2015

2. (a) (i) State and Prove the first isomorphism theorem on groups. (1+4=5)

Statement : Let, $f: G \to G_1$ be a Homomorphism of groups. Then the quotient group $G/\ker f$ is isomorphic to the subgroup $\operatorname{Im} f$ of G_1 (i.e. $G/\ker f \simeq \operatorname{Im} f$).

Proof : Let, $H = \ker f$.

We show that $G/H \simeq \operatorname{Im} f$, defined a function $\psi : G/H \to \operatorname{Im} f$ by $\psi(aH) = f(a)$ $\forall\, aH \in G/H$.

We 1st show that ψ is well defined,

For this let, $aH = bH$ in G/H. Then $a^{-1}b \in H = \ker f$.

and so $f(a^{-1}b) = e \Rightarrow e = f(a^{-1}) \cdot f(b)$ [$\because f$ is Homomorphism]

$$= [f(a)]^{-1} \cdot f(b)$$

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

Consequently, $\psi(aH) = f(a) = f(b) = \psi(bH)$ and so ψ is well defined.

Now for any $xH, yH \in G/H$, $\psi(xH \cdot yH) = \psi(xyH) = f(xy) = f(x) \cdot f(y)$

~~$= \psi(xH) \cdot \psi(yH)$~~. [$\because f$ is a Homomorphism]

$= \psi(xH) \cdot \psi(yH)$.

Hence, ψ is a Homomorphism.

Since, $\operatorname{Im} f = f(G)$, we find that for any $a \in \operatorname{Im} f$, $\exists\, u \in G$ such that $f(u) = a$ and $uH \in G/H$, we shows that $\psi(uH) = f(u) = a$.

So, ψ is surjective.

Let, $aH, bH \in G/H$, so that $\psi(aH) = \psi(bH)$. Then $f(a) = f(b)$.

Hence, $f(a^{-1}b) = \{f(a)\}^{-1} f(b) = \{f(b)\}^{-1} f(b) = e$.

$\Rightarrow a^{-1}b \in \ker f = H$.

This follows that $aH = bH$. So, ψ is injective.

Hence, ψ is an isomorphism.

i.e. $G/\ker f \simeq \operatorname{Im} f \;[= f(G)]$.

2. (a) (ii) Let, G be group and H be a non-empty subset of G. State and Prove a NASC for H to be a subgroup of G. (1+4=5)

Ans: Statement : Let, $(G, \circ)$ be a group. A non-empty subset H of G forms a subgroup iff $a, b \in H \Rightarrow a \circ b^{-1} \in H$.

~~Proof~~

Let, $(H, \circ)$ be a subgroup of G. Since, $(H, \circ)$ is a group.

Let, $b \in H \Rightarrow b^{-1} \in H$. and Hence for $a \in H$, $b^{-1} \in H \Rightarrow a \circ b^{-1} \in H$.

Conversely, let H be a non-empty subset of G. such that $a \in H, b \in H \Rightarrow a \circ b^{-1} \in H$

Now, $a \in H$, $a^{-1} \in H \Rightarrow a \circ a^{-1} \in H \Rightarrow e \in H$.

$\therefore$ Identity element exist in H.

Let, $e \in H$, $a \in H \Rightarrow e \circ a^{-1} \in H \Rightarrow a^{-1} \in H$.

Inverse of each element exist in H.

Let, $a \in H, b \in H \Rightarrow a \in H, b^{-1} \in H \Rightarrow a \circ (b^{-1})^{-1} \in H \Rightarrow a \circ b \in H$.

i.e. Closure Property holds in H.

Since, H is a non-empty subset of G and 'o' is associative on G, 'o' is associative on H.

Associative Property holds in H, it is Heriditary.

$\therefore (H, \circ)$ is a group, and Hence $(H, \circ)$ is a sub-group of $(G, \circ)$.

(iii) If a, b are two elements of a group G such that $ab = ba^{-1}$ and $ba = ab^{-1}$. Prove that $a^4 = b^4 = e$. 2.

Ans: We have, $ab = ba^{-1} \to (1)$ and $ba = ab^{-1} \to (2)$

or, $ab \cdot a = ba^{-1}a$

or, $a \cdot ab^{-1} = b \cdot e$.

or, $a^2 b^{-1} \cdot b = b \cdot b$

or, $a^2 = b^2 \longrightarrow (3)$

Now, multipling (1) and (2), we get

$ab \cdot ba = ba^{-1} \cdot ab^{-1}$

or, $ab^2 a = b \cdot e \cdot b^{-1}$

or, $a \cdot ab^2 a = abb^{-1}$

or, $a^2 b^2 \cdot a \cdot a = a \cdot e \cdot a$

or, $a^2 b^2 a^2 = a^2$

or, $b^2 \cdot b^2 \cdot b^2 = b^2$

or, $b^6 = b^2$

or, $b^4 = e. \longrightarrow (4)$

$\therefore$ From (3), $(a^2)^2 = (b^2)^2 \Rightarrow a^4 = b^4 \Rightarrow a^4 = e$. [From (4)]

Hence, $a^4 = b^4 = e$.

