Homeworks 3, 4, 5

Chapter 15
Theorems: 15.1 (All 8 parts), 15.2, 15.3, 15.4, 15.5 (and Corollaries 1 and 2 of this theorem)
Examples: 1-7, 10
Exercises (page 287)
Problems: 1-6, 8-19, 21-23, 42, 64, 66

Chapter 16
Theorem: 16.1
Theorem: 16.2 (Statement only)
Corollaries 1-3 of Theorem 16.2
Theorems: 16.3, 16.4
Examples: 1-3
Exercises (page 300)
Problems: 5-8, 13-18, 21, 22, 24, 29, 30, 32, 41
(the material listed above is the Test 2 Material)
The exercises and theorems covered since test 2 are included in Homeworks 6 and 7 and in this handout.

THEOREMS

1. **Theorem 15.1** Let $\phi$ be a ring homomorphism from a ring $R$ to a ring $S$. Let $A$ be a subring of $R$ and $B$ be an ideal of $S$. Then

   (a) For any $r \in R$ and any positive integer $n$, $\phi(nr) = (\phi(r))^n$. $n \phi(r) \quad \text{and} \quad \phi(r^n) = (\phi(r))^n$

   (b) $\phi(A) = \{\phi(a) | a \in R\}$ is a subring of $S$.

   (c) If $A$ is an ideal of $R$ and $\phi$ is onto, then $\phi(A)$ is an ideal of $S$.

   (d) $\phi^{-1}(B) = \{r \in R | \phi(r) \in B\}$ is an ideal of $S$.

   (e) If $R$ is commutative, then $\phi(R)$ is commutative.

   (f) If $R$ has a unity $1$, $S \neq \{0\}$ and $\phi$ is onto, then $\phi(1)$ is the unity of $S$.

   (g) $\phi$ is an isomorphism if and only if $\phi$ is onto and Ker $\phi = \{0\}$.

   (h) If $\phi$ is an isomorphism from $R$ onto $S$, then $\phi^{-1}$ is an isomorphism from $S$ onto $R$.

2. **Theorem 15.2** Let $\phi$ be a ring homomorphism from a ring $R$ to a ring $S$. Then Ker $\phi$ is an ideal of $R$.

3. **Theorem 15.3** Let $\phi$ be a ring homomorphism from a ring $R$ to a ring $S$. Then the mapping from $R$/Ker $\phi$ to $\phi(R)$, given by $r + \text{Ker } \phi \rightarrow \phi(r)$, is an isomorphism.

   In symbols, $R$/Ker $\phi \cong \phi(R)$.

4. **Theorem 15.4** Let $R$ be a ring and let $A$ be an ideal of $R$. Then the mapping $r \rightarrow r + A$ is a ring homomorphism from $R$ onto $R/A$.

5. **Theorem 15.5** Let $R$ be a ring with unity 1. The mapping $\phi : \mathbb{Z} \rightarrow R$ given by $n \rightarrow n.1$ is a ring homomorphism.

6. **Corollary 1**

   (a) If $R$ is a ring with unity and the characteristic of $R$ is $n > 0$, then $R$ contains a subring isomorphic to $\mathbb{Z}_n$.

   (b) If $R$ is a ring with unity and the characteristic of $R$ is 0, then $R$ contains a subring isomorphic to $\mathbb{Z}$.

7. **Corollary 2** For any positive integer $m$, the mapping $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_m$ given by $x \rightarrow x \mod m$ is a ring homomorphism.

8. **Theorem 16.1** If $D$ is an integral domain, then $D[x]$ is an integral domain.

9. **Corollary 1** Let $F$ be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$. 
10. Corollary 2 Let $F$ be a field and $a \in F$, and $f(x) \in F[x]$. Then $a$ is a zero of $f(x)$ if and only if $x-a$ is a factor of $f(x)$.

11. Corollary 3 A polynomial of degree $n$ over a field $F$ has at most $n$ zeros (counting multiplicities) in $F$.

12. Theorem 16.3 Let $F$ be a field. Then $F[x]$ is a principal ideal domain.

13. Theorem 16.4 Let $F$ be a field, $I$ a nonzero ideal in $F[x]$, and $g(x)$ an element of $F[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in $I$.

14. Let $F$ be field. If $f(x) \in F[x]$ and $\deg f(x) = 2$ or $3$, then $f(x)$ is reducible over $F$ if and only if $f(x)$ has a zero in $F$.

