A ring $R$ is a set with two binary operations, addition “$\oplus$” and multiplication “$\otimes$”, such that for all $a, b, c \in R$:

1. $a \oplus b = b \oplus a$.
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. There is an element 0 in $R$ such that $a \oplus 0 = a$.
4. There is an element $-a$ in $R$ such that $a \oplus (-a) = 0$.
5. $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.
6. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ and $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$. 
**Definition**

The ring $R$ is *commutative* if and only if $a \otimes b = b \otimes a$ for all $a, b \in R$. 
Definition
The ring $R$ is *commutative* if and only if $a \otimes b = b \otimes a$ for all $a, b \in R$.

A *unity* in a ring is a nonzero element that is an identity under multiplication.
Definition
The ring $R$ is commutative if and only if $a \otimes b = b \otimes a$ for all $a, b \in R$.

A unity in a ring is a nonzero element that is an identity under multiplication. If the nonzero element $a \in R$ has a multiplicative inverse then we say that it is a unit of the ring $R$. 
Definition
The ring $R$ is *commutative* if and only if $a \otimes b = b \otimes a$ for all $a, b \in R$.

A *unity* in a ring is a nonzero element that is an identity under multiplication. If the nonzero element $a \in R$ has a multiplicative inverse then we say that it is a *unit* of the ring $R$.

Theorem
*If a ring has a unity then it is unique.*
Let $R$ be commutative ring. The set of formal symbols

$$R[x] = \{a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_1 \cdot x + a_0 \mid a_0, a_1, \cdots, a_n \in R, n \text{ is nonnegative integer}\}$$

is called the ring of polynomials over $R$. 
Let $R$ be commutative ring and let

$$f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_1 \cdot x + a_0$$

and

$$g(x) = b_m \cdot x^n + b_{m-1} \cdot x^{m-1} + b_{m-2} \cdot x^{m-2} + \cdots + b_1 \cdot x + b_0$$

belong to $R[x]$. Then

$$f(x) + g(x) = (a_s + b_s) \cdot x^s + (a_{s-1} + b_{s-1}) \cdot x^{s-1} + (a_{s-2} + b_{s-2}) \cdot x^{s-2} + \cdots + (a_1 + b_1) \cdot x + a_0 + b_0$$

where $s$ is the maximum of $m$ and $n$. 
Let $R$ be commutative ring and let

$$f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_1 \cdot x + a_0$$

and

$$g(x) = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + b_{m-2} \cdot x^{m-2} + \cdots + b_1 \cdot x + b_0$$

belong to $R[x]$. Then

$$f(x)g(x) = c_{m+n} \cdot x^{m+n} + c_{m+n-1} \cdot x^{m+n-1} + \cdots + c_1 \cdot x + c_0$$

where

$$c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$$

for $k = 0, 1, \cdots, m + n$. 
Definition

A **field** $\mathbb{F}$ is a ring $(\mathbb{F}, \oplus, \otimes)$ such that $(\mathbb{F}, \oplus)$ and $(\mathbb{F} \setminus \{0\}, \otimes)$ are commutative groups.
Let \( f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_1 \cdot x + a_0 \) be a polynomial of degree \( n \) of one variable \( x \) over a field \( F \) (namely \( a_n, a_{n-1}, \ldots, a_1, a_0 \in F \)).

**Theorem:** A polynomial of degree \( n \) over a field has at most \( n \) zeroes.

**Note:** The statement is not true for arbitrary polynomial rings. For example, the polynomial \( 6 \cdot x \) has 6 zeroes in \( \mathbb{Z}_{24} \), namely 0, 4, 8, 12, 16 and 20 are roots of the equation \( 6 \cdot x = 0 \) in \( \mathbb{Z}_{24} \).
Division algorithm for $F[x]$

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_1 \cdot x + a_0$ and $g(x) = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + b_{m-2} \cdot x^{m-2} + \cdots + b_1 \cdot x + b_0$ are polynomials of one variable $x$ over a field $F$ such that $m < n$.