2.c.(i) Define a Boolean algebra. Let X be a non-empty set. Justify whether P(X) the power set of X is a Boolean algebra. 2+3

Ans: A non-empty set B on which two binary operations + (addition), $\cdot$ (multiplication) and one unary operation ' (complementation) are defined, is said to be Boolean algebra if the following postulates are satisfied.

1. + and · are commutative.

1(a) $a+b=b+a$ 1(b) $a\cdot b=b\cdot a$, $\forall a,b\in B$.

2. '+' is distributive over '·' and '·' is distributive over '+'.

2(a) $a+(b\cdot c)=(a+b)\cdot(a+c)$ 2b. $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$, $\forall a,b,c\in B$.

3. $\exists$ in B distinct elements 0 and I which are identity elements for '+' and '·' respectively.

3.(a) $a+0=a$, $\forall a\in B$ 3(b) $a\cdot I=a$, $\forall a\in B$.

4. $\forall a\in B$ the operation ' satisfies,

4(a) $a+a'=I$ 4(b) $a\cdot a'=0$.

The Boolean algebra is denoted by $(B,+,\cdot,')$ or by B only.

(ii) Let, R be a ring such that $a^2=a$ for every $a\in R$. Prove that R is commutative. (5)

Ans: $(a+b)=(a+b)^2=(a+b)\cdot(a+b)=a\cdot(a+b)+b\cdot(a+b)$.

$=(aa+ab)+ba+bb)$

$=(a+ab)+(ba+b)$ $[\because a^2=a, b^2=b]$

$=(a+ab)+(b+ba)$

$=[(a+ab)+b]+ba$

$=[a+(ab+b)]+ba$

$=[a+(b+ab)]+ba$

$=[(a+b)+ab]+ba$

or, $(a+b)+0$ $=(a+b)+(ab+ba)$.

Therefore, $0=ab+ba$ by left cancellation law.

Hence, by ~~xxx~~ we have $ab=ba$. [Each element is its own additive inverse and so $-ba=ba$]

(iii) Prove that every field is an integral domain. Illustrate with an example that the converse is not true.

2+2.

Ans: To prove the theorem, we are to prove that in a field $\exists$ no divisors of zero, i.e. if F be a field and $a,b\in F$ then $a\cdot b=0\Rightarrow$ either $a=0$ or $b=0$

If $a\neq0$, then a^{-1} exists and we have since $a\cdot b=0$.

$a^{-1}(a\cdot b)=a^{-1}0$

Therefore, $(a^{-1}a)\cdot b=0$, i.e $1\cdot b=0$, since $a^{-1}\cdot a=1$

i.e. $b=0$, since, $1\cdot b=b$. Here 0 is the additive identity and 1 is the multiplicative identity.

Similarly, if $b\neq0$ we can show that $a=0$.

Thus the field, having no zero divisors, is an integral domain.

- But the converse is not true.

Let, $S=(\mathbb{Z},+,\cdot)$, forms a commutative ring with unity, does not contain divisors of zero. Therefore S is an integral domain but not a field. Since, inverse of each element does not exist except 1 and -1.

2.d.(i) Let, I be an Ideal of a ring R. Define $\phi : R \to R/I$ by $\phi(a) = a+I$ for every $a \in R$. Show that ϕ is a ringhomomorphism and $\ker\phi = I$.

Ans: The fact that ϕ preserves addition and multiplication follows from the def^n of addition and multiplication in R/I. It is surjective, since any coset $a+I$ is the image of $a \in R$. Finally, the kernel is the set of all $a \in R$ such that $\phi(a) = 0+I$, the zero element of R/I. But $a+I = 0+I$ iff $a \equiv 0 \pmod{I}$ iff $a \in I$. Thus the kernel is just I.

(ii) Give an example with justification of a subring of a ring which is not an Ideal.

Ans: The ring $\mathbb{Q}$ and the integers $\mathbb{Z}$. Clearly $\mathbb{Z}$ is a subring of $\mathbb{Q}$, but it is not an ideal of $\mathbb{Q}$ (which has only two ideals, 0 and itself).

Let, $a, b \in \mathbb{Z}$ and $r \in \mathbb{Q}$.

Here, $a-b \in \mathbb{Z}$ and $a.r$, $r.a$ may not always belongs to $\mathbb{Z}$.

$\therefore$ $\mathbb{Z}$ is not an ideal.