prove that $\cap_{n\geq 1} P_n$ is a prime ideal.*

Proof:

Assume $P_1 \supseteq P_2 \supseteq \cdots \supseteq P_n \supseteq P_{n+1} \supseteq \cdots$ is a decreasing sequence of prime ideals in a commutative ring R. We first will show $\cap_{n\geq 1} P_n$ is an ideal.

Since P_n is an ideal for each n, then $0 \in P_n$ for each n.

If $a, b \in \cap_{n\geq 1} P_n$, then $a, b \in P_n$ for each n, hence $a - b \in P_n$ for each n.

If $a \in \cap_{n\geq 1} P_n$ and $r \in R$, then $ar \in P_n$ for each n, hence $ar \in \cap_{n\geq 1} P_n$.

$\therefore$ $\cap_{n\geq 1} P_n$ is an ideal.

We now show $\cap_{n\geq 1} P_n$ is a prime ideal.

Suppose $ab \in \cap_{n\geq 1} P_n$. Then $ab \in P_n$ for each n. If $a \in P_n$ for each n, then we're done.

Suppose $\exists$ i such that $a \notin P_i$. Then $a \notin P_j$ for any $j \geq i$, as $P_j \subseteq P_i$.

Since P_j is a prime ideal for every $j \geq i$, then $b \in P_j$ for every $j \geq i$.

And since $P_j \subseteq P_r$ for every $r \in \{1, 2, \ldots, j\}$ then $b \in P_n$, for each $n \geq 1$.

Hence $b \in \cap_{n\geq 1} P_n$. $\therefore$ $\cap_{n\geq 1} P_n$ is a prime ideal.

(Thanks Mark. And Clairice. And Alex.)

6.4 *Let $f : A \to R$ be a ring homomorphism, where A and R are commutative nonzero rings. Give an example of a prime ideal P in A with $f(P)$ not a prime ideal in R.*

Example:

Define $f : \mathbb{Z} \to \mathbb{Q}$ by $f(a) = a$. Let $P = (2)$. Then $f(P)$ is not a prime ideal in $\mathbb{Q}$.

Proof:

$\mathbb{Z}$ and $\mathbb{Q}$ are commutative nonzero rings and (2) is a prime ideal in $\mathbb{Z}$.

So we have $f(P) = \mathbb{E}$ in $\mathbb{Q}$ where $\mathbb{E}$ = {even integers}.

However, since $\mathbb{Q}$ is a field, the only ideals in $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$.

$\therefore$ $f(P)$ is not a prime ideal in $\mathbb{Q}$.

6.5 *Let $f: A \to R$ be a ring homomorphism. If Q is a prime ideal in R, prove that $f^{-1}(Q)$ is a prime ideal in A. Conclude that if J/I is a prime ideal in R/I, where $I \subseteq J \subseteq R$, then J is a prime ideal in R.*

Proof:
Let $f: A \to R$ be a ring homomorphism. Assume Q is a prime ideal in R.
We first will show $f^{-1}(Q)$ is an ideal in A.
By homomorphism properties we know $0_A \in f^{-1}(Q)$ as $0_R \in Q$.
Let $x, y \in f^{-1}(Q)$. Then $f(x) - f(y) = f(x - y) \in Q$, hence $x - y \in f^{-1}(Q)$.
Let $x \in f^{-1}(Q)$ and $a \in A$. Then $f(x)f(a) = f(xa) \in Q$, hence $xa \in f^{-1}(Q)$.
$\therefore$ $f^{-1}(Q)$ is an ideal in A. We now show $f^{-1}(Q)$ is prime.
Suppose $\exists$ $a, b \in A$ such that $ab \in f^{-1}(Q)$.
Then $f(a)f(b) = f(ab) \in Q$. Thus, $f(a) \in Q$ or $f(b) \in Q$ as Q is prime.
$\therefore$ $a \in f^{-1}(Q)$ or $b \in f^{-1}(Q)$, hence $f^{-1}(Q)$ is prime.
Conclusion:
Suppose I is a prime ideal in a ring R, and $I \subset J \subset R$.
Define $f: R \to R/I$ by $f(a) = a + I$. If J/I is a prime ideal in R/I, then $f^{-1}(J/I) = J$ is a prime ideal in R.

6.7 *Prove that if P is a prime ideal in a commutative ring R and if $r^n \in P$ for some $r \in R$ and $n \geq 1$, then $r \in P$.*
Proof:
We will prove the result by induction on n.
Assume P is a prime ideal in a commutative ring R and $r^n \in P$ for some $r \in R$.
Let $n = 1$. Then $r^1 = r \in P$.
Let $n \geq 1$ and assume $r^n \in P \Rightarrow r \in P$. Since $r^n \in P$ and $r \in R$, then $r \bullet r^n$ and $r^{n+1} \in P$.
And since $r^{n+1} = r \bullet r^n$ and P is a prime ideal, then $r \in P$ or $r^n \in P$.
If $r \in P$, the proof is complete. If $r^n \in P$, then by our induction hypothesis, $r \in P$.
$\therefore$ $\forall$ $n \geq 1$, $r^n \in P \Rightarrow r \in P$.

