Unit - II

POLYNOMIAL RINGS

Defn [Polynomial]

Let $(R, +, .)$ be a ring.

An expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 x^0$$

where $a_i \in R$ for $0 \le i \le n$ is called a polynomial in the indeterminate x with coefficients from R.

If $a_n \neq 0$ then a_n is the leading coefficient and we say that $f(x)$ has degree n.

The term $a_0 x^0$ is constant term of $f(x)$

If $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 x^0$ is another polynomial in x over R then $f(x) = g(x)$ if $m = n$ and $a_i = b_i$ for all $0 \le i \le n$.

Notation

$R[x]$ represents the set of all polynomials in indeterminate x with coefficients from the ring $(R, +, .)$.

Polynomial ring:

Let $R[x]$ be the set of all polynomials in the indeterminate x with coefficients from the ring $(R, +, \cdot)$.

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 x^0$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 x^0 \in R[x]$$

Assume $n \geq m$.

Define a binary operations '+' and '.' in $R[x]$ by,

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$f(x) \cdot g(x) = (a_n b_m) x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1) x^1 + (a_0 b_0) x^0.$$

then $(R[x], +, \cdot)$ is a ring and it is called a polynomial ring.

Notes.

* Zero polynomial $= 0x^0$ where 0 is zero element in R.
  Zero polynomial has no degree.
* Constant polynomial $= ax^0$ where $a \neq 0 \in R$.
  Constant polynomial is of degree '0'.

* If $f(x) = 4x^3 + 2x^2 + 3x^1 + 1x^0$

$g(x) = 3x^2 + x^1 + 2x^0 \in \mathbb{Z}[x]$.

Then $f(x) + g(x) = 4x^3 + (2+3)x^2 + (3+1)x^1 + (1+2)x^0$

$= 4x^3 + 5x^2 + 4x^1 + 3x^0$.

$f(x) \cdot g(x) = \left(4x^3 + 2x^2 + 3x^1 + 1x^0\right) \cdot (3x^2 + x^1 + 2x^0)$

$= 12x^5 + [6+4]x^4 + [8+2+9]x^3 + [4+3+3]x^2$

$+ [6+1]x^1 + (2)x^0$.

$= 12x^5 + 10x^4 + 19x^3 + 10x^2 + 7x^1 + 2x^0$.

* We know that $\left(\frac{\mathbb{Z}}{5}, \oplus, \odot\right)$ is a ring

$\oplus \rightarrow$ addition modulo 5

$\odot \rightarrow$ multiplication modulo 5.

Let $R = \mathbb{Z}_5$.

Take $f(x) = 3x^2 + 2x^1 + 3x^0$

$g(x) = 2x^2 + 4x^1 + 4x^0 \in \mathbb{Z}_5[x]$.

Then $f(x) + g(x) = (3 \oplus 2)x^2 + (2 \oplus 4)x^1 + (3 \oplus 4)$

$= 0 \cdot x^2 + 1x^1 + 2x^0$

Similarly, $f(x) \cdot g(x) = [3 \odot 2]x^4 + [3 \odot 4 \oplus 2 \odot 2]x^3$

$+ [3 \odot 4 + 2 \odot 4 + 2 \odot 3]x^2$

$+ [2 \odot 4 + 4 \odot 3]x^1 + (3 \odot 4)x^0$

$= 1x^4 + [2 \oplus 4]x^3 + [2 \oplus 3 \oplus 1]x^2 + [4 \oplus 2]x^1 + 2x^0$

$= 1x^4 + 3x^3 + 10 \cdot x^2 + 6x^1 + 2x^0$.

* $R \rightarrow$ Ring

$R[x] \rightarrow$ polynomial ring.

If R is commutative then $R[x]$ is also commutative.

If R is a ring with identity 1 then

$R[x]$ is also ring with identity $0x^n + 0x^{n-1} + \cdots + 0.x + 1x^0$.

If R is an integral domain then $R[x]$ is also integral domain.

* Let $f(x) = 4x^2 + 1 \in Z_8[x]$.

$g(x) = 2x + 3$

$f(x)$ has degree 2

$g(x)$ has degree 1.

We may expect $f(x) \cdot g(x)$ has degree 3.

