Theorems and Corollaries of Chapter 4

Theorem 4.1: If R is a ring, then there exists a ring P that contains an element x that is not in R and has these properties:

i. R is a subring of P.
ii. $xa = ax$ for every a in R.
iii. Every element of P can be written in the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \qquad for\ some\ n \geq 0\ and\ a_i\ in\ R.$$

iv. The representation of elements in P in (iii) is unique in the sense that if $n \leq m$

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$

then $a_i = b_i$ for $i \leq n$ and $b_i = 0_R$ for each $i > n$.

v. $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0_R$ if and only if $a_i = 0_R$ for all i.

Theorem 4.2: If R is an integral domain and $f(x)$ and $g(x)$ are nonzero polynomials in $R[x]$, then

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x).$$

Corollary 4.3: If R is an integral domain, then so is $R[x]$.

Theorem 4.4 (The Division Algorithm in F[x]): Let F be a field and $f(x)$ and $g(x)$ in $F[x]$ with $g(x) \neq 0_F$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0_F$ or $\deg r(x) < \deg g(x)$.

Theorem 4.5: Let F be a field and $f(x)$ and $g(x)$ in $F[x]$, not both zero. Then there is a unique greatest common divisor $d(x)$ of $f(x)$ and $g(x)$. Furthermore, there exist (not necessarily unique) polynomials $u(x)$ and $v(x)$ such that $d(x) = f(x)u(x) + g(x)v(x)$.

Corollary 4.6: Let F be a field and $f(x)$ and $g(x)$ in $F[x]$, not both zero. A monic polynomial $d(x)$ in $F[x]$ is the greatest common divisor of $f(x)$ and $g(x)$ if and only if $d(x)$ satisfies these conditions:

i. $d(x)$ divides both $f(x)$ and $g(x)$;
ii. if $c(x)$ divides both $f(x)$ and $g(x)$, then $c(x)$ also divides $d(x)$.

Theorem 4.7: Let F be a field and $f(x)$, $g(x)$, and $h(x)$ in $F[x]$. If $f(x)$ divides $g(x)h(x)$ and $f(x)$ and $g(x)$ are relatively prime, then $f(x)$ divides $h(x)$.

Theorem 4.8: Let R be an integral domain. Then $f(x)$ is a unit in $R[x]$ if and only if $f(x)$ is a constant polynomial that is a unit in R.

Theorems and Corollaries of Chapter 4

Corollary 4.9: Let F be a field. Then $f(x)$ is a unit in $F[x]$ if and only if $f(x)$ is a nonzero constant polynomial.

Theorem 4.10: Let F be a field. A nonzero polynomial $f(x)$ is reducible in $F[x]$ if and only if $f(x)$ can be written as the product of two polynomials of lower degree.

Theorem 4.11: Let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Then the following conditions are equivalent:

1. $p(x)$ is irreducible.
2. if $b(x)$ and $c(x)$ are any polynomials such that $p(x)$ divides $b(x)c(x)$, then $p(x)$ divides either $b(x)$ or $c(x)$.
3. if $r(x)$ and $s(x)$ are any polynomials such that $p(x) = r(x)s(x)$, then $r(x)$ or $s(x)$ is a nonzero constant polynomial.

Theorem 4.12: Let F be a field and $p(x)$ an irreducible polynomial in $F[x]$. If $p(x)$ divides $a_1(x)a_2(x) \ldots a_n(x)$, then $p(x)$ divides at least one of the $a_i(x)$.

Theorem 4.13: Let F be a field. Every nonconstant polynomial $f(x)$ in $F[x]$ is a product of irreducible polynomials in $F[x]$. This factorization is unique in the sense that if

$$f(x) = p_1(x)p_2(x) \ldots p_r(x) \qquad \textit{and} \qquad f(x) = q_1(x)q_2(x) \ldots .\, q_s(x)$$

with each $p_i(x)$ and $q_j(x)$ irreducible, then $r = s$. After the appropriate reordering, $p_i(x)$ is an associate of $q_i(x)$ for all i.

Theorem 4.14 (The Remainder Theorem): Let F be a field, $f(x)$ in $F[x]$, and a in F. The remainder when $f(x)$ is divided by the polynomial $x - a$ is $f(a)$.

Theorem 4.15 (The Factor Theorem): Let F be a field, $f(x)$ in $F[x]$, and a in F. Then a is a root of the polynomial $f(x)$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.

Corollary 4.16: Let F be a field and $f(x)$ a nonzero polynomial of degree n in $F[x]$. Then $f(x)$ has at most n roots in F.

Corollary 4.17: Let F be a field and $f(x)$ in $F[x]$, with $\deg f(x) \geq 2$. If $f(x)$ is irreducible in $F[x]$, then $f(x)$ has no roots in F.

Corollary 4.18: Let F be a field and $f(x)$ in $F[x]$, with degree 2 or 3. Then $f(x)$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in F.

Corollary 4.19: Let F be an infinite field and $f(x)$ and $g(x)$ in $F[x]$. Then $f(x)$ and $g(x)$ induce the same function from F to F if and only if $f(x) = g(x)$ in $F[x]$.