MA208 Solutions Week 1 Sem B2000

Exercise 1.3 page 3

1) All binary operations except b) 2) e),g) and i) are not closed.

3) a) $a*b=a+b+1$ b) $a*b=ab/(a+b)$ c) $a*b=a+\_b+ab$

4) a) if a= -2 and b = 2 we see * not well defined on **Z,Q** or **R** (division by zero) it is consequently not closed
   b) & d) both well defined and also closed on **Z,Q** or **R**
   c) well defined on **Z,Q** and **R**, closed **R,** not closed on **Z** or **Q**

Exercise 1.6 page 6

1) c), d), e), j) and k) are commutative a), c), d), e), j) and k) are associative

2)

	a)	b)	c)	d)	e)
Commutative	Y	Y	N	Y	Y
Associative	Y	N	Y	N	Y

3) a) no identity b) no identity c) no identity d) 0 e) 0

4) d) a has inverse a e) there are no inverses

5) ∅ is the identity with respect to union of sets. There are no inverses.

6) (a*b)*c = (a+b+ab)*c = (a+b+ab) +c + (a+b+ab)c = a + b + c + bc + ab + ac + abc
a*(b*c) = a*(b+c+bc) = a + (b+c+bc) + a(b+c+bc) = a + b + c + bc + ab + ac + abc

So (a*b)*c = a*(b*c) and hence * satisfies the assoc. law

Let e be the identity w.r.t. *
So $a*e = a$ for all $a \in Z$
$\Rightarrow$ $a + e + ae = a$ for all $a \in Z$
$e(1 + a) = 0$ for all $a \in Z$ $\Rightarrow$ $e = 0$
So 0 is the identity w.r.t. *
If a has an inverse $\bar{a}$ then
$a * \bar{a} = 0$ $\Rightarrow$ $a + \bar{a} + a\bar{a} = 0$ $\Rightarrow$ $\bar{a}(1 + a) = -a$ $\Rightarrow$ $\bar{a} = -a/(1+a)$
So every element except –1 has an inverse.

Exercise 2.2 page 8

	+	–	×	÷
N	No inverses	Not associative, No identity	No inverses	Not well-defined
Z	ABELIAN GROUP	Not associative, No identity	No inverses	Not well-defined
Q	ABELIAN GROUP	Not associative, No identity	No inverses	Not well-defined

	+	−	×	÷
Q – {0}	Identity not in set	Not associative, No identity	ABELIAN GROUP	Not associative, No identity
R	ABELIAN GROUP	Not associative, No identity	0 has no inverse	Not well-defined
R – {0}	Identity not in set	Not associative, No identity	ABELIAN GROUP	Not associative, No identity
m × n matrices	ABELIAN GROUP	Not associative, No identity	Not well-defined	
n × n matrices	ABELIAN GROUP	Not associative, No identity	Not all elements have inverses	
n × n non-sing. matrices	Not closed	Not associative, No identity	GROUP (not abelian)	

2. a) Not a group - no identity or inverses

b) $\{5a : a \in \mathbf{Z}\}(+)$ (the set of multiples of 5 with the binary operation addition)
$5a + 5b = 5(a+b) \in \mathbf{Z}$, $\forall a,b \in \mathbf{Z}$, so the set is closed w.r.t. +
+ of integers is associative, so addition of multiples of 5 is also associative.
$5a + 0 = 0 + 5a = 5a$ $\forall a \in \mathbf{Z}$ so 0 is the identity
$5a + (-5a) = (-5a) + 5a = 0$, $\forall a \in \mathbf{Z}$ so $-5a$ is the inverse of $5a$

Hence $\{5a : a \in \mathbf{Z}\}$ (+) is a group.

c) Not a group - no inverses

d) $\{z : z \in \mathbf{C}$ and $|z|=1\}$ (.)
Let z_1, and $z_2 \in \mathbf{C}$ such that $|z_1| = |z_2| = 1$
Then $z_1 z_2 \in \mathbf{C}$ and $|z_1||z_2| = 1.1 = 1$ so we have closure.
Multiplication of complex numbers is associative.
$1.\ z = z.\ 1 = z$ $\forall z \in \mathbf{C}$, hence the identity is 1
Let $z^{-1} = 1$ then $z^{-1} = 1/z$ so $|z^{-1}| = 1/1 = 1$ hence $z^{-1} \in$ the set
Similarly $z z^{-1} = 1$. Hence z^{-1} is the inverse of z, $\forall z \in \mathbf{C}$
Hence $\{ z : z \in \mathbf{C}$ and $|z|=1\}$(.) is a group.

e) Group
f) Not a group - not closed, no inverses
g) Not a group - not closed, no identity

Exercise 2.3 page 9

1.