But $f(x) \cdot g(x) = [4 \odot 2]x^3 + [4 \odot 3]x^2 + [1 \odot 2]x^1 + [1 \odot 3]x^0$

$= 0.x^3 + 4x^2 + 2x^1 + 3x^0$

$= 4x^2 + 2x + 3$ which has degree 2.

∴ In general $f(x) \cdot g(x)$ has degree need be equal to $\deg f(x) + \deg g(x)$

Defn [Root of a polynomial].

Let R be a ring with identity.

Let $f(x) \in R[x]$ with degree ≥ 1.

If $r \in R$ and $f(r) = \text{zero}$ then r is a root of $f(x)$.

Here $f(r) =$ zero element in Ring.

Examples

(1) Let R be the set of all real numbers.

Then $(R, +, \cdot)$ is a ring.

$R[x]$ is polynomial ring.

Take $f(x) = x^2 - 2 \in R[x]$.

Then $f(x)$ has roots namely $\sqrt{2}, -\sqrt{2}$.

Since $f(\sqrt{2}) = (\sqrt{2})^2 - 2$

$= 2 - 2$

$= 0$

$=$ zero element in $(R, +, \cdot)$

Also $f(-\sqrt{2}) = (-\sqrt{2})^2 - 2$

$= 2 - 2$

$= 0$

$=$ zero element in $(R, +, \cdot)$

② Let $f(x) = x^2 + 3x + 2 \in Z_6[x]$.

What are the roots of $f(x)$?

$$Z_6 = \{0, 1, 2, 3, 4, 5\}.$$

$f(0) = (0)^2 + 3(0) + 2$

$= (000) + 0 + 2$

$= 2$

$\neq$ zero element in Z_6.

$\therefore$ 0 is not a root.

$f(1) = (1)^2 + 3(1) + 2$

$= 1 + 3 + 2$

$= 6$

$\equiv 0$ (zero element in Z_6) $\therefore$ 1 is a root

$f(2) = (2)^2 + 3(2) + 2$

$= 4 + 6 + 2$

$= 12$

$\equiv 0$ (zero element in Z_6). $\therefore$ 2 is a root

$f(3) = (3)^2 + 3(3) + 2$

$= 9 + 9 + 2$

$= 20$

$\equiv 2 \neq$ zero element in Z_6

$\therefore$ 3 is not a root.

$f(4) = (4)^2 + 3(4) + 2 = 16 + 12 + 2 = 30 \equiv 0$

$\therefore$ 4 is a root.

$f(5) = (5)^2 + 3(5) + 2 = 25 + 15 + 2 = 42 \equiv 0$

$\therefore$ 5 is a root.

Other examples of Polynomial rings.

① $Q[x]$, $Q \to$ set of all rationals.

② $R[x]$, $R \to$ set of all real numbers.

③ $C[x]$, $C \to$ set of all complex numbers.

Defn [Divisor]

Let F be a field.

The non-zero polynomial $f(x) \in F[x]$ is called a divisor of $g(x)$ if $\exists$ $q(x) \in F[x]$ such that

$$f(x) \cdot q(x) = g(x)$$

In other words, $g(x)$ is a multiple of $f(x)$.

$$f(x) \;\big|\; g(x) \qquad q(x)$$
$$\vdots$$
$$0$$

Example.

Let $(Q, +, \cdot)$ be the field.

Take $f(x) = x - 2$

Then $f(x)$ is a divisor of $x^2 - 5x + 6$.

$\because$ $x^2 - 5x + 6 = (x-2)(x-3)$.

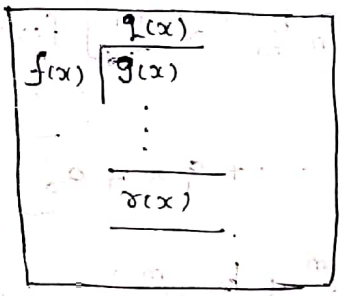
In otherwords $x^2 - 5x + 6$ is a multiple of $(x-2)$.

theorem ① **Division algorithm**

Let $f(x), g(x) \in F[x]$ with $f(x)$ is non-zero polynomial. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x) f(x) + r(x) \quad \text{where } r(x) = 0$$

(or) $\deg r(x) < \deg f(x)$.