15. Let $F$ be a field and let $p(x) \neq 0 \in F[x]$. Then $p(x)$ is irreducible iff $\langle p(x) \rangle$ is a prime ideal.

16. If $R$ is a principal ideal domain, then every nonzero prime ideal $I$ is a maximal ideal.

17. Let $F$ be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over $F$.

$\langle p(x) \rangle$ is irreducible over $F \iff \langle p(x) \rangle$ is a prime ideal in $F[x] \iff F[x]/\langle p(x) \rangle$ is a field.
18. Let $F$ be a field and $p(x)$ an irreducible polynomial over $F$. Then $F[x]/(p(x))$ is a field. Since $\deg(p(x))$ is a maximal ideal of $F[x]$.

19. If $F$ is a field and $p(x) \in F[x]$ is irreducible, then the quotient ring $F[x]/(p(x))$ is a field containing (an isomorphic copy of) $F$ and a root of $F$.

Show $\phi : F \to F[x]/(p(x))$ given by $a \mapsto a + (p(x))$ is an isomorphism and $(a + p(x))a \in F[x]$ is a subfield of $F[x]/(p(x))$ that is isomorphic to $F$. Next, show $\theta = x + (p(x))$ is a root of $p(x)$ are identified with $a_0 + (p(x)), a_1 + (p(x)), \ldots, a_n + (p(x))$.

20. Let $E$ be a field and $F \subseteq E$ be a subfield of $E$, and $a \in E$. In $E$, let

$F[a] = \{ f(a) : f(x) \in F[x] \}$, and

$F(a) = \{ f(a) : f(x), g(x) \in F[x], g(a) \neq 0 \}$. Then

(a) $F[a]$ is a subring of $E$ containing $F$ and $a$.

(b) $F[a]$ is the smallest subring of $E$ containing $F$ and $a$.

(c) $F(a)$ is a subfield of $E$ containing $F$ and $a$.

(d) $F(a)$ is the smallest subfield of $E$ containing $F$ and $a$.

21. Let $E$ be a field and $F \subseteq E$ be a subfield of $E$, let $a \in E$ and let $p(x) \in F[x]$ be a monic irreducible having $a$ as a root. Then $I = \{ g(x) \in F[x] : g(a) = 0 \}$ is a proper ideal of $F[x]$.

22. Let $E$ be a field and $F \subseteq E$ be a subfield of $E$, let $a \in E$, and let $p(x) \in F[x]$ be a monic irreducible having $a$ as a root.

(i) $\deg(p) \leq \deg(f)$ for every $f(x) \in F[x]$ having $a$ as a root.

Let $f(x) \in F[x]$ having $a$ as a root. Then $f(x) \in I = \{ g(x) \in F[x] : g(a) = 0 \}$. Now $d = \gcd(f, p) \in I$, since it is a linear combination of $f$ and $p$ and therefore has $a$ as a root. But $p$ is irreducible over $F$ if $d = 1$ or $d = p$ because 1 and $p$ are the only monic divisors of $p$. However, $d = 1$ is an impossibility since $1 \notin I$. Thus, $d = p$ and $p|f$. So $\deg(p) \leq \deg(f)$.

(ii) $p(x)$ is the only monic polynomial in $F[x]$ of degree $\deg(p)$ that has $a$ as a root.

Suppose $q$ is another monic polynomial in $F[x]$ such that $\deg(q) = \deg(p)$. Since $q$ has a root, then $q|p \in F[x]$ has $a$ as a root. So, by (i), $q|p$. Thus, $p = q$.

23. Let $E$ be a field and $F \subseteq E$ be a subfield of $E$, and let $a \in E$ be algebraic over $F$.

(i) There is a monic irreducible polynomial $p(x) \in F[x]$ having $a$ as a root; Define $\phi : F[x] \to E$ by $\phi(f(x)) = f(a) \forall f(x) \in F[x]$. Then $\phi$ is a homomorphism. By the First Isomorphism Theorem $F[x]/\ker \phi \cong \phi(E)$. Now $\phi(F[x])$ is an integral domain since $\phi$ is a homomorphism and $F[x]$ is an integral domain. So $F[x]/\ker \phi$ is an integral domain. Since $a \in E$ is algebraic over $F$, $\ker \phi \neq \{0\}$ and $\ker \phi \neq F[x]$ since $1 \notin \ker \phi$. By Theorem 14.3, $\ker \phi$ is a prime ideal in $F[x]$. By Theorem 16.3, since $F[x]$ is a PID, $F[x]$ is a monic polynomial $p(x) \in F[x]$ such that $\ker \phi = \langle p(x) \rangle$. Since a nonzero polynomial $p(x) \in F[x]$ is irreducible if $\langle p(x) \rangle$ is a prime ideal, $p(x)$ is irreducible.

