Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 7
October 26, 2007

Section 6.3

3. (a) $\Rightarrow$: We know that for all integers p, we have the isomorphism $\mathbf{Z}/(p) \simeq \mathbf{Z}_p$. If p is a prime, then since the integers mod p is a field, (p) is a maximal ideal in $\mathbf{Z}$ by Theorem 6.15. $\Leftarrow$: Conversely, if (p) is a maximal ideal in $\mathbf{Z}$, then $\mathbf{Z}/(p) \simeq \mathbf{Z}_p$ is a field (again by Theorem 6.15). This only occurs when p is a prime number since $\mathbf{Z}_n$ has zero-divisors whenever n is composite.

(b) This follows by a similar argument, using Theorem 6.15 and Theorem 5.10: $(p(x))$ is a maximal ideal if and only if $F[x]/(p(x))$ is a field, and that is true if and only if $p(x)$ is an irreducible polynomial in $F[x]$.

4. $\Rightarrow$: If R is an integral domain, then $R/(0_R) \simeq R$ is an integral domain, so (0_R) is a prime ideal by Theorem 6.14. $\Leftarrow$: If (0_R) is a prime ideal in R, then $R \simeq R/(0_R)$ is an integral domain.

Comment: This may also be proved by a more direct argument as follows: R is an integral domain if and only if R is a commutative ring with identity that has no zero divisors. This is equivalent to saying that whenever $a, b \in R$ satisfy $ab = 0_R$, then $a = 0_R$ or $b = 0_R$. However, that is equivalent to saying that (0_R) is a prime ideal by the definition.

5. The maximal ideals in $\mathbf{Z}_6$ are $M_1 = (2) = \{0, 2, 4\}$ and $M_2 = (3) = \{0, 3\}$. In each case including any element not already in the ideal produces an ideal containing a unit, hence equal to $\mathbf{Z}_6$. Similarly, the maximal ideals in $\mathbf{Z}_{12}$ are $M_1 = (2) = \{0, 2, 4, 6, 8, 10\}$ and $M_2 = (3) = \{0, 3, 6, 9\}$. (*Comment*: Notice that these are exactly the ideals generated by the classes of the prime integers dividing $6, 12$.)

6. (a) In $\mathbf{Z}_8$, the ideals are the zero ideal (which is not maximal since it is contained in other ideals not equal to the whole ring below), $(1) = (3) = (5) = (7) = \mathbf{Z}_8$ (which is not maximal by definition), $M = (2) = \{0, 2, 4, 6\} = (6)$, and $(4) = \{0, 4\}$. Since $(4) \subset (2) \subset \mathbf{Z}_8$, (4) is not maximal. Hence M is the only maximal ideal: If we take any ideal I with $M \subseteq I \subseteq \mathbf{Z}_8$, then $M = (2)$ or $I = \mathbf{Z}_8$.

Similarly, in $\mathbf{Z}_9$, the only maximal ideal is $M = (3) = (6) = \{0, 3, 6\}$, since $(1) = (2) = (4) = (5) = (7) = (8) = \mathbf{Z}_9$. If $M \subseteq I \subseteq \mathbf{Z}_9$, then $I = M$ or $I = \mathbf{Z}_9$.

(b) In $\mathbf{Z}_{10}$, both (2) and (5) are maximal. In $\mathbf{Z}_{15}$, both (3) and (5) are maximal. This can be seen either by arguing as in part a, or by noting that by computations with the coset addition and multiplication tables like what we did on the last problem set, $\mathbf{Z}_{10}/(2) \simeq \mathbf{Z}_2$, and $\mathbf{Z}_{10}/(5) \simeq \mathbf{Z}_5$. Both of these are fields, so (2) and (5) are maximal ideals by Theorem 6.15. Similarly, $\mathbf{Z}_{15}/(3) \simeq \mathbf{Z}_3$ and $\mathbf{Z}_{15}/(5) \simeq \mathbf{Z}_5$. Both of these are fields, so (3) and (5)

are maximal. *Comment:* The general fact that is being hinted at in these problems is that $\mathbf{Z}_n$ has just one maximal ideal if and only if $n = p^r$ for some prime and some $r \geq 2$. This is true because the maximal ideals in $\mathbf{Z}_n$ are in one-to-one correspondence with the primes dividing n.

11. We will show that

$$\mathbf{Z}[x]/(x-1) \simeq \mathbf{Z}. \tag{1}$$

Since $\mathbf{Z}$ is an integral domain but not a field, the isomorphism (1) will show that $(x-1)$ is a prime ideal but not a maximal ideal using Theorems 6.14 and 6.15. To establish (1), consider the mapping

$$\begin{aligned} \varphi : \mathbf{Z}[x] &\to \mathbf{Z} \\ f(x) &\mapsto f(1) \end{aligned}$$

Then φ is a ring homomorphism since for all $f(x), g(x) \in \mathbf{Z}[x]$,

$$\varphi(f(x) + g(x)) = f(1) + g(1) = \varphi(f(x)) + \varphi(g(x))$$

and

$$\varphi(f(x) \cdot g(x)) = f(1) \cdot g(1) = \varphi(f(x)) \cdot \varphi(g(x)).$$