Proof:-

Let $S = \{ g(x) - t(x) f(x) \mid t(x) \in F(x) \}$

Case (i) If $0 \in S$

Then $0 = g(x) - t(x) f(x)$ for some $t(x) \in F(x)$.

Take $t(x) = q(x)$.

$\Rightarrow 0 = g(x) - q(x) f(x)$

$\Rightarrow g(x) = q(x) f(x)$.

$\Rightarrow g(x) = q(x) \cdot f(x) + r(x)$ where $r(x) = 0$.

Case (ii) If $0 \notin S$

Consider the degree of elements in S.

Let $r(x) = g(x) - q(x) \cdot f(x)$ be the element in S which has minimum degree.

Since $r(x) \neq 0$, the theorem is over if $\deg r(x) < \deg f(x)$.

Suppose $\deg r(x) \geq \deg f(x)$.

Take $r(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$.

where $a_n \neq 0$.

$f(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0$

where $b_m \neq 0$.

Here $n \geq m$.

Define $h(x) = r(x) - \left[a_n b_m^{-1} x^{n-m}\right] f(x)$ ⟶ ①

(or) $h(x) = \left[a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0\right]$

$- \left[a_n b_m^{-1} x^{n-m}\right]\left[b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0\right]$

$= \left[a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0\right]$

$- \left[a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_1 x^{n-m+1} + a_n b_m^{-1} b_0 x^{n-m}\right]$

$\Rightarrow \deg h(x) < \deg r(x)$.

Also from ①

$h(x) = r(x) - \left[a_n b_m^{-1} x^{n-m}\right] f(x)$.

Sub $r(x) = g(x) - q(x).f(x)$ in above

$h(x) = g(x) - q(x).f(x) - \left[a_n b_m^{-1} x^{n-m}\right] f(x)$

$= g(x) - \left[q(x) + a_n b_m^{-1} x^{n-m}\right] f(x)$.

$h(x) = g(x) - s(x) f(x)$

where $s(x) = q(x) + a_n b_m^{-1} x^{n-m} \in F(x)$.

$\therefore h(x) \in S$ with $\deg h(x) < \deg r(x)$.

Which is a $\Rightarrow \Leftarrow$ to $r(x)$ has minimum degree in S.

$\therefore \deg r(x) < \deg f(x)$.

This proves the existence of $r(x)$ & $q(x)$.

To prove the uniqueness:

Suppose $g(x) = q_1(x) f(x) + r_1(x) \longrightarrow (2)$

and $g(x) = q_2(x) f(x) + r_2(x) \longrightarrow (3)$

where $\deg r_1(x) < \deg f(x)$ (or) $r_1(x) = 0$

& $\deg r_2(x) < \deg f(x)$ (or) $r_2(x) = 0$.

$(2) - (3)$

$\Rightarrow 0 = [q_1(x) - q_2(x)] f(x) + [r_1(x) - r_2(x)]$

$\Rightarrow [q_2(x) - q_1(x)] f(x) = r_1(x) - r_2(x)$.

Since $\deg [r_1(x) - r_2(x)] < \deg f(x)$, the above equality holds good if $q_1(x) - q_2(x) = 0$.

$\Rightarrow q_1(x) = q_2(x)$.

$\therefore r_1(x) = r_2(x)$.

$\therefore \exists$ unique $r(x)$ and $q(x)$ such that

$g(x) = q(x) f(x) + r(x)$ where $r(x) = 0$

(or) $\deg r(x) < \deg f(x)$.

Problem If $f(x) = 3x^2+4x+2$ and

$g(x) = 6x^4+4x^3+5x^2+3x+1$

are polynomials in $Z_7[x]$.

Using division algorithm find the quotient and remainder when $g(x)$ is divided by $f(x)$.

Soln

$$\begin{array}{r|l} & 2x^2+x+6 \\ \hline 3x^2+4x+2 & 6x^4+4x^3+5x^2+3x+1 \\ & \overset{(-)}{6x^4}\overset{(-)}{+}x^3\overset{(-)}{+}4x^2 \\ \hline & 3x^3+x^2+3x+1 \\ & \overset{(-)}{3}x^3\overset{(-)}{+}4x^2\overset{(-)}{+}2x \\ \hline & 4x^2+x+1 \\ & \overset{(-)}{4}x^2\overset{(-)}{+}3x\overset{(-)}{+}5 \\ \hline & 5x+3 \end{array}$$

