CHARACTERISTIC OF A RING

CHARACTERISTIC OF A RING

Definition: The characteristic of a ring R is the least positive integer n such that $n.a = 0$ for all $a \in R$ and is denoted by $Char(R) = n$. If no such positive integer exists, then R is said to have characteristic 0.

Examples:

- The ring $(Z_3, +, .)$ has characteristic 3.
- The ring $(Z_4, +, .)$ has characteristic 4.
- The ring $(Z, +, .)$ and $(Q, +, .)$ both have characteristic 0.
- The characteristic of a field $(F, +, .)$ is either 0 or a prime number.
- The characteristic of a finite field is a prime number p.

Theorem : The characteristic of a field $(F, +, .)$ is either 0 or a prime number

Proof: Let $(F, +, .)$ be a field.

If $Char(F) = 0$, then there is nothing to prove.

If $Char(F) \neq 0$, then let $Char(F) = n$.

To prove n is prime.

Suppose n is not a prime, then $n = pq$, where $1 < p < n, 1 < q < n$.

i.e p and q are proper factors of n.

Since $Char(F) = n$, we have $na = 0 \; \forall \; a \in F$.

Take $a = 1$, then $n.1 = 0$.(1 is the identity of F)

$\Rightarrow \; (pq).1 = 0 \Rightarrow (p.1)(q.1) = 0$

$$[\because (pq).1 = \underbrace{1 + 1 + \ldots + 1}_{pq \text{terms}} = \underbrace{(1 + 1 + \cdots + 1)}_{p\text{terms}} \underbrace{(1 + 1 + \cdots + 1)}_{q\text{terms}}]$$

Since F is a field, F is an integral domain and so, it has no divisor of zero,

$\therefore$ either $p.1 = 0$ or $q.1 = 0$.

Since p and q are less than n, it contradicts the definition of chararcterics of F.

$\therefore n$ is a prime number.

Note:

1. The characteristic of a ring need not be a prime. For example $Char(Z_6) = 6$, which is not a prime.
2. The characteristic of a finite field is a prime number P.

3. The fields $(Q,+,.),(R,+,.)$ are of characteristic zero.

Theorem : The number of elements of a finite field is p^n, where p is a prime and n is a positive integer.

Proof: For a prime p, Z_p is field having p elements and $Char(Z_p) = p$, since $p.a = 0$ for all $a \in Z_p$.

Consider the polynomial $f(x) = x^{p^n} - x$ in $Z_p[x]$.

Now, the derivative $x^{p^n}x^{p^n-1} - 1 = f'(x)$.

Since , $Char(Z_p) = p$, $Char(Z_p[x]) = p$. $\therefore p.g(x) = 0$ for all $g(x) \in Z_p[x]$.

Hence $p.x^{p^n-1} = 0 \Rightarrow p^n.x^{p^n-1} = 0$.

Thus $f'(x) = -1 =$ a constant polynomial.

So, $f(x)$ and $f'(x)$ have no common root.

Hence $f(x)$ has no multiple roots. i.e all the roots of $f(x)$ are distinct.

If K is the smallest extension field (splitting field) containing all the roots of $f(x)$. Then $f(x)$ has p^n distinct roots in K.

In K, let F be the set of all elements satisfying $f(x)$.

$F = \{a \in K / a^{p^n} = a\} \subset K$.

Hence F has only p^n elements.

Claim: To prove that F is a field.

Let $a, b \in F$. Then $a^{p^n} = a$ and $b^{p^n} = b$.

$(a.b)^{p^n} = a^{p^n}.b^{p^n} = a.b \Rightarrow a.b \in F$.

$(a+b)^{p^n} = a^{p^n} + p^nC_1a^{p^n-1}b + p^nC_2a^{p^n-2}b^2 + \cdots + p^nC_ra^{p^n-r}b^r + \cdots b^{p^n}$.

Since $Char(K) = p$, $p.a^{p^n-r}b^r = 0$, $r = 1,2,3 \ldots$

$\therefore (a.b)^{p^n} = a^{p^n} + b^{p^n} = a + b \Rightarrow a + b \in F$.

Similarly, $(a-b)^{p^n} = a - b \Rightarrow a - b \in F$.

Hence, F is a subfield of K.

In addition the field F consisting of p^n elements, where p is a prime and n is a positive integer

CONGRUENCE RELATION IN $F[x]$

Definition:

Let $s(x) \in F[x]$ and $s(x) \neq 0$ and $f(x), g(x) \in F[x]$. We say that $f(x)$ is congruent to $g(x)$ modulo $s(x)$ and write

$f(x) \equiv g(x) \pmod{s(x)}$ if $s(x)$ divides $f(x) - g(x)$

i.e., $f(x) - g(x) = q(x)\, s(x)$ for some $q(x) \in F[x]$

This relation congruence of polynomial is an equivalence relation on $F[x]$

The equivalence class of $f(x)$ is denoted by $[f(x)]$

$[f(x)] = \{ t(x) \in F[x] \mid f(x) \equiv t(x) \pmod{s(x)} \}$

We define addition and multiplication of congruence classes as in z_n

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$

$$[f(x)].[g(x)] = [f(x) \,.\, g(x)]$$

Definition:

Let R be a commutative ring with unity and $a \in R$, then the ideal generated by single element a is called a principal ideal and it is denoted by $< a >$

Thus $< a > = \{ ra \mid r \in R \}$

Now, we state a theorem without proof for polynomials.