The mapping φ is onto $\mathbf{Z}$ since for all $n \in \mathbf{Z}$, $n = \varphi(f(x))$ for the constant polynomial $f(x) = n + 0x + \cdots$. The kernel of φ consists of all polynomials $f(x) \in \mathbf{Z}[x]$ such that $\varphi(f(x)) = f(1) = 0$. We claim that this is precisely the ideal $(x-1)$. If $f(x) \in (x-1)$, then $f(x) = (x-1)g(x)$ for some $g(x) \in \mathbf{Z}[x]$. Then it is clear that $\varphi(f(x)) = f(1) = 0$. So $(x-1) \subseteq \ker(\varphi)$. On the other hand, if $f(x) \in \ker(\varphi)$, then by the Factor Theorem (Theorem 4.15), in $\mathbf{Q}[x]$ it follows that $(x-1)|f(x)$. By Theorem 4.22 (or a direct argument), this implies that $f(x) = (x-1)g(x)$ for some $g(x) \in \mathbf{Z}[x]$. Hence $\ker(\varphi) = (x-1)$. But now, "putting everything together" we have that

$$\mathbf{Z} = \mathrm{im}(\varphi) \simeq \mathbf{Z}[x]/\ker(\varphi) = \mathbf{Z}[x]/(x-1)$$

by the First Isomorphism Theorem. This establishes (1) and concludes the proof.

12. Let $M = \{(pa, b) \in \mathbf{Z} \times \mathbf{Z} : a, b \in \mathbf{Z}\}$. Then M is an ideal since it is nonempty, closed under differences:

$$(pa, b) - (pa', b') = (p(a - a'), b - b') \in M,$$

and closed under products by arbitrary elements in $\mathbf{Z} \times \mathbf{Z}$:

$$(c, d) \cdot (pa, b) = (p(ca), bd) \in M.$$

(Note: $\mathbf{Z} \times \mathbf{Z}$ is a commutative ring under the componentwise sum and product, so this suffices.) Now to show M is maximal we will establish the isomorphism

$$(\mathbf{Z} \times \mathbf{Z})/M \simeq \mathbf{Z}_p. \tag{2}$$

Since the integers mod p is a field when p is prime, M is maximal by Theorem 6.15. To prove (2), note that the distinct cosets of M are the $(r,0)+M$ for $r=0,1,\ldots,p-1$: Every (c,d) belongs to one of these cosets since when we divide p into c we get $c=qp+r$ with $0\le r\le p-1$. So

$$(c,d)=(r,0)+(pq,d)\in(r,0)+M.$$

Then the coset addition and multiplication operations are

$$((r,0)+M)+((r',0)+M)=(r+r',0)+M=(r+r' \bmod p,0)+M$$

and

$$((r,0)+M)\cdot((r',0)+M)=(r\cdot r',0)+M=(r\cdot r' \bmod p,0)+M.$$

This shows (2).

13. Take $I=\{(0,b):b\in\mathbf{Z}\}$ for instance. Then I is an ideal since it is nonempty, closed under sums, and closed under products by arbitrary $(c,d)\in\mathbf{Z}\times\mathbf{Z}$. It is prime but not maximal because $(\mathbf{Z}\times\mathbf{Z})/I\simeq\mathbf{Z}$. This follows from the First Isomorphism Theorem applied to the projection

$$\begin{aligned}\pi:\mathbf{Z}\times\mathbf{Z}&\to\mathbf{Z}\\(a,b)&\mapsto a\end{aligned}$$

This π is a ring homomorphism since

$$\pi((a,b)+(c,d))=\pi(a+b,c+d)=a+b=\pi(a,b)+\pi(c,d)$$

and

$$\pi((a,b)\cdot(c,d))=\pi(ab,cd)=ab=\pi(a,b)\cdot\pi(c,d).$$

We have

$$\operatorname{im}(\pi)=\mathbf{Z}\simeq(\mathbf{Z}\times\mathbf{Z})/\ker(\pi)=(\mathbf{Z}\times\mathbf{Z})/I.$$

By Theorems 6.14 and 6.15, I is prime but not maximal since $\mathbf{Z}$ is an integral domain but not a field.

17. (Note: the surjective hypothesis here is only needed to show that $I\neq R$, part of the way prime ideals are defined in the text. This is not always included in the definition of a prime ideal. The reason to do it as Hungerford does is so that, for instance, $\mathbf{Z}=(1)$ is not counted as a prime ideal in $\mathbf{Z}$. Then you can say a nonzero ideal $I\in\mathbf{Z}$ is a prime ideal if and only if $I=(p)$ for a prime number p.) To be complete, we begin by showing that the set I is an ideal in R. First, I is nonempty since $f(0_R)=0_S\in J$, so $0_R\in I$. If $a,b\in I$, then $f(a),f(b)\in J$. But then $f(a)-f(b)=f(a-b)\in J$ since J is an ideal. Hence $a-b\in I$. Similarly for all $r\in R$, $a\in I$, we have $f(ra)=f(r)f(a)$. Since J is an ideal, $f(a)\in J$, and $f(r)\in S$, this is in J. Hence $ra\in I$.

Now suppose J is a prime ideal in S. According to Hungerford's way of defining prime ideals, this means $J\neq S$. But then since f is surjective, it must be the case that $I\neq R$. If $a,b\in R$ and $ab\in I$, then $f(ab)=f(a)f(b)\in J$. Since J is prime, this implies $f(a)\in J$ or $f(b)\in J$. Hence $a\in I$ or $b\in I$. Therefore I is a prime ideal in R.