replace -3 by $-3+7$

$4/3 = 4 \cdot 3^{-1}$
$= 4 \cdot 5$
$= 6.$

$4/3 = 4 \cdot 3^{-1}$
$= 4 \cdot 5$
$= 6.$

$\therefore$ quotient $= q(x) = 2x^2+x+6.$

remainder $= r(x) = 5x+3.$

$\therefore$ $g(x) = q(x) f(x) + r(x)$

$= (2x^2+x+6)(3x^2+4x+2) + (5x+3)$

Theorem ② **Remainder Theorem**

For $f(x) \in F[x]$ and $a \in F$, the remainder is $f(a)$ when $f(x)$ is divided by $(x-a)$.

Proof

Using division algorithm;

$$\begin{array}{r|l} & q(x) \\ \hline x-a & f(x) \\ & \overline{r(x)} \end{array}$$

$$f(x) = q(x)(x-a) + r(x)$$

where $r(x) = 0$ (or) $\deg r(x) < \deg (x-a) = 1$.

$\Rightarrow r(x)$ is constant polynomial

$\Rightarrow r(x) = b$ for some $b \in F$.

$\therefore f(x) = q(x)(x-a) + b \longrightarrow ①$

Sub $x = a$ in ①

$$f(a) = q(a)(a-a) + b.$$

$$\Rightarrow f(a) = 0 + b$$

$$\Rightarrow f(a) = b.$$

$\therefore$ remainder $= r(x) = b = f(a)$.

Hence the proof.

Theorem ③ The Factor Theorem

If $f(x) \in F[x]$ and $a \in F$, then $(x-a)$ is a factor of $f(x)$ iff a is a root of $f(x)$.

Proof. Let $f(x) \in F[x]$ and $a \in F$.

Assume that $(x-a)$ is a factor of $f(x)$.

Claim: a is a root of $f(x)$.

Since $(x-a)$ is a factor of $f(x)$,

$$f(x) = q(x).(x-a)$$

$$f(a) = q(a)\,(a-a)$$

$$= 0 \quad [\text{zero element in } F].$$

$\therefore$ a is a root of $f(x)$.

Conversely, assume that a is a root of $f(x)$.

Claim: $(x-a)$ is a factor of $f(x)$.

Divide $f(x)$ by $(x-a)$.

$$\begin{array}{r|l} & q(x) \\ \hline (x-a) & f(x) \\ & \vdots \\ \hline & r(x) \end{array}$$

$\therefore$ $f(x) = q(x)\,(x-a) + r(x)$

$$f(x) = q(x)\,(x-a) + r \rightarrow (1) \quad \left(\text{say } r(x) = r\right)$$

$\because \deg r(x) < (x-a)$

Since 'a' is a root of $f(x)$,

$$f(a) = q(a)\,(a-a) + r = 0$$

$$\Rightarrow \boxed{r = 0}$$

Sub $r=0$ in (1), $f(x) = q(x)\,(x-a)$.

$\Rightarrow (x-a)$ is a factor of $f(x)$.

Theorem ④ If $f(x) \in F[x]$ has degree $n \geq 1$, then $f(x)$ has at most 'n' roots in F.

Proof:- We prove this theorem by mathematical induction on the degree of $f(x)$.

When $\deg f(x) = 1$,

$f(x) = ax + b$ where $a \neq 0$.

$$f(-a^{-1}b) = a(-a^{-1}b) + b$$
$$= -b + b$$
$$= 0.$$

$\therefore -a^{-1}b$ is a root of $f(x)$.

Suppose $f(x)$ has two roots namely c_1, c_2.

$\Rightarrow f(c_1) = 0$ & $f(c_2) = 0$.

$\Rightarrow ac_1 + b = 0$ & $ac_2 + b = 0$.

$\Rightarrow ac_1 + b = ac_2 + b$. (∵ Both have same values)

$\Rightarrow ac_1 = ac_2$ ——— (1) (using cancellation law)

Since F is a field, $a^{-1} \in F$.

Operate a^{-1} on (1) both sides

$$a^{-1}ac_1 = a^{-1}ac_2$$
$$\Rightarrow 1.c_1 = 1.c_2$$
$$\Rightarrow c_1 = c_2.$$

$\therefore$ Two roots are same.

