GROUPS

Compiled by: Nyasha P. Tarakino (Trockers)

+263772978155/+263717267175

ntarakino@gmail.com

APRIL 2018

SYLLABUS (6042) REQUIREMENTS

- define a binary operation
- define closure, commutation, association, distribution, identity and inverse element
- define a group
- use the basic properties to show that a given structure is, or is not, a group
- solve problems involving binary operations and properties of a group

NOTES

1.0 Definition of a Binary Operation

If G is a nonempty set, a *binary operation* μ on G is a function $\mu : G \times G \to G$ (Kreher, 2012).

Example

$(+)$ is a binary operation defined on the integers $\mathbb{Z}$. Instead of writing $+(3,5) = 8$ we instead write $3 + 5 = 8$. Indeed the binary operation μ is usually thought of as *multiplication* and instead of $\mu(a,b)$ we use notation such as $ab, a + b, a \circ b$ and $a * b$. If the set G is a finite set of n elements we can present the binary operation, say $*$, by an n by n array called the *multiplication table*. If a, $b \in G$, then the (a,b)–*entry* of this table is $a * b$.

Example

Multiplication table for a binary operation $*$ on the set $G = \{a,b,c,d\}$.

$*$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$
$\boldsymbol{a}$	a	b	c	a
$\boldsymbol{b}$	a	c	d	d
$\boldsymbol{c}$	a	b	d	c
$\boldsymbol{d}$	d	a	c	b

Note that $(a * b) * c = b * c = d$ but $a * (b * c) = a * d = a$.

- A *binary operation* $*$ on set G is *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

Subtraction $(-)$on $\mathbb{Z}$ is not an associative binary operation, but addition $(+)$ is. Other examples of associative binary operations are matrix multiplication and function composition. A set G with a associative binary operation $*$ is called a *semi-group*. The most important semi-groups are groups.

1.1 Definition of a Group

1. A group $(G,\circ)$ is a non-empty set G with a binary operation $\circ$ which
   – is **closed**, (for every a and b in G, $a \circ b$ also lies in G),
   – is **associative**, (for every a, b and c in $G, (a \circ b) \circ c = a \circ (b \circ c)$),
   – has a unique **identity** element, (an element e such that $e \circ a = a \circ e = a$ for all a in G),
   – every element has its own **inverse**, (for every a in G there exists a^{-1} such that $a \circ a^{-1} = a^{-1} \circ a = e$). (J.M. Stone)

2. A *group* G is a non-empty set with a function
   $$m : G \times G \to G;$$
   where we usually abbreviate $m(g,h)$ *to* $g * h$ or simply gh, such that the following hold:
   (1) *(Associativity)* $f(gh) = (fg)h$ for all $f;\ g;\ h \in G$.
   (2) *(Identity)* There is an element $e \in G$ such that for all $g \in G$ we have $eg = ge = g$.
   (3) *(Inverse)* For every $g \in G$ there is an element $h \in G$ such that $gh = hg = e$. (Goren, 2003)

3. A *group* is a set G with a special element e on which an associative binary operation $*$ is defined that satisfies:
   (i) $e * a = a$ for all $a \in G$;
   (ii) for every $a \in G$, there is an element $b \in G$ such that $b * a = e$. (Kreher, 2012).

- Let G be a group. The unique element $e \in G$ satisfying $e * a = a$ for all $a \in G$ is called the *identity* for the group G. If $a \in G$, unique element $b \in G$ such that $b\ a = e$ is called the *inverse* of a and we denote it by $b = a^{-1}$ (Kreher, 2012).

N.B.: For simplicity I will use the binary operation $*$ instead of $\circ$.

A group can be represented as a Latin square. For example

$*$	e	a	b
e	$e*e$	$e*a$	$e*b$
a	$a*e$	$a*a$	$a*b$
b	$b*e$	$b*a$	$b*b$

Each row and column must contain every element of G once only. You can find the identity easily from this by looking for the row or column which is unchanged. Inverses are easy to find from a Latin Square; you merely look for which other element makes it the identity.

