Math 241

Problem Set 1 solution manual

Exercise. A1.1

a- Let us show that f: $\mathbb{R} \longrightarrow \mathbb{R}$
given by $f(x) = ax + b$,for $a \in \mathbb{R}^*$ and $b \in \mathbb{R}$ is a bijection.

i
- injective:
  Let $f(x_1) = f(x_2)$ required to show $x_1 = x_2$ so we have $ax_1 + b = ax_2 + b$ (by adding $-b$ to both side of the equality) then $ax_1 = ax_2$
  then $x_1 = x_2$ by cancellation since $\mathbb{R}$ is a group under multiplication
  then f is injective.
- surjective:
  Let $y \in \mathbb{R}$, required to find $x \in \mathbb{R}$ such that $f(x) = y$.
  Let $x = \frac{y-b}{a}$, then it is easy to see that $f(x) = y$.
  Hence f is surjective.

ii Now let us find f^{-1}:
we have $y = ax + b$
$y - b = ax$
$x = \frac{y-b}{a}$

Now let $g(x) = \frac{x-b}{a}$, and let us verify that $g = f^{-1}$ it is easy to prove : $fog = id_{\mathbb{R}}$, and $gof = id_{\mathbb{R}} \implies g = f^{-1}$

b- First we need to prove that o is a binary operation over G , i.e we need to show that the composite of two functions in G is a function in G.
Let $f_1 = f_{a,b}$, and $f_2 = f_{c,d} \in$ G. then $f_1 o f_2 = f_1(f_2(x)) = f_1(cx + d) = a(cx + d) + b = acx + ad + b = f_{ac,ad+b}$ which is a function in G. now let us prove G is a group.

(a) G has an identity element:
consider $f_{1,0}(x) = x$
$f_{1,0} o f_{a,b} = f_{1,0}(ax + b) = ax + b = f_{a,b}(x)$.
similarly $f_{a,b} o f_{1,0} = f_{a,b}$.

(b) the operation o is associative:
$f_{a,b} o (f_{c,d} o f_{e,f})(x) = f_{a,b}(f_{c,d} o f_{e,f}(x)) = f_{a,b}(f_{c,d}(f_{e,f}(x))) = f_{a,b}(f_{c,d}(ex + f))$
$= f_{a,b}(cex + cf + d) = acex + acf + ad + b$.
doing the same for $(f_{a,b} o f_{c,d}) o f_{e,f}(x)$ we will get the same result.
$\implies$ o is associative.

(c) $\forall\ f_{a,b} \in$ G $f_{a,b}$ have an inverse, which is the inverse found in part (a), moreover this inverse belongs to G, since $f_{a,b})^{-1} = f_{\frac{1}{a}, \frac{-b}{a}}$.

So G is a group under composition.

c- consider the subgroup H of $GL_2(\mathbb{R})$ defined by $\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ such that $a \in \mathbb{R}^*$ and $b \in \mathbb{R}$ $\}$

(a) Let us prove that H is a group of GL_2.
-for any two matrices A = $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ and B = $\begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}$ $\in GL_2$ A.B = $\begin{bmatrix} ac & ad+b \\ 0 & 1 \end{bmatrix}$
, which is in H.
-identity belongs to H, since for $a = 1$, and $b = 0$ the matrix we get is the identity matrix.
-for every element A = $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$, we have A^{-1}= $\begin{bmatrix} \frac{1}{a} & \frac{-b}{a} \\ 0 & 1 \end{bmatrix}$ $\in$ H .
So we get that H is a subgroup of GL_2.

(b) Now let us prove that H is isomorphic to the group G given above:
Consider the map : ϕ : H $\longrightarrow$ G defined by $\phi(f_{a,b})$= $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$.
-Let us first prove that it is a homomorphism:
$\phi(f_{a,b} o f_{c,d}) = \phi(f_{ac,ad+b})$= $\begin{bmatrix} ac & ad+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} . \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} = \phi(f_{a,b}).\phi(f_{c,d})$. $\Longrightarrow$
ϕ is a group homomorphism.
-injective : Let $\phi(f_{a,b})$= $\phi(f_{c,d})$
$\Longrightarrow \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}$
$\Longrightarrow$ $a = c$, and $b = d$, $\Longrightarrow$ $f_{a,b}$=$f_{c,d}$.
-surjective is obvious.
$\Longrightarrow$ ϕ is a group isomorphism.