$\therefore f(x)$ has at most one root in F.

Assume that the result is true for $f(x)$ where $\deg f(x) = k$.

It is enough to prove the result holds for $f(x)$ where $\deg f(x) = k+1$.

Let $f(x) \in F[x]$ with $\deg f(x) = k+1$.

Suppose $f(x)$ has no root in F, then the proof of the theorem is over.

Let $r \in F$ be the root of $f(x)$.

$\Rightarrow f(r) = 0$.

Also $f(x) = (x-r) \cdot q(x)$ [By Factor thm]

$\Rightarrow \deg q(x) = k$.

By the hypothesis of mathematical induction, $q(x)$ has atmost k roots.

$\Rightarrow f(x)$ can have atmost $(k+1)$ roots.

$\therefore$ By mathematical induction, the results for any $n \in Z^+$

$\therefore$ If $\deg f(x) = n$ then $f(x)$ has atmost n roots in F.

Irreducible polynomials, Finite fields

Defn : [reducible, irreducible]

Let $f(x) \in F[x]$ with $\deg f(x) \geq 2$.

F is a field.

We call $f(x)$ is reducible over F if $\exists$ $g(x), h(x) \in F[x]$ such that $f(x) = g(x).h(x)$ where $\deg g(x), \deg h(x) \geq 1$.

If $f(x)$ is not reducible over F, then it is irreducible over F.

Note

* prime and irreducible have same meaning.

Examples

(1) $x^2 - 5x + 6$ is reducible in $Q(x)$.

$\because$ $x^2 - 5x + 6 = (x-2)(x-3)$

Both $(x-2)$ & $(x-3) \in Q(x)$ with their degrees ≥ 1.

(2) $x^2 + 1$ is not reducible in $Q(x)$.

$\therefore$ $x^2 + 1$ is irreducible.

(3) $x^2 + 1$ is reducible in $\mathbb{C}(x)$.

$\because$ $x^2 + 1 = (x+i)(x-i)$.

Defn [Monic polynomial]

A polynomial $f(x) \in F[x]$ is called monic if its leading coefficient is '1'

Example

① $f(x) = x^4 + 3x^2 + 2x + 100 \in \mathbb{Q}[x]$

leading coefficient is 1.

$\therefore$ $f(x)$ is monic polynomial.

② $g(x) = 2x^4 + 3x + 2 \in \mathbb{Q}[x]$.

leading coefficient is $2 \neq 1$.

$\therefore$ $g(x)$ is not monic.

Defn [Greatest common Divisor]

If $f(x), g(x) \in F[x]$, then $h(x) \in F[x]$ is a greatest common divisor of $f(x)$ and $g(x)$ if it satisfies following

(i) $h(x)$ must devide both $f(x)$ and $g(x)$

(ii) Suppose another $k(x)$ divide both $f(x)$ and $g(x)$ then $k(x)$ must devide $h(x)$.

Procedure for Finding G.c.d.

Suppose given $f(x), g(x) \in F[x]$.

Aim :- To find G.c.d of $f(x)$ & $g(x)$.

Step(1) Find the degrees of given polynomials.

Step(2) Divide the polynomial which has greater degree by the smaller one.

If the remainder is zero, smaller degree polynomial is g.c.d.

Otherwise go step (3)

Step (3) Divide the ~~smaller degree~~ Divisor in previous step by the remainder.

Proceed in this manner until the remainder is zero.

The last non zero remainder is their g.c.d.

Problem (U.Q) Find the g.c.d of $x^{10} - x^7 - x^5 + x^3 + x^2 - 1$ and $x^8 - x^5 - x^3 + 1$ in $Q(x)$

Soln

Divide $x^{10} - x^7 - x^5 + x^3 + x^2 - 1$ by $x^8 - x^5 - x^3 + 1$

Step①

$$
\begin{array}{r|l}
 & x^2 \\
\hline
x^8 - x^5 - x^3 + 1 & x^{10} - x^7 - x^5 + x^3 + x^2 - 1 \\
 & x^{10} - x^7 - x^5 + x^2 \\
\hline
(-) & x^3 - 1
\end{array}
$$

remainder is $x^3 - 1$

Step② Divide $x^8 - x^5 - x^3 + 1$ by $x^3 - 1$.

$$
\begin{array}{r|l}
 & x^5 - 1 \\
\hline
x^3 - 1 & x^8 - x^5 - x^3 + 1 \\
 & x^8 - x^5 \\
\hline
(-) & -x^3 + 1 \\
 & -x^3 + 1 \\
\hline
(-) & 0
\end{array}
$$

remainder is 0.