Example

If you are asked to show that something is a group in an exam you must tick off each of the above criteria one-by-one. For example show that the set $\{1, -1, i, -i\}$ forms a group under complex number multiplication. Firstly create table

$*$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{1}$	1	-1	i	-1
$\mathbf{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	a	1	-1

N.B.: So we can see that it is closed. Complex number multiplication is associative. Identity element:(1.) Inverses:

- $1^{-1} = 1$,
- $(-1)^{-1} = -1$,
- $i^{-1} = -i$ and
- $(-i)^{-1} = i$.

Definition: A *Latin square* of side n is an n by n array in which each cell contains a single element form an n-element set $S = \{s_1, s_2, \ldots, s_n\}$, such that each element occurs in each row exactly once. It is in *standard form* with respect to the sequence $s_1, s_2, \ldots, s_n$ if the elements in the first row and first column are occurring in the order of this sequence.

Example

A Latin square of side 6 in standard form with respect to the sequence $\{e, g_1, g_2, g_3, g_4, g_5\}$.

e	g_1	g_2	g_3	g_4	g_5
g_1	e	g_3	g_4	g_5	g_2
g_2	g_3	e	g_5	g_1	g_4
g_3	g_4	g_5	e	g_2	g_1
g_4	g_5	g_1	g_2	e	g_3
g_5	g_2	g_4	g_1	g_3	e

The above Latin square is not the multiplication table of a group, because for this square:

$$(g_1 * g_2) * g_3 = g_3 * g_3 = e$$

but

$$g_1 * (g_2 * g_3) = g_1 * g_5 = g_2$$

- A group is commutative or Abelian if $a *$ b = b $* a$ for all a and b in G. If you have a Latin Square for the group you can see if it is Abelian by seeing if it symmetrical along the leading diagonal.

Definition: A group G is *abelian* if $a * b = b * a$ for all elements $a, b \in G$.

- The order of a group is the number of elements the group contains. If a group contains an infinite number of elements it is said to be of infinite order.

- The order of an element a of G is the smallest n such that $a^n = e$. If no such n exists then the element is said to have infinite order. A group is cyclic if every element of a group can be generated by powers of a single element.

- A subgroup (of a group) is any non-empty subset of G which also forms a group under the same binary operation $*$. (A subgroup includes the subset containing just e and the subset G itself.) A proper subgroup is any subgroup with order not one or the same as the original group.

- A good way to find subgroups (beyond the cases where it is obvious) is to consider the powers of the elements of the original group; if you get back to e then the set of elements gone through will be a subgroup. For example in a group of order 16, if you take an element a and discover that $a^4 = e$ (i.e. the order of a is 4) then the set $\{e, a, a^2, a^3\}$ will form a subgroup.

- Lagrange's theorem states that the order of any subgroup must divide the order of the original group. For example a group of order 8 could potentially only have subgroups of order $1, 2, 4$ or 8. It could therefore potentially only have proper subgroups of order 2 or 4. Some useful corollaries of Lagrange's Theorem include:
    a) The order of an element must divide the order of the group.
    b) A group of prime order must be cyclic.

- Two groups $(G,*)$ and $(H,\circ)$ are isomorphic if there exists a one-to-one mapping between them which preserves their structure, i.e.

$$a \leftrightarrow x \text{ and } b \leftrightarrow y \Leftrightarrow a * b \leftrightarrow x \circ y.$$

A good way to show that groups are not isomorphic is to consider the orders of the elements of G and H: If they are different, then they cannot be isomorphic. In an exam you must make the mappings (something) ↔ (something else) very clear; i.e. list them out!

- You need to know the structure of groups up to order 7. Groups of order $2, 3, 5$ and 7 must be cyclic (prime order) and therefore every group of order p (say), must be isomorphic to every other group of order p. These groups are all isomorphic to $(Z_p, +)$, the group of $\{0, 1, 2, p - 1\}$ under addition mod p.

