Ch 15: 10, 24
Ch 15: 43, 47, 48, 57
Ch 16: 4, 9, 17, 18
Ch 16: 12, 19, 24, 39, 40, 41

__Chapter 15__

10) **a) Is 2Z isomorphic to 3Z?**
Suppose such an isomorphism $\phi: 2Z \to 3Z$ exists. Then $\phi(2) = 3n$ for some $n \in Z$.
$\phi(2)\phi(2) = \phi(2*2) = \phi(4) = \phi(2+2) = \phi(2) + \phi(2)$. So we must have
$\phi(2)\phi(2) = \phi(2) + \phi(2) \to (3n)(3n) = 3n + 3n \to 9n^2 = 6n$
$n = 0$ or $n = 2/3$. But both are impossible.
ϕ cannot exist.

b) Is 2Z isomorphic to 3Z?
Similarly, $\phi(2) = 4n$ for some integer n.
$\phi(2)\phi(2) = \phi(2) + \phi(2) \to (4n)(4n) = 4n + 4n \to 16n^2 = 8n$
$n = 0$ or $n = 1/2$. But both are impossible.
f cannot exist.

24) **Consider homomorphism $\phi: Z \oplus Z \to Z \oplus Z$. What are the possibilities for $\phi((1, 0))$?**
Claim: ϕ carries idempotents to idempotents.
Proof: Let x be an idempotent. Then $(\phi(x))^2 = \phi(x)\phi(x) = \phi(x^2) = \phi(x)$.
We can find 9 such homomorphisms:
$\phi((a, b)) = (a, b)$; $\phi((a, b)) = (b, a)$; $\phi((a, b)) = (a, a)$
$\phi((a, b)) = (a, 0)$; $\phi((a, b)) = (0, a)$; $\phi((a, b)) = (b, b)$
$\phi((a, b)) = (0, b)$; $\phi((a, b)) = (b, 0)$; $\phi((a, b)) = (0, 0)$

We see that there are 4 possibilities for $\phi((1, 0))$; they are (1, 0), (0, 1), (1, 1), (0, 0).

43) **Let R and S be commutative rings with unity. If ϕ is a homomorphism from R onto S and the characteristic of R is nonzero, prove that char(S) divides char(R)**

By Theorem 13.3, char(R) is the order of 1_R under addition.
char(S) is the order of 1_S under addition.
<u>ϕ is onto</u>. Since S is nontrivial, $\phi(1_R) = 1_S$ by Theorem 15.1, part 6.
by Theorem 10.1 (Properties of Group Homomorphisms),
the order of $\phi(1_R) = 1_S$ under addition must divide that of 1_R.
so char(S) divides char(R) .

47) **Suppose that R and S are commutative rings with unities. let ϕ be a ring homomorphism from R onto S and let A be an ideal of S.**
a) If A is prime in S, show that $\phi^{-1}(A) = \{x \in R \mid \phi(x) \in A\}$ is prime in R.

Theorem 15.1, part 4 states that $\phi^{-1}(A)$ is an ideal of R.
let $ab \in \phi^{-1}(A)$. Then $\phi(ab) = \phi(a)\phi(b) \in A$
Since A is prime, $\phi(a)\phi(b) \in A$ implies that $\phi(a) \in A$ or $\phi(b) \in A$,
hence $a \in \phi^{-1}(A)$ or $b \in \phi^{-1}(A)$.

b) If A is maximal in S, show that $\phi^{-1}(A)$ is maximal in R.

<u>Solution 1</u> (the "direct" method):
Suppose that there is some ideal I in R that <u>properly contains</u> $\phi^{-1}(A)$.

$\phi^{-1}(A) \subseteq I$, so $\phi(\phi^{-1}(A)) \subseteq \phi(I)$. A well-known result from set/function theory states that if ϕ is surjective, then $\phi(\phi^{-1}(A)) = A$. So $A \subseteq \phi(I)$.

$\phi^{-1}(A)$ is properly contained in I, so there exists an element b such that $b \in I$ and $b \notin \phi^{-1}(A)$.
Then by definition $\phi(b) \in \phi(I)$ and $\phi(b) \notin A$.
Hence $A - \phi(I)$ is nonempty and <u>A is properly contained in $\phi(I)$</u>.

But A is maximal, meaning that $\phi(I) = S$.
Clearly $I \subseteq R$. Now suppose $r \in R$. Then $\phi(r) \in S = \phi(I)$
For some $r' \in I$, $\phi(r) = \phi(r')$. Then $0 = \phi(r) - \phi(r') = \phi(r - r')$
$(r - r') \in \text{Ker } \phi = \phi^{-1}(\{0\}) \subseteq \phi^{-1}(A) \subseteq I \rightarrow r' + (r - r') = r \in I \rightarrow I = R$.
So $\phi^{-1}(A)$ must be maximal.

<u>Solution 2</u> ("book method")
Consider the natural ring homomorphism $\varphi: S \rightarrow S/A$ defined by $\varphi(s) = s + A$.
By theorem 15.4, A is the kernel of this homomorphism.
Then the homomorphism $(\varphi \circ \phi): R \rightarrow S/A$ defined by $(\varphi \circ \phi)(r) = \phi(r) + A$ has $\phi^{-1}(A)$ as its kernel.

The mapping given by $\psi(r + \phi^{-1}(A)) = \phi(r) + A$ is an isomorphism from $R/\phi^{-1}(A)$ to $(\varphi \circ \phi)(R)$, by Theorem 15.3.