Stop the process.

The last non zero remainder $= x^3 - 1$

$=$ required g.c.d

Homework

① Find the g.c.d of

$f(x) = x^2 + x - 2$

$g(x) = x^5 - x^4 + x^3 + x^2 - x - 1$ in $\mathbb{Q}[x]$.

② Find the gcd of

$f(x) = x^4 + x^3 + 1$

$g(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$.

Defn [Characteristic of ring]

Let $(R,+,.)$ be a ring. If there is a least positive integer n such that $nr = 0 \quad \forall r \in R$, then we say that the ring $(R,+,.)$ has characteristic n and we write $\text{Char}(R) = n$.

When no such integer exists, R is said to have characteristic zero.

Notes

$nr = r + r + \dots + r$ [n times].

Examples

① The ring $(Z_3, \oplus, \odot)$ has characteristic 3.

$$Z_3 = \{0, 1, 2\}$$

$0 \oplus 0 \oplus 0 = 0.$

$1 \oplus 1 \oplus 1 = 0$

$2 \oplus 2 \oplus 2 = 0.$

$\therefore$ Z_3 has characteristic 3.

② Both rings $(Z,+,\cdot)$ and $(\mathbb{Q},+,\cdot)$ have characteristic zero.

③ $Z_3[x]$ is infinite ring but has characteristic 3.

$$Z_3[x] = \{\text{polynomials in } x \text{ with coefficients in } Z_3\}$$

For example, $2x^2+x+1 \in Z_3[x]$.

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

$$= (2\oplus 2\oplus 2)x^2 + (1\oplus 1\oplus 1)x + (1\oplus 1\oplus 1)$$

$$= 0x^2 + 0.x + 0$$

$$=$$ zero polynomial in $Z_3[x]$.

Likewise, $f(x)+f(x)+f(x) =$ zero polynomial in $Z_3[x]$.

$\forall f(x) \in Z_3[x]$.

$\therefore Z_3[x]$ has characteristic 3.

Theorem (5) Let $(F,+,\cdot)$ be a field and $\text{char}(F)>0$, then $\text{char}(F)$ must be prime.

Proof:-

Let $(F,+,\cdot)$ be a field. and $\text{char}(F)>0$.

Let 'u' be the identity element in $(F,+,\cdot)$

Take $\text{char}(F) = n > 0$.

Claim: n is a prime number.

Suppose n is not a prime

Then $n = mk$ where $m,k \in Z^+$

with $1 < m,k < n$.

Since $\text{char}(F) = n$, $nr = 0$ [zero est in F] $\forall r \in F$.

$\Rightarrow nu = 0$. ①

$\Rightarrow mku = 0$.

$\Rightarrow \underbrace{u+u+\cdots+u}_{mk \text{ times}} = 0$

$\Rightarrow \underbrace{(u+u+\cdots+u)}_{m \text{ times}} \cdot \underbrace{(u+u+\cdots+u)}_{k \text{ times}} = 0$. ②

($\because u$ is identity, $u \cdot u = u$)

$\Rightarrow mu \cdot ku = 0$.

$\Rightarrow mu = 0$ (or) $ku = 0$. ③

Without loss of generality, take $mu = 0$

$\Rightarrow mur = 0.r$

$\Rightarrow mr = 0$ ($\because u$ is identity, $u \cdot r = r$)

$\forall r \in F$.

(ii) We have $mr = 0 \quad \forall r \in F$ where $m < n$.

Which is a $\Rightarrow \Leftarrow$ to $\text{char}(F) = n$.

$\therefore$ n is a prime number.

Defn [order of a ring]

Let $(R, +, \cdot)$ be a ring.

Then order of $(R, +, \cdot)$ = number of elements in R.

If number of elements in R is infinite, then order of $(R, +, \cdot)$ is infinite.

Examples

① The ring $(Z_7, \oplus, \odot)$ has order 7.

Since $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

In general, $(Z_n, \oplus, \odot)$ has order n.

