Theorems and Corollaries of Chapter 5

Theorem 5.1: Let F be a field and $p(x)$ a non-zero polynomial in $F[x]$. Then the relation of congruence modulo $p(x)$ is

i. reflexive: $f(x) \equiv f(x) \ mod \ p(x)$ for all $f(x) \in F[x]$;
ii. symmetric: if $f(x) \equiv g(x) \ mod \ p(x)$, then $g(x) \equiv f(x) \ mod \ p(x)$;
iii. transitive: if $f(x) \equiv g(x) \ mod \ p(x)$ and $g(x) \equiv h(x) \ mod \ p(x)$, then $f(x) \equiv h(x) \ mod \ p(x)$.

Theorem 5.2: Let F be a field and $p(x)$ a non-zero polynomial in $F[x]$. If $f(x) \equiv g(x) \ mod \ p(x)$ and $h(x) \equiv k(x) \ mod \ p(x)$, then

i. $f(x) + h(x) \equiv g(x) + k(x) \ mod \ p(x)$,
ii. $f(x)h(x) \equiv g(x)k(x) \ mod \ p(x)$.

Theorem 5.3: $f(x) \equiv g(x) \ mod \ p(x)$ if and only if $[f(x)] = [g(x)]$.

Corollary 5.4: Two congruence classes modulo $p(x)$ are either disjoint or identical.

Corollary 5.5: Let F be a field and $p(x)$ a polynomial of degree n in $F[x]$. Let S be the set consisting of the zero polynomial and all the polynomials of degree less than n in $F[x]$. Then every congruence class modulo $p(x)$ is the class of some polynomial in S, and the congruence classes of different polynomials in S are distinct.

Theorem 5.6: Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$. If $[f(x)] = [g(x)]$ and $[h(x)] = [k(x)]$ in $F[x]/\langle p(x)\rangle$, then

$$[f(x) + h(x)] = [g(x) + k(x)] \quad \text{and} \quad [f(x)h(x)] = [g(x)k(x)]$$

Theorem 5.7: Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$. Then the set $F[x]/\langle p(x)\rangle$ of congruence classes modulo $p(x)$ is a commutative ring with identity. Furthermore, $F[x]/\langle p(x)\rangle$ contains a subring that is isomorphic to F.

Theorem 5.8: Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$. Then $F[x]/\langle p(x)\rangle$ is a commutative ring with identity that contains F.

Theorem 5.9: Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$. If $f(x) \in F[x]$ and $f(x)$ is relatively prime to $p(x)$, then $[f(x)]$ is a unit in $F[x]/\langle p(x)\rangle$.

Theorem 5.10: Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$. Then the following statements are equivalent:

i. $p(x)$ is irreducible in $F[x]$;
ii. $F[x]/\langle p(x)\rangle$ is a field;
iii. $F[x]/\langle p(x)\rangle$ is an integral domain.

Theorem 5.11: Let F be a field and $p(x)$ an irreducible polynomial in $F[x]$. Then $F[x]/\langle p(x)\rangle$ is an extension field of F that contains a root of $p(x)$.

Corollary 5.12: Let F be a field and $f(x)$ a non-constant polynomial in $F[x]$. Then there is an extension field K of F that contains a root of $f(x)$.