- There are two groups of order 4:

(i) $(Z_4, +)$

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{a^2}$	$\boldsymbol{a^3}$
$\boldsymbol{e}$	e	a	a^2	a^3
$\boldsymbol{a}$	a	a^2	a^3	e
$\boldsymbol{a^2}$	a^2	a^3	e	a
$\boldsymbol{a^3}$	a^3	e	a	a^2

&

(ii) the Klein four-group

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{ba}$
$\boldsymbol{e}$	e	a	b	ba
$\boldsymbol{a}$	a	e	ba	b
$\boldsymbol{b}$	b	ba	e	a
$\boldsymbol{ba}$	ba	b	a	e

Whereas the cyclic group is generated by a single element a, the Klein four-group is generated by two elements, a and b with $a^2 = b^2 = e$ and $ab = ba$. In the Klein four-group every element is self inverse (i.e. has order 2).

- For groups of order 6 there are two fundamental types, the cyclic group isomorphic to $(Z_6, +)$ and the dihedral group D_3 which represents the symmetries of the regular triangle under rotation and reflection. The group is generated by (a) the rotation $\frac{2\pi}{3}$ and (b) reflection with $a^3 = b^2 = e$ and $ab = ba^2$. The table is:

$*$	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e	ba^2	b	ba
a^2	a^2	e	a	ba	ba^2	b
b	b	ba	ba^2	e	a	a^2
ba	ba	ba^2	b	a^2	e	a
ba^2	ba^2	b	ba	a	a^2	e

Definition : Two groups G and H are said to be *isomorphic* if there is a one to one correspondence $\theta : H \to G$ such that $\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$ for all $g_1, g_2 \in G$. The mapping θ is called an *isomorphism* and we say that G *is isomorphic to* H. This last statement is abbreviated by $G \cong H$. If θ satisfies the above property but is not a one to one correspondence, we say θ is *homomorphism*.

1.2 UNIQUENESS

Some properties are unique.

Lemma 1.2.1 *If G is a group and $a \in G$, then $a * a = a$ implies $a = e$.*

Proof. Suppose $a \in G$ satisfies $a * a = a$ and let $b \in G$ be such that $b * a = e$. Then $b * (a * a) = b * a$ and thus

$$a = e * a = (b * a) * a = b * (a * a) = b * a = e$$

Lemma 1.2.2 *In a group G*

(i) *if $b * a = e$, then $a * b = e$ and*

(ii) *$a * e = a$ for all $a \in G$*

Furthermore, there is only one element $e \in G$ satisfying (ii) *and for all $a \in G$, there is only one $b \in G$ satisfying $b * a = e$.*

Proof. Suppose $b * a = e$, then

$$(a * b) * (a * b) = a * (b * a) * b = a * e * b = a * b.$$

Therefore by Lemma 1.2.1 $a * b = e$.

Suppose $a \in G$ and let $b \in G$ be such that $b * a = e$. Then by (i)

$$a * e = a * (b * a) = (a * b) * a = e * a = a$$

Now we show uniqueness. Suppose that $a * e = a$ and $a * f = a$ for all $a \in G$. Then

$$(e * f) * (e * f) = e * (f * e) * f = e * f * e = e * f$$

Therefore by Lemma 1.2.1 $e * f = e$. Consequently

$$f * f = (f * e) * (f * e) = f * (e * f) * e = f * e * e = f * e = f$$

and therefore by Lemma 1.2.1 $f = e$. Finally suppose $b_1 * a = e$ and $b_2 * a = e$. Then by (i) and (ii)

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

WORKED EXAMPLES

Example 1: *Some examples of groups.*

1. The integers $\mathbb{Z}$ under addition $+$.
2. The non-zero complex numbers $\mathbb{C}$ is a group under multiplication.
3. The set $GL_2(\Re)$ of 2 *by* 2 invertible matrices over the reals with matrix multiplication as the binary operation. This is the *general linear group* of 2 *by* 2 matrices over the reals $\Re$.
4. The set of matrices

$$\left\{e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};\ a = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix};\ b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};\ c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$$

under matrix multiplication. The multiplication table for this group is:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

5. The set of complex numbers $G = \{1, -1, i, -i\}$ forms a group under complex number multiplication. The multiplication table for this group is:

$*$	1	-1	i	$-i$
1	1	-1	i	-1
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	a	1	-1

ASSIGNMENT

1. Let G be the subset of complex numbers of the form $e^{\frac{2k\pi}{n}i}, k \in Z$. Show that G is a group under multiplication. How many elements does G have?