(ii) $F[x]/\langle p(x) \rangle \cong F(a)$, in fact, there is an isomorphism $\Phi : F[x]/\langle p(x) \rangle \to F(a)$, fixing $F$ pointwise, with $\Phi(x + \langle p(x) \rangle) = a$.

According to the First Isomorphism Theorem, $\Psi : F[x]/\langle p(x) \rangle \to \phi(F[x])$ is an isomorphism that is given by $\Psi(f(x + \langle p(x) \rangle) = \phi(f(a))$. Thus $\Psi(x + \langle p(x) \rangle) = a$ and $\Psi(c + \langle p(x) \rangle) = c \forall c \in F$. Thus, we identify the subfield $F' = \{ c + \langle p(x) \rangle | c \in F \}$ with $F$.

(iv) $[F(a) : F] = \deg(p)$. Assume that $\deg(p) = n$. Then every element of $F[x]/\langle p(x) \rangle$ can be written uniquely as $c_{n-1}x^{n-1} + \ldots + c_1x + c_0 + \langle p(x) \rangle$, where $c_0, c_1, \ldots, c_{n-1} \in F$. Since $\Psi(x + \langle p(x) \rangle) = a$ and $\Psi(c + \langle p(x) \rangle) = c \forall c \in F$, every element of $F[x]/\langle p(x) \rangle$ can be written uniquely as $c_{n-1}x^{n-1} + \ldots + c_1a + c_0$. Hence, $\{1, a, \ldots, a^{n-1}\}$ is a basis of $F(a)$ over $F$. 

EXERCISES (Page 367) Problems:

1. Describe the elements of $\mathbb{Q}(\sqrt{5})$.

2. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

3. Find the splitting field of $x^3 - 1$ over $\mathbb{Q}$. Express your answer in the form $\mathbb{Q}(a)$.

4. Find the splitting field of $x^4 + 1$ over $\mathbb{Q}$.

5. Find the splitting field of $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ over $\mathbb{Q}$.

6. Let $a, b \in \mathbb{R}$ with $b \neq 0$. Show that $\mathbb{R}(a + bi) = \mathbb{C}$.

7. Find a polynomial $p(x) \in \mathbb{Q}[x]$ such that $\mathbb{Q}(\sqrt{1 + \sqrt{5}})$ is ring-isomorphic to $\mathbb{Q}[x]/\langle p(x) \rangle$.

8. Let $F = \mathbb{Z}_2$ and let $f(x) = x^3 + x + 1 \in F[x]$. Suppose that $a$ is zero of $f(x)$ in some extension of $F$. How many elements does $F(a)$ have? Express each member of $F(a)$ in terms of $a$. Write out a complete multiplication table for $F(a)$.

9. Let $F(a)$ be the field described in Exercise 8. Express each of $a^3$, $a^{-2}$, $a^{100}$ in the form $c_2a^2 + c_1a + a_0$.

10. Let $F(a)$ be the field described in Exercise 8. Show that $a^2$ and $a^2 + a$ are zeros of $x^3 + x + 1$.

11. Describe the elements in $\mathbb{Q}(\pi)$.

12. Let $F = \mathbb{Q}(\pi^3)$. Find a basis for $F(\pi)$ over $F$.

16. Suppose $\beta$ is a zero of $f(x) = x^4 + x + 1$ in some field extension $E$ of $\mathbb{Z}_2$. Write $f(x)$ as a product of linear factors in $E[x]$.

20. Let $F$ be a field, and let $a$ and $b$ belong to $F$ with $a \neq 0$. If $c$ belongs to some extension of $F$, prove that $F(c) = F(ac + b)$.

23. Determine all subfields of $\mathbb{Q}(\sqrt{2})$.

24. Let $E$ be an extension of the field $F$ and let $a$ and $b$ belong to $E$. Prove that $F(a, b) = F(a)(b) = F(b)(a)$.

25. Write $x^3 + 2x + 1$ as a product linear polynomials over some field extension of $\mathbb{Z}_3$. 