**Theorem:** There is a unique polynomial $r(x)$ of degree smaller than $m$, and another unique polynomial, $h(x)$, both over $F$, such that $f(x) = h(x) \cdot g(x) + r(x)$.

The polynomial $r(x)$ is called the **remainder** of $f(x)$ modulo $g(x)$.$^1$

---

$^1$Maple commands: $\text{rem}(f(x), g(x), x)$ and $\text{gcd}(f(x), g(x))$. 
A polynomial $f(x)$ from $F[x]$ is called *irreducible* polynomial if it cannot be expressed as a product of two polynomials of lower degree.
A polynomial \( f(x) \) from \( F[x] \) is called *irreducible* polynomial if it cannot be expressed as a product of two polynomials of lower degree. A polynomial that is not irreducible is called *reducible* polynomial.

**Theorem**

Let \( F \) be a field. If \( f(x) \in F[x] \) and \( \deg(f(x)) \) is 2 or 3, then \( f(x) \) is reducible over \( F \) if and only if it has a zero in \( F \). If \( f(x) \) is irreducible over \( F \), then \( f(x) \) has no root in \( F \).

**Note:** Polynomials of degree larger than 3 may be reducible over a field, and to not have zeroes in the field. For example, \( x^4 + 2x^2 + 1 = (x^2 + 1)^2 \) is reducible in \( \mathbb{Q}[x] \), but has no zeroes in \( \mathbb{Q} \).
Polynomial analog of Euclid’s Lemma:

**Theorem**

Let $F$ be a field and let $f(x), g(x), p(x) \in F[x]$. If $p(x)$ is irreducible over $F$ and $p(x)$ is irreducible over $F$ and $p(x) | a(x)b(x)$, then either $p(x) | a(x)$ or $p(x) | b(x)$. 
**Definition:** A field \((F, \oplus, \otimes)\) is called a **finite field** if the set \(F\) is finite.

**Theorem:** \((\mathbb{Z}_p, +, \cdot)\) is a field if and only if \(p\) is prime.
Definition: A field \((F, \oplus, \otimes)\) is called a finite field if the set \(F\) is finite.

Theorem: \((\mathbb{Z}_p, +, \cdot)\) is a field if and only if \(p\) is prime.

This field is called the Galois field of order \(p\) and is denoted by \(GF(p)\).
Let \((F, \oplus, \otimes)\) be a finite field with multiplicative identity element, 1, and additive identity element, 0. There must be a positive integer, \(m\), such that \(1 + 1 + \cdots + 1\) equals 0. The minimal such \(m\) is called the characteristic of \(F\), \(\text{char}(F)\).

**Theorem:** For any finite field \(F\), \(\text{char}(F)\) is a prime number.
Galois Fields $GF(p^n)$

**Definition**
Let $K$ and $F$ be fields. If $F \subseteq K$, then $F$ is called a *subfield* of $K$, or $K$ is called an *extension field* of $F$.

These fields are denoted by $GF(p^n)$ and are called **Galois fields** of order $p^n$. A subfield of $GF(p^n)$ has order $p^d$, where $d$ is a divisor of $n$. 
The Galois Field $GF(p^n)^*$

**Definition:** $GF(p^n)^* = GF(p^n) \setminus \{0\}$.

**Theorem**

The multiplicative group $GF(p^n)^*$ is a cyclic group of order $p^n - 1$.

The generator of the multiplicative group $GF(p^n)^*$ is called a *primitive element* of the field $GF(p^n)$. The number of primitive elements in $GF(p^n)$ is $\phi(p^n - 1)$ where $\phi(m)$ is the Euler’s totient function, which gives the number of positive integers less than or equal $m$ and coprime to $m$. 
Definition: A map between groups $f : G \rightarrow H$ is called a **homomorphism** if it preserves group operation, 

$$f(g_1g_2) = f(g_1)f(g_2)$$ for all $g_1, g_2 \in G$.

Definition: An **isomorphism** is a bijective map $f$ such that both $f$ and its inverse $f^{-1}$ are homomorphisms.

