Definition 12.1 ***Ring***
A *ring* R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all a, b, c in R:

1. $a+b=b+a$.
2. $(a+b)+c=a+(b+c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a+0=a$ for all a in R.
4. There is an element $-a$ in R such that $a+(-a)=0$.
5. $a(bc)=(ab)c$.
6. $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.

Theorem 12.1 ***Rules of Multiplication***
Let a, b, and c belong to a ring R. Then

1. $a0=0a=0$.
2. $a(-b)=(-a)b=-(ab)$.
3. $(-a)(-b)=ab$.
4. $a(b-c)=ab-ac$ and $(b-c)a=ba-ca$.

Furthermore, if R has a unity element 1, then

5. $(-1)a=-a$.
6. $(-1)(-1)=1$.

Theorem 12.2 ***Uniqueness of the Unity and Inverses***
If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Definition 12.2 ***Subring***
A subset S of a ring R is a *subring of* R if S is itself a ring with the operations of R.

Theorem 12.3 ***Subring Test***
A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication – that is, if $a-b$ and ab are in S whenever a and b are in S.

Definition 13.1 ***Zero Divisors***
A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab=0$.

Definition 13.2 ***Integral Domain***
An *integral domain* is a commutative ring with unity and no zero-divisors.

Theorem 13.1 ***Cancellation***
Let a, b, and c belong to an integral domain If $a \neq 0$ and $ab=ac$, then $b=c$.

Definition 13.3 ***Field***
A *field* is a commutative ring with unity in which every nonzero element is a unit.

Theorem 13.2 ***Finite Integral Domains are Fields***
A finite integral domain is a field.

Corollary 13.2.1 $\mathbb{Z}_\mathbf{p}$ ***Is a Field***
For every prime p, $\mathbb{Z}_p$, the ring of integers modulo p is a field.

Definition 13.4 ***Characteristic of a Ring***
The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.

Theorem 13.3 ***Characteristic of a Ring with Unity***
Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

Theorem 13.4 ***Characteristic of an Integral Domain***
The characteristic of an integral domain is 0 or prime.

Definition 14.1 ***Ideal***
A subring A of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

Theorem 14.1 ***Ideal Test***
A nonempty subset A of a ring R is an ideal of R if

1. $a - b \in A$ whenever $a, b \in A$.
2. ra and ar are in A whenever $a \in A$ and $r \in R$.

Theorem 14.2 ***Existence of Factor Rings***
Let R be a ring and let A be a subring of R. The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.

Remark
A *proper* ideal is an ideal I of some ring R such that it is a proper subset of R; that is, $I \subset R$.

Definition 14.2 ***Prime Ideal, Maximal Ideal***
A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal* ideal of a commutative ring R is a *proper* ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Theorem 14.3 R/A ***Is an Integral Domain If and Only If*** **A** ***Is Prime***
Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

Theorem 14.4 R/A ***Is a Field If and Only If*** **A** ***Is Maximal***
Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

Definition 15.1 ***Ring Homomorphism, Ring Isomorphism***
A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b)$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*.

Theorem 15.1 ***Properties of Ring Homomorphisms***
Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.

1. For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.
2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.
3. If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.
4. $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.

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

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

7. ϕ is an isomorphism if and only if ϕ is onto and $\ker \phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.

Theorem 15.2 ***Kernels Are Ideals***
Let ϕ be a ring homomorphism from a ring R to a ring S. Then $\ker \phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

Theorem 15.3 ***First Isomorphism Theorem for Rings***
Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\ker \phi$ to $\phi(R)$, given by $r + \ker \phi \to \phi(r)$, is an isomorphism. In symbols, $R/\ker \phi \approx \phi(R)$. This theorem is often referred to as the *Fundamental Theorem of Ring Homomorphisms.*

Theorem 15.4 ***Ideals Are Kernels***
Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an idea lA is the kernel of the mapping $r \to r + A$ from R to R/A. This mapping is known as the *natural homomorphism* from R to R/A.

Theorem 15.5 ***Homomorphism from $\mathbb{Z}$ to a Ring with Unity***
Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.

Corollary 15.5.1 ***A Ring with Unity Contains $\mathbb{Z}_n$ or $\mathbb{Z}$***
If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 15.5.2 ***$\mathbb{Z}_m$ Is a Homomorphic Image of $\mathbb{Z}$***
For any positive integer m, the mapping of $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \to x \mod m$ is a ring homomorphism.

Corollary 15.5.3 ***A Field Contains $\mathbb{Z}_p$ or $\mathbb{Q}$***
If $\mathbb{F}$ is a field of characteristic p, then $\mathbb{F}$ contains a subfield isomorphic to $\mathbb{Z}_p$. If $\mathbb{F}$ is a field of characteristic 0, then $\mathbb{F}$ contains a subfield isomorphic to the rational numbers.