Now consider $(\varphi \circ \phi)(R)$. ϕ is surjective, and clearly φ is also surjective (for each $(s + A) \in S/A$, we can easily see that $\varphi^{-1}(\{s + A\})$ has at least one element). So the mapping $\varphi \circ \phi$ is surjective and $(\varphi \circ \phi)(R) = S/A$. Hence $R/\phi^{-1}(A) \cong S/A$.

A is maximal in S, so by Theorem 14.4, S/A is a field. But this means that $R/\phi^{-1}(A)$ is also a field by isomorphism (this is easily checked). Again by Theorem 14.4, $\phi^{-1}(A)$ is maximal.

48) **A principal ideal ring is a ring with the property that every ideal has the form $\langle a \rangle$. Show that the homomorphic image of a principal ideal ring is a principal ideal ring.**

Consider a principal ideal ring R and the ring homomorphism $\phi: R \rightarrow S$. From Theorem 15.1 part 2, $\phi(R)$ is a subring of S.
Now consider an ideal I in $\phi(R)$. By From Theorem 15.1 part 4, then $\phi^{-1}(I)$ is an ideal of R.
Because R is a principal ideal ring, there exists some $a \in R$ such that $\phi^{-1}(I) = \langle a \rangle$.
Note that $\phi(\langle a \rangle) = I$ because I is contained in the image.

Suppose $s \in \langle \phi(a) \rangle$. Then $s = s'\phi(a)$ for some $s' \in \phi(R)$. But $a \in \langle a \rangle = \phi^{-1}(I)$, so $\phi(a) \in I$. By the definition of an ideal, $s'\phi(a) \in I$ for ALL $s' \in \phi(R)$. So $s \in I$ and hence $\langle \phi(a) \rangle \subseteq I$.
Suppose $s \in I \subseteq \phi(R)$. Then $s = \phi(r)$ for some $r \in \langle a \rangle$. Then $r = r'a$ for some $r' \in R$ (definition of $\langle a \rangle$). Thus $s = \phi(r) = \phi(r'a) = \phi(r')\phi(a)$. Hence $s \in \langle \phi(a) \rangle$ and $I \subseteq \langle \phi(a) \rangle$.

Thus $I = \langle \phi(a) \rangle$, and $\phi(R)$ must be a principal ideal ring.

57) **Let $Z[i] = \{a + bi \mid a, b \in Z\}$. Show that the field of quotients of $Z[i]$ is ring-isomorphic to $Q[i] = \{r + si \mid r, s \in Q\}$.**

Direct verification

<u>Chapter 16</u>

4) Direct verification

9) Direct verification

17) Direct verification – This is directly dependent on the fact that there are no zero-divisors in an integral domain.

18) **Prove that the ideal $\langle x \rangle$ in $Q[x]$ is maximal.**

Suppose J is an ideal in Q[x] that properly contains the ideal $\langle x \rangle$. But the only kind of element that can belong in J and not $\langle x \rangle$ is a polynomial that contains a nonzero rational constant. Since J is closed under addition, we can simply subtract the non-constant parts (which belong in $\langle x \rangle$) from this polynomial, leaving only the rational constant which is a unit in J. An ideal that contains a unit must be the entire ring, so $J = Q[x]$. Hence $\langle x \rangle$ is maximal in Q[x].

Or, we can consider an arbitrary element of the factor ring $Q[x]/\langle x \rangle$, namely $p(x) + \langle x \rangle$. If p(x) has no nonzero constants, then $p(x) + \langle x \rangle = \langle x \rangle$, which is the additive identity in $Q[x]/\langle x \rangle$. However, if p(x) has a nonzero constant p_0, then $p(x) + \langle x \rangle$ can be rewritten as $p_0 + \langle x \rangle$, which has a multiplicative inverse $(1/p_0) + \langle x \rangle$. So $Q[x]/\langle x \rangle$ is a field, hence $\langle x \rangle$ is maximal.

12) Simple computation: in $Z_7[x]$, $5x^4 + 3x^3 + 1 = (3x^2 + 2x + 1)(\underline{4x^2 + 3x + 6}) + (\underline{6x + 2})$

19) Direct verification (given in back of book)

24) **Prove that Z[x] is not a principal ideal domain. (Compare this with Theorem 16.3.)**

A counterexample is sufficient. There are many ideals in Z[x] that cannot be generated by a single polynomial. One is given in the answer to #39.

39) **Give an example of a commutative ring R with unity and a maximal ideal I of R such that I[x] is not a maximal ideal of R[x].**

Let R = Z and I = $\langle 2 \rangle$. Then the ideal of Z[x] consisting of polynomials with the terms of highest and/or lowest power having even coefficients is one that properly contains $\langle 2 \rangle[x]$, since the coefficients of the middle terms need not be even.

40) **Let R be a commutative ring with unity. If I is a prime ideal of R, prove that I[x] is a prime ideal of R[x].**

Direct verification (or consult http://math.arizona.edu/~lebovitz/415/415feb10.pdf)

41) **Let f(x) and g(x) belong to F[x], where F is a field. If f(x) and g(x) are relatively prime, prove that there exist polynomials h(x) and k(x) in F[x] such that f(x)h(x) and g(x)k(x) = 1.**

F[x] is a PID, so $\langle f(x), g(x) \rangle = \langle a(x) \rangle$ for some a(x) in F[x]. The fact that a(x) divides both f(x) and g(x) implies that a(x) is a constant, hence a unit. So $1 \in \langle 1 \rangle = F[x] = \langle f(x), g(x) \rangle$.