Theorem

*For every prime $p$ and every positive integer $n$ there exists a finite field of order $p^n$. Moreover, any two finite fields of order $p^n$ are isomorphic.*
Definition
An ideal in a ring $R$ is a nonempty subset $I$ of $R$ satisfying:

▶ $(I, +)$ is a subgroup of $(R, +)$.
▶ For all $x \in I$ and $r \in R$, $r \cdot x \in I$ and $x \cdot r \in I$.

Definition: For any $a, b \in R$, $a \equiv b \ mod \ I$ whenever $a - b \in I$.

Theorem
The relation “mod $I$” is an equivalence relation on $R$.

The set of equivalence classes is called a quotient ring and it is denoted by $R/I$.

Theorem
Let $f(x)$ be a polynomial in $F[x]$ and $\langle f(x) \rangle$ be the ideal generated by $f(x)$. The quotient ring $F[x]/\langle f(x) \rangle$ is a field if and only if $f(x)$ is irreducible in $F[x]$. 
**Theorem:** Let $f(x)$ be an irreducible polynomial of degree $n$ over $GF(p)$. The arithmetic of the finite field $GF(p^n)$ can be realized by the set of polynomials over $GF(p)$ whose degree is at most $n - 1$, where addition and multiplication are done modulo $f(x)$.

**Example**
Find an inverse element of $x^7 + x^6 + x^3 + x + 1$ in $GF(2^8)$. 
The Galois field $GF(2^2)$

Let $\mathbb{Z}_2[x]$ be the set of polynomials over $\mathbb{Z}_2$. The finite field $GF(2^2)$ can be realized as the set of polynomials of degree at most 1 over $\mathbb{Z}_2$, with addition and multiplication done modulo the irreducible polynomial $f(x) = x^2 + x + 1$. 
Constructing a finite field of order $p^n$ where $p$ is prime and $n \geq 1$

1. $\mathbb{Z}_p[x]$ is the set of polynomials with coefficients in $\mathbb{Z}_p$.
2. Choose $f(x)$ to be irreducible polynomial of degree $n$ and coefficients in $\mathbb{Z}_p$.
3. Let $GF(p^n)$ be $\mathbb{Z}_p[x] \ mod \ f(x)$. Then $GF(p^n)$ is a field of order $p^n$. 
The finite field $GF(2^8)$ can be realized as the set of polynomials over $\mathbb{Z}_2$ of degree 7, with addition and multiplication done modulo the irreducible polynomial $f(x) = x^8 + x^4 + x^3 + x + 1$.

The coefficients of polynomials over $\mathbb{Z}_2$ are 0 or 1. So, a polynomial of degree $k - 1$ can be written as a string of $k$ bits. For example, with $k = 8$: $x^7 + x^6 + x^3 + x + 1$ is represented by $(0, 1, 1, 0, 0, 0, 1, 1)$ and $x$ is represented by $(0, 0, 0, 0, 0, 0, 1, 0)$.

The addition corresponds to bit-wise XOR. For example, $(x^7 + x^6 + x^3 + x + 1) + (x)$ corresponds to $(0, 1, 1, 0, 0, 0, 1, 1) \oplus (0, 0, 0, 0, 0, 0, 1, 0)$ which is equal to $(0, 1, 1, 0, 0, 0, 1, 0)$, so $(x^7 + x^6 + x^3 + x + 1) + (x) = x^7 + x^6 + x^3 + 1$. 
Example: Implementing $GF(2^8)$

The multiplication has two stages. The first stage is polynomial multiplication, which results in a polynomial of at most $2 \cdot (k - 1)$ degree. The second stage is finding the remainder of this polynomial modulo the irreducible polynomial of degree $k$.

For example, $(x^7 + x^6 + x^3 + x + 1) \cdot (x) = x^8 + x^7 + x^4 + x^2 + x$ and $x^8 + x^7 + x^4 + x^2 + x \equiv x^7 + x^3 + x^2 + 1 \mod (x^8 + x^4 + x^3 + x + 1)$