•	1	-1
1	1	-1
-1	-1	1

2.

•	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

3.

.	I	A	B	C
I	I	A	B	C
A	B	C	I	
B	B	C	I	A
C	C	I	A	B

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

4.

.	1	r	r^2	r^3	r^4	r^5
1	1	r	r^2	r^3	r^4	r^5
r	r	r^2	r^3	r^4	r^5	1
r^2	r^2	r^3	r^4	r^5	1	r
r^3	r^3	r^4	r^5	1	r	r^2
r^4	r^4	r^5	1	r	r^2	r^3
r^5	r^5	1	r	r^2	r^3	r^4

5.

+	$(0, 0, 0, 0)$	$(1, 1, 0, 1)$	$(0, 0, 1, 1)$	$(1, 1, 1, 0)$
$(0, 0, 0, 0)$	$(0, 0, 0, 0)$	$(1, 1, 0, 1)$	$(0, 0, 1, 1)$	$(1, 1, 1, 0)$
$(1, 1, 0, 1)$	$(1, 1, 0, 1)$	$(0, 0, 0, 0)$	$(1, 1, 1, 0)$	$(0, 0, 1, 1)$
$(0, 0, 1, 1)$	$(0, 0, 1, 1)$	$(1, 1, 1, 0)$	$(0, 0, 0, 0)$	$(1, 1, 0, 1)$
$(1, 1, 1, 0)$	$(1, 1, 1, 0)$	$(0, 0, 1, 1)$	$(1, 1, 0, 1)$	$(0, 0, 0, 0)$

Exercise 3.2 page 12

1. a) anything of the form (a,a) together with (-31,-7), (-31,9), (-17,3), (-17,7),(-17,31),(-7,9), (-4,0), (-4,8), (0,8), (3,7), (3,31), (7,31)

   b) anything of the form (a,a) together with (-31,-7), (-31,-4), (-31,8), (-17, 7), (-17,31), (-7,-4), (-7,8), (-4, 8), (0,3), (0,9), (3,9), (7,31)

2. a) { .. . , -12,-7,-2,3,8,13,. . .} b) { . . ., -16, -10, -4, 2, 8, 14, ...}
   c) { . . . , -5, -3, -1, 1, 3, 5, . . . } d) { . . . , 4, 7, 10, 13, 16, . . .}
   e) { . . . , -11, -7, -3, 1, 5, 9 . . .} f) { . .. ., -14, -9, -4, 1, 6, . . .}

3) a) $[1]_4$ b) $[0]_3$ c) $[2]_4$ d) $[2]_7$ e) $[5]_6$ f) $[3]_5$

Exercise 3.3 page 15

1)

⊕	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

⊕	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

2) a) $[1]_2$ b) $[3]_4$ c) $[2]_5$ d) $[3]_6$ e) $[0]_2$
f) $[2]_4$ g) $[0]_5$ h) $[2]_6$

3) a)

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

b)

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

c)

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

4) a) Yes e.g. $[2]_6 \odot [3]_6 = [0]_6$ b) $[0]_m$ is possible only when m is not prime.

5) Prove the addition of congruence classes is associative.

Let $[x]_m$, $[y]_m$ and $[z]_m$ be congruence classes modulo m, where $m \in \mathbf{N}$ and $x, y, z \in \mathbf{Z}$

Then $([x]_m [y]_m) [z]_m = [x + y]_m [z]_m = [(x + y) + z]_m$ (i)

And $[x]_m ([y]_m) [z]_m) = [x]_m [y+ z]_m = [x + (y+ z)]_m$ (ii)

but addition of integers is associative hence $(x + y) + z = x + (y + z)$, thus (i) and (ii) are equal.
Thus the addition of congruence classes is associative.