Solution Outlines for Chapter 14

4: Find a subring of $\mathbb{Z} \oplus \mathbb{Z}$ that is not an ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

$I = \{(a,a)|a \in \mathbb{Z}\}$ is a subring but not an ideal since $(1,2)(a,a) = (a,2a) \notin I$.

6: Find all maximal ideals in:

a. $\mathbb{Z}_8$: (2)

b. $\mathbb{Z}_{10}$: (2), (5)

c. $\mathbb{Z}_{12}$: (2), (3)

d. $\mathbb{Z}_n$: The maximal ideals are of the form (p) where p is a prime that divides n.

8: Prove that the intersection of any set of ideals of a ring is an ideal.

Let J be the intersection of ideals, and $a, b \in J$. Then a and b are in each ideal so $a - b$, ra and ar are in each ideal as well (here, r is an arbitrary ring element). Then $a - b$, ra and ar are each in J and J is an ideal. Notice that J is non-empty since each ideal contains 0.

11: In the ring of integers, find a positive integer a such that:

1. $< a >=< 2 > + < 3 >$ Since $< a > \in 1 = -2 + 3$, $a = 1$.
2. $< a >=< 6 > + < 8 >$ $a = 2$
3. $< a >=< m > + < n >$ $a = gcd(m, n)$

14: Let A and B be ideals of a ring. Prove that $AB \subseteq A \cap B$.

Let $x \in AB$. Then x is of the form ab for some $a \in A$ and $b \in B$. Since A is an ideal, $ab \in A$. Similarly, $ab \in B$. Hence $x \in A \cap B$.

20: Suppose that R is a commutative ring and $|R| = 30$. If I is an ideal of R and $|I| = 10$, prove that I is a maximal ideal.

Let R be an order 30 commutative ring, and I be an ideal of R with order 10. Then R/I has order 3 and is thus isomorphic to $\mathbb{Z}_3$. Since $\mathbb{Z}_3$ is a field, I must be a maximal ideal.

28: Show that $\mathbb{R}[x]/ < x^2 + 1 >$ is a field.

To show that $\mathbb{R}[x]/ < x^2 + 1 >$ is a field, we only need to show that $< x^2 + 1 >$ is maximal in $\mathbb{R}[x]$. Suppose that $I =< x^2 + 1 > \subset J \subseteq \mathbb{R}[x]$. Then there exists an $f(x) \in J$ such that $f(x) \notin I$. Hence $f(x) = q(x) \cdot (x^2+1) + r(x)$ for some polynomials $q(x), r(x) \in \mathbb{R}[x]$ with $0 \leq deg(r(x)) < 2$. Moreover, $r(x) \neq 0$. Hence $r(x)$ is linear and of the form $ax + b$ for some non-zero real numbers a, b. Now, $f(x) - q(x)(x^2 + 1) \in J$ so $r(x) = ax + b \in J$.

Since $ax - b \in R[x]$, $(ax + b)(ax - b) = a^2x^2 - b^2 \in J$. Similarly, $a^2(x^2 + 1) \in J$. Thus $(a^2x^2 + a^2) - (a^2x^2 - b^2) = a^2 + b^2 \in J$. Since $a^2 + b^2$ in not zero, J contains a constant and all constants in $R[x]$ are units. Hence $1 \in J$ and $J = R$. Therefore we can conclude that $< x^2 + 1 >$ is indeed maximal as desired.

 # 32: Let $R = \mathbb{Z}_8 \oplus \mathbb{Z}_{30}$. Find all maximal ideals of R, and for each maximal ideal I, identify the size of the field R/I.

$< 1 > \oplus < 2 >$. In this case the size of the quotient field is $(8 * 30)/(8 * 15) = 2$.
$< 1 > \oplus < 3 >$. In this case the size of the quotient field is $(8 * 30)/(8 * 10) = 3$.
$< 1 > \oplus < 5 >$. In this case the size of the quotient field is $(8 * 30)/(8 * 6) = 5$.
$< 2 > \oplus < 1 >$. In this case the size of the quotient field is $(8 * 30)/(4 * 30) = 2$.