2. Find all Latin squares of side 4 in standard form with respect to the sequence $1, 2, 3, 4$. For each square found determine whether or not it is the multiplication table of a group.

3. If G is a finite group, prove that, given $x \in G$, that there is a positive integer n such that $x^n = e$. The smallest such integer is called the *order* of x and we write $|x| = n$.

4. Let G be a *finite* set and let $*$ be an associative binary operation on G satisfying for all $a, b, c \in G$(i) if $a * b = a * c$, then $b = c$; and(ii) if $b * a = c * a$, then $b = c$.

   Then G must be a group under $*$ (Also provide a counter example that shows that this is false if G is infinite.)

5. Show that the Latin Square

e	g_1	g_2	g_3	g_4	g_5	g_6
g_1	e	g_3	g_5	g_6	g_2	g_4
g_2	g_3	e	g_4	g_1	g_6	g_5
g_3	g_2	g_1	g_6	g_5	g_4	e
g_4	g_5	g_6	g_2	e	g_3	g_1
g_5	g_6	g_4	e	g_2	g_1	g_3
6	g_4	g_5	g_1	g_3	e	g_2

   is not the multiplication table of a group.

PAST EXAM QUESTIONS

Question

(i) Show that the set of numbers $\{3, 5, 7\}$, under multiplication *modulo* 8, does not form a group. **[2]**

(ii) The set of numbers $\{3, 5, 7, a\}$, under multiplication *modulo* 8, forms a group. Write down the value of a. **[1]**

(iii) State, justifying your answer, whether or not the group in part **(ii)** is isomorphic to the multiplicative group $\{e, r, r^2, r^3\}$, where e is the identity and $r^4 = e$. **[2]**

Question

(a) A group G of order 6 has the combination table shown below.

	e	***a***	***b***	***p***	***q***	***r***
e	e	a	b	p	q	r
a	a	b	e	r	p	q
b	b	e	a	q	r	p
p	p	q	r	e	a	b
q	q	r	p	b	e	a
r	r	p	q	a	b	e

(i) State, with a reason, whether or not G is commutative. **[1]**

(ii) State the number of subgroups of G which are of order 2. **[1]**

(iii) List the elements of the subgroup of G which is of order 3. **[1]**

(b) A multiplicative group H of order 6 has elements e, c, c^2, c^3, c^4, c^5, where e is the identity. Write down the order of each of the elements c^3, c^4 and c^5. **[3]**

Question

In this question G is a group of order n, where $3 \leq n < 8$.

(i) In each case, write down the smallest possible value of n:

(a) if G is cyclic, **[1]**

(b) if G has a proper subgroup of order 3, **[1]**

(c) if G has at least two elements of order 2. **[1]**

(ii) Another group has the same order as G, but is not isomorphic to G. Write down the possible value(s) of n. **[2]**

Question

The function f is defined by $f: x \to \frac{1}{1-2x}$ for $x \in \mathbb{R}, x \neq 0, x \neq \frac{1}{2}, x \neq 1$. The function g is defined by $g(x) = ff(x)$.

(i) Show that $g(x) = \frac{1-x}{1-2x}$ and that $gg(x) = x$. **[4]**

It is given that f and g are elements of a group K under the operation of composition of functions.

The element e is the identity, where e : x → x for $x \in R, x \neq 0, x \neq \frac{1}{2}, x \neq 1$.

(ii) State the orders of the elements f and g. **[2]**

(iii) The inverse of the element f is denoted by h. Find $h(x)$. **[2]**

(iv) Construct the operation table for the elements e, f, g, h of the group K. **[4]**

Question

The set M consists of the six matrices $\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$, where $n \in \{0, 1, 2, 3, 4, 5\}$. It is given that M forms a group $(M, \times)$ under matrix multiplication, with numerical addition and multiplication both being carried out $modulo$ 6.

