

Theorem: Finite integral domains are fields.

Pf. Let  $D$  be a finite integral domain and following are all of its elements,

$$0, 1, a_1, a_2, \dots, a_n$$

To show  $D$  is a field it is sufficient to show that every nonzero element of  $D$  have multiplicative inverse.

Let  $a (\neq 0) \in D$ . Now consider the following sequence of elements

$$a, aa_1, aa_2, \dots, aa_n \quad \text{elements of } D$$

All these elements are distinct, because

$$\text{for } aa_i = aa_j$$

$$\Rightarrow a_i = a_j \quad [\text{by cancellation law}]$$

Again all these elements  $a, aa_1, \dots, aa_n$  are nonzero as they are elements of an integral domain (integral domain has no zero divisor i.e. product of two non zero element cannot be zero).

Since  $D$  is finite so the elements  $a, aa_1, aa_2, \dots, aa_n$  are the same elements as  $1, a_1, a_2, \dots, a_n$  ~~but~~ in some order.

So we can conclude that  
either  $a1 = 1$

$$\Rightarrow a1 = 1 \cdot 1 \Rightarrow a = 1$$

or

$$a a_i = 1 \text{ for some } i, 1 \leq i \leq n$$

Thus if  $a = 1$ ,  $a$  is its own inverse.

otherwise  $\exists$  some  $a_i \in D$  s.t.  $a a_i = 1 = a_i a$ .

$\Rightarrow a_i$  is the inverse of  $a$ ,

$\therefore$  every nonzero element  $a$  of  $D$  has  
multiplicative inverse. Hence  $D$  is a  
field.