6.15 *A Boolean ring is a commutative ring R in which $a^2 = a$ for all $a \in R$. Prove that every prime ideal in a Boolean ring is a maximal ideal. (See Exercise 8.21 on page 533).* ***Hint****. When is a Boolean ring a domain?*

Proof:
If $R = \{0\}$, then the result is true vacuously. So we can assume $R \neq \{0\}$.
Let I be a prime ideal in R.
Let $a \in R$ such that $a \neq 0$ and $a \notin I$. We know a exists as I is a proper ideal.
Since I is a prime ideal, then R/I is an integral domain, by Proposition 6.4 (An ideal I in a commutative ring R is a prime ideal $\Leftrightarrow$ R/I is a domain.)
Thus, $(a + I)(a + I) = a^2 + I = a + I \Rightarrow a^2 - a + I = a(a - 1) + I = 0 + I$.
Since R/I is an integral domain, then $a \in I$ or $a - 1 \in I$.
Since $a \notin I$ by assumption, then $a - 1 \in I$, hence $a + I = 1 + I$.
Thus $a + I$ is the multiplicative identity in R/I.
This gives us that $R/I = \{0_{R/I}, 1_{R/I}\}$.
$\therefore$ R/I is a field. $\therefore$ I is maximal in R.

6.16 (ii) *A commutative ring is called a local ring if it has a unique maximal ideal. If R is a local ring with a unique maximal ideal m, prove that $a \in R$ is a unit if and only if $a \notin m$.*
Hint*. You may assume that every nonunit in a commutative ring lies in some maximal ideal (this result is proved using Zorn's lemma).*

Proof:
Assume R is a local ring with a unique maximal ideal m, and $a \in R$ is a unit.
Let I be an ideal in R such that $a \in I$.
Since a is a unit, then $1 = a \bullet a^{-1} \in$ I, hence $I = R$. $\therefore$ $I \neq m$, as m is maximal.

Conversely, assume $a \notin m$. Then $(a) \not\subset m$. Since every ideal is contained in some maximal ideal and m is the unique maximal ideal of R, then $m \subseteq (a) = R$.
Thus, $1 = ax \in R$, hence a is a unit.

Worksheet:

---

2. *If p is a prime integer, prove that M is a maximal ideal in* $\mathbb{Z} \times \mathbb{Z}$, *where* $M = \{(pa, b) | a, b \in \mathbb{Z}\}$.

Proof:
Let p be a prime integer.
We first will show M is an ideal in $\mathbb{Z} \times \mathbb{Z}$. $(p \bullet 0, 0) \in \mathbb{Z} \times \mathbb{Z}$, so $M \neq \emptyset$.
If $(pa_1, b_1), (pa_2, b_2) \in M$, then $(pa_1, b_1) - (pa_2, b_2) = (p(a_1 - a_2), b_2 - b_2) \in M$.
Let $(m, n) \in \mathbb{Z} \times \mathbb{Z}$. Then $(pa, b) \bullet (m, n) = (pam, bn) \in M$. $\therefore$ M is an ideal.
We now will show M is maximal.
Suppose J is an ideal in $\mathbb{Z} \times \mathbb{Z}$, that properly contains M.
Then $\exists$ $(x, y) \in J$ such that $(x, y) \notin M$.
So $p \nmid x$, which implies gcd $(p, x) = 1$, as p is prime.
Thus, $\exists$ $r, s \in \mathbb{Z}$ such that $1 = rp + xs$.
And since $(rp, 1) \in J$ and $(xs, 1) \in J$, then $(1, 1) \in J$. Hence $J = \mathbb{Z} \times \mathbb{Z}$.
$\therefore$ M is maximal.

---

3. *Find an ideal in* $\mathbb{Z} \times \mathbb{Z}$ *that is prime but not maximal.*

Example:

Here we assume (x, y) denotes an ordered pair in $\mathbb{Z} \times \mathbb{Z}$.
If $I = \{(a, 0) | a \in \mathbb{Z}\}$ is prime but not maximal.

Proof:
Suppose $(m, 0) \in I$. Let $m = ab$ and $0 = cd$ be any factorizations of m, 0 in $\mathbb{Z}$.
Then $c = 0$ or $d = 0$ as $\mathbb{Z}$ is an integral domain, and $a \in \mathbb{Z}$ or $b \in \mathbb{Z}$ (in fact a and b are in $\mathbb{Z}$.) Thus, if $(a, c) \bullet (b, d) = (m, 0)$, then $(a, c) \in I$ or $(b, d) \in I$.
And if $(a, d) \bullet (b, c) = (m, 0)$, then $(a, d) \in I$ or $(b, c) \in I$. $\therefore$ I is a prime ideal.
However, $I \subset \{(a, 2k) | a, k \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$, so I is not maximal.