Theorem 15.6 ***Field of Quotients***
Let D be an integral domain. Then there exists a field $\mathbb{F}$ (called the field of quotients in D) that contains a subring isomorphic to D.

Definition 16.1 ***Ring of Polynomials over* R**
Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, n \in \mathbb{Z}^+\}$$

is called the *ring of polynomials over R in the indeterminate x.*
Two elements

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

of $R[x]$ are considered equal if and only if $a_i = b_i$ for all nonnegative integers i. (Define $a_i = 0$ when $i > n$ and $b_i = 0$ when $i > m$.)

Definition 16.2 ***Addition and Multiplication in* R[x]**
Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

belong to $R[x]$. Then

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0$$

where s is the maximum of m and n, $a_i = 0$ for $i > n$, and $b_i = 0$ for $i > m$. Also,

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1x + c_0$$

where

$$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_1b_{k-1} + a_0b_k$$

for $k = 0, \ldots, m + n$.

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

Theorem 16.2 *Division Algorithm for* $\mathbb{F}$[x]
Let $\mathbb{F}$ be a field and let $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Corollary 16.2.1 *Remainder Theorem*
Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Corollary 16.2.2 *Factor Theorem*
Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Corollary 16.2.3 *Polynomials of Degree* n *Have at Most* n *Zeros*
A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Definition 16.3 *Principal Ideal Domain (PID)*
A *principal ideal domain* is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some a in R.

Theorem 16.3 $\mathbb{F}$[x] *Is a PID*
Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a principal ideal domain.

Theorem 16.4 *Criterion for* I = ⟨g(x)⟩
Let $\mathbb{F}$ be a field, I a nonzero ideal in $\mathbb{F}[x]$, and $g(x)$ an element of $\mathbb{F}[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

Definition 17.1 *Irreducible Polynomial, Reducible Polynomial*
Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible over* D, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called *reducible over* D.

Theorem 17.1 *Reducibility Test for Degrees 2 and 3*
Let $\mathbb{F}$ be a field. If $f(x) \in \mathbb{F}[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over $\mathbb{F}$ if and only if $f(x)$ has a zero in $\mathbb{F}$.

Definition 17.2 *Content of a Polynomial, Primitive Polynomial*
The *content* of a nonzero polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the a'a are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, \ldots, a_0$. A *primitive polynomial* is an element of $\mathbb{Z}[x]$ with content 1.

Lemma 17.2 *Gauss's Lemma*
The product of two primitive polynomials is primitive.

Theorem 17.3 *Reducibility over* $\mathbb{Q}$ *Implies Reducibility over* $\mathbb{Z}$
Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Theorem 17.4 *Mod* p *Irreducibility Test*
Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $\overline{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg \overline{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 17.5 ***Eisenstein's Criterion***
Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

If there is a prime p such that $p \nmid a_n, p \mid a_{n-1}, \ldots, p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Corollary 17.5.1 ***Irreducibility of* $\mathbf{p}$*th Cyclotomic Polynomial***
For any prime p, the pth cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

Theorem 17.6 $\langle \mathbf{p(x)} \rangle$ ***Is Maximal If and Only If*** $\mathbf{p(x)}$ ***Is Irreducible***
Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $\mathbb{F}[x]$ if and only if $p(x)$ is irreducible over $\mathbb{F}$.

Corollary 17.6.1 $\mathbb{F}[\mathbf{x}]/\langle \mathbf{p(x)} \rangle$ ***Is a Field***
Let $\mathbb{F}$ be a field and $p(x)$ be an irreducible polynomial over $\mathbb{F}$. Then $\mathbb{F}[x]/\langle p(x) \rangle$ is a field.

Corollary 17.6.2 $\mathbf{p(x)} \mid \mathbf{a(x)b(x)}$ ***Implies*** $\mathbf{p(x)} \mid \mathbf{a(x)}$ ***or*** $\mathbf{p(x)} \mid \mathbf{b(x)}$
Let $\mathbb{F}$ be a field and let $p(x), a(x), b(x) \in \mathbb{F}[x]$. If $p(x)$ is irreducible over $\mathbb{F}$ and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Theorem 17.7 ***Unique Factorization in*** $\mathbb{Z}[\mathbf{x}]$
Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form $b_1 b_2 \ldots b_s p_1(x) p_2(x) \ldots p_m(x)$, where the b_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if

$$b_1 b_2 \ldots b_s p_1(x) p_2(x) \ldots p_m(x) = c_1 c_2 \ldots c_t q_1(x) q_2(x) \ldots q_n(x)$$

where the b_i's and the c_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree, then $s = t, m = n$, and, after renumbering the c's and $q(x)$'s, we have $b_i = \pm c_i$, for $i = 1, \ldots, s$, and $p_i(x) = \pm q_i(x)$, for $i = 1, \ldots, m$.