<u>Ring</u> : A nonempty set R is said to be a <u>ring</u> if in R there are defined two operations, denoted by $+$ and $\cdot$ respectively, such that for all a, b, c in R:

① $a+b$ is in R.

② $a+b = b+a$.

③ $(a+b)+c = a+(b+c)$.

④ There is an element 0 in R such that $a+0=a$ for every a in R.

⑤ There exists an element $-a$ in R such that $a+(-a)=0$.

⑥ $a \cdot b$ is in R

⑦ $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

⑧ $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(b+c)\cdot a = b\cdot a + c\cdot a$ (the two distributive laws).

If there is an element 1 in R such that $a\cdot 1 = 1\cdot a = a$ for every a in R, then we say that R is a <u>ring with unit element</u>.

If the multiplication of R is such that $a\cdot b = b\cdot a$ for every a, b in R, then we call R a <u>commutative ring</u>.

If the elements of R different from 0 form an abelian group under multiplication, then R is called a <u>field</u>.

Example 1 : $(\mathbb{Z}, +, \cdot)$ is a commutative ring with unit element. $(\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\})$.

Example 2 : For $m \geq 2$, $(m\mathbb{Z}, +, \cdot)$ is a commutative ring but has no unit element. $(m\mathbb{Z} = \{\dots, -2m, -m, 0, m, 2m, \dots\})$.

Example 3 : $(\mathbb{Q}, +, \cdot)$ is a field. Here $\mathbb{Q}$ is the set of rational numbers.

Example 4 : $(\mathbb{Z}_m, +_m \cdot_m)$ is a commutative ring with unit element. $(\mathbb{Z}_m = \{0, 1, \dots, m-1\})$

Example 5 : For a prime p, $(\mathbb{Z}_p, +_p, \cdot_p)$ is a field.

If R is a commutative ring, then $a \neq 0 \in R$ is said to be a zero-divisor if there exists a $b \in R$, $b \neq 0$, such that $ab = 0$.

Example 6 : Consider $(\mathbb{Z}_6, +_6, \cdot_6)$. 2 and 3 are zero-divisors because in $\mathbb{Z}_6$, $2 \cdot 3 \pmod 6$ $= 3 \cdot 2 \pmod 6 = 0 \pmod 6$.

A commutative ring is an integral domain if it has no zero-divisors.

Example 7 : $(\mathbb{Z}, +, \cdot)$ is an integral domain.

A finite integral domain is a field.

Proof : Let D be a finite integral domain. In order to prove that D is a field we must

① Produce an element $1 \in D$ such that $a1 = a$ for every $a \in D$.

② For every element $a \neq 0 \in D$ produce an element $b \in D$ such that $ab = 1$.

Let $x_1, x_2, \ldots, x_n$ be all the elements of D, and suppose that $a \neq 0 \in D$. Consider the elements $x_1 a, x_2 a, \ldots, x_n a$; they are all in D. We claim that they are all distinct. For suppose that $x_i a = x_j a$ for $i \neq j$; then $(x_i - x_j) a = 0$. Since D is an integral domain and $a \neq 0$, this forces $x_i - x_j = 0$, and so $x_i = x_j$, contradicting $i \neq j$. Thus $x_1 a, x_2 a, \ldots, x_n a$ are n distinct elements lying in D, which has exactly n elements. By the pigeonhole principle these must account for all the elements of D. Every element $y \in D$ can be written as $x_i a$ for some x_i. In particular, since $a \in D$, $a = x_{i_0} a$ for some $x_{i_0} \in D$. Since D is commutative, $a = x_{i_0} a = a x_{i_0}$. For $y \in D$, let $y = x_i a$ for some $x_i \in D \Rightarrow y x_{i_0} = (x_i a) x_{i_0} = x_i (a x_{i_0}) = x_i a = y \Rightarrow x_{i_0}$ is a unit element of D. $1 \in D \Rightarrow \exists\, b \in D$ such that $1 = ba$.

A field cannot have zero divisors.
Let F be a field. Let a and b be in F.
Suppose $a \cdot b = 0$. Then this implies that (assuming $b \neq 0$)
$(a \cdot b) \cdot (b^{-1}) = 0 \cdot b^{-1} \Rightarrow a \cdot (b \cdot b^{-1}) = 0$
$\Rightarrow a \cdot 1 = \boxed{a = 0}$. $\Rightarrow$ F cannot have zero divisors.

<u>Polynomial Rings over Fields:</u> Let F be a field. By $F[x]$ we denote the set of all polynomials in the variable x, such that all coefficients of any polynomial in $F[x]$ is in F.

$$F[x] = \{ a_n x^n + \cdots + a_0 \mid n \in Z^+, a_i \in F \ \forall i \in [0..n] \}$$

Here $Z^+ = \{0, 1, 2, \ldots\}$

If we consider $(F[x], +, \cdot)$ where $+$ and $\cdot$ are polynomial addition and multiplication, then we can easily verify that it is a Ring.
We can compare $F[x]$ with Z. Both are rings.
For a prime p, Z_p is a field. Similarly from $F[x]$ we can create a field similar to Z_p.
First we have to choose an <u>irreducible polynomial</u> $p(x) \in F[x]$. We say that $p(x) \in F[x]$ is irreducible over $F[x]$, if we cannot write $p(x)$ as $p(x) = p_1(x) \cdot p_2(x)$, where both $p_1(x) \neq 1$ and $p_2(x) \neq 1$ are in $F[x]$.

<u>$GF(p^m)$: Galois Fields of order p^m</u>: Let p be a prime, and let $a(x) \in Z_p[x]$ be an irreducible polynomial over $Z_p(x)$ of degree m. Let $Z_p(x)/(a(x))$ be the set of all remainders when a polynomial in $Z_p(x)$ is divided by $a(x)$:

$$Z_p(x)/(a(x)) = \{ r(x) \mid r(x) \text{ is the remainder when } P(x) \in Z_p(x) \text{ is divided by } a(x) \}$$

We can easily verify that $(Z_p(x)/(a(x)), +_{a(x)}, \cdot_{a(x)})$ is a <u>Ring</u>, where $+_{a(x)}$ is adding polynomials mod $a(x)$, $\cdot_{a(x)}$ is multiplying polynomials mod $a(x)$. The addition and multiplication of coefficients is performed in the field Z_p. We can say something more about $Z_p[x]/(a(x))$: It is an <u>integral domain</u>. We cannot have zero divisors in $Z_p(x)/(a(x))$. Suppose we have $r_1(x) \neq 0$, and $r_2(x) \neq 0$ in $Z_p(x)/(a(x))$ such that $r_1(x)(\cdot_{a(x)})\, r_2(x) = 0 \Rightarrow r_1(x)\, r_2(x) \equiv 0 \pmod{a(x)}$

$\Rightarrow r_1(x)\, r_2(x) = r_3(x)\, a(x)$

$\Rightarrow a(x) \mid r_1(x) \cdot r_2(x)$. Since $a(x)$ is irreducible, this implies that either $a(x) \mid r_1(x)$ or $a(x) \mid r_2(x)$

$\Rightarrow$ either $r_1(x) \equiv 0 \pmod{a(x)}$ or $r_2(x) \equiv 0 \pmod{a(x)}$, which is a contradiction to our assumption that $r_1(x) \neq 0$, and $r_2(x) \neq 0$ in $Z_p(x)/(a(x))$. $\Rightarrow$ $Z_p(x)/(a(x))$ is an integral domain. From our previous result that a finite integral domain is a field $\Longrightarrow$ $Z_p(x)/(a(x))$ is a <u>finite field</u> having p^m elements.