Section. 0

Exercise. 1
$\{ x \in \mathbb{R}$ — $x^2 = 3 \} = \{ - \sqrt{3} , \sqrt{3} \}$.

Exercise. 2
$\{$ m $\in \mathbb{Z}$ — $x^2 = 3 \} = \Phi$.

Exercise. 3
$\{$ m $\in \mathbb{Z}$ — $m.n = 60$ for some $n \in \mathbb{Z}$ $\}$ = The set of all divisors of 60 in $\mathbb{Z}$
=$\{$ -1,-2, -3, -4, -5, -6, -10, -12, -15, -20, -30, -60, 60, 30, 20, 15, 12, 10, 6, 5, 4, 3, 2, 1 $\}$.

Exercise. 12

a. We define f: A $\longrightarrow$ B : by
$f(1) = 4$
$f(2) = 4$
$f(3) = 6$
This map is defined over the entire set A (i.e for each $a \in$ A $f(a)$ is defined)
Also its range is a subset of B, so the map is well defined then it is a function.
injective:Notice that $f(1) = f(2)$, with 1$\neq$2. then f is not injective.

surjective Notice that for $b = 2$ ∈B $\nexists$ a ∈A such that $f(a) = b$. So f is not surjective.

b. This is also a function , which is neither injective nor surjective, and the proof is similar to the above argument in (a).

c. We define f: A $\longrightarrow$ B : by
$f(1) = 6$
$f(1) = 2$
$f(1) = 4$
This is can't describe a function from A to B because it is not defined for all elements of A, moreover it doesn't satisfy a=b $\implies$ $f(a) = f(b)$.

d. We define f: A $\longrightarrow$ B : by
$f(1) = 6$
$f(2) = 2$
$f(3) = 4$
This is a function by the same argument of part (a).

injective: it is clear that $f(a) = f(b)$ only if $a = b$, from the definition of the function, so it is injective.

surjective: Also it is easy to see that for all elements of $b \in$ B we can find a corresponding element $a \in$ A such that $f(a) = b$.

So f is a bijection from A into B.

e. This is also a function, which is neither injective nor surjective, and the proof is similar to the above argument in (a).

f. This doesn't describe a function since it is not defined for all elements of A ($f(3)$ is not defined).

Section. 1

Exercise. 22
10 $+_1 7$ 16 = (26 mod 17)= 9.

Exercise. 29
x $+_{15}$ 7 = 3 in $\mathbb{Z}_{15}$.
Notice that $7^{'}$=8 since 7 $+_{15}$ 8 = (15 mod 15)= 0 (i.e the inverse of 7 is 8 in $\mathbb{Z}_{15}$).
We add 8 to both sides of the equation to get : x $+_{15}$ 7 $+_1 5$ 8 = 3 $+_{15}$ 8 = 11 mod(15),
i.e x = 11 + k.15 for any k $\in \mathbb{Z}$, but since we need our answer in $\mathbb{Z}_{15}$ we can only choose k to be 0.

So our x = 11.

Exercise. 32

x	$x +_{17} +x +_{17} x$
0	0
1	3
2	6
3	2
4	5
5	1
6	4

In modular arithmetics this is :
$x +_7 x +_7 x = 5 \bmod(7)$
$\Leftrightarrow 3x = 5 \bmod(7)$
$\Leftrightarrow 5.3.x = 5.5 \bmod(7)$
$\Leftrightarrow x = 4 \bmod(7)$.

Exercise. 33
$x +_{12} x = 2$ (mod 12) the solution is { $x \in \mathbb{Z}$ — $x +_{12} x = 2 \bmod(12)$ } = { 1 , 7 }.

Section. 2

Exercise. 8 -
Let $\star$ be defined on $\mathbb{Q}$ by $a \star b = ab + 1$.
-commutative : $\forall a, b \in \mathbb{Q}$
$a \star b = a.b + 1$, and $b \star a = b.a + 1$, where the (.) used is the usual multiplication which is commutative, so $a \star b = b \star a$. So $\star$ is commutative.

