Embedding of integral domain in field

Q. Prove that any integral domain can be embedded in a field.

or

Prove that a commutative ring without zero divisors can be embedded in a field

Let D be an integral domain. We form the Cartesian product $D \times (D-\{0\})$ such that

$$D \times (D-\{0\}) = \{(a,b) : a, b \in D \text{ and } b \neq 0\}$$

We now define a relation $\sim$ on $D \times (D-\{0\})$ such that

$$(a,b) \sim (c,d) \iff ad = bc$$

We shall show that $\sim$ is an equivalence relation

Let $(a,b), (c,d), (e,f) \in D \times (D-\{0\})$

(i) $(a,b) \sim (a,b)$, since $ab = ba$

$\therefore \sim$ is reflexive

(ii) $(a,b) \sim (c,d) \Rightarrow ad = bc$
$\Rightarrow bc = ad$
$\Rightarrow cb = da$
$\Rightarrow (c,d) \sim (a,b)$

$\therefore \sim$ is symmetric

(iii) $(a,b) \sim (c,d)$ & $(c,d) \sim (e,f) \Rightarrow ad = bc$ & $cf = de$
$\Rightarrow adcf = bcde$
$\Rightarrow af = be$
$\Rightarrow (a,b) \sim (e,f)$

$\therefore \sim$ is transitive

Hence $\sim$ is an equivalence relation

This equivalence relation will partition the set $D \times (D-\{0\})$ into mutually disjoint classes.

Let $[a,b]$ be the equivalence class of $(a,b) \in D \times (D-\{0\})$ and F be the set of all equivalence classes.

Now by suitable definitions of addition & multiplication we shall make F a field.

We define $[a,b]+[c,d]=[ad+bc,\ bd]$
& $[a,b][c,d]=[ac,\ bd]$, $[a,b],[c,d]\in F$
From the above definitions it is clear that F is closed under addition & multiplication.

Before showing the other postulates for being a field we shall first show that addition & multiplication so defined are well defined.

Let $[a,b]=[a',b']$ & $[c,d]=[c',d']$

Then we have to prove that
$[a,b]+[c,d]=[a',b']+[c',d']$
& $[a,b][c,d]=[a',b'][c',d']$

Since we have $[a,b]=[a',b']$, therefore $ab'=ba'$ — (1)
& since $[c,d]=[c',d']$, therefore $cd'=dc'$ — (2)

Now, $(ad+bc)b'd' = adb'd'+bcb'd' = ab'dd'+bb'cd'$
$= ba'dd'+bb'dc'$ [from (1) & (2)]
$= bda'd'+bdb'c'$
$= bd(a'd'+b'c')$

$\therefore [ad+bc,\ bd]=[a'd'+b'c',\ b'd']$ [As in (1) & (2)]

$\therefore [a,b]+[c,d]=[a',b']+[c',d']$
i.e. addition is well defined.

Again, $acb'd' = ab'cd' = ba'dc'$ [from (1) & (2)]
$= bda'c'$

$\therefore [ac,\ bd]=[a'c',\ b'd']$

$\therefore [a,b][c,d]=[a',b'][c',d']$
i.e. multiplication is well defined.

Let $[a,b],[c,d],[e,f]\in F$

Associative law for addition

$([a,b]+[c,d])+[e,f] = [ad+bc,\ bd]+[e,f]$
$= [(ad+bc)f+(bd)e,\ (bd)f]$
$= [adf+bcf+bde,\ bdf]$

Also, $[a,b]+([c,d]+[e,f]) = [a,b]+[cf+de,\ df]$
$= [a(df)+b(cf+de),\ b(df)]$
$= [adf+bcf+bde,\ bdf]$

$\therefore ([a,b]+[c,d])+[e,f] = [a,b]+([c,d]+[e,f])$

i.e. associative law for addition holds.

Existence of zero element

There exists a zero element $[0,1] \in F$ such that

$$[a,b]+[0,1] = [a1+b0,\ b1] = [a,b]$$
$$= [0,1]+[a,b]$$

Existence of additive inverse

For every element $[a,b] \in F$ there exists inverse element $[-a,b] \in F$ such that

$$[a,b]+[-a,b] = [ab+(-ba),\ bb] = [ab-ab,\ bb] = [0,bb] = [0,1],$$
since $(0,bb) \sim (0,1)$
$$= [-a,b]+[a,b]$$

Commutative law for addition

$$[a,b]+[c,d] = [ad+bc,\ bd] = [bc+ad,\ bd] = [cb+da,\ db]$$
$$= [c,d]+[a,b]$$

i.e. commutative law for addition holds

Associative law for multiplication

$$([a,b][c,d])[e,f] = [ac,\ bd][e,f] = [ace,\ bdf]$$

Also, $[a,b]([c,d][e,f]) = [a,b][ce,\ df] = [ace,\ bdf]$

i.e. Associative law for multiplication holds

Existence of unity element

There exists an unity element $[1,1] \in F$ such that

$$[a,b][1,1] = [a1,\ b1] = [a,b]$$
$$= [1,1][a,b]$$

Existence of multiplicative inverse

For every non-zero element $[a,b] \in F$ there exists an inverse element $[b,a] \in F$ such that $[a,b][b,a] = [ab,\ ba] = [1,1]$, since $(ab,ba) \sim (1,1)$

Commutative law for multiplication

$$[a,b][c,d] = [ac,\ bd] = [ca,\ db] = [c,d][a,b]$$

i.e. commutative law for multiplication exists.

Distributive laws:

$[a,b]([c,d]+[e,f]) = [a,b][cf+de, df]$

$= [a(cf+de), b(df)]$

$= [acf+ade, bdf]$

Also, $[a,b][c,d]+[a,b][e,f] = [ac, bd]+[ae, bf]$

$= [acbf+bdae, bdbf]$

$= [acf+ade, bdf]$ $[\because (acbf+bdae, bdbf \sim (acf+ade, bdf)]$

$\therefore [a,b]([c,d]+[e,f]) = [a,b][c,d]+[a,b][e,f]$

Similarly, $([c,d]+[e,f])[a,b] = [c,d][a,b]+[e,f][a,b]$

i.e. distributive laws hold.

Thus F is a field.

Let D^* be a subset of F consisting of all elements of the form $[a,1]$, $a \in D$. Clearly D^* is a subfield.

Let us define a mapping $\phi: D \to D^*$ such that $\phi(a) = [a,1]$

ϕ is one-one, since $\phi(a) = \phi(b) \Rightarrow [a,1] = [b,1]$

$\Rightarrow (a,1) \sim (b,1)$

$\Rightarrow a1 = 1b$

$\Rightarrow a = b$

ϕ is onto, since every element $[a,1] \in D^*$ is the image of every element $a \in D$ under the mapping ϕ.

ϕ is homomorphism, since $\phi(a+b) = [a+b, 1]$

$= [a,1]+[b,1]$

$= \phi(a)+\phi(b)$

& $\phi(ab) = [ab, 1]$

$= [a,1][b,1]$

$= \phi(a)\phi(b)$

$\therefore D$ is isomorphic to D^*

Thus the integral domain D is embedded in the field F.