MATH 456-01

Solutions to Homework 17

Section 6.3
p. 166: 1, 3, 4, 5, 7, 8, 11, 16, 20

1. If n is composite, then $n = ab$ for some $a, b \in \mathbb{Z}, 1 < a, b < n$. Thus $ab = n \in (n)$, but $a \notin (n)$ and $b \notin (n)$ (since n divides neither a nor b).

3. (a) Suppose first that p is prime and I is an ideal of $\mathbb{Z}$ such that $(p) \subseteq I \subseteq \mathbb{Z}$. If $(p) \neq I$, then there exists $n \in I - (p)$. Such an n is not a multiple of p, so, since p is prime, $(n, p) = 1$. Therefore, there are integers x and y such that $nx + py = 1$. But $n, p \in I$, so $nx + py \in I$. That is, $1 \in I$, so $I = \mathbb{Z}$. Therefore, I is maximal.

   Conversely, suppose that (p) is a maximal ideal of $\mathbb{Z}$. If $p = ab$, then $(p) \subseteq (a) \subseteq \mathbb{Z}$, so $(a) = (p)$ or $(a) = \mathbb{Z}$. In the first case, $p|a$ and $a|p$, so $a = \pm p$. In the second case, $(a) = \pm 1$. Thus, in either case, we have a trivial factorization of p, so p is prime.

   Here is the easy way: p is prime if and only if $\mathbb{Z}/(p) \cong \mathbb{Z}_p$ is an integral domain, which, since $\mathbb{Z}_p$ is finite, is true if and only if $\mathbb{Z}_p$ is a field, which is true if and only of (p) is maximal.

   (b) Suppose first that $p(x)$ is prime and I is an ideal of $F[x]$ such that $(p(x)) \subseteq I \subseteq F[x]$. If $(p(x)) \neq I$, then there exists $n(x) \in I - (p(x))$. Such an $n(x)$ is not a multiple of $p(x)$, so, since $p(x)$ is irreducible, $(n(x), p(x)) = 1$. Therefore, there are polynomials $g(x)$ and $h(x)$ such that $n(x)g(x) + p(x)h(x) = 1$. But $n(x), p(x) \in I$, so $n(x)g(x) + p(x)h(x) \in I$. That is, $1 \in I$, so $I = F[x]$. Therefore, I is maximal.

   Conversely, suppose that $(p(x))$ is a maximal ideal of $F[x]$. If $p(x) = a(x)b(x)$, then $(p(x)) \subseteq (a(x)) \subseteq \mathbb{Z}$, so $(a(x)) = (p(x))$ or $(a(x)) = F[x]$. In the first case, $p(x)|a(x)$ and $a(x)|p(x)$, so $a(x)$ is an associate of $p(x)$. In the second case, $(a(x))$ is a constant polynomial. Thus, in either case, we have a trivial factorization of $p(x)$, so $p(x)$ is prime.

4. If R is an integral domain and $ab \in (0)$, then $ab = 0$. Thus $a = 0$ or $b = 0$, so $a \in (0)$ or $b \in (0)$. Therefore, (0) is a prime ideal. On the other hand, if (0) is a prime ideal and $ab = 0$, then $ab \in (0)$, so $a \in (0)$ or $b \in (0)$. Thus $a = 0$ or $b = 0$, so R is an integral domain.

5. The ideals in $\mathbb{Z}_6$ are $(0), (1) = (5), (2) = (4)$, and (3). Of these, $(2) = (4)$ and (3) are maximal.

   The ideals in $\mathbb{Z}_{12}$ are $(0), (1) = (5) = (7) = (11), (2) = (10), (3) = (9), (4) = (8)$, and (6). Of these $(2) = (10)$ and $(3) = (9)$ are maximal.

7. Let $a \in F, a \neq 0$. If (0) is maximal, then $(0, a) = F$, so there are elements $b, c \in F$ such that $0(b) + a(c) = 1$. Thus $ac = 1$, so a has an inverse. Since a was arbitrary, F is a field. Conversely, if F is a field, then the only ideals are (0) and F, so (0) is maximal.

8. By Exercise 27 in 6.1, since $(2, 3) = 1$, $(2) \cap (3) = (6)$. But (2) and (3) are prime ideals, while (6) is not.

11. Define ϕ from $\mathbb{Z}[x]$ to $\mathbb{Z}$ by $\phi(p(x)) = p(1)$. We have seen several times that evaluation is a homomorphism, and this one is surjective. Certainly $x - 1 \in \ker \phi$. If $\frac{(}{x}) \in \ker \phi$, then $f(x) = (x-1)g(x)$ for some $g(x) \in \mathbb{Z}[x]$ by the Factor Theorem and Theorem 4.22, so $f(x) \in (x - 1)$. Therefore, $\ker \phi = (x - 1)$. Thus $\mathbb{Z}[x]/(x - 1) \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain but not a field, $(x - 1)$ is a prime ideal but not a maximal ideal.

16. M is clearly an ideal: if $a, b \in M$, then $a - b \in M$, and if $a \in M$ and $r \in 2\mathbb{Z}$, then $ar \in M$. If $M \subseteq J \subseteq 2\mathbb{Z}$ but $J \neq M$, then there is an element $a \in J - M$. Thus a is not a multiple of 4, but a is even, so $a = 4q + 2$ for some integer q. Thus $4q - a = 2 \in J$ since $4 \in J$, so $J = 2\mathbb{Z}$. Therefore, M is maximal.

20. Define ϕ from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ by $\phi(m, n) = m$. Then ϕ is a surjective homomorphism and $\ker \phi = (0) \times \mathbb{Z}$, so $\mathbb{Z} \times \mathbb{Z}/(0) \times \mathbb{Z} \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain but not a field, $0 \times \mathbb{Z}$ is a prime ideal but not a maximal ideal. [Note the technique in Exercises 11 and 13 – this is a way to come up with ideals with certain properties!