Theorem:

Let $F = z_p$, p is a prime and $f(x)$ be an irreducible polynomial of degree n over z_p. Then the quotient ring $\frac{F[x]}{<f(x)>}$ is a field having p^n elements, Where $< f(x) >$ is the ideal generated by $f(x)$.

Example 1:

In $Z_2[x]$, $s(x) = x^2 + x + 1$. show that $s(x)$ is irreducible over $\frac{Z_2[x]}{<s(x)>}$ and construct the field.

Solution:

Given $s(x) = x^2 + x + 1$ in $Z_2[x]$

and $Z_2 = \{0,1\}$

Now,

$s(0) = 1 \neq 0$

$s(1) = 3 \equiv 1(mod\ 2) \neq 0$

Therefore $s(x)$ has no root in $Z_2[x]$

Hence $s(x)$ is irreducible in $Z_2[x]$.

Therefore $\frac{Z_2[x]}{<s(x)>}$ is a field

Since degree of $s(x) = 2$, this field has $2^2 = 4$ elements.

This field consists of 4 different equivalence classes $(mod\ s(x))$

Let $s(x), f(x) \in F[x]$

Then by division algorithm, we have

$f(x) = q(x)(x^2 + x + 1) + r(x)$

where $r(x) = 0$ or $\deg r(x) = 0 < \deg (x^2+x+1)$

Therefore degree of $r(x)$ is either 0 or 1

Here, $r(x) =, ax + b,$ $a, b \in Z_2$

Since $f(x) - r(x) = q(x)(x^2 + x + 1)$

$f(x) \equiv r(x)\ (mod\ (x^2 + x + 1))$

Therefore $[f(x)] = [r(x)]$

Therefore the different equivalence classes $mod\ (x^2 + x + 1)$ correspond to the different values of $r(x)$

Each of a and b can take two values from Z_2 and so 2 . 2 = 4 values for $r(x)$

They are,

(i) If $a = 0$, $b = 0$, then $r(x) = 0$

(ii) If $a = 0$, $b = 1$, then $r(x) = 1$

(iii) If $a = 1$, $b = 0$, then $r(x) = x$

(iv) If $a = 1$, $b = 1$, then $r(x) = x + 1$

Therefore four elements of the field are If $[0]$, $[1]$, $[x]$, $[x + 1]$

Therefore $\frac{Z_2[x]}{<x^2+x+1>} = \{[0],\ [1],\ [x], [x + 1]\}$

Example 2:

If $\frac{Z_2[x]}{<x^2+x+1>} = \{[0],\ [1],\ [x], [x + 1]\}$ is a field, then find $[x]^{-1}$.

Solution:

Since $\frac{Z_2[x]}{<x^2+x+1>} = \{[0],\ [1],\ [x], [x + 1]\}$ is a field

The non zero elements $[1]$, $[x]$ and $[x + 1]$ form a group under multiplication,

We write $[a]$ as a

Therefore, $[1] = 1$

$[x] = x$

$[x + 1] = x + 1$

Now, $1 . 1 = 1$

$1 . x = x$

$1 . (x + 1) = x + 1$

$x . 1 = x$

$x . x = x^2$

Also,

$x^2 = 1 . (x^2 + x + 1) + (x + 1)$ in $Z_2[x]$

Therefore, $x . x = x^2 \equiv x + 1 \ (mod\ (x^2 + x + 1))$.

$$x.(x+1) = x^2 + x$$

Also, $x^2 + x = 1(x^2 + x + 1) + 1$ in $Z_2[x]$

Therefore, $x.(x+1) = x^2 + x \equiv 1(mod(x^2 + x + 1))$

$$(x+1).1 = x + 1$$

$$(x+1).x = x^2 + x \equiv 1 \ (mod \ (x^2 + x + 1))$$

$$(x+1).(x+1) = x^2 + 1 \ \text{ in } Z_2[x]$$

Also,

$$x^2 + 1 = 1.(x^2 + x + 1) + x \text{ in } Z_2[x]$$

Therefore $(x+1).(x+1) = x^2 + 1 \equiv x \ (mod \ (x^2 + x + 1))$

.	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Since 1 is the multiplicative identity.

We find $x.(x+1) = 1$

Therefore inverse of x is $(x+1)$

Hence $[x]^{-1} = [x+1]$.