 # 33: How many elements are in $\mathbb{Z}[i]/ < 3 + i >$? Give reasons for your answer.

First we notice that $(3 + i)(3 - i) = 10 \in< 3 + i >$. Hence $10+ < 3 + i >=< 3 + i >$. Now what about the i terms? Observe that $i+ < 3+i >= i+(-3-i)+ < 3+i >= -3+ < 3+i >= 7+ < 3+i >$. Hence $a+bi+ < 3+bi >$ can be expressed as just $a+ < 3+bi$, and a ranges from 0 to 9. Moreover, it is clear that $1+ < 3 + i >$ has (additive) order 10. Thus the quotient ring is simply $\{k+ < 3 + i > \big| k \in \{0, 1, \ldots, 9\}\}$. So there are 10 elements in the quotient ring.

 # 36: Let R be a ring and let I be an ideal of R. Prove that the factor ring R/I is commutative if and only if $rs - sr \in I$ for all r and s in R.

Let R and I be as above. Assume R/I is commutative. Then for all $r, s \in R$, $(r + I)(s + I) = rs + I = sr + I = (s + I)(r + I)$. Since $rs + I = sr + I$, $rs - sr \in I$ (property of cossets in additive notation). Now assume that $rs - sr \in I$ for all $r, s \in R$. Then $rs + I = sr + I$ but reversing the calculation above shows that this implies the quotient ring is commutative.

 # 38: Prove that $I =< 2 + 2i >$ is not a prime ideal of $\mathbb{Z}[i]$. How many elements are in $\mathbb{Z}[i]/I$? What is the characteristic of $\mathbb{Z}[i]/I$?

Notice that $2(1 + i) = 2 + 2i \in I$ but $2 \notin I$ and $1 + i \notin I$. This shows I is not a prime ideal. Notice, $(2+2i)(1-i) = 2-2i+2i+2 = 4 \in I$ and $i+I = -(i+2)+I = -i+2+I$. So $a + bi + I$ would have a in $0, 1, 2, 3$ and b in $0, 1$. Thus there are $4 * 2 = 8$ elements in the quotient ring. The characteristic is n such that $n(a + bi) + I = I$, and hence it is 4.

 # 39: In $\mathbb{Z}_5[x]$, let $I =< x^2 + x + 2 >$. Find the multiplicative inverse of $2x + 3 + I$ in $\mathbb{Z}_5[x]/I$.

To be the multiplicative inverse, we need $(f(x)+I)(2x+3+I) = (f(x)*(2x+3))+I = 1+I$. Observe $(3x + 1)(2x + 3) + I = 6x^2 + 11x + 3 + I = x^2 + x + 3 + I = 1 + I$. Hence the multiplicative inverse is $3x + 1 + I$.

 # 46: Let R be a commutative ring and let A be any ideal of R. Show that the *nil radical* of A, $N(A) = \{r \in R | r^n \in A$ for some positive integer $n\}$ is an ideal of R.

Let $x, y \in A$. Then there exists an $n, m \in \mathbb{Z}_{>0}$ such that $x^n \in A$ and $y^m \in A$. Now $(x+y)^{n+m}$ expands such that for each term either the power of $x \geq n$ or the power of $y \geq m$. Hence, since A is an ideal, each term is in A so $x + y \in A$. Thus $x + y \in N(A)$. Now, let $r \in R$. Then $(rx)^n = r^n x^n$ since R is commutative. We know that $x^n \in A$ and $r^n \in R$, so $r^n x^n \in A$. Thus $rx \in N(A)$. Similarly, $xr \in N(A)$.

 # 47: Let $R = \mathbb{Z}_{27}$. Find:

a. $N(< 0 >)$.

   By definition, $N(< 0 >) = \{a \in \mathbb{Z}_{27} | a^n \in < 0 > \text{ for some } n \in \mathbb{Z}_{\geq 0}\} =< 3 >$.

b. $N(< 3 >)$.

   $< 3 >$

c. $N(< 9 >)$.

   $< 3 >$

 # 49: Let R be a commutative ring. Show that $R/N(< 0 >)$ has no nonzero nilpotent elements.

Suppose that $x + N(< 0 >)$ is a nilpotent element in $R/N(< 0 >) = R/I$. Then $(x + I)^n = x^n + I$ is I for some $n \in \mathbb{Z}_{>0}$. This implies that $x^n \in I$. Hence there exists an m such that $(x^n)^m = 0$, by the definition of $N(< 0 >)$. But this implies that $x \in I$. Hence $x + I = I$ and was zero to begin with.