(i) Determine whether $(M, \times)$ is a commutative group, justifying your answer. **[2]**

(ii) Write down the identity element of the group and find the inverse of $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ **[3]**

(iii) State the order of $\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$ and give a reason why $(M,\times)$has no subgroup of order 4. **[2]**

(iv) The multiplicative group G has order 6. All the elements of G, apart from the identity, have order 2 or 3. Determine whether G is isomorphic to $(M,\times)$justifying your answer. **[2]**

Question

The elements of a group G are the complex numbers $a + bi$ where $a, b \in \{0,1,2,3,4.\}$ These elements are combined under the operation of addition *modulo* 5.

(i) State the identity element and the order of G. **[2]**

(ii) Write down the inverse of $2 + 4i$. **[1]**

(iii) Show that every non-zero element of G has order 5. **[3]**

Question

The set $S = \{a, b, c, d\}$ under the binary operation $*$ forms a group G of order 4 with the following operation table.

	a	b	c	d
a	d	a	b	c
b	a	b	c	d
c	b	c	d	a
d	c	d	a	b

(i) Find the order of each element of G. **[3]**

(ii) Write down a proper subgroup of G. **[1]**

(iii) Is the group G cyclic? Give a reason for your answer. **[1]**

(iv) State suitable values for each of a, b, c and d in the case where the operation $*$ is multiplication of complex numbers. **[1]**

Question

A multiplicative group Q of order 8 has elements $\{e, p, p^2, p^3, a, ap, ap^2, ap^3\}$, where e is the identity. The elements have the properties $p^4 = e$ and $a^2 = p^2 = (ap)^2$.

(i) Prove that $a = pap$ and that $p = apa$. **[2]**

(ii) Find the order of each of the elements $p2, a, ap, ap^2$. **[5]**

(iii) Prove that $\{e, a, p^2, ap^2\}$ is a subgroup of Q. **[4]**

(iv) Determine whether Q is a commutative group. **[4]**

Question

G consists of the set $\{1, 3, 5, 7\}$ with the operation of multiplication $modulo$ 8.

(i) Write down the operation table and, assuming Associativity, show that G is a group. **[5]**

(ii) State the order of each element. **[1]**

(iii) Find all the proper subgroups of G. **[1]**

The group H consists of the set $\{1, 3, 7, 9\}$ with the operation of multiplication $modulo$ 10.

(iv) Explaining your reasoning, determine whether H is isomorphic to G. **[2]**

Question

The group G consists of the set $\{1, 3, 7, 9, 11, 13, 17, 19\}$ combined under multiplication $modulo$ 20.

(i) Find the inverse of each element. **[3]**

(ii) Show that G is not cyclic. **[3]**

(iii) Find two isomorphic subgroups of order 4 and state an isomorphism between them. **[5]**

Question

Elements of the set $\{p, q, r, s, t\}$ are combined according to the operation table shown below.

	p	q	r	s	t
p	t	s	p	r	q
q	s	p	q	t	r
r	p	q	r	s	t
s	r	t	s	q	p
t	q	r	t	p	s

(i) Verify that $q(st) = (qs)t$. **[2]**

(ii) Assuming that the associative property holds for all elements, prove that the set $\{p, q, r, s, t\}$, with the operation table shown, forms a group G. **[4]**

(iii) A multiplicative group H is isomorphic to the group G. The identity element of H is e and another element is d. Write down the elements of H in terms of e and d. **[2]**

*******DONT BE SATISFIED BY MEDIOCRE WHILST EXCELLENCE IS THERE*******

CONTRIBUTIONS ARE WELCOME; FEEL FREE TO CONTACT ME SO THAT WE CAN IMPROVE THE DOCUMENT TOGETHER.

ENJOY

Nyasha P. Tarakino (Trockers)

+263772978155/+263717267175

ntarakino@gmail.com