② The ring $(Z, +, \cdot)$ is of infinite order.

$\because Z = \{0, 1, -1, 2, -2, \ldots\}$.

③ The ring $(\mathbb{Q}, +, \cdot)$ has infinite order.

Theorem ⑥ A finite field F has order p^t where p is prime and $t \in Z^+$.

Q.Q 16 mark

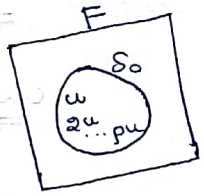
Proof:-

Let F be a finite field.

$\Rightarrow$ char(F) = p where p is prime.

Let 'u' be the identity element in F.

Consider $S_0 = \{u, 2u, 3u, \ldots, pu = 0\}$



Clearly $S_0 \subseteq F$ and $|S_0| = p$.

Claim①: S_0 is a set of distinct elements.

Suppose $mu = nu$ for some $1 < m, n \leq p$.

$\Rightarrow (m-n)u = 0$

$\Rightarrow (m-n)u.r = 0.r$

$\Rightarrow (m-n)r = 0 \quad \forall r \in F.$ ——→ ①

Also $(m-n) < p$.

By ①, Which is a $\Rightarrow \Leftarrow$ to char(F) = p.

∴ S_0 is a set of distinct elements

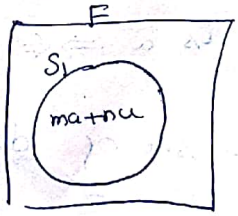
Hence the Claim①

If $S_0 = F$ then the theorem is over.

If $S_0 \neq F$, choose $a \in F - S_0$.

Consider $S_1 = \{ma + nu \,/\, 0 < m, n \leq p\}$.

Clearly $S_1 \subseteq F$ and $|S_1| = p^2$



p choices for m
&
p choices for n.

Claim ②: S_1 is a set of distinct elements

Suppose not, then

$m_1 a + n_1 u = m_2 a + n_2 u$ where $0 < m_1, m_2, n_1, n_2 \leq p$

$\Rightarrow (m_1 - m_2) a + (n_1 - n_2) u = 0$

$\Rightarrow (m_1 - m_2) a + (n_1 - n_2) = 0$ ($\because u$ is identity) $\longrightarrow$ ②

$\Rightarrow$ either $(m_1 - m_2) = 0$ (or) $(n_1 - n_2) = 0$.

Case (i):

If $(m_1 - m_2) = 0$

From ②, $(n_1 - n_2) = 0$.

$(n_1 - n_2) r = 0.r \quad \forall r \in F$.

ie) $(n_1 - n_2) r = 0 \quad \forall r \in F$.

~~char(F) = 0~~

$\Rightarrow$ char $(F) = |(n_1 - n_2)|$ where $|n_1 - n_2| < p$.

Which is a $\Rightarrow\Leftarrow$ to char$(F) = p$.

Case (i):

If $(n_1 - n_2) = 0$.

From ②, $(m_1 - m_2) a = 0$

Since $a \neq 0$, $a^{-1} \in F$.

$\Rightarrow (m_1 - m_2) a.a^{-1} = 0.a^{-1}$

$\Rightarrow (m_1 - m_2) u = 0$.

$\Rightarrow (m_1 - m_2) = 0$

$\Rightarrow (m_1 - m_2) r = 0.r \quad \forall r \in F$.

$\Rightarrow$ char $(F) = |(m_1 - m_2)|$ where $|(m_1 - m_2)| < p$.

Which is a $\Rightarrow\Leftarrow$ to char$(F) = p$.

$\therefore S_1$ is a set of distinct elements.

$\therefore$ S_1 is a subset of F with distinct elements and $|S_1| = p^2$.

If $S_1 = F$, then the theorem is over.

If $S_1 \neq F$, choose $b \in F - S_1$.

Consider $S_2 = \{ lb + ma + nc \;/\; 0 \leq l, m, n \leq p \}$.

$|S_2| = p^3$ and $S_2 \subseteq F$.

Now S_2 is a set of distinct elements.

If $S_2 = F$, then the theorem is over.

Otherwise continue in this manner.

Since F is finite, at some stage we will have $F = S_{t-1}$ with $|S_{t-1}| = p^t$.

$\therefore$ $|F| = p^t$.

Hence the proof.