-associative : $\forall a, b \in \mathbb{Q}$
$(a \star b) \star c = (ab + 1) \star c = (ab + 1)c + 1 = abc + c + 1$, while
$a \star (b \star c) = abc + a + 1 \neq (a \star b) \star c$.
Now consider the following example: Let $a = 1$, $b = 1$, and $c = 2$ then we get $(a \star b) \star c$ =2+2+1=5, while $a \star (b \star c)$ =2+1+1=4.
So $\star$ is not associative.

Exercise. 9 -
- $\forall a, b \in \mathbb{Q}$
$a \star b = \frac{a.b}{2} = \frac{b.a}{2} = b \star a$. So $\star$ commutative.

- $\forall a, b \in \mathbb{Q}$
$a \star (b \star c) = \frac{a.\frac{b.c}{2}}{2} = \frac{abc}{4} = \frac{\frac{a.b}{2}.c}{2} = (a \star b) \star c$. So $\star$ is associative.

Exercise. 23 -

H = $\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ — $a, b \in \mathbb{R}$ $\}$

Let A $=\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, and B $=\begin{bmatrix} c & -d \\ d & c \end{bmatrix}$ be two elements in H.

Then

-Under addition : A+B$=\begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix}$, which is an element of H. So His closed under addition.

-Under multiplication: A.B$=\begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & ac-bd \end{bmatrix} = \begin{bmatrix} u & -v \\ v & u \end{bmatrix}$ for $u = ac - bd$ and $v = ad + bc$.
So H is closed under multiplication.

Exercise. 26 -
Given $\star$ associative: prove $(a \star b) \star (c \star d) = [(d \star c) \star a] \star b$.
start with : $[(d \star c) \star a] \star b$, and cosider $(d \star c) = u \in$ S (Note that $u = (c \star d)$ since $\star$ commutative).
we get $(u \star a) \star b = u \star (a \star b)$ since $\star$ is associative.
Then $u \star (a \star b) = (a \star b) \star u$ since $\star$ is commutative.
Then we get $[(d \star c) \star a] \star b = (a \star b) \star u = (a \star b) \star (c \star d)$.

Section. 3

Exercise. 33 -
H = $\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ — $a, b \in \mathbb{R}$ $\}$

a.

Consider the function ϕ : ($\mathbb{C}$, +) $\longrightarrow$ (H,+).

Defined by $\phi(a + ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

-ϕ **is well defined** :

- for $a + ib = c + id$ we have $a = c$ and $b = d$ which implies $\phi(a + ib)$=$\phi(c + id)$.
- For any $z \in \mathbb{C}$, $\phi(z) \in$ H.

-ϕ **is a homomorphism** :

For $z_1 = a + ib$, and $z_2 = c + id$ we need to show $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$.

$\phi(z_1 + z_2)$=$\phi(a + ib + c + id)$=$\phi(a + c + i(b + d)) = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix}$

$= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \phi(z_1) + \phi(z_2)$.

-ϕ **is injective** :

Let $\phi(z_1) = \phi(z_2)$ for $z_1 = a + ib$, and $z_2 = c + id$.

Then : $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$

Then $a = c$, and $b = d$, which implies $z_1 = z_2$. $\implies$ ϕ is injective.

-ϕ **is surjective** :

Let A=$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ $\in$ H, then consider $z = a + ib \in \mathbb{C}$, it is clear that $\phi(z)$=A.

$\implies$ ϕ is surjective.

Note that instead of proving Φ inective and surjective we can just prove that ϕ has a well defined inverse function which is :

$\phi^{-1}(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}) = a + ib$. So ($\mathbb{C}$,+) $\cong$ (H,+)

b.

Consider the same function ϕ introduced above, it is still a well defined bijection from $(\mathbb{C}, \cdot)$ to (H,$\cdot$). So we only need to show that it is a homomorphism.

For $z_1 = a + ib$, and $z_2 = c + id$ we need to show $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$.

$$\phi(z_1.z_2)=\phi((a+ib).(c+id))=\phi(ac-bd+i(ad+bc)) = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}$$

$$= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} . \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \phi(z_1)\ .\ \phi(z_2).$$

So ϕ ia an isomorphism. $\implies$ ($\mathbb{C}$,.) $\cong$ (H,.)

Section. 4

Exercise. 8 -

The set { 1 , 3 , 5 , 7 } with multiplication $._8$ modulo 8 is a group. Its table is

$._8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1