MTH3121 Algebra Problem Sheet 2 : Saral 30 618 428

Question 3 a

Lets call the group represented by R^+ under multiplication,

M and the group represented by R^+ under the operation $x * y = \frac{1}{3} xy$,

O. So for M and O to be isomorphic there must be a bijection such that :
$f : M \longrightarrow O$ such that :

$f(a * b) = f(a) * f(b)$, for all $a, b \in M$

From looking at the $\frac{1}{3}$ it seems like a bijection could be $f(x) = 3x$. Lets see if this is it.

$f(a * b) = f(ab)$ (Just applying the multiplication binary operation)

$f(ab) = 3ab$ (Applying $f(x) = 3x$)

$3ab = \frac{1}{3}(3a)(3b)$ (Separating out some terms)

$\frac{1}{3}(3a)(3b) = \frac{1}{3} f(a) f(b)$ (Applying $f(x) = 3x$)

$\frac{1}{3} f(a) f(b) = f(a) * f(b)$ $\left(\text{Applying the binary operation } x * y = \frac{1}{3} xy\right)$

Thus we have shown that $f(a * b) = f(a) * f(b)$

But wait is the supposed bijection , $f(x) = 3x$, even a bijection ?

First we have to show that it is injective (one - to - one) :

For any $a, b \in R$

$f(a) = 3a$

$f(b) = 3b$

if $f(a) = f(b)$ then $3a = 3b$

$3a = 3b \Longrightarrow a = b$

Therefore $f(x)$ is injective

Now is it surjective ?

For this to be the case we would need that for anthing
$y \in$ (some codomain) there exists an $x \in$ (some domain) such that :

$f(x) = y$

This would imply that :

$y = 3x$

and thus $x = \frac{y}{3}$, we have found an x for every y in the codomain.

This means that f (x) is surjective.

Since it is both injective and surjective, f (x) = 3 x, is a bijection.

Question 4

a) Max order of an element of S_6 is 6,
whereas for D_{720} it is 720. Therefore S_6 and D_{720} are not isomorphic.

b) Max order of an element of D_{18} is 18,
where as for Z_{36} it is 36. Therefore D_{18} and Z_{36} are not isomorphic.

c) Max order of an element of D_{60} is 60,
whereas for S_5 it is 6. Therefore D_{60} and S_5 are not isomorphic.

d) The only element of finite order in R under addition is 0. This has order 1. For R^* under multiplication − 1 has order 2 and 1 has order 1.

Thus R^+ and R^* have different numbers of elements of finite order and therefore they are not isomorphic.

Question 5

a) f = (1 7 6) (2 3 9 8 5)

g = (1 3 8 7) (2 4) (5 9)

f g = (1 9 2 4 3 5 8 6)

g f = (2 8 9 7 6 3 5 4)

f^{-1} = (1 6 7) (2 5 8 9 3)

f^2 = (1 6 7) (2 9 5 3 8)

f^3 = (1 7 6) (2 3 9 8 5)

f^{2121} = (1 7 6) (2 3 9 8 5), 2121 is divisible by 3 so applying f to itself 2121 times gives the same result as applying f to itself 3 times.

b) First we will look at f. The two cycles in f are:

$1 \longrightarrow 7 \longrightarrow 6 \longrightarrow 1$ . . . . . (Cycle 1)

$2 \longrightarrow 3 \longrightarrow 9 \longrightarrow 8 \longrightarrow 5 \longrightarrow 2$ . . . . . (Cycle 2)

For any number in cycle 1 to come back to itself we need m iterations where m is divisible by 3.

For any number in cycle 2 to come back to itself we need m iterations where m is divisible by 5.

Therefore m is divisible by both 3 and 5 and lcm(3,5) = 15

Thus the order of f is 15.

For g using the same arguments, its order would be divisible by both 4 and 2. lcm(4,2) = 8

Therefore the order of g is 8.

c) p = (1 6 7) (2 8 3 5 9)

Question 10 a

For GL_2 (R) to be a group under matrix multiplication we need an identity, an inverse and for the matrix multiplcation to be associative.

Lets first find the identity, lets call the identity I where :

$I = \begin{bmatrix} m & n \\ o & p \end{bmatrix}$ where m, n, o, p ∈ R such that mp − on ≠ 0

For an identity and for some matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2$ (R) we would need the following operations to hold :

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} m & n \\ o & p \end{bmatrix} = \begin{bmatrix} am + bo & an + bp \\ am + do & cn + dp \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ (Operation 1)

$\begin{bmatrix} m & n \\ o & p \end{bmatrix} \times \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} am + nc & mb + nd \\ oa + pc & ob + pd \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ (Operation 2)

From Operation 1 and 2 we can derive the following equations :

bo = nc (Equation 1)

am + nc = a (Equation 2)

ob + pd = d (Equation 3)

Now after doing a bunch of arithmetic I got absoluetly no where and I had even more equations than the ones I listed.

BUT then I looked at Equation 1 VERY closely.

n and o are entries in I, our identity matrix and Equation 1 is saying in english terms :

"No matter what b and c you give me for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(R)$, bo = nc"

How can this even be possible ? n and o are constant in our identity matrix, they dont change their values but b and c can change and yet bo = nc.

The only way this is possible is if n = o = 0.

Therefore we know our I looks something like :

$\begin{bmatrix} m & 0 \\ 0 & p \end{bmatrix}$

Now what are m and p. We can find what m is using Equation 1 and substituting n = 0 into it giving :

am = a (Equation 4)

Thus m = 1

To find p we can use Equation 3 and substitute o = 0 into it to give :

pd = d (Equation 5)

Thus p = 1

At this point I also know that $a = p = 0$ are also solutions to Equation 4 and 5 but we are only looking at the entries relevant to our Identity matrix.

Thus the identity is :

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Now do we have an inverse ?

For an inverse we need for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(R)$ there is another $\begin{bmatrix} w & x \\ y & z \end{bmatrix} \in GL_2(R)$ such that :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{bmatrix} = I \qquad (\text{Equation 6})$$

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} aw + xc & wb + xd \\ ya + zc & by + dz \end{bmatrix} = I \qquad (\text{Equation 7})$$

I won't show all the arithmetic here but after doing it I found that :

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} d\left(\frac{y-x}{b-c}\right) & \frac{by}{c} \\ \frac{xc}{b} & a\left(\frac{y-x}{b-c}\right) \end{bmatrix}$$

Thus we have an inverse.

Now is matrix multiplication associative for $GL_2(R)$?

For matrix multiplication to be associative for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$, $\begin{bmatrix} i & j \\ k & l \end{bmatrix} \in GL_2(R)$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} * \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right) = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) * \begin{bmatrix} i & j \\ k & l \end{bmatrix} \qquad (\text{Equation 8})$$

Lets see if Equation 8 holds :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} ei + fk & ej + fl \\ gi + hk & gj + hl \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} * \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$\begin{bmatrix} a(ei + fk) + b(gi + hk) & a(ej + fl) + b(gj + hl) \\ c(ei + fk) + d(gi + hk) & c(ej + fl) + d(gj + hl) \end{bmatrix} = \begin{bmatrix} (ae + bg)i + (af + bh)k & (ae + bg)j + (af + bh)l \\ (ce + dg)i + (cf + dh)k & (ce + dg)j + (cf + dh)l \end{bmatrix} \quad (\text{Multiplying everything out})$$

$$\begin{bmatrix} (aei + afk + bgi + bhk) & (aej + afl + bgj + bhl) \\ (cei + cfk + dgi + dhk) & (cej + cfl + dgj + dhl) \end{bmatrix} = \begin{bmatrix} (aei + bgi + afk + bhk) & (aej + bgj + afl + bhl) \\ (cei + dgi + cfk + dhk) & (cej + dgj + cfl + dhl) \end{bmatrix}$$

(Expanding the brackets in each entry)

Looking closely we see that LHS = RHS which shows that matrix multiplication is also associative in $GL_2(R)$.

Thus $GL_2(R)$ is a group under matrix multiplcation.

Question 10 b

Question 11 b

Lets deal with the first part of this statement. Lets take the group G to be abelian.

If G is abelian we know that from some elements a and b of G :

$a * b = b * a$

Therefore :

$f(a * b) = f(b * a)$

$f(b * a) = (b * a)^{-1}$ (from applying $f(g) = g^{-1}$)

$(b * a)^{-1} = a^{-1} * b^{-1}$ (Since a and b are elements of a group)

$a^{-1} * b^{-1} = f(a) * f(b)$ (from applying $f(g) = g^{-1}$)

Thus $f(a * b) = f(a) * f(b)$, so this part of the function $f(g) = g^{-1}$ holds.

But is f a bijection? For some elements $a, b \in G$:

If, $f(a) = f(b) \Longrightarrow a^{-1} = b^{-1} \Longrightarrow a = b$

Thus f is injective.

For f to be surjective we need that for all $b \in G$, there exists an $a \in G$ such that :

$f(a) = b$

Thus :

$a^{-1} = b$

$a^{-1} * a = b * a$ (Performing a binary operation with a on both sides)

$e = b * a$ (Since $a^{-1} * a = e$)

Thus $a = b^{-1}$, so for every b there does exist an a such that $f(a) = b$.

This shows that; if G is abelian then f is an isomorphism

Now to go the other way if f is an isomorphism then we know that for some $a, b \in G$:

$f(a * b) = f(a) * f(b)$

We also know that :

$f(a * b) = (a * b)^{-1}$ (Applying $f(g) = g^{-1}$)

Equating these two equations gives us :

$f(a) * f(b) = (a * b)^{-1}$

$a^{-1} * b^{-1} = (a * b)^{-1}$ (Applying $f(g) = g^{-1}$)

$a^{-1} * b^{-1} = b^{-1} * a^{-1}$ (Since a and b are elements of a group)

$a^{-1} * b^{-1} * a = b^{-1} * a^{-1} * a$ (Applying binary operation with a on both sides)

$a^{-1} * b^{-1} * a = b^{-1} * e$ (Using associativity and that $a^{-1} * a = e$)

$a^{-1} * b^{-1} * a = b^{-1}$ (Since $b^{-1} * e = b^{-1}$)

$a^{-1} * b^{-1} * a * b = b^{-1} * b$ (Applying binary operation with b on both sides)

$a^{-1} * b^{-1} * a * b = e$ (Since $b^{-1} * b = e$)

$a * a^{-1} * b^{-1} * a * b = a * e$ (Applying binary operation with a on both sides)

$e * b^{-1} * a * b = a$ (Since $a * a^{-1} = e$ and $a * e = a$)

$b^{-1} * a * b = a$ (Using associativity and that $e * b^{-1} = e$)

$b * b^{-1} * a * b = b * a$ (Applying the binary operation with b on both sides)

$e * a * b = b * a$ (Since $b * b^{-1} = e$)

$a * b = b * a$ (Using associativity and that $e * a = a$)

Thus if f is an isomorphism then G is abelian.

Since we have shown both sides of the statement we can conclude that :

If G is a group and considering the function $f : G \to G$ defined by $f(g) =$
$g - 1$. The group G is abelian
if and only if f is an isomorphism.