B.Sc Part II (Hons)

paper - 03

A finite domain as a field.

Theorem :- A finite Commutative ring without Zero divisor is a field.

or

Every finite Integral domain is a field.

Proof:- let D be a finite Commutative ring without zero divisors having n elements $a_1, a_2, a_3, \ldots a_n$. In order to prove that D is a field (i) We must produce an element $1 \in D$ such that $1a = a$ for all $a \in D$ and (ii) We should show that every non-zero element of D has an inverse i.e for every element $a \neq 0 \in D$ there exists an element $b \in D$ such that $ba = 1$.

let $a \neq 0 \in D$

Consider the n products $aa_1, aa_2, aa_3, \ldots aa_n$. All these are elements of D since D is an integral domain and therefore it is closed with respect to multiplication.

All these elements are distinct.

Suppose on the contrary that $aa_i = aa_j$, for $i \neq j$.

Then $a(a_i - a_j) = 0$ ——— (1)

Since D is without zero divisors and $a \neq 0$

$\therefore$ (1) $\Rightarrow a_i - a_j = 0 \Rightarrow a_i = a_j$ Contradicting $i \neq j$.

Hence $aa_1, aa_2, aa_3, \ldots aa_n$ are all the n distinct elements of D placed in some order, so one of these elements will be equal to a.

Thus there exists an element say a_p that $aa_p = a = a_pa$ ∵ D is Commutative.

We shall show that this element a_p is multiplicative identity of D.

Let y be an element of D. Then from the above discussion, for some $x \in D$, we shall have $ax = y = xa$.

Now $a_p y = a_p(ax)$ ∵ $ax = y$

$= (a_p a)x = ax$ ∵ $a_p a = a$

$= y = y a_p$ ∵ D is Commutative

Thus $a_p y = y = y a_p$ for all $y \in D$. Therefore a_p is the unit element of the ring D.

Let us denote it by 1.

Now $1 \in D$. Therefore from the above discussion, one of the n products $aa_1, aa_2, \ldots, aa_n$ will be equal to 1. Thus there exists an element say $b \in D$ such that $ab = 1 = ba$.

∴ b is the multiplicative inverse of the non-zero element $a \in D$. Thus every non-zero element of D is inversible.

Hence D is a field.

Ex:- If m is Composite, this ring possesses proper zero divisors and hence it cannot be an integral domain or a field.

Ans:- The set $I/(m)$ of residue classes (mod. m) is

$I/(m) = [\{0\}, \{1\}, \{2\}, \text{——} \{m-1\}]$ we ~~have already verified that~~ know that $I/(m)$ is a commutative ring with unity. If m is composite say $m = pq$ where $p, q > 0$, then $\{p\}\{q\} = \{pq\} = \{m\} = 0$ where $\{p\}\{q\}$ are different from $\{0\}$. Hence if m is composite, $I/(m)$ possesses zero divisors and hence $I/(m)$ cannot be an integral domain and hence not a field.

Anand Kumar Sir's.