Homework #3 Solutions

pp 268-271: 12, 14, 18, 42, 44 pp 268-271: 6, 30, 32, 36, 52, 56

p 268, #6 We will find the maximal ideals in the general case of $\mathbb{Z}_n$ only. The ideals of $\mathbb{Z}_n$ are, first of all, additive subgroups of $\mathbb{Z}_n$. These we know to all have the form $\langle d \rangle$ where d divides n. But, as we know, the set $\langle d \rangle$ is the ideal generated by d. So we have just proven that

The ideals in $\mathbb{Z}_n$ are precisely the sets of the form $\langle d \rangle$ where d divides n.

Since we are interested in maximal ideals, and this concept is defined in terms of containment of ideals in one another, we now need to determine when we can have $\langle d_1 \rangle \subset \langle d_2 \rangle$. This is the case if and only if $d_1 \in \langle d_2 \rangle$, which is true if and only if there is an element $a \in \mathbb{Z}$ so that $ad_2 = d_1$, i.e. if and only if d_2 divides d_1.

We are now ready to prove the main result: an ideal I in $\mathbb{Z}_n$ is maximal if and only if $I = \langle p \rangle$ where p is a prime dividing n. If I has this form and J is another ideal in $\mathbb{Z}_n$ with $I \subset J$ then $J = \langle d \rangle$ for some d dividing n. By our comments above this means that d divides p, i.e. $d = 1$ or $d = p$, which means that $J = \mathbb{Z}_n$ or $J = I$, proving that I is maximal. For the converse, suppose $I = \langle d \rangle$ (d dividing n) is maximal but d is not prime. Then $d = kl$ with $d > k, l > 1$. But then $I \underset{\neq}{\subseteq} \langle k \rangle \underset{\neq}{\subseteq} \mathbb{Z}_n$. The first inequality follows from the fact that $k < d$ implies $k \notin I$. The second follows from the fact that k is a divisor of n but is not 1, therefore is not a unit in $\mathbb{Z}_n$ and so $1 \notin \langle k \rangle$. But this string of inequalities implies that I is not maximal, a contradiction. Therefore d must be prime, and we are finished.

p 269, #12 As usual, we use the two step ideal test. It is clear that AB is nonempty since $0 \in A, B$ so that $0 = 0 \cdot 0 \in AB$. Let $x, y \in AB$. Then $x = a_1b_1 + a_2b_2 + \cdots a_nb_n$ and $y = c_1d_1 + c_2d_2 + \cdots + c_md_m$ for some $a_i, c_i \in A$, $b_i, d_i \in B$ and $m, n \in \mathbb{Z}^+$. Then

$$\begin{aligned} x - y &= a_1b_1 + a_2b_2 + \cdots a_nb_n - (c_1d_1 + c_2d_2 + \cdots + c_m) \\ &= a_1b_1 + a_2b_2 + \cdots a_nb_n - c_1d_1 - c_2d_2 - \cdots - c_m \\ &= a_1b_1 + a_2b_2 + \cdots a_nb_n + (-c_1)d_1 + (-c_2)d_2 + \cdots + (-c_m)d_m \in AB \end{aligned}$$

since $a_i, -c_i \in A$, $b_i, d_i \in B$ and $m + n \in \mathbb{Z}^+$. If $r \in R$ then we have

$$\begin{aligned} rx &= r(a_1b_1 + a_2b_2 + \cdots a_nb_n) \\ &= r(a_1b_1) + r(a_2b_2) + \cdots + r(a_nb_n) \\ &= (ra_1)b_1 + (ra_2)b_2 + \cdots + (ra_n)b_n \in AB \end{aligned}$$

since $ra_i \in A$ for all i. A similar line of reasoning shows that $xr \in AB$, since $b_ir \in B$ for all i. Since AB is nonempty, is closed under subtraction, and is closed under left and right multiplication by R we conclude that AB is an ideal.

p 269, #14 Let $x \in AB$. Then, as above, $x = a_1b_1 + a_2b_2 + \cdots a_nb_n$ for some $a_i \in A$ and $b_i \in B$. Since A is closed under right multiplication by R, each $a_ib_i \in A$, and therefore $x = a_1b_1 + a_2b_2 + \cdots a_nb_n \in A$ since A is closed under addition as well. Likewise, closure of B

under right multiplication implies that $a_ib_i \in B$ for all i so that $x = a_1b_1 + a_2b_2 + \cdots a_nb_n \in B$ as well. Hence, $x \in A \cap B$. Since x was an arbitrary element of AB we conclude that $AB \subset A \cap B$.

p 269, #18 We are given $\langle 35 \rangle \subsetneqq J \subsetneqq I$ in $\mathbb{Z}$. Since every ideal in $\mathbb{Z}$ is principal we can write $J = \langle n \rangle$ and $I = \langle m \rangle$ for some $m, n \in \mathbb{Z}^+$. The containments above therefore imply that n divides, but does not equal, 35 and m divides, but does not equal, n. It follows that $n = 5$ or 7 and $m = 1$. That is, $J = \langle 5 \rangle$ or $J = \langle 7 \rangle$ and $I = \mathbb{Z}$.

p 270, #30 Since $\mathbb{Z}_8$ and $\mathbb{Z}_{30}$ both have identities, we know that the ideals in $R = \mathbb{Z}_8 \oplus \mathbb{Z}_{30}$ all have the form $I \oplus J$ where I is an ideal in $\mathbb{Z}_8$ and J is an ideal in $\mathbb{Z}_{30}$. In order for $I \oplus J$ to be maximal, one of I or J must be maximal and the other must be the entire ring. By an earlier exercise, then, the maximal ideals in R are $< \langle 2 \rangle \oplus \mathbb{Z}_{30}$, $\mathbb{Z}_8 \oplus \langle 2 \rangle$, $\mathbb{Z}_8 \oplus \langle 3 \rangle$ and $\mathbb{Z}_8 \oplus \langle 5 \rangle$. It is easy to see that

$$\begin{aligned}
(\mathbb{Z}_8 \oplus \mathbb{Z}_{30})/(\langle 2 \rangle \oplus \mathbb{Z}_{30}) &\cong (\mathbb{Z}_8/\langle 2 \rangle) \oplus (\mathbb{Z}_{30}/\mathbb{Z}_{30}) \cong \mathbb{Z}_2 \\
(\mathbb{Z}_8 \oplus \mathbb{Z}_{30})/(\mathbb{Z}_8 \oplus \langle 2 \rangle) &\cong (\mathbb{Z}_8/\mathbb{Z}_8) \oplus (\mathbb{Z}_{30}/\langle 2 \rangle) \cong \mathbb{Z}_2 \\
(\mathbb{Z}_8 \oplus \mathbb{Z}_{30})/(\mathbb{Z}_8 \oplus \langle 3 \rangle) &\cong (\mathbb{Z}_8/\mathbb{Z}_8) \oplus (\mathbb{Z}_{30}/\langle 3 \rangle) \cong \mathbb{Z}_3 \\
(\mathbb{Z}_8 \oplus \mathbb{Z}_{30})/(\mathbb{Z}_8 \oplus \langle 5 \rangle) &\cong (\mathbb{Z}_8/\mathbb{Z}_8) \oplus (\mathbb{Z}_{30}/\langle 5 \rangle) \cong \mathbb{Z}_5.
\end{aligned}$$

p 270, #32 Let $J = I + \langle 2 \rangle = \langle x, 2 \rangle$. Then $I \subsetneqq J$ since $2 \in J$ but $2 \notin I$. On the other hand, $J \neq \mathbb{Z}[x]$: the elements of J all have the form $f(x) = xg(x) + 2h(x)$, $g, h \in \mathbb{Z}[x]$, so that $f(0) = 2h(0)$ is an even integer, but the constant polynomial 1 clearly does not have this property. It follows that I is not maximal.

p 270, #36 Notice that $2(1+i) = 2 + 2i$ but $2, 1+i \notin I$. This is because the elements of I all have the form $(a+bi)(2+2i) = 2(a-b) + 2(a+b)i$ for some $a, b \in \mathbb{Z}$, but neither 2 nor $1+i$ can be written in this form. Thus I is not prime.

Since the real and imaginary parts of any element in I are both even integers, and $2, 2i \notin I$, it follows that the cosets $I, 1+I, 2+I, 3+I, 1+i+I, 1+(1+i)+I, 2+(1+i)+I, 3+(1+i)+I$ are distinct. Moreover, given $a+bi$ in $\mathbb{Z}[i]$, we have $a+bi = (a-b) + b(1+i)$. If we write $a - b = 4k + r$ with $r \in \mathbb{Z}_4$ and $b = 2l + s$ with $s \in \mathbb{Z}_2$ then we have

$$a + bi = (4k + r) + (2l + s)(1+i) = 4k + (2+2i)l + r + s(1+i)$$

so that

$$a + bi + I = r + s(1+i) + I$$

since $2+2i, 4 \in I$. That is, $a + bi + I$ is one of the cosets we have already listed. Hence, $\mathbb{Z}[i]/I$ has exactly 8 elements. The characteristic of $\mathbb{Z}[i]/I$ is 4 since $1, 2, 3 \notin I$ but $4 \in I$ implies that the additive order of $1 + I$ is 4.

p 270, #42 We use the ideal test. Since $0^1 = 0 \in A$, we see that $0 \in N(A)$ so that $N(A) \neq \emptyset$. Let $a, b \in N(A)$. Then there exist $m, n \in \mathbb{Z}^+$ so that $a^m, b^n \in A$. Thus, for any $r \in R$ we have

$$(ra)^m = r^m a^m \in A$$

since $r^m \in R$ and A is an ideal (here we have used that R is commutative). Therefore $ra \in N(A)$. As R is commutative, this implies that $N(A)$ is closed under multiplication (on either side) by elements of R. It remains to show that $a - b \in N(A)$. We begin by writing, via the binomial theorem,

$$(a-b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} (-1)^{m+n-k} a^k b^{m+n-k}.$$

For $k \geq m$ in this sum, $a^k \in A$, and since A is an ideal this means $\binom{m+n}{k}(-1)^{m+n-k}a^k b^{m+n-k} \in A$. Similarly, for $k < m$ we have $m + n - k > n$ so that $b^{m+n-k} \in A$ and, as above, $\binom{m+n}{k}(-1)^{m+n-k}a^k b^{m+n-k} \in A$. Since A is closed under addition we conclude that $(a - b)^{m+n} \in A$ so that $a - b \in N(A)$, as needed.

p 270, #44 In order for $a \in \mathbb{Z}_{36}$ to be in $N(\langle 0 \rangle)$ we must have a^n divisible by 36 for some $n \in \mathbb{Z}^+$. This happens if and only if a is divisible by all of the prime factors of 36, which are 2 and 3. That is, a must be divisible by 6. Hence $N(\langle 0 \rangle) = \langle 6 \rangle$.

It is clear that $\langle 3 \rangle \subset N(\langle 3 \rangle)$. By above, $\langle 3 \rangle$ is maximal so that $N(\langle 3 \rangle) = \langle 3 \rangle$ or $N(\langle 3 \rangle) = \mathbb{Z}_{36}$. The latter is impossible since $1 \notin N(\langle 3 \rangle)$. Hence $N(\langle 3 \rangle) = \langle 3 \rangle$.

One can easily verify that $N(N(A)) = N(A)$ for any ideal A. Therefore $N(\langle 6 \rangle) = N(N(\langle 0 \rangle)) = N(\langle 0 \rangle) = \langle 6 \rangle$.

p 271, #52 Let $I = \langle 1 - i \rangle$. We start by noting that $2i = -(-2i) = -(1-i)^2 \in I$. GIven $x + iy \in \mathbb{Z}[i]$, write $x + y = 2k + r$ where $r = 0$ or 1. Then

$$(x + iy) + I = (x(1-i) + (x+y)i) + I = (x+y)i + I = (k(2i) + ri) + I = ri + I.$$

Hence, there are at most two cosets in $\mathbb{Z}[i]/I$: I and $i + I$. It is easy to verify that $i \notin I$ and therefore that $i + I \neq I$. Hence, $\mathbb{Z}[i]/I$ has *exactly* two elements. Since the only nonzero element is $i + I$ and

$$(i + I)^2 = i^2 + I = -1 + I = (1 - 2) + I = 1 + I$$

(as $2 = -i(2i) \in I$) we conclude that $\mathbb{Z}[i]/I$ is a field with two elements.

p 271, #56 We first prove that I is indeed maximal. Let J be an ideal in R with $I \subsetneq J$. Then J must contain an element $x \in R$, $x \notin I$. By hypothesis, x must be a unit in R. Since J is an ideal containing a unit, we have $J = R$. Thus, I is maximal.

Now we show that I is the only maximal ideal. Let J be a maximal ideal in R and let $x \in J$. If $x \notin I$ then, again using the hypothesis, x must be a unit in R. This would imply that $J = R$, which contradicts the fact that J is maximal. Hence, $x \in I$. That is, we have shown that $J \subset I$. Since J is maximal and $I \neq R$, we must have $J = I$. That is, if J is a maximal ideal in R then $J = I$. Hence, I is the only maximal ideal in R.

A commutative ring with a unique maximal